# DIN EN 18031-2

ICS 33.060.20; 35.030

## Gemeinsame Sicherheitsanforderungen für Funkanlagen – Teil 2: Funkanlagen, die Daten verarbeiten, insbesondere internetfähige Funkanlagen, Kinderbetreuungsfunkanlagen, Spielzeugfunkanlagen und tragbare Funkanlagen; Deutsche Fassung EN 18031-2:2024

Common security requirements for radio equipment –
Part 2: Radio equipment processing data, namely Internet connected radio equipment, childcare radio equipment, toys radio equipment and wearable radio equipment;
German version EN 18031-2:2024

Exigences de sécurité communes applicables aux équipements radioélectriques –
Partie 2: Équipements radioélectriques qui traitent des données, à savoir les équipements radioélectriques connectés à l'internet, les équipements radioélectriques destinés à la garde d'enfants, les jouets dotés d'équipements radioélectriques et les équipements radioélectriques portables;
Version allemande EN 18031-2:2024

Gesamtumfang 227 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)



www.din.de
www.dinmedia.de
3568394

# Nationales Vorwort

Das Dokument EN 18031-2:2024 wurde vom Technischen Komitee CEN/CENELEC/JTC 13 „Cybersicherheit und Datenschutz“ erarbeitet, dessen Sekretariat von DIN (Deutschland) gehalten wird.

Das zuständige deutsche Normungsgremium ist der Gemeinschaftsarbeitsausschuss NA 043-04-13 GA „DIN/DKE Gemeinschaftsgremium Cybersecurity“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

DIN EN 18031 besteht unter dem allgemeinen Titel *Gemeinsame Sicherheitsanforderungen für Funkanlagen* aus den folgenden Teilen:

— *Teil 1: Funkanlagen mit Internetanschluss*

— *Teil 2: Funkanlagen, die Daten verarbeiten, insbesondere internetfähige Funkanlagen, Kinderbetreuungsfunkanlagen, Spielzeugfunkanlagen und tragbare Funkanlagen*

— *Teil 3: Internetfähige Funkanlagen, die virtuelles Geld oder Geldwerte verarbeiten*

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DIN (www.din.de) durch eine Suche nach der Dokumentennummer aufgerufen werden.

EUROPÄISCHE NORM

EUROPEAN STANDARD

NORME EUROPÉENNE

# EN 18031-2

August 2024

ICS 33.060.20

Deutsche Fassung

# Gemeinsame Sicherheitsanforderungen für Funkanlagen — Teil 2: Funkanlagen, die Daten verarbeiten, insbesondere internetfähige Funkanlagen, Kinderbetreuungsfunkanlagen, Spielzeugfunkanlagen und tragbare Funkanlagen

Common security requirements for radio equipment — Part 2: radio equipment processing data, namely Internet connected radio equipment, childcare radio equipment, toys radio equipment and wearable radio equipment

Exigences de sécurité communes applicables aux équipements radioélectriques — Partie 2: Équipements radioélectriques qui traitent des données, à savoir les équipements radioélectriques connectés à l'internet, les équipements radioélectriques destinés à la garde d'enfants, les jouets dotés d'équipements radioélectriques et les équipements radioélectriques portables

Diese Europäische Norm wurde vom CEN am 1. August 2024 angenommen.

Die CEN und CENELEC-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist. Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim CEN-CENELEC-Management-Zentrum oder bei jedem CEN und CENELEC-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CEN und CENELEC-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Management-Zentrum mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CEN und CENELEC-Mitglieder sind die nationalen Normungsinstitute von Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, der Republik Nordmazedonien, Rumänien, Schweden, der Schweiz, Serbien, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.

**CEN-CENELEC Management-Zentrum:**
**Rue de la Science 23, B-1040 Brüssel**

# Inhalt

## Bilder

## Tabellen

## Europäisches Vorwort

Dieses Dokument (EN 18031-2:2024) wurde vom Technischen Komitee CEN/CENELEC/JTC 13 „Cybersicherheit und Datenschutz“ erarbeitet, dessen Sekretariat von DIN gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis Februar 2025, und etwaige entgegenstehende nationale Normen müssen bis Februar 2025 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CEN ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Dieses Dokument wurde im Rahmen eines Normungsauftrages erarbeitet, den die Europäische Kommission CEN-CENELEC erteilt hat. Der Ständige Ausschuss der EFTA-Staaten genehmigt anschließend diese Aufträge für die Mitgliedsstaaten.

Zum Zusammenhang mit EU-Rechtsvorschriften siehe informativen Anhang ZA, der Bestandteil dieses Dokuments ist.

Rückmeldungen oder Fragen zu diesem Dokument sollten an das jeweilige nationale Normungsinstitut des Anwenders gerichtet werden. Eine vollständige Liste dieser Institute ist auf den Internetseiten von CEN abrufbar.

Entsprechend der CEN-CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Bulgarien, Dänemark, Deutschland, die Republik Nordmazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Serbien, Slowakei, Slowenien, Spanien, Tschechische Republik, Türkei, Ungarn, Vereinigtes Königreich und Zypern.

# Einleitung

Die Hersteller müssen wachsam sein, um die allgemeine Resilienz gegen Cybersicherheitsbedrohungen zu verbessern, die durch die zunehmende Konnektivität von Funkanlagen [36] und die wachsende Fähigkeit böswilliger Akteure, Benutzern, Organisationen und der Gesellschaft Schaden zuzufügen, entstehen.

Die in dieser Ausgangsnorm dargelegten Sicherheitsanforderungen wurden entwickelt, um die Fähigkeit von Funkanlagen zu verbessern, ihre Sicherheits- und Datenschutzwerte gegenüber häufigen Bedrohungen der Cybersicherheit zu schützen und öffentlich bekannte, ausnutzbare Schwachstellen einzudämmen.

Es ist wichtig anzumerken, dass bewährte Verfahrensweisen zur Verteidigung in der Tiefe sowohl vom Hersteller als auch vom Benutzer erforderlich sind, um eine umfassende Cybersicherheit von Funkanlagen zu erreichen. Insbesondere ist keine Einzelmaßnahme ausreichend, um die vorgegebenen Ziele zu erreichen; tatsächlich ist üblicherweise eine Reihe von Mechanismen und Maßnahmen erforderlich, um nur eine Sicherheitszielsetzung zu erreichen. Die Leitlinien in diesem Dokument enthalten Listen von Beispielen. Diese Beispiele sind nur Hinweise auf Möglichkeiten, denn es gibt andere Möglichkeiten, die nicht aufgeführt sind, und selbst die Anwendung der angegebenen Beispiele ist nicht ausreichend, wenn die gewählten Mechanismen und Maßnahmen nicht in koordinierter Weise implementiert werden.

# 1 Anwendungsbereich

Dieses Dokument legt allgemeine Sicherheitsanforderungen und zugehörige Beurteilungskriterien für Funkanlagen [36] (im Folgenden als „Anlagen“ bezeichnet) fest, die personenbezogene Daten [40] oder Verkehrsdaten [41] oder Ortsdaten [41] entweder für Internet verbundene Funkanlagen [37], ausschließlich für die Kinderbetreuung entwickelte oder vorgesehene Funkanlagen [37], Spielzeuge [39] oder Wearable-Funkanlagen [37] verarbeiten.

# 2 Normative Verweisungen

Es gibt keine normativen Verweisungen in diesem Dokument.

# 3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

— ISO Online Browsing Platform: verfügbar unter https://www.iso.org/obp

— IEC Electropedia: verfügbar unter https://www.electropedia.org/

**3.1**
**Zugangssteuerungsmechanismus**
Funktionalität von Anlagen, um den Zugang zu spezifischen *Ressourcen* der Anlage zu gewähren, einzuschränken oder zu verweigern

Anmerkung 1 zum Begriff: Der Zugang zu spezifischen Geräteressourcen kann sich unter anderem auf Folgendes beziehen:

— das Lesen spezifischer Daten; oder

— das Schreiben spezifischer Daten in den dauerhaften Speicher der Anlage; oder

— die Durchführung einer bestimmten Anlagenfunktionalität, beispielsweise einer Audioaufzeichnung.

**3.2**
**Authentisierung**
Sicherstellung, dass eine Entität das ist, was sie angibt zu sein

Anmerkung 1 zum Begriff: Eine Entität kann unter anderem angeben:

— eine bestimmte Person, ein Besitzer eines Benutzerkontos, ein Gerät oder ein Dienst zu sein; oder

— ein Mitglied einer spezifischen Gruppe, beispielsweise einer zum Zugang zu einer bestimmten Geräteressource autorisierten Gruppe; oder

— durch eine andere Entität für den Zugang zu einer bestimmten Geräteressource autorisiert zu sein.

**3.3**
**Authentisierungsmechanismus**
Funktionalität von Anlagen, um zu verifizieren, dass eine *Entität* das ist, was sie angibt zu sein

Anmerkung 1 zum Begriff: Üblicherweise beruht die Verifizierung auf der Untersuchung von Nachweisen eines oder mehrerer Elemente aus den folgenden Kategorien:

— Wissen; und

— Besitz; und

— Inhärenz.

**3.4**
**Authentifikator**
etwas, das bekannt ist oder im Besitz und unter der Kontrolle einer *Entität* und zur *Authentisierung* verwendet wird

Anmerkung 1 zum Begriff: In der Regel handelt es sich um ein physisches Gerät oder ein Passwort.

BEISPIEL Ein Passwort oder ein Token können als Authentifikator verwendet werden.

**3.5**
**Beurteilungsziel**
Erklärung, die als Teil der Beurteilungseingabe bereitgestellt wird und in der die Gründe für die Durchführung der Beurteilung dargelegt werden

[QUELLE: ISO/IEC 33001:2015, 3.2.6 [29]]

**3.6**
**bewährte Verfahrensweisen**
Maßnahmen, für die nachgewiesen wurde, dass sie eine angemessene Sicherheit für den entsprechenden Anwendungsfall bieten

**3.7**
**Brute-Force-Angriff**
Angriff auf ein Kryptosystem, bei dem ein Satz von Schlüsseln, *Passwörtern* oder anderen Daten durch Versuch und Irrtum durchsucht wird

**3.8**
**Kommunikationsmechanismus**
Funktionalität von Anlagen, die die Kommunikation über eine *Maschinenschnittstelle* ermöglicht

**3.9**
**vertraulicher kryptographischer Schlüssel**
*vertraulicher Sicherheitsparameter*, mit Ausnahme von *Passwörtern*, die bei der Anwendung eines kryptographischen Algorithmus oder eines kryptographischen Protokolls verwendet werden

**3.10**
**vertrauliche personenbezogene Informationen**
*personenbezogene Informationen*, deren Offenlegung den Schutz der Daten des Benutzers oder Teilnehmers kompromittieren kann

**3.11**
**Konfiguration von vertraulichen Datenschutzfunktionen**
*Konfiguration von Datenschutzfunktionen*, deren Offenlegung den Schutz der Daten des Benutzers oder Teilnehmers kompromittieren kann

**3.12**
**vertraulicher Sicherheitsparameter**
*Sicherheitsparameter*, dessen Offenlegung den Schutz der Daten des Benutzers oder Teilnehmers kompromittieren kann

**3.13**
**Denial-of-Service**
Verhinderung oder Unterbrechung des autorisierten Zugangs zu einer Geräte*ressource* oder Verlangsamung des Betriebs und der Funktionen von Anlagen

[QUELLE: IEC 62443-1-1:2019, 3.2.42 [30]] modifiziert

**3.14**
**Gerät**
Produkt außerhalb der Anlage

**3.15**
**Entität**
Benutzer, *Gerät,* Anlage oder Dienst

**3.16**
**Entropie**
Messgröße für die Unordnung, Zufälligkeit oder Variabilität in einem geschlossenen System

**3.17**
**externe Schnittstelle**
*Schnittstelle* eines Geräts, die von außerhalb der Anlage zugänglich ist

Anmerkung 1 zum Begriff: Maschinen-, Netzwerk- und Benutzungsschnittstellen sind spezifische Arten von externen Schnittstellen.

**3.18**
**Werkeinstellung**
definierter Zustand, in dem die Konfigurationseinstellungen und die Konfiguration der Anlage auf Anfangswerte eingestellt sind

Anmerkung 1 zum Begriff: Eine Werkeinstellung kann Sicherheitsaktualisierungen einschließen, die nach der Markteinführung der Anlage installiert wurden.

**3.19**
**fest einprogrammiert**
Praxis der *Software*entwicklung, bei der Daten direkt in den Quellcode eines Programms oder eines anderen ausführbaren Objekts eingebettet werden

**3.20**
**Initialisierung**
Prozess, bei dem die Netzwerkverbindung der Anlage für den Betrieb konfiguriert wird

Anmerkung 1 zum Begriff: Die Initialisierung kann die Möglichkeit bieten, Authentisierungsmerkmale für einen Benutzer oder für den Netzwerkzugang zu konfigurieren.

**3.21**
**Schnittstelle**
gemeinsame Begrenzung, über die *Entitäten* Informationen austauschen

**3.22**
**Begründung**
dokumentierte Informationen, die den Nachweis erbringen, dass eine Behauptung wahr ist, wobei von allgemeinem Fachwissen ausgegangen wird

Anmerkung 1 zum Begriff: Dieser Nachweis kann z. B. unterstützt werden durch

— eine Beschreibung der vorgesehenen Anlagenfunktionalität,

— eine Beschreibung der Betriebsumgebung, in der die Anlage eingesetzt wird,

— eine Beschreibung der technischen Eigenschaften der Anlage, z. B. der Sicherheitsmaßnahmen,

— eine Analyse der maßgeblichen Risiken im Zusammenhang mit dem Betrieb der Anlage im Rahmen seiner vernünftigerweise vorhersehbaren Verwendung und der vorgesehenen Anlagenfunktionalität.

**3.23**
**Protokolldaten**
Aufzeichnung(en) bestimmter (Prozess-)Ereignisse auf einem EDV-Gerät

**3.24**
**Protokollierungsmechanismus**
Anlagenfunktionalität zur Protokollierung interner Aktivitäten

**3.25**
**Maschinenschnittstelle**
*externe Schnittstelle* zwischen der Anlage und einem Dienst oder einem *Gerät*

**3.26**
**Netzwerkschnittstelle**
*externe Schnittstelle*, die es ermöglicht, dass Anlagen Zugang zu einem Netzwerk haben oder bereitstellen

Anmerkung 1 zum Begriff: Beispiele für Netzwerkschnittstellen sind LAN-Anschlüsse (verkabelt) oder kabellose Netzwerkschnittstellen, die die Kommunikation über WLAN oder drahtlose Kurzstreckentechnologie ermöglichen, z. B. mithilfe einer 2,4-GHz-Antenne.

**3.27**
**Betriebszustand**
Zustand, in der die Anlage ordnungsgemäß entsprechend der vorgesehenen Anlagenfunktionalität [38] und innerhalb der für die Nutzung vorgesehenen Betriebsumgebung arbeiten

**3.28**
**optionaler Dienst**
Dienst, der zur Ersteinrichtung der Anlage nicht erforderlich ist und der kein Teil der Grundfunktionalität ist, der jedoch für die vorgesehene Anlagenfunktionalität [38] relevant und Teil der Werksvoreinstellung ist

BEISPIEL Ein SSH-Dienst ist für die Grundfunktionalität der Anlage nicht erforderlich, aber er kann verwendet werden, um einen Fernzugriff auf die Anlage zuzulassen.

**3.29**
**Passwort**
Zeichenfolge (Buchstaben, Zahlen oder andere Symbole), die zur Authentisierung einer *Entität* verwendet werden

Anmerkung 1 zum Begriff: Persönliche Identifikationsnummern (PINs) gelten ebenfalls als eine Möglichkeit eines Passwortes.

**3.30**
**personenbezogene Informationen**
personenbezogene Daten [40], Verkehrsdaten [41] oder Ortsdaten [41]

**3.31**
**personenbezogene Informationen besonderer Kategorien**
*personenbezogene Informationen*, bei denen es sich um genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder zur sexuellen Orientierung einer natürlichen Person handelt oder aus denen die rassische oder ethnische Herkunft, politi-

sche Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen

[QUELLE: gestützt auf Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) [31]]

**3.32**
**Datenschutzwert**
*sensible personenbezogene Informationen* bzw. *vertrauliche personenbezogene Informationen* oder *Konfiguration sensibler Datenschutzfunktionen* bzw. *Konfiguration vertraulicher Datenschutzfunktionen* oder *Datenschutzfunktionen*

**3.33**
**Datenschutzfunktion**
Funktionalität der Anlage, das *personenbezogene Informationen* verarbeitet

**3.34**
**Konfiguration von Datenschutzfunktionen**
von der Anlage verarbeitete Daten, die das Verhalten der *Datenschutzfunktionen* eines Geräts definieren

**3.35**
**öffentlicher Sicherheitsparameter**
*sensibler Sicherheitsparameter*, der nicht vertraulich ist

**3.36**
**resilient**
fähig zu sein, ungünstige Bedingungen, Belastungen, Angriffe oder Kompromittierungen von Systemen, die Cyber-Ressourcen nutzen oder durch diese ermöglicht werden, vorherzusehen, ihnen zu widerstehen, sie zu beheben und sich ihnen anzupassen

[QUELLE: NIST SP 800-172 [32]]

**3.37**
**Ressource**
Funktionseinheit oder Datenelement, das zur Durchführung der erforderlichen Operationen benötigt wird

[QUELLE: IEC [33]]

**3.38**
**Risiko**
Kombination der Wahrscheinlichkeit eines Schadenseintritts und seines Schadensausmaßes

[QUELLE: ISO/IEC Guide 51:2014 [34]]

**3.39**
**Sicherheitswert**
sensibler Sicherheitsparameter bzw. vertraulicher Sicherheitsparameter oder Sicherheitsfunktion

**3.40**
**Sicherheitsfunktion**
Maßnahmen am Gerät, die den Schutz der personenbezogenen Daten und der Privatsphäre des Benutzers und des Teilnehmers sicherstellen

**3.41**
**Sicherheitsparameter**
von der Anlage verarbeitete Daten, die das Verhalten der *Sicherheitsfunktion* der Anlage definieren

**3.42**
**Sicherheitsstufe**
Zahl, die den Arbeitsaufwand angibt, der erforderlich ist, um einen kryptographischen Algorithmus oder ein System zu brechen

Anmerkung 1 zum Begriff: Der Arbeitsaufwand kann zum Beispiel die Anzahl der Operationen sein, die erforderlich sind, um einen kryptographischen Algorithmus oder ein System zu brechen.

**3.43**
**sensible personenbezogene Informationen**
*personenbezogene Informationen*, deren Manipulation den Schutz der Daten des Benutzers oder Teilnehmers kompromittieren kann

**3.44**
**Konfiguration von sensiblen Datenschutzfunktionen**
*Konfiguration von Datenschutzfunktionen*, deren Manipulation den Schutz der Daten des Benutzers oder Teilnehmers kompromittieren kann

**3.45**
**sensibler Sicherheitsparameter**
*Sicherheitsparameter*, dessen Manipulation den Schutz der Daten des Benutzers oder Teilnehmers kompromittieren kann

**3.46**
**Sicherheitsaktualisierung**
*Software*-Aktualisierung, die Sicherheitsschwachstellen durch *Software*-Patches oder andere Eindämmungsmaßnahmen behandelt

**3.47**
**Software**
Zusammenstellung von Programmen, Verfahren, Regeln, Dokumentation und Daten, die den Betrieb eines Geräts betreffen

Anmerkung 1 zum Begriff: Software beinhaltet auch Firmware.

**3.48**
**Speichermechanismus**
Funktionalität von Anlagen, die die Speicherung von Informationen ermöglicht

**3.49**
**Aktualisierungsmechanismus**
Funktionalität von Anlagen, die die Änderung der Geräte*software* ermöglicht

**3.50**
**Benutzungsschnittstelle**
*externe Schnittstelle* zwischen der Anlage und einem Benutzer

**3.51**
**Schwachstelle**
Schwäche, Design- oder Implementationsfehler, die/der zu einem unerwarteten unerwünschten Ereignis führen kann, das die Sicherheit der beteiligten Anlagen, des Netzwerks, der Anwendung oder des Protokolls gefährdet

[QUELLE: (ITSEC) (Definition durch ENISA, „Computersystem“ wurde durch „Gerät“ ersetzt) [35]]

# 4 Abkürzungen

| | |
|---|---|
| ACM | Zugangssteuerungsmechanismus (en: access control mechanism) |
| API | Anwendungsprogrammierschnittstelle (en: application programming interface) |
| AU | Beurteilungseinheit (en: assessment unit) |
| AUM | Authentisierungsmechanismus (en: authentication mechanism) |
| CCK | vertrauliche(r) kryptographische(r) Schlüssel (en: confidential cryptographic key(s)) |
| CRY | Kryptographie (en: cryptography) |
| CSP | vertraulicher Sicherheitsparameter (en: confidential security parameter) |
| CWE | allgemeine Schwachstellenaufzählung (en: common weakness enumeration) |
| DHCP | dynamisches Host-Konfigurationsprotokoll (en: dynamic host configuration protocol) |
| DLM | Löschungsmechanismus (en: deletion mechanism) |
| DN | Entscheidungsknoten (en: decision node) |
| DoS | Denial of Service |
| DT | Entscheidungsbaum (en: decision tree) |
| E | Nachweis (en: evidence) |
| E.Info | evidence.information |
| E.Just | evidence.justification |
| GEC | allgemeine Gerätefähigkeiten (en: general equipment capabilities) |
| IC | Umsetzungskategorie (en: implementation category) |
| ICMP | Internet-Steuerungsmeldungsprotokoll (en: internet control message protocol) |
| IP | Internet-Protokoll (en: internet protocol) |
| LAN | lokales Netzwerk (en: local area network) |
| LGM | Protokollierungsmechanismus (en: logging mechanism) |
| MitM | Man-in-the-Middle |
| OS | Betriebssystem (en: operating system) |
| OTP | Einmalpasswort (en: one-time password) |
| PIN | Persönliche Identifikationsnummer (en: personal identification number) |
| PKI | Public-Key-Infrastruktur |
| PSP | öffentlicher Sicherheitsparameter (en: public security parameter) |
| SCM | sicherer Kommunikationsmechanismus (en: secure communication mechanism) |
| SDO | Normungsorganisation (en: standards development organization) |
| SQL | strukturierte Abfragesprache (en: structured query language) |
| SSM | sicherer Speichermechanismus (en: secure storage mechanism) |
| SSP | sensibler Sicherheitsparameter (en: sensitive security parameter) |
| SUM | sicherer Aktualisierungsmechanismus (en: secure update mechanism) |
| UNM | Benutzer-Benachrichtigungsmechanismus (en: user notification mechanism) |
| USB | universeller serieller Bus (en: universal serial bus) |
| WLAN | drahtloses lokales Netzwerk (en: wireless local area network) |

# 5 Anwendbarkeit dieses Dokuments

Dieses Dokument nutzt das Konzept von Mechanismen, die den Anwender dieses Dokuments anleiten, wann bestimmte Sicherheitsmaßnahmen anzuwenden sind. Mechanismen behandeln die Anwendbarkeit und Angemessenheit anhand eines Satzes von Anforderungen, einschließlich Beurteilungskriterien. Für jedes der angegebenen Elemente wird eine Entscheidung über die Anwendbarkeit/Nichtanwendbarkeit getroffen.

Falls zutreffend, folgt eine Entscheidung über die Angemessenheit der einzelnen Elemente (bestanden/nicht bestanden). Wenn beispielsweise die Anwendbarkeit einer Anforderung auf externe Schnittstellen geprüft wird, dann wird die Entscheidung, ob die Anforderung erfüllt werden muss, für jede externe Schnittstelle unabhängig getroffen.

Die Mechanismen und deren Anwendung werden mithilfe der in der nachstehenden Tabelle dargestellten Struktur dokumentiert:

**Tabelle 1 — Struktur der Anforderungen**

| **Abschnitt Nr.** | **Titel** | **Beschreibung, wie das Dokument anzuwenden ist** |
|---|---|---|
| 6.x | XXX Mechanismus | Mechanismus für jede spezifische Einheit (z. B. externe Schnittstelle oder Sicherheitswert) |
| 6.x.1 | XXX-1 Anwendbarkeit der Mechanismen | Anwendbarkeit des Mechanismus |
| 6.x.1.1 | Anforderung | Für jede spezifische Einheit ist zu bestimmen und zu beurteilen, ob der Mechanismus erforderlich ist.<br>ANMERKUNG Die Anwendbarkeit und Angemessenheit des Mechanismus kann in einer Anforderung zusammengefasst werden. |
| 6.x.1.2 | Begründung | |
| 6.x.1.3 | Leitlinie | |
| 6.x.1.4 | Beurteilungskriterien | |
| 6.x.1.4.1 | Beurteilungsziel | |
| 6.x.1.4.2 | Umsetzungskategorien | |
| 6.x.1.4.3 | Erforderliche Informationen | |
| 6.x.1.4.4 | Konzeptuelle Beurteilung | |
| 6.x.1.4.5 | Beurteilung der funktionalen Vollständigkeit | |
| 6.x.1.4.6 | Beurteilung der funktionalen Suffizienz | |
| 6.x.2 | XXX-2 Angemessene Mechanismen | Angemessenheit des Mechanismus |
| 6.x.2.1 | Anforderung | Für jede spezifische Einheit, für die der Mechanismus wie in XXX-1 festgelegt erforderlich ist, ist zu bestimmen und zu beurteilen, ob der Mechanismus ordnungsgemäß implementiert wurde.<br>ANMERKUNG Für die Angemessenheit eines Mechanismus können mehrere Unterabschnitte vorhanden sein, die sich auf spezifische Eigenschaften beziehen. |
| 6.x.2.2 | Begründung | |
| 6.x.2.3 | Leitlinie | |
| 6.x.2.4 | Beurteilungskriterien | |
| 6.x.2.4.1 | Beurteilungsziel | |
| 6.x.2.4.2 | Umsetzungskategorien | |
| 6.x.2.4.3 | Erforderliche Informationen | |
| 6.x.2.4.4 | Konzeptuelle Beurteilung | |
| 6.x.2.4.5 | Beurteilung der funktionalen Vollständigkeit | |
| 6.x.2.4.6 | Beurteilung der funktionalen Suffizienz | |
| 6.x.y | XXX-Nr. Unterstützende Anforderungen | Anwendbarkeit und Angemessenheit von unterstützenden Anforderungen für den Mechanismus |

**Tabelle 1** (*fortgesetzt*)

| Abschnitt Nr. | Titel | | Beschreibung, wie das Dokument anzuwenden ist |
|---|---|---|---|
| 6.x.y.1 | Anforderung | | Für jede spezifische Einheit, für die der durch XXX-1 festgelegte Mechanismus erforderlich ist, ist zu bestimmen und zu beurteilen, ob die unterstützende Anforderung implementiert werden muss (es können spezifische Bedingungen gelten, beispielsweise wenn die Anlage ein Spielzeug ist), und falls sie implementiert werden muss, ob die Implementation ordnungsgemäß ist.<br>ANMERKUNG Einige Kapitel enthalten mehrere Anforderungen, was zu leichten Abweichungen bei der Nummerierung führt. |
| 6.x.y.2 | Begründung | | |
| 6.x.y.3 | Leitlinie | | |
| 6.x.y.4 | Beurteilungskriterien | | |
| 6.x.y.4.1 | | Beurteilungsziel | |
| 6.x.y.4.2 | | Umsetzungskategorien | |
| 6.x.y.4.3 | | Erforderliche Informationen | |
| 6.x.y.4.4 | | Konzeptuelle Beurteilung | |
| 6.x.y.4.5 | | Beurteilung der funktionalen Vollständigkeit | |
| 6.x.y.4.6 | | Beurteilung der funktionalen Suffizienz | |

Die Beurteilungen werden durchgeführt, indem die dokumentierten Beurteilungsfälle untersucht werden; es sind möglicherweise nicht alle Beurteilungsfälle für jeden Mechanismus verfügbar:

— Konzeptuelle Beurteilung

  Es ist zu untersuchen, ob die verfügbare Dokumentation und Begründung die erforderlichen Nachweise bereitstellen (beispielsweise die Begründung, warum ein Mechanismus für eine bestimmte Netzwerkschnittstelle nicht anwendbar ist).

— Beurteilung der funktionalen Vollständigkeit

  Es ist zu untersuchen und zu prüfen, ob die verfügbare Dokumentation vollständig ist (beispielsweise durch den Einsatz von Netzwerk-Scannern, um zu verifizieren, ob alle externen Schnittstellen ordnungsgemäß identifiziert, dokumentiert und beurteilt wurden).

— Beurteilung der funktionalen Suffizienz

  Es ist zu untersuchen und zu prüfen, ob die Implementation angemessen ist (beispielsweise ist mithilfe von Fuzzing-Tools zu prüfen, ob eine Netzwerkschnittstelle Angriffen mit fehlerhaften Daten gegenüber resilient ist).

Jede Beurteilung ist weiter in die folgenden Unterabschnitte gegliedert, bei denen ein Entscheidungsbaum zur Steuerung der Beurteilung genutzt werden darf:

— Zweck der Beurteilung

— Voraussetzungen

— Beurteilungseinheiten

— Entscheidungszuweisung

Unter den erforderlichen Informationen sind Informationen aufgeführt, die durch die technische Dokumentation bereitgestellt werden müssen. Dieses Dokument fordert nicht, dass jedes erforderliche Informationselement als getrenntes Dokument zur Verfügung gestellt werden muss.

Für den Abschnitt „Beurteilungskriterien“ werden die folgenden Kennungen mit der definierten Syntax verwendet, um die Elemente zu strukturieren, die für die Durchführung einer Beurteilung erforderlich sind:

— Erforderliche Informationen

  E.<Type>.<MechanismAbbreviation-<Nr».<CategoryName>

  Kennung für die Kategorie der erforderlichen Informationen mit Ausnahme von DTs

— Erforderliche Informationen für Entscheidungsbäume

  E.<Type>.DT.<MechanismAbbreviation-<Nr»

  Kennung für die Kategorie der erforderlichen Informationen im Zusammenhang mit DTs

— Umsetzungskategorie

  IC.<MechanismAbbreviation-<Nr».<ImplemenationCategoryName>

  Kennung für die Umsetzungskategorie

— Beurteilungseinheit

  AU.<MechanismAbbreviation-<Nr».<AssessmentUnitName>

  Kennung für die Beurteilungseinheit

— Entscheidungsbaumknoten

  DT.<MechanismAbbreviation-<Nr».DN-<Number>

  Kennung für einen bestimmten Knoten innerhalb des DT

Die Platzhalter werden wie folgt verwendet:

— <Type>: „Info“ oder „Just“, um die Art der erforderlichen Dokumentation anzugeben, die als „Information“ oder „Begründung“ dienen könnten.

— <CategoryName>: Bezeichnung der Kategorie für die erforderliche Dokumentation. Ein <CategoryName> könnte zusätzliche Unterkategorienamen enthalten, die durch „.“ getrennt sind.

— <ImplemenationCategoryName>: Bezeichnung der Umsetzungskategorie, die die definierte Implementation beschreibt.

— <AssessmentUnitName>: Bezeichnung der Beurteilungseinheit für eine bestimmte Umsetzungskategorie.

— <MechanismAbbreviation-<Nr»: Abkürzung des Namens der spezifischen Anforderung, die zu den Beurteilungskriterien gehört.

# 6 Anforderungen

## 6.1 [ACM] Zugangssteuerungsmechanismus (en: Access Control Mechanism)

### 6.1.1 [ACM-1] Anwendbarkeit von Zugangssteuerungsmechanismen

#### 6.1.1.1 Anforderung

Die Anlage muss Zugangssteuerungsmechanismen einsetzen, um den Zugang von Entitäten zu Sicherheitswerten und Datenschutzwerten zu verwalten, außer bei Zugang zu Sicherheitswerten oder Datenschutzwerten, für die gilt:

— öffentliche Zugänglichkeit entspricht der vorgesehenen Funktionalität der Anlage; oder

— physische oder logische Maßnahmen in der Zielbetriebsumgebung der Anlage beschränken die Zugänglichkeit für autorisierte Entitäten; oder

— rechtliche Implikationen lassen keine Zugangssteuerungsmechanismen zu.

#### 6.1.1.2 Begründung

Sicherheitswerte und Datenschutzwerte sind möglicherweise nicht autorisierten Zugangsversuchen ausgesetzt. Zugangssteuerungsmechanismen beschränken die Möglichkeit, dass nicht autorisierte Entitäten auf diese Werte zugreifen.

#### 6.1.1.3 Leitlinie

Die Anforderung fordert keine Zugangssteuerungsmechanismen für Werte, die nicht durch sie abgedeckt sind (z. B. für die Dosiertaste einer Kaffeemaschine). Darüber hinaus fordert sie keine Zugangssteuerungsmechanismen für Sicherheitswerte oder Datenschutzwerte, die grundsätzlich abgedeckt sind, die aber bei der vorgesehenen Anlagenfunktionalität allgemein für die Öffentlichkeit zugänglich sind oder bei denen die für die Nutzung vorgesehene Betriebsumgebung sicherstellt, dass nur ein autorisierter Zugang möglich ist. Wenn die Anlage auf die Zugangssteuerung durch die vorgesehene Betriebsumgebung angewiesen ist, muss sichergestellt werden, dass diese Zugangssteuerung angemessen ist, wie in ACM-2 beschrieben.

Im Allgemeinen kann die vollständige öffentliche Zugänglichkeit zu Datenschutzwerten nicht als eine begründete vorgesehene Anlagenfunktionalität betrachtet werden, insbesondere wenn der Schutz personenbezogener Daten von Kindern und die Kinderbetreuung betroffen sind. Bestimmte Szenarien, die die öffentliche Zugänglichkeit zu Datenschutzwerten beinhalten, können jedoch als vorgesehene Anlagenfunktionalität betrachtet werden, wenn sie Teil einer eindeutig angegebenen Funktionalität sind oder (für nicht kindliche Benutzer) über UNM übertragen werden.

Funkschnittstellen können zugänglich sein, selbst wenn sich die Anlage in einer Umgebung befindet, die eine physische Manipulation durch eine nicht autorisierte Entität verhindert, beispielsweise sind kabellose Netzwerke oft von außerhalb des Wohnbereichs des Benutzers zugänglich.

Beispielsweise können je nach den technischen Eigenschaften, der vorgesehenen Funktionalität und der für die Nutzung der Anlage vorgesehenen Betriebsumgebung unter Umständen keine Zugangssteuerungsmechanismen für maßgebliche Sicherheitswerte oder Datenschutzwerte erforderlich sein, wenn:

— alle Entitäten mit Zugang zum Gerät ( die Anlage wird Vorgabesgemäß in einem Bereich mit physischer Zugangsteuerung betrieben) für den Zugang zu diesen Sicherheitswerten oder Datenschutzwerten autorisiert sind (z. B. die WPS-Taste an einem Home-Router);

— die Anlagenfunktionalität nur Informationen (über Sicherheitswerte oder Datenschutzwerte) bereitstellt, die öffentlich zugänglich sein sollen (z. B. Übertragung durch drahtlose Kurzstrecken-Werbebeacons).

Zugangssteuerungsmechanismen benötigen Eigenschaften, mit denen die Zugangsrechte verknüpft werden können. Dies können unter anderem die folgenden Eigenschaften sein:

— verifizierte Angaben von Entitäten (beispielsweise Eigentümer eines Benutzerkontos, Mitglied einer spezifischen Gruppe oder durch eine andere Entität autorisiert zu sein);

— bestimmte Zustände der Anlage oder der Geräteumgebung (so kann beispielsweise ein elektronischer Pilotenkoffer während des Betriebs in der Luft andere Zugangsrechte für einen lokalen Benutzer haben, als wenn er am Boden aufbewahrt wird);

— die externe Schnittstelle, über die ein Zugang erfolgt (beispielsweise kann ein lokaler Zugang, bei dem offensichtlich eine physische Zugangskontrolle eingerichtet ist, andere Zugangsrechte haben als ein Fernzugriff);

— verschiedene Kombinationen der genannten Eigenschaften sowie zusätzliche Eigenschaften.

#### 6.1.1.4 Beurteilungskriterien

##### 6.1.1.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung ACM-1.

##### 6.1.1.4.2 Umsetzungskategorien

Nicht anwendbar.

##### 6.1.1.4.3 Erforderliche Informationen

[E.Info.ACM-1.SecurityAsset]: Beschreibung jedes Sicherheitswerts, der über Entitäten zugänglich ist, einschließlich:

— [E.Info.ACM-1.SecurityAsset.Access]: mögliche Zugänge von Entitäten auf den Sicherheitswert der Anlage; und

— (wenn die Zugangssteuerung durch die Anlage fehlt, weil die öffentliche Zugänglichkeit des Sicherheitswertes die vorgesehene Funktionalität des Gerätes ist) [E.Info.ACM-1.SecurityAsset.PublicAccess]: Beschreibung der vorgesehenen Funktionalität der Anlage im Hinblick auf die öffentliche Zugänglichkeit des Sicherheitswerts; und

— (wenn die Zugangssteuerung durch die Anlage nicht vorhanden ist, weil physische oder logische Maßnahmen in der Zielbetriebsumgebung der Anlage bestehen, die den Zugang auf autorisierte Entitäten beschränken) [E.Info.ACM-1.SecurityAsset.Environment]: Beschreibung:

  — der physischen oder logischen Zugangssteuerungsmaßnahmen in der Zielbetriebsumgebung der Anlage; und

  — der Art und Weise der Authentisierung/Autorisierung von Entitäten in der Zielbetriebsumgebung der Anlage; und

— (wenn die rechtlichen Implikationen keine Zugangssteuerungsmechanismen zulassen) [E.Info.ACM-1.SecurityAsset.Legal]: Verweisungen auf alle entsprechenden Absätze oder Textstellen in allen maßgeblichen Rechtsdokumenten, einschließlich einer Beschreibung, wie diese auf die Anlage oder den betroffenen Wert anzuwenden sind; und

— (wenn Zugangssteuerungsmechanismen für Entitäten, die Zugang zum Sicherheitswert haben, angeblich erforderlich sind) [E.Info.ACM-1.SecurityAsset.ACM]: Beschreibung jedes Zugangssteuerungsmechanismus, der den Zugang von Entitäten zum Sicherheitswert verwaltet.

[E.Info.ACM-1.PrivacyAsset]: Beschreibung jedes Datenschutzwerts, der über Entitäten zugänglich ist, einschließlich:

— [E.Info.ACM-1.PrivacyAsset.Access]: mögliche Zugänge von Entitäten auf den Datenschutzwert der Anlage; und

— (wenn die Zugangssteuerung durch die Anlage fehlt, damit die öffentliche Zugänglichkeit des Datenschutzwertes die vorgesehene Funktionalität des Gerätes ist) [E.Info.ACM-1.PrivacyAsset.PublicAccess]: Beschreibung der vorgesehenen Funktionalität der Anlage im Hinblick auf die öffentliche Zugänglichkeit des Datenschutzwerts; und

— (wenn die Zugangssteuerung durch die Anlage nicht vorhanden ist, weil physische oder logische Maßnahmen in der Zielbetriebsumgebung der Anlage bestehen, die den Zugang auf autorisierte Entitäten beschränken) [E.Info.ACM-1.PrivacyAsset.Environment]: Beschreibung:

  — der physischen oder logischen Zugangssteuerungsmaßnahmen in der Zielbetriebsumgebung der Anlage; und

  — der Art und Weise der Authentisierung/Autorisierung von Entitäten in der Zielbetriebsumgebung der Anlage; und

— (wenn die rechtlichen Konsequenzen keine Zugangssteuerungsmechanismen zulassen) [E.Info.ACM-1.PrivacyAsset.Legal]: Verweisungen auf alle entsprechenden Absätze oder Textstellen in allen maßgeblichen Rechtsdokumenten, einschließlich einer Beschreibung, wie diese auf die Anlage oder den betroffenen Wert anzuwenden sind; und

— (wenn Zugangssteuerungsmechanismen für Entitäten, die Zugang zum Datenschutzwert haben, angeblich erforderlich sind) [E.Info.ACM-1.PrivacyAsset.ACM]: Beschreibung jedes Zugangssteuerungsmechanismus, der den Zugang von Entitäten zum Datenschutzwert verwaltet.

[E.Info.DT.ACM-1]: Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 1 für jeden in [E.Info.ACM-1.SecurityAsset] bzw. [E.Info.ACM-1.PrivacyAsset] dokumentierten Sicherheitswert und Datenschutzwert.

[E.Just.DT.ACM-1]: Begründung für den gewählten Pfad durch den in [E.Info.DT.ACM-1] dokumentierten Entscheidungsbaum mit den folgenden Eigenschaften:

— (wenn eine Entscheidung aus [DT.ACM-1.DN-1 zu „NICHT ANWENDBAR“ führt) basiert die Begründung für die Entscheidung [DT.ACM-1.DN-1] auf [E.Info.ACM-1.SecurityAsset.PublicAccess] oder [E.Info.ACM-1.PrivacyAsset.PublicAccess]; und

— (wenn eine Entscheidung aus [DT.ACM-1.DN-2 zu „NICHT ANWENDBAR“ führt) basiert die Begründung für die Entscheidung [DT.ACM-1.DN-2] auf [E.Info.ACM-1.SecurityAsset.Environment] oder [E.Info.ACM-1.PrivacyAsset.Environment]; und

— (wenn eine Entscheidung aus [DT.ACM-1.DN-3 zu „NICHT ANWENDBAR“ führt) basiert die Begründung für die Entscheidung [DT.ACM-1.DN-3] auf [E.Info.ACM-1.SecurityAsset.Legal] oder [E.Info.ACM-1.PrivacyAsset.Legal]; und

— die Begründung für die Entscheidung [DT.ACM-1.DN-4] basiert auf [E.Info.ACM-1.SecurityAsset.ACM] oder [E.Info.ACM-1.PrivacyAsset.ACM].

#### 6.1.1.4.4 Konzeptuelle Beurteilung

##### 6.1.1.4.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob Zugangssteuerungsmechanismen implementiert wurden, wo sie nach ACM-1 erforderlich sind.

#### 6.1.1.4.4.2 Voraussetzungen

Keine.

#### 6.1.1.4.4.3 Beurteilungseinheiten

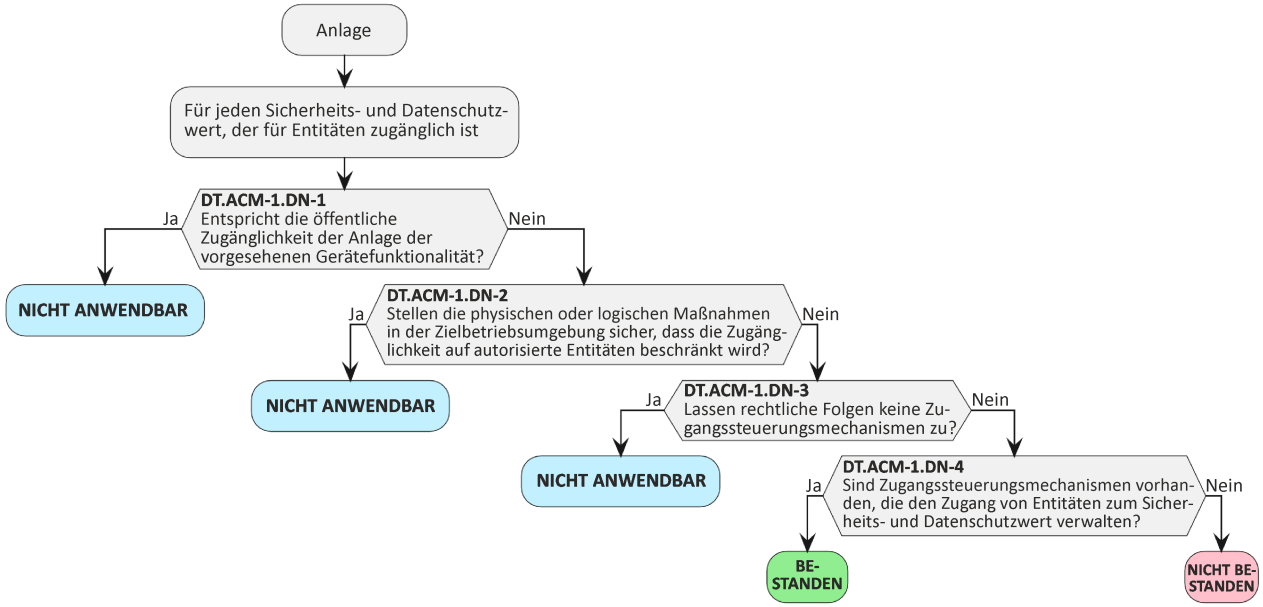



**Bild 1 — Entscheidungsbaum für Anforderung ACM-1**

Für jeden in [E.Info.ACM-1.SecurityAsset] dokumentierten Sicherheitswert und jeden in [E.Info.ACM-1.PrivacyAsset] dokumentierten Datenschutzwert ist zu prüfen, ob der Pfad durch den in [E.Info.DT.ACM-1] dokumentierten Entscheidungsbaum mit „NICHT ANWENDBAR“ oder „BESTANDEN“ endet.

Für jeden in [E.Info.DT.ACM-1] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.ACM-1] dokumentierte Begründung zu untersuchen.

#### 6.1.1.4.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— mindestens ein Pfad durch den in [E.Info.DT.ACM-1] dokumentierten Entscheidungsbaum mit „BESTANDEN“ endet; und

— kein Pfad durch den in [E.Info.DT.ACM-1] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; und

— die in [E.Just.DT.ACM-1] angegebenen Informationen korrekte Begründungen für alle Pfade durch den in [E.Info.DT.ACM-1] dokumentierten Entscheidungsbaum sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— alle Pfade durch den in [E.Info.DT.ACM-1] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; oder

— eine in [E.Just.DT.ACM-1] angegebene Begründung für einen Pfad durch den in [E.Info.DT.ACM-1] dokumentierten Entscheidungsbaum nicht korrekt ist oder fehlt.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

#### 6.1.1.4.5 Beurteilung der funktionalen Vollständigkeit

##### 6.1.1.4.5.1 Zweck der Beurteilung

Zweck der funktionalen Beurteilung ist es, zu überprüfen, ob alle Sicherheitswerte und Datenschutzwerte, zu denen die Entitäten Zugang haben, in [E.Info.ACM-1.PrivacyAsset] oder [E.Info.ACM-1.SecurityAsset] dokumentiert sind.

##### 6.1.1.4.5.2 Voraussetzungen

Die Anlage befindet sich im Betriebszustand.

##### 6.1.1.4.5.3 Beurteilungseinheiten

Es ist funktional zu beurteilen, ob in den Anlagen Sicherheitswerte vorhanden sind, zu denen Entitäten Zugang haben und die nicht in [E.Info.ACM-1.SecurityAsset] dokumentiert sind, und ob in den Anlagen Netzwerkwerte vorhanden sind, zu denen Entitäten Zugang haben und die nicht in [E.Info.ACM-1.PrivacyAsset] dokumentiert sind, z. B. durch Inspektion aller Teile der Software wie integrierte Software, installierte Anwendungen und Schnittstellen für angeschlossene Peripheriegeräte.

##### 6.1.1.4.5.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn alle gefundenen Sicherheitswerte in [E.Info.ACM-1.SecurityAsset] dokumentiert sind und alle gefundenen Datenschutzwerte in [E.Info.ACM-1.PrivacyAsset] dokumentiert sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn ein Sicherheitswert gefunden wird, der nicht in [E.Info.ACM-1.SecurityAsset] dokumentiert ist, oder wenn ein Datenschutzwert gefunden wird, der nicht in [E.Info.ACM-1.PrivacyAsset] dokumentiert ist.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

#### 6.1.1.4.6 Beurteilung der funktionalen Suffizienz

##### 6.1.1.4.6.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob Zugangssteuerungsmechanismen implementiert wurden, wo sie nach ACM-1 erforderlich sind.

##### 6.1.1.4.6.2 Voraussetzungen

Die Anlage befindet sich im Betriebszustand.

##### 6.1.1.4.6.3 Beurteilungseinheiten

Für jeden in [E.Info.ACM-1.SecurityAsset] dokumentierten Sicherheitswert und jeden in [E.Info.ACM-1.PrivacyAsset] dokumentierten Netzwerkwert ist funktional das Vorhandensein von Zugangssteuerungsmechanismen entsprechend [E.Info.ACM-1.SecurityAsset.ACM] oder [E.Info.ACM-1.PrivacyAsset.ACM] durch Zugang zu den Werten im Anschluss an [E.Info.ACM-1.PrivacyAsset.PublicAccess] und [E.Info.ACM-1.SecurityAsset.PublicAccess] zu bestätigen.

##### 6.1.1.4.6.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn kein Nachweis vorliegt, dass ein in [E.Info.ACM-1.SecurityAsset.ACM] oder [E.Info.ACM-1.PrivacyAsset.ACM] dokumentierter Zugangssteuerungsmechanismus nicht implementiert ist.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn ein Nachweis vorliegt, dass ein in [E.Info.ACM-1.SecurityAsset.ACM] oder [E.Info.ACM-1.PrivacyAsset.ACM] dokumentierter Zugangssteuerungsmechanismus nicht implementiert ist.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

### 6.1.2 [ACM-2] Entsprechende Zugangssteuerungsmechanismen

#### 6.1.2.1 Anforderung

Die nach ACM-1 erforderlichen Zugangssteuerungsmechanismen müssen sicherstellen, dass nur autorisierte Entitäten Zugang zu den geschützten Sicherheitswerten und Datenschutzwerten haben.

#### 6.1.2.2 Begründung

Sicherheitswerte und Datenschutzwerte sind möglicherweise nicht autorisierten Zugangsversuchen ausgesetzt. Angemessene Zugangssteuerungsmechanismen stellen sicher, dass diese Werte vor nicht autorisierten Zugriffen geschützt sind.

#### 6.1.2.3 Leitlinie

Diese Anforderung soll sicherstellen, dass die Zugangskontrollmechanismen, die zum Schutz der maßgeblichen Sicherheitswerte und Datenschutzwerte verwendet werden, so ausgewählt und konfiguriert wurden, dass nicht autorisierte Zugänge verweigert werden. Aufgrund vielfältiger Zugangsverfahren und Kontrollmechanismen für Werte (beispielsweise durch Anzeige auf einem Wearable-Bildschirm), Anwendungsfälle für Anlagen und Betriebsumgebungen ist es schwierig, ein allgemeines Modell für Entitäten und die damit verbundenen Zugangsrechte festzulegen.

Ob ein Zugangssteuerungsmechanismus einen nicht autorisierten Zugang verweigern kann, hängt immer davon ab, welche externen Annahmen erfüllt werden müssen. Beispielsweise, ob das Teilen von Passwörtern oder der nicht autorisierte physische Zugang unzulässig ist.

Abhängig von den technischen Geräteeigenschaften und der für die Nutzung vorgesehenen Betriebsumgebung nutzen Zugangssteuerungsmechanismen angemessene Eigenschaften, mit denen die Zugangsrechte verknüpft sind, und stellen sicher, dass alle beteiligten Entitäten Informationen über die Autorisierung erhalten.

Wenn Zugangssteuerungsmechanismen auf Authentisierungsmechanismen beruhen, vergleiche AUM, als Beispiel:

— kann eine autorisierte Entität, z. B. eine spezifische Person, der Besitzer eines Benutzerkontos, eines Geräts oder Dienstes, nach der Authentisierung auf den Sicherheitswert oder Datenschutzwert zugreifen, um beispielsweise die Sicherheitskonfiguration zu ändern; oder

— kann ein Mitglied einer spezifischen autorisierten Gruppe nach der Authentisierung auf einen Sicherheitswert oder einen Datenschutzwert zugreifen; oder

— kann eine Entität, die durch eine andere Entität dafür autorisiert wurde, auf einen spezifischen Sicherheitswert oder Datenschutzwert zugreifen.

Bei der Festlegung von angemessenen Zugangssteuerungsmechanismen für Sicherheitswerte und Datenschutzwerte sind die folgenden Aspekte wichtig:

— das Risiko, das mit dem Zugang einer Entität zu einem Sicherheitswert oder Datenschutzwert verbunden ist;

— die Art des Zugangs zu einem Sicherheitswert oder Datenschutzwert, den die Anlagenfunktionalität zulässt;

— die Schnittstelle, über die auf den Sicherheitswert oder Datenschutzwert zugegriffen wird; und

— die Auswirkungen der Zugangssteuerung, die durch die vorgesehene betriebliche Einsatzumgebung gegeben ist.

Bei der Festlegung der Zugangsrechte von Entitäten zu Sicherheitswerten oder Datenschutzwerten (autorisierten Entitäten für einen bestimmten Zugang zu Werten) sind die folgenden Aspekte wichtig:

— das Risiko, das mit dem Zugang einer Entität zu einem Sicherheitswert oder Datenschutzwert verbunden ist;

— das „Need-to-know-Prinzip“: ist es erforderlich, dass die Entität Informationen von einem Sicherheitswert oder Datenschutzwert erhält;

— das „Need-to-use-Prinzip“: hat eine Entität einen begründeten Bedarf, eine Funktionalität eines Sicherheitswerts oder Datenschutzwerts zu nutzen;

— das „Least-Privilege-Prinzip“: alles ist verboten, außer es ist erlaubt,

— die eindeutig angegebene Funktionalität der Anlage, beispielsweise bezüglich der Zugänglichkeit von Sicherheitswerten oder Datenschutzwerten oder der Interoperabilität mit Komponenten einer vorhandenen Infrastruktur.

Bei der Festlegung der Zugangsrechte von Kindern auf Datenschutzwerte oder der Zugangsrechte anderer Entitäten auf die Datenschutzwerte von Kindern sind die Anforderungen und Fähigkeiten von Kindern wichtige Aspekte, die berücksichtigt werden müssen.

Darüber hinaus kann bei der Nutzung von Zugangsrechten, die die Privatsphäre verletzen könnten, Die Anlage je nach seinen Fähigkeiten und der vorgesehenen Anlagenfunktionalität eine Funktionalität bereitstellen, die den Benutzer auf die Ausführung solcher Zugangsrechte aufmerksam macht (beispielsweise indem ein Symbol auf dem Bildschirm angezeigt wird, wenn die Stimmaufzeichnungs- oder Geolokalisierungsfunktionalität von einer Anwendung verwendet wird).

#### 6.1.2.4 Beurteilungskriterien

##### 6.1.2.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung ACM-2.

##### 6.1.2.4.2 Umsetzungskategorien

[IC.ACM-2.RBAC]: Die Methoden zur Validierung der Angemessenheit des Zugangssteuerungsmechanismus beruhen ausschließlich auf der rollenbasierten Zugangssteuerung.

[IC.ACM-2.DAC]: Die Methoden zur Validierung der Angemessenheit des Zugangssteuerungsmechanismus beruhen ausschließlich auf der benutzerbestimmbaren Zugangssteuerung.

[IC.ACM-2.MAC]: Die Methoden zur Validierung der Angemessenheit des Zugangssteuerungsmechanismus beruhen ausschließlich auf der systembestimmten Zugangssteuerung.

[IC.ACM-2.Generic]: Die Methoden zur Validierung der Angemessenheit des Zugangssteuerungsmechanismus beruhen nicht ausschließlich auf in ACM-2-RBAC, ACM-2-DAC oder ACM-2-MA beschriebenen Methoden.

##### 6.1.2.4.3 Erforderliche Informationen

[E.Info.ACM-2.SecurityAsset]: Beschreibung jedes Sicherheitswerts, für den ACM-1 Zugangssteuerungsmechanismen erfordert, einschließlich:

— [E.Info.ACM-2.SecurityAsset.ACM]: Beschreibung der nach ACM-1 geforderten Zugangssteuerungsmechanismen, der den Zugang von Entitäten zu den Sicherheitswerten verwaltet, und der Art und Weise, wie die Mechanismen sicherstellen, dass nur autorisierte Entitäten Zugang zu den Sicherheitswerten haben, je nach Umsetzungskategorie.

[E.Info.ACM-2.PrivacyAsset]: Beschreibung jedes Datenschutzwerts, für den ACM-1 Zugangssteuerungsmechanismen erfordert, einschließlich:

— [E.Info.ACM-2.PrivacyAsset.ACM]: Beschreibung der nach ACM-1 geforderten Zugangssteuerungsmechanismen, der den Zugang von Entitäten zu den Datenschutzwerten verwaltet, und der Art und Weise, wie die Mechanismen sicherstellen, dass nur autorisierte Entitäten Zugang zu den Datenschutzwerten haben, je nach Umsetzungskategorie.

[E.Info.DT.ACM-2]: Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 2 für jeden in [E.Info.ACM-2.SecurityAsset] dokumentierten Sicherheitswert und in [E.Info.ACM-2.PrivacyAsset] dokumentierten Datenschutzwert.

[E.Just.DT.ACM-2]: Begründung für den gewählten Pfad durch den in [E.Info.DT.ACM-2] dokumentierten Entscheidungsbaum mit den folgenden Eigenschaften:

— die Begründung für die Entscheidung [DT.ACM-2.DN-1] basiert auf [E.Info.ACM-2 PrivacyAsset.ACM] oder [E.Info.ACM-2.SecurityAsset.ACM].

ANMERKUNG Eine Begründung beinhaltet eine Beschreibung der Entitäten, ihre Zugangsrechte zum entsprechenden Sicherheitswert oder Datenschutzwert und das Verfahren, wie durch Zugangssteuerungsmechanismen sichergestellt wird, dass nur autorisierter Zugang zum entsprechenden Wert gewährt wird.

#### 6.1.2.4.4 Konzeptuelle Beurteilung

##### 6.1.2.4.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob die Zugangssteuerungsmechanismen, die nach ACM-1 erforderlich sind, wie nach ACM-2 erforderlich implementiert sind.

##### 6.1.2.4.4.2 Voraussetzungen

Keine.

##### 6.1.2.4.4.3 Beurteilungseinheiten

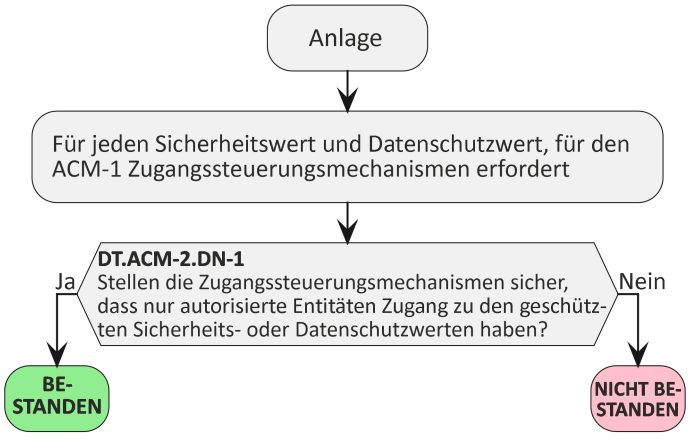



**Bild 2 — Entscheidungsbaum für Anforderung ACM-2**

Für jeden in [E.Info.ACM-2.SecurityAsset] dokumentierten Sicherheitswert und jeden in [E.Info.ACM-2.PrivacyAsset] dokumentierten Datenschutzwert ist zu prüfen, ob der Pfad durch den in [E.Info.DT.ACM-2] dokumentierten Entscheidungsbaum mit „BESTANDEN“ endet.

Für jeden in [E.Info.DT.ACM-2] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.ACM-2] dokumentierte Begründung zu untersuchen.

#### 6.1.2.4.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— alle Pfade durch den in [E.Info.DT.ACM-2] dokumentierten Entscheidungsbaum mit „BESTANDEN“ enden; und

— die in [E.Just.DT.ACM-2] angegebenen Informationen korrekte Begründungen für alle Pfade durch den in [E.Info.DT.ACM-2] dokumentierten Entscheidungsbaum sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— ein Pfad durch den in [E.Info.DT.ACM-2] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; oder

— eine in [E.Just.DT.ACM-2] angegebene Begründung für einen Pfad durch den in [E.Info.DT.ACM-2] dokumentierten Entscheidungsbaum nicht korrekt ist oder fehlt.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

#### 6.1.2.4.5 Beurteilung der funktionalen Vollständigkeit

Die Beurteilung der funktionalen Vollständigkeit wird durch die Beurteilung der funktionalen Suffizienz der Anwendbarkeit des Zugangssteuerungsmechanismus abgedeckt.

Deshalb ist diese Beurteilung der funktionalen Vollständigkeit nicht notwendig.

#### 6.1.2.4.6 Beurteilung der funktionalen Suffizienz

#### 6.1.2.4.6.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob die Zugangssteuerungsmechanismen implementiert wurden, wie sie nach ACM-2 erforderlich sind.

#### 6.1.2.4.6.2 Beurteilungseinheiten

Für jeden in [E.Info.ACM-2.SecurityAsset] dokumentierten Sicherheitswert und in [E.Info.ACM-2.PrivacyAsset] dokumentierten Datenschutzwert:

[AU.ACM-2.RBAC]: Wenn die in [E.Info.ACM-2.SecurityAsset.ACM] oder [E.Info.ACM-2.PrivacyAsset.ACM] dokumentierten Zugangssteuerungsmechanismen zu [IC.ACM-2.RBAC] gehören, ist funktional zu bestätigen, dass

— jedem Benutzer Rollen mit entsprechenden Autorisierungen zugewiesen werden; und

— die wenigsten Privilegien mit den Rollen verbunden sind; und

— der Zugang zu den Sicherheitswerten oder Datenschutzwerten nur für autorisierte Benutzer entsprechend ihrer Rolle möglich ist; und

— Rollenänderungen nur von autorisierten Benutzern vorgenommen werden können.

[AU.ACM-2.DAC]: Wenn die in [E.Info.ACM-2.SecurityAsset.ACM] oder [E.Info.ACM-2.PrivacyAsset.ACM] dokumentierten Zugangssteuerungsmechanismen zu [IC.ACM-2.DAC] gehören, ist funktional zu bestätigen, dass

— jedem Benutzer Identitäten mit entsprechenden Autorisierungen zugewiesen werden; und

— die wenigsten Privilegien mit den Identitäten verbunden sind; und

— der Zugang zu den Sicherheitswerten oder Datenschutzwerten nur für autorisierte Benutzer entsprechend ihrer Identität möglich ist; und

— Identitätsänderungen nur von autorisierten Benutzern vorgenommen werden können.

[AU.ACM-2.MAC]: Wenn die in [E.Info.ACM-2.SecurityAsset.ACM] oder [E.Info.ACM-2.PrivacyAsset.ACM] dokumentierten Zugangssteuerungsmechanismen zu [IC.ACM-2.MAC] gehören, ist funktional zu bestätigen, dass

— der Zugang zu den Sicherheitswerten oder Datenschutzwerten nur für autorisierte Benutzer möglich ist, nachdem eine Freigabe durch den Betriebssystem- und/oder Systemadministrator erteilt wurde; und

— die Erteilung der Freigabe mit dem „Least-Privilege-Prinzip“ verbunden ist; und

— der Wechsel des Betriebssystem- und/oder des Systemadministrators, der für die Freigabe des Benutzers zuständig ist, nur vom autorisierten Systemadministrator vorgenommen werden kann.

[AU.ACM-2.Generic]: Wenn die in [E.Info.ACM-2.SecurityAsset.ACM] oder [E.Info.ACM-2.PrivacyAsset.ACM] dokumentierten Zugangssteuerungsmechanismen zu [IC.ACM-2.Generic] gehören, ist funktional zu bestätigen, dass

— der Zugang zu den Sicherheitswerten oder Datenschutzwerten nur für autorisierte Benutzer möglich ist; und

— das „Least-Privilege-Prinzip“ für die Benutzer befolgt wird; und

— die Änderung von Einstellungen, die sich auf den Zugangssteuerungsmechanismus beziehen, oder die Änderung von Privilegien der Benutzer nur von autorisierten Benutzern vorgenommen werden dürfen.

#### 6.1.2.4.6.3 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn für jeden in [E.Info.ACM-2.SecurityAsset] dokumentierten Sicherheitswert und in [E.Info.ACM-2.PrivacyAsset] dokumentierten Datenschutzwert die Bestätigungen in der von der Umsetzungskategorie abhängigen Beurteilungseinheit erfolgreich sind.

Die Entscheidung NICHT BESTANDEN für den Beurteilungsfall wird zugewiesen, wenn für ein in [E.Info.ACM-2.SecurityAsset] dokumentierter Sicherheitswert oder ein in [E.Info.ACM-2.PrivacyAsset] dokumentierter Datenschutzwert eine Bestätigung in der von der Umsetzungskategorie abhängigen Beurteilungseinheit nicht erfolgreich ist.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

### 6.1.3 [ACM-3] Standardmäßige Zugangssteuerung für Kinder bei Spielzeugen

#### 6.1.3.1 Anforderung

Falls es sich bei der Anlage um ein Spielzeug handelt, müssen die Zugangssteuerungsmechanismen bei jeder Datenschutzfunktion, mit der Kinder auf externe Inhalte zugreifen können und bei der der Zugang von Kindern durch nach ACM-1 erforderlichen Zugangssteuerungsmechanismen verwaltet wird, sicherstellen, dass der Zugang von Kindern zu externen Inhalten über die Datenschutzfunktion standardmäßig auf Inhalte von autorisierten Entitäten beschränkt ist.

#### 6.1.3.2 Begründung

Inhalte von externen Quellen, auf die Kinder zugreifen, können für eine nicht autorisierte Kommunikation oder Interaktion genutzt werden oder anderweitig den Schutz der Privatsphäre von Kindern kompromittieren. Indem der Zugang von Kindern standardmäßig nur auf autorisierte Entitäten beschränkt wird, wird die Vermeidung der entsprechenden Gefährdungen unterstützt.

#### 6.1.3.3 Leitlinie

Datenschutzfunktionen, die Kindern den Zugang zu Inhalten erlauben, können unter anderem die folgenden umfassen:

— Chat-Funktionen,

— Sprach- oder Video-Anruffunktionen,

— Funktionen, die Inhalte aus externen Quellen anzeigen.

Um sicherzustellen, dass der Standardzugang von Kindern zu Inhalten aus externen Quellen auf den Inhalt von autorisierten Entitäten beschränkt wird, ist es unter anderem möglich:

— Kindern allen Zugang zu externen Quellen zu verweigern; oder

— Kindern allen Zugang zu externen Quellen zu verweigern, außer diese sind explizit in einer Zulassungsliste aufgeführt, bei deren Erstellung sichergestellt wurde, dass sie nur den Zugang zu Inhalten von autorisierten Entitäten enthält.

#### 6.1.3.4 Beurteilungskriterien

##### 6.1.3.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung ACM-3.

##### 6.1.3.4.2 Umsetzungskategorien

[IC.ACM-3.RBAC]: Die Methoden zur Validierung, ob die in [E.Info.ACM-3.ACM] dokumentierten Zugangssteuerungsmechanismen standardmäßig ausschließlich auf einer rollenbasierten Zugangssteuerung beruhen und sicherstellen, dass der Zugang von Kindern zu externen Inhalten über die Datenschutzfunktion standardmäßig auf Inhalte von autorisierten Entitäten beschränkt ist.

[IC.ACM-3.DAC]: Die Methoden zur Validierung, ob die in [E.Info.ACM-3.ACM] dokumentierten Zugangssteuerungsmechanismen standardmäßig ausschließlich auf einer benutzerbestimmbaren Zugangssteuerung beruhen und sicherstellen, dass der Zugang von Kindern zu externen Inhalten über die Datenschutzfunktion standardmäßig auf Inhalte von autorisierten Entitäten beschränkt ist.

[IC.ACM-3.MAC]: Die Methoden zur Validierung, ob die in [E.Info.ACM-3.ACM] dokumentierten Zugangssteuerungsmechanismen standardmäßig ausschließlich auf einer systembestimmten Zugangssteuerung beruhen und sicherstellen, dass der Zugang von Kindern zu externen Inhalten über die Datenschutzfunktion standardmäßig auf Inhalte von autorisierten Entitäten beschränkt ist.

[IC.ACM-3.Generic]: Die Methoden zur Validierung, ob die in [E.Info.ACM-3.ACM] dokumentierten Zugangssteuerungsmechanismen standardmäßig nicht ausschließlich auf einer der in ACM-3-RBAC, ACM-3-DAC oder ACM-3-MAC beschriebenen Methoden beruhen und sicherstellen, dass der Zugang von Kindern zu externen Inhalten über die Datenschutzfunktion standardmäßig auf Inhalte von autorisierten Entitäten beschränkt ist.

#### 6.1.3.4.3 Erforderliche Informationen

[E.Info.ACM-3.PrivacyAsset]: Beschreibung jeder Datenschutzfunktion, bei der Kinder auf externe Inhalte zugreifen können, einschließlich:

— [E.Info.ACM-3.PrivacyAsset.TrustedSources]: Liste der autorisierten Entitäten, die externe, für Kinder geeignete Inhalte anbieten.

[E.Info.ACM-3.ACM]: Beschreibung jedes Zugangssteuerungsmechanismus, der nach ACM-1 erforderlich ist und der den Zugang von Kindern für jede in [E.Info.ACM-3.PrivacyAsset] dokumentierte Datenschutzfunktion verwaltet, einschließlich:

— Beschreibung, wie die Beschränkung des Zugangs von Kindern zu Inhalten nur von autorisierten Entitäten implementiert wird.

[E.Info.DT.ACM-3]: Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 3 für jede Datenschutzfunktion, bei der der Zugang von Kindern durch in [E.Info.ACM-3.ACM] dokumentierten Zugangssteuerungsmechanismen verwaltet wird.

[E.Just.DT.ACM-3]: Begründung des gewählten Pfads durch den Entscheidungsbaum für jede Datenschutzfunktion, bei der der Zugang von Kindern durch in [E.Info.ACM-3.ACM] dokumentierten Zugangssteuerungsmechanismen verwaltet wird mit der folgenden Eigenschaft:

— die Begründung [DT.ACM-3.DN-2] basiert auf [E.Info.ACM-3.ACM] und [E.Info.ACM-3.PrivacyAsset.TrustedSources].

#### 6.1.3.4.4 Konzeptuelle Beurteilung

##### 6.1.3.4.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob die Zugangssteuerungsmechanismen für den Zugang von Kindern zu Datenschutzfunktionen wie nach ACM-3 erforderlich implementiert sind.

##### 6.1.3.4.4.2 Voraussetzungen

Keine.

#### 6.1.3.4.4.3 Beurteilungseinheiten

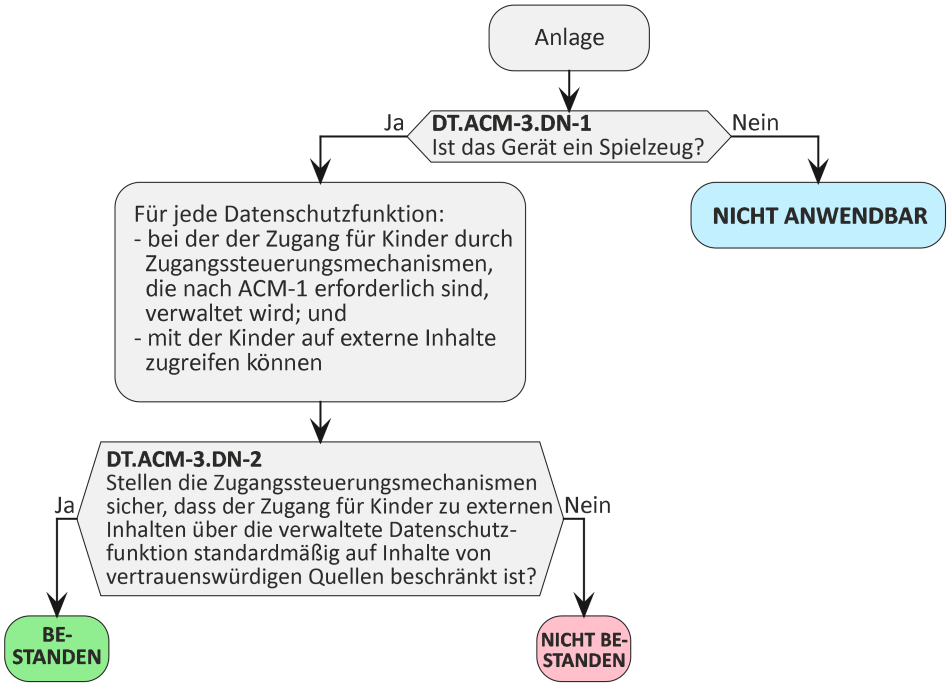



**Bild 3 — Entscheidungsbaum für Anforderung ACM-3**

Für jede in [E.Info.ACM-3.PrivacyAsset] dokumentierte Datenschutzfunktion, bei der Kinder auf externe Inhalte zugreifen können und bei der der Zugang durch Zugangssteuerungsmechanismen entsprechend [E.Info.ACM-3.ACM] verwaltet wird, ist zu prüfen, ob der Pfad durch den in [E.Info.DT.ACM-3] dokumentierten Entscheidungsbaum mit „BESTANDEN“ endet.

Für jeden in [E.Info.DT.ACM-3] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.ACM-3] dokumentierte Begründung zu untersuchen.

#### 6.1.3.4.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— mindestens ein Pfad durch den in [E.Info.DT.ACM-3] dokumentierten Entscheidungsbaum mit „BESTANDEN“ endet; und

— kein Pfad durch den in [E.Info.DT.ACM-3] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; und

— die in [E.Just.DT.ACM-3] angegebenen Informationen korrekte Begründungen für alle Pfade durch den in [E.Info.DT.ACM-3] dokumentierten Entscheidungsbaum sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— ein Pfad durch den in [E.Info.DT.ACM-3] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; oder

— eine in [E.Just.DT.ACM-3] angegebene Begründung für einen Pfad durch den in [E.Info.DT.ACM-3] dokumentierten Entscheidungsbaum nicht korrekt ist oder fehlt.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

#### 6.1.3.4.5 Beurteilung der funktionalen Vollständigkeit

##### 6.1.3.4.5.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob die Dokumentation von Datenschutzfunktionen, bei denen Kinder auf externe Inhalte zugreifen können, vollständig ist.

##### 6.1.3.4.5.2 Voraussetzungen

Die Anlage befindet sich im Betriebszustand.

##### 6.1.3.4.5.3 Beurteilungseinheiten

Es ist funktional zu beurteilen, ob Datenschutzfunktionen vorhanden sind, die Kindern den Zugang zu externen Inhalten ermöglichen, die nicht in [E.Info.ACM-3.PrivacyAsset] aufgeführt sind, indem die folgenden Schritte durchgeführt werden:

1) Es sind alle Datenschutzfunktionen der Anlage aufzulisten, über die Kinder auf externe Inhalte zugreifen können, z. B. durch Inspektion aller Teile der Software, wie beispielsweise Prüfung der Einstellungen des Internetbrowsers, Untersuchung des Zugriffs auf den App-Store, Inspektion der installierten Apps, Untersuchung der eingebauten oder installierten Kindersicherung.

2) Die in Schritt 1 erstellte Liste der funktional identifizierten Datenschutzfunktionen wird mit der in [E.Info.ACM-3.PrivacyAsset] angegebenen Liste der Datenschutzfunktionen verglichen und etwaige Diskrepanzen markiert.

##### 6.1.3.4.5.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn alle entdeckten Datenschutzfunktionen, bei denen Kinder auf externe Inhalte zugreifen können, in [E.Info.ACM-3.PrivacyAsset] dokumentiert sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn eine entdeckte Datenschutzfunktion, bei der Kinder auf externe Inhalte zugreifen können, nicht in [E.Info.ACM-3.PrivacyAsset] dokumentiert ist.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

#### 6.1.3.4.6 Beurteilung der funktionalen Suffizienz

##### 6.1.3.4.6.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob die Zugangssteuerungsmechanismen sicherstellen, dass der Zugang von Kindern zu externen Inhalten über die Datenschutzfunktion standardmäßig auf Inhalte von autorisierten Entitäten beschränkt ist.

##### 6.1.3.4.6.2 Voraussetzungen

Die Anlage befindet sich im Betriebszustand.

##### 6.1.3.4.6.3 Beurteilungseinheiten

[AU.ACM-3.RBAC]: Wenn die in [E.Info.ACM-3.ACM] dokumentierten Zugangssteuerungsmechanismen zu [IC.ACM-3.RBAC] gehören, ist funktional zu bestätigen, dass

— Kindern entsprechende Rollen zugewiesen werden, die nur den Zugriff auf Inhalte von autorisierten Entitäten über die Datenschutzfunktion erlauben, die wiederum den Zugriff auf externe Inhalte erlaubt; und

— die wenigsten Privilegien mit der Rolle der Kinder verbunden sind; und

— Rollenänderungen nur von autorisierten Benutzern vorgenommen werden können.

[AU.ACM-3.DAC]: Wenn die in [E.Info.ACM-3.ACM] dokumentierten Zugangssteuerungsmechanismen zu [IC.ACM-3.DAC] gehören, ist funktional zu bestätigen, dass

— Kindern assoziierte Identitäten zugewiesen werden, die nur den Zugriff auf Inhalte von autorisierten Entitäten über die Datenschutzfunktion erlauben, die wiederum den Zugriff auf externe Inhalte erlaubt; und

— die wenigsten Privilegien mit der Identität der Kinder verbunden sind; und

— Identitätsänderungen nur von autorisierten Benutzern vorgenommen werden können.

[AU.ACM-3.MAC]: Wenn die in [E.Info.ACM-3.ACM] dokumentierten Zugangssteuerungsmechanismen zu [IC.ACM-3.MAC] gehören, ist funktional zu bestätigen, dass

— Kinder nur dann eine Freigabe vom Betriebssystem und/oder Systemadministrator erhalten, wenn sie versuchen, über die Datenschutzfunktion, die den Zugang zu externen Inhalten erlaubt, auf Inhalte von autorisierten Entitäten zuzugreifen; und

— die Erteilung der Freigabe mit dem „Least-Privilege-Prinzip“ verbunden ist; und

— der Wechsel des Betriebssystem- und/oder des Systemadministrators, der für die Freigabe des Benutzers zuständig ist, nur vom autorisierten Systemadministrator vorgenommen werden kann.

[AU.ACM-3.Generic]: Wenn die in [E.Info.ACM-3.ACM] dokumentierten Zugangssteuerungsmechanismen zu [IC.ACM-3.Generic] gehören, ist funktional zu bestätigen, dass

— Kinder nur über die Datenschutzfunktion, die den Zugriff auf externe Inhalte erlaubt, auf Inhalte von autorisierten Entitäten zugreifen können; und

— das „Least-Privilege-Prinzip“ für Kinder befolgt wird; und

— die Änderung von Einstellungen, die sich auf den Zugangssteuerungsmechanismus beziehen, oder die Änderung von Privilegien der Kinder nur von autorisierten Benutzern vorgenommen werden dürfen.

#### 6.1.3.4.6.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn für jeden in [E.Info.ACM-3.ACM] dokumentierten Zugangssteuerungsmechanismus die Bestätigungen in der von der Umsetzungskategorie abhängigen Beurteilungseinheit erfolgreich sind.

Die Entscheidung NICHT BESTANDEN für den Beurteilungsfall wird zugewiesen, wenn für einen in [E.Info.ACM-3.ACM] dokumentierten Zugangssteuerungsmechanismus eine Bestätigung in der von der Umsetzungskategorie abhängigen Beurteilungseinheit nicht erfolgreich ist.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

### 6.1.4 [ACM-4] Standard-Zugangssteuerung zu Datenschutzwerten von Kindern für Spielzeuge und Kinderbetreuungsgeräte

#### 6.1.4.1 Anforderung

Wenn die Anlage ein Spielzeug oder ein Gerät für die Kinderbetreuung ist, müssen alle nach ACM-1 erforderlichen Zugangssteuerungsmechanismen für Datenschutzfunktionen und personenbezogene Informationen von Kindern den Zugang Dritter (ausgenommen das Kind und dessen Eltern/Erziehungsberechtigte) zu den

vom Gerät verarbeiteten Datenschutzfunktionen und personenbezogenen Informationen standardmäßig einschränken, außer bei autorisierten Zugriffen, die für die vorgesehene Anlagenfunktionalität erforderlich sind.

#### 6.1.4.2 Begründung

Die standardmäßige Offenlegung von Datenschutzfunktionen oder personenbezogenen Informationen für Dritte kann den Schutz der Privatsphäre von Kindern kompromittieren, selbst wenn ein Einverständnis vorliegt. Die Beschränkung der Standard-Zugangsrechte Dritter zu den Datenschutzfunktionen und personenbezogenen Informationen von Kindern auf die für den Betrieb der Anlage notwendigen Rechte trägt zum Schutz der Privatsphäre bei.

#### 6.1.4.3 Leitlinie

Wenn Datenschutzwerte durch mehrere Zugangssteuerungsmechanismen geschützt werden, kann die Standardkonfiguration aller Zugangssteuerungsmechanismen die Standard-Zugänglichkeit zu den Datenschutzwerten beeinflussen.

Es kann notwendig sein, dass externe Entitäten, wie z. B. Cloud-Dienste, die unter der Kontrolle des Geräteherstellers stehen, auf die personenbezogenen Informationen von Kindern für die vorgesehene Anlagenfunktionalität zugreifen. Ein Beispiel ist eine Kinderuhr, bei der die Eltern den Standortverlauf der Uhr, der unabhängig vom aktuellen Netzverbindungsstatus der Uhr in einem Cloud-Dienst aufgezeichnet wird, nachverfolgen können.

Da Kinder durch Cyberkriminalität gefährdet sind, wird den Entwicklern von Standardeinstellungen dringend empfohlen, das Wohl der Kinder zu berücksichtigen.

#### 6.1.4.4 Beurteilungskriterien

##### 6.1.4.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung ACM-4.

##### 6.1.4.4.2 Umsetzungskategorien

[IC.ACM-4.RBAC]: Die Methoden zur Validierung, ob die in [E.Info.ACM-4.ACM] dokumentierten Zugangssteuerungsmechanismen standardmäßig ausschließlich auf einer rollenbasierten Zugangssteuerung beruhen und sicherstellen, dass der Zugang anderer „dritter“ Entitäten zu den vom Gerät verarbeiteten Datenschutzfunktionen und personenbezogenen Informationen von Kindern auf den für den Betrieb der Anlage erforderlichen Zugang beschränkt ist.

[IC.ACM-4.DAC]: Die Methoden zur Validierung, ob die in [E.Info.ACM-4.ACM] dokumentierten Zugangssteuerungsmechanismen standardmäßig ausschließlich auf einer benutzerbestimmbaren Zugangssteuerung beruhen und sicherstellen, dass der Zugang anderer „dritter“ Entitäten zu den vom Gerät verarbeiteten Datenschutzfunktionen und personenbezogenen Informationen von Kindern auf den für den Betrieb der Anlage erforderlichen Zugang beschränkt ist.

[IC.ACM-4.MAC]: Die Methoden zur Validierung, ob die in [E.Info.ACM-4.ACM] dokumentierten Zugangssteuerungsmechanismen standardmäßig ausschließlich auf einer systembestimmten Zugangssteuerung beruhen und sicherstellen, dass der Zugang anderer „dritter“ Entitäten zu den vom Gerät verarbeiteten Datenschutzfunktionen und personenbezogenen Informationen von Kindern auf den für den Betrieb der Anlage erforderlichen Zugang beschränkt ist.

[IC.ACM-4.Generic]: Die Methoden zur Validierung, ob die in [E.Info.ACM-4.ACM] dokumentierten Zugangssteuerungsmechanismen standardmäßig nicht ausschließlich auf einer der in ACM-4-RBAC, ACM-4-DAC oder ACM-4-MAC beschriebenen Methoden beruhen und sicherstellen, dass der Zugang anderer „dritter“ Entitäten zu den vom Gerät verarbeiteten Datenschutzfunktionen und personenbezogenen Informationen von Kindern auf den für den Betrieb der Anlage erforderlichen Zugang beschränkt ist.

#### 6.1.4.4.3 Erforderliche Informationen

[E.Info.ACM-4.PrivacyAsset]: Beschreibung aller vom Gerät verarbeiteten Datenschutzfunktionen und personenbezogenen Informationen von Kindern, auf die von anderen Entitäten außer den Kindern oder deren Eltern/Erziehungsberechtigten zugegriffen werden kann.

[E.Info.ACM-4.ACM]: Beschreibung der einzelnen Zugangssteuerungsmechanismen, die nach ACM-1 erforderlich sind und die den Zugang Dritter (ausgenommen die Kinder oder deren Eltern/Erziehungsberechtigte) zu allen vom Gerät verarbeiteten Datenschutzfunktionen und personenbezogenen Informationen verwalten, einschließlich:

— Beschreibung, wie die Zugriffe Dritter in der Standardkonfiguration verwaltet werden; und

— Beschreibung, wie die Beschränkungen des Zugriffs Dritter implementiert werden; und

(wenn der autorisierte Zugang für die vorgesehene Anlagenfunktionalität erforderlich ist) [E.Info.ACM-4.AuthorisedAccess]: Liste aller autorisierten Dritten, einschließlich:

— Liste aller in [E.Info.ACM-4.PrivacyAsset] dokumentierten Werte, zu denen der Dritte Zugang hat, für jeden autorisierten Dritten; und

— Beschreibung, wie die vorgesehene Anlagenfunktionalität von dem in [E.Info.ACM-4.PrivacyAsset] für jeden autorisierten Dritten dokumentierten autorisierten Zugang zu den betroffenen Werten abhängt.

[E.Info.DT.ACM-4]: Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 4 für alle Datenschutzfunktionen und vom in [E.Info.ACM-4.PrivacyAsset] dokumentierten Gerät verarbeiteten personenbezogenen Informationen von Kindern, bei denen der Zugang Dritter (ausgenommen die Kinder und deren Eltern oder Erziehungsberechtigte) durch in [E.Info.ACM-4.ACM] dokumentierten Zugangssteuerungsmechanismen verwaltet wird.

[E.Just.DT.ACM-4]: Begründung für jeden gewählten Pfad durch den in [E.Info.DT.ACM-4] dokumentierten Entscheidungsbaum mit den folgenden Eigenschaften:

— (wenn eine Entscheidung aus [DT.ACM-4.DN-2] zu „NICHT ANWENDBAR“ führt) basiert die Begründung für die Entscheidung [DT.ACM-4.DN-2] auf [E.Info.ACM-4.AuthorisedAccess]; und

— die Begründung für die Entscheidung [DT.ACM-4.DN-3] basiert auf [E.Info.ACM-4.ACM].

#### 6.1.4.4.4 Konzeptuelle Beurteilung

##### 6.1.4.4.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob die Zugangssteuerungsmechanismen implementiert wurden, wie sie nach ACM-4 erforderlich sind.

##### 6.1.4.4.4.2 Voraussetzungen

Keine.

#### 6.1.4.4.4.3 Beurteilungseinheiten

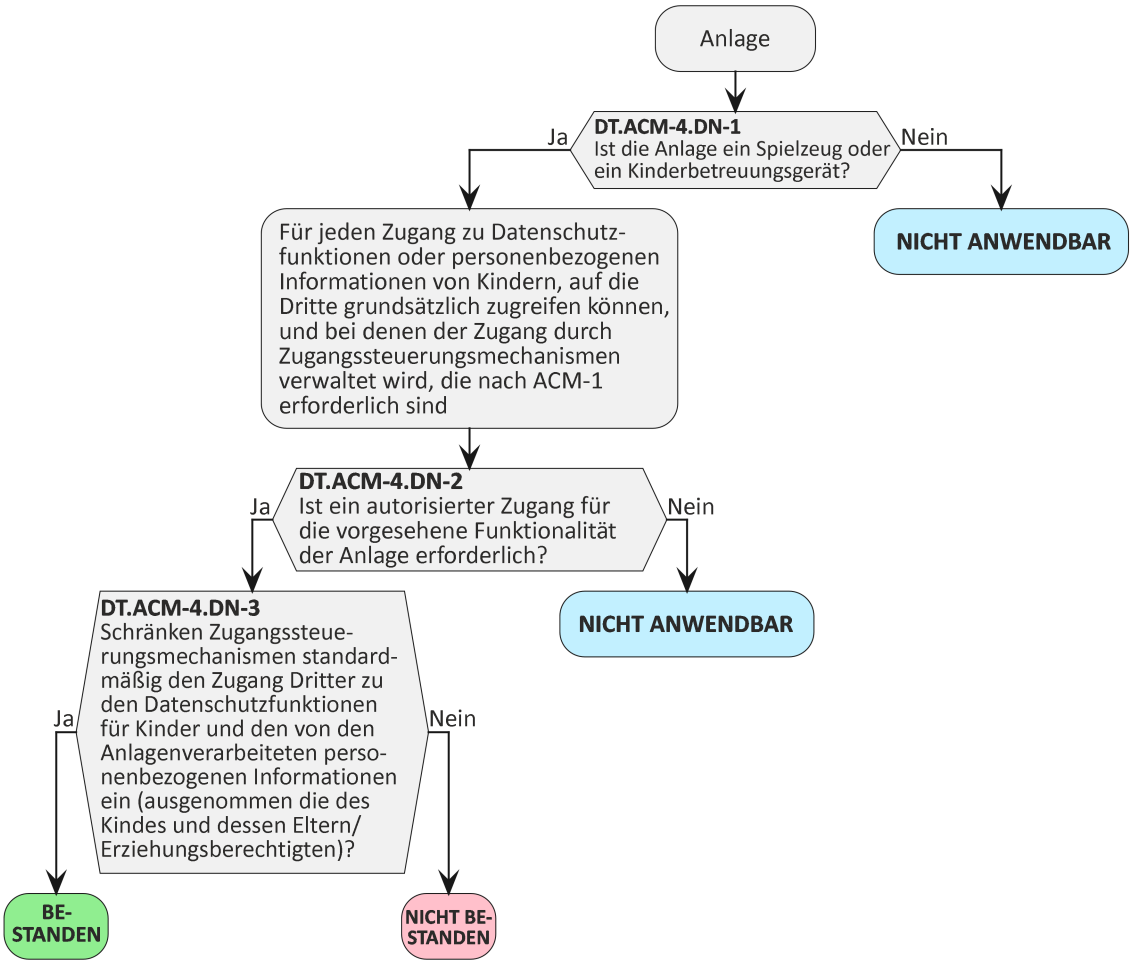



**Bild 4 — Entscheidungsbaum für Anforderung ACM-4**

Für alle in [E.Info.ACM-4.PrivacyAsset] dokumentierten Datenschutzfunktionen und personenbezogenen Informationen von Kindern, auf die Dritte (ausgenommen die Kinder oder deren Eltern/Erziehungsberechtigte) zugreifen können und bei denen der Zugang durch Zugangssteuerungsmechanismen entsprechend [E.Info.ACM-4.ACM] verwaltet wird, ist zu prüfen, ob der Pfad durch den in [E.Info.DT.ACM-4] dokumentierten Entscheidungsbaum mit „NICHT ANWENDBAR“ oder „BESTANDEN“ endet.

Für jeden in [E.Info.DT.ACM-4] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.ACM-4] dokumentierte Begründung zu untersuchen.

#### 6.1.4.4.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— mindestens ein Pfad durch den in [E.Info.DT.ACM-4] dokumentierten Entscheidungsbaum mit „BESTANDEN“ endet; und

— kein Pfad durch den in [E.Info.DT.ACM-4] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; und

— die in [E.Just.DT.ACM-4] angegebenen Informationen korrekte Begründungen für alle Pfade durch den in [E.Info.DT.ACM-4] dokumentierten Entscheidungsbaum sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— ein Pfad durch den in [E.Info.DT.ACM-4] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; oder

— eine in [E.Just.DT.ACM-4] angegebene Begründung für einen Pfad durch den in [E.Info.DT.ACM-4] dokumentierten Entscheidungsbaum nicht korrekt ist oder fehlt.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

#### 6.1.4.4.5 Beurteilung der funktionalen Vollständigkeit

##### 6.1.4.4.5.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob die Dokumentation der vom Gerät verarbeiteten Datenschutzfunktionen und personenbezogenen Informationen von Kindern, auf die Dritte (ausgenommen die Kinder oder deren Eltern/Erziehungsberechtigte) zugreifen können, vollständig ist.

##### 6.1.4.4.5.2 Voraussetzungen

Die Anlage befindet sich im Betriebszustand.

##### 6.1.4.4.5.3 Beurteilungseinheiten

Es ist funktional zu beurteilen, ob es Datenschutzfunktionen und personenbezogene Informationen von Kindern auf der Anlage gibt, auf die Dritte (ausgenommen die Kinder oder deren Eltern/Erziehungsberechtigte) zugreifen können und die nicht in [E.Info.ACM-4.PrivacyAsset] aufgeführt sind, indem die folgenden Schritte durchgeführt werden:

1) Es sind alle Datenschutzfunktionen der Anlage für Kinder und deren persönliche Informationen auf der Anlage aufzulisten, auf die Dritte außer den Kindern oder ihren Eltern/Erziehungsberechtigten zugreifen können, z. B. durch Inspektion aller Teile der Software, wie beispielsweise Prüfung der Einstellungen des Internetbrowsers, Untersuchung des Zugriffs auf den App-Store, Inspektion der installierten Apps, Untersuchung der eingebauten oder installierten Kindersicherung.

2) Die Liste aus Schritt 1 ist mit der Liste von [E.Info.ACM-4.PrivacyAsset] zu vergleichen und alle Datenschutzfunktionen oder personenbezogenen Informationen auf der Anlage zu markieren, die identifiziert/gefunden wurden und die nicht in [E.Info.ACM-4.PrivacyAsset] aufgeführt sind.

##### 6.1.4.4.5.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn alle vom Gerät verarbeiteten Datenschutzfunktionen und personenbezogenen Informationen von Kindern, auf die Dritte (ausgenommen die Kinder oder deren Eltern/Erziehungsberechtigte) zugreifen können, in [E.Info.ACM-4.PrivacyAsset] dokumentiert sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn vom Gerät verarbeitete Datenschutzfunktionen und personenbezogene Informationen von Kindern entdeckt wurden, auf die Dritte (ausgenommen die Kinder oder deren Eltern/Erziehungsberechtigte) zugreifen können, die nicht in [E.Info.ACM-4.PrivacyAsset] dokumentiert sind.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

#### 6.1.4.4.6 Beurteilung der funktionalen Suffizienz

##### 6.1.4.4.6.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob die Zugangssteuerungsmechanismen standardmäßig sicherstellen, dass der Zugang anderer „dritter" Entitäten zu den vom Gerät verarbeiteten Datenschutzfunktionen und personenbezogenen Informationen von Kindern auf den für den Betrieb der Anlage erforderlichen Zugang beschränkt ist.

##### 6.1.4.4.6.2 Beurteilungseinheiten

[AU.ACM-4.RBAC]: Wenn die in [E.Info.ACM-4.ACM] dokumentierten Zugangssteuerungsmechanismen zu [IC.ACM-4.RBAC] gehören, ist funktional zu bestätigen, dass

— Dritten von anderen Entitäten entsprechende Rollen zugewiesen werden, die den Zugang zu den vom Gerät verarbeiteten Datenschutzfunktionen und personenbezogenen Informationen der Kinder auf das für den Betrieb der Anlage erforderliche Maß beschränken; und

— die wenigsten Privilegien mit der Rolle Dritter bei anderen Entitäten verbunden sind; und

— Rollenänderungen nur von autorisierten Benutzern vorgenommen werden können.

[AU.ACM-4.DAC]: Wenn die in [E.Info.ACM-4.ACM] dokumentierten Zugangssteuerungsmechanismen zu [IC.ACM-4.DAC] gehören, ist funktional zu bestätigen, dass

— Dritten von anderen Entitäten zugehörige Identitäten zugewiesen werden, die den Zugang zu den vom Gerät verarbeiteten Datenschutzfunktionen und personenbezogenen Informationen der Kinder auf das für den Betrieb der Anlage erforderliche Maß beschränken; und

— die wenigsten Privilegien mit der Identität Dritter bei anderen Entitäten verbunden sind; und

— Identitätsänderungen nur von autorisierten Benutzern vorgenommen werden können.

[AU.ACM-4.MAC]: Wenn die in [E.Info.ACM-4.ACM] dokumentierten Zugangssteuerungsmechanismen zu [IC.ACM-4.MAC] gehören, ist funktional zu bestätigen, dass

— Dritte anderer Entitäten, die auf die Datenschutzfunktion der Kinder und die von den Datenschutzwerten der Anlage verarbeiteten personenbezogenen Informationen zugreifen möchten, nur dann eine Freigabe durch das Betriebssystem und/oder den Systemadministrator erhalten, wenn dies für den Betrieb der Anlage erforderlich ist; und

— die Erteilung der Freigabe mit dem „Least-Privilege-Prinzip" verbunden ist; und

— der Wechsel des Betriebssystem- und/oder des Systemadministrators, der für die Freigabe des Benutzers zuständig ist, nur vom autorisierten Systemadministrator vorgenommen werden kann.

[AU.ACM-4.Generic]: Wenn die in [E.Info.ACM-4.ACM] dokumentierten Zugangssteuerungsmechanismen zu [IC.ACM-4.Generic] gehören, ist funktional zu bestätigen, dass

— Dritte von anderen Entitäten nur dann auf die Datenschutzfunktion der Kinder und auf die von den Datenschutzwerten der Anlage verarbeiteten personenbezogenen Informationen zugreifen dürfen, wenn dies für den Betrieb der Anlage erforderlich ist; und

— das „Least-Privilege-Prinzip" für Dritte anderer Entitäten befolgt wird; und

— die Änderung von Einstellungen, die sich auf den Zugangssteuerungsmechanismus beziehen, oder die Änderung von Privilegien Dritter anderer Entitäten nur von autorisierten Benutzern vorgenommen werden dürfen.

#### 6.1.4.4.6.3 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn für jeden in [E.Info.ACM-4.ACM] dokumentierten Zugangssteuerungsmechanismus die Bestätigungen in der von der Umsetzungskategorie abhängigen Beurteilungseinheit erfolgreich sind.

Die Entscheidung NICHT BESTANDEN für den Beurteilungsfall wird zugewiesen, wenn für einen in [E.Info.ACM-4.ACM] dokumentierten Zugangssteuerungsmechanismus eine Bestätigung in der von der Umsetzungskategorie abhängigen Beurteilungseinheit nicht erfolgreich ist.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

### 6.1.5 [ACM-5] Zugangssteuerung durch Eltern/Erziehungsberechtigte für Kinder bei Spielzeugen

#### 6.1.5.1 Anforderung

Wenn die Anlage ein Spielzeug ist, muss für jeden Sicherheits- und Datenschutzwert, der für Kinder zugänglich ist, jeder nach ACM-1 erforderliche Zugangssteuerungsmechanismus, der den Zugang von Kindern verwaltet, durch eine autorisierte Entität konfigurierbar sein, um den Zugang von Kindern zu den geschützten Sicherheits- und Datenschutzwerten einzuschränken.

#### 6.1.5.2 Begründung

Berücksichtigt man das Schutzbedürfnis und die sich entwickelnden Fähigkeiten von Kindern, insbesondere bei der Beurteilung der Auswirkungen der Datenschutz- und Sicherheitskonfiguration, dann ist es erforderlich, dass Eltern oder Erziehungsberechtigte den möglichen Zugang zu den Sicherheits- und Datenschutzwerten ihrer Kinder einschränken können, um Gefahren für deren Privatsphäre abzuwehren.

#### 6.1.5.3 Leitlinie

Die Anforderung verlangt, dass der Zugang von Kindern zu Sicherheits- und Datenschutzwerten durch autorisierte Entitäten eingeschränkt werden kann; dies sind üblicherweise die Eltern oder Erziehungsberechtigten des Kindes.

Wenn beispielsweise die Fähigkeit zur Kopplung eines Spielzeugs mit einem Mobiltelefon über eine drahtlose Nahbereichsschnittstelle durch einen Elternteil/Erziehungsberechtigten kontrolliert werden kann, dann können diese verhindern, dass Kinder eine Kopplung mit böswilliger Absicht initiieren. Allerdings könnten Eltern/Erziehungsberechtigte einem Kind die Erlaubnis geben, eine Kopplung mit einem Mobiltelefon zu initiieren.

Es ist wichtig, dass die Zugangssteuerungskonfiguration durch Eltern/Erziehungsberechtigte einfach durchzuführen ist.

#### 6.1.5.4 Beurteilungskriterien

##### 6.1.5.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung ACM-5.

##### 6.1.5.4.2 Umsetzungskategorien

[IC.ACM-5.RBAC]: Die Methoden zur Validierung, ob die in [E.Info.ACM-5.ACM] dokumentierten Zugangssteuerungsmechanismen standardmäßig ausschließlich auf einer rollenbasierten Zugangssteuerung beruhen und von einer autorisierten Entität konfigurierbar sind, um den Zugriff von Kindern auf die für Kinder zugänglichen Sicherheitswerte und Datenschutzwerte zu beschränken.

[IC.ACM-5.DAC]: Die Methoden zur Validierung, ob die in [E.Info.ACM-5.ACM] dokumentierten Zugangssteuerungsmechanismen standardmäßig ausschließlich auf einer benutzerbestimmbaren Zugangssteuerung

beruhen und von einer autorisierten Entität konfigurierbar sind, um den Zugriff von Kindern auf die für Kinder zugänglichen Sicherheitswerte und Datenschutzwerte zu beschränken.

[IC.ACM-5.MAC]: Die Methoden zur Validierung, ob die in [E.Info.ACM-5.ACM] dokumentierten Zugangssteuerungsmechanismen standardmäßig ausschließlich auf einer systembestimmten Zugangssteuerung beruhen und von einer autorisierten Entität konfigurierbar sind, um den Zugriff von Kindern auf die für Kinder zugänglichen Sicherheitswerte und Datenschutzwerte zu beschränken.

[IC.ACM-5.Generic]: Die Methoden zur Validierung, ob die in [E.Info.ACM-5.ACM] dokumentierten Zugangssteuerungsmechanismen standardmäßig nicht ausschließlich auf einer der in ACM-5-RBAC, ACM-5-DAC oder ACM-5-MAC beschriebenen Methoden beruhen und von einer autorisierten Entität konfigurierbar sind, um den Zugriff von Kindern auf die für Kinder zugänglichen Sicherheitswerte und Datenschutzwerte zu beschränken.

#### 6.1.5.4.3 Erforderliche Informationen

[E.Info.ACM-5.SecurityAsset]: Beschreibung aller Sicherheitswerte, die für Kinder zugänglich sind.

[E.Info.ACM-5.PrivacyAsset]: Beschreibung aller Datenschutzwerte, die für Kinder zugänglich sind.

[E.Info.ACM-5.ACM]: Beschreibung aller Zugangssteuerungsmechanismen, die nach ACM-1 erforderlich sind und den Zugang von Kindern zu jedem in [E.Info.ACM-5.SecurityAsset] dokumentierten Sicherheitswert und jedem in [E.Info.ACM-5.PrivacyAsset] dokumentierten Datenschutzwert, der vom Gerät verarbeitet wird, verwalten, einschließlich:

— Beschreibung, wie eine Entität autorisiert ist, um den Zugang von Kindern zu den geschützten Sicherheits- und Datenschutzwerten einzuschränken; und

— Beschreibung, wie diese Beschränkungen implementiert werden.

[E.Info.DT.ACM-5]: Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 5 für jeden Sicherheitswert und Datenschutzwert, bei denen der Zugang von Kindern durch in [E.Info.ACM-5.ACM] dokumentierten Zugangssteuerungsmechanismen verwaltet wird.

[E.Just.DT.ACM-5]: Begründung für jeden gewählten Pfad durch den in [E.Info.DT.ACM-5] dokumentierten Entscheidungsbaum mit der folgenden Eigenschaft:

— die Begründung für die Entscheidung [DT.ACM-5.DN-2] basiert auf [E.Info.ACM-5.ACM].

#### 6.1.5.4.4 Konzeptuelle Beurteilung

##### 6.1.5.4.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob die Zugangssteuerungsmechanismen, die den Zugang von Kindern verwalten, durch eine autorisierte Entität konfigurierbar sind, um den Zugang von Kindern zu den verwalteten Sicherheitswerten und Datenschutzwerten einzuschränken.

##### 6.1.5.4.4.2 Voraussetzungen

Keine.

#### 6.1.5.4.4.3 Beurteilungseinheiten

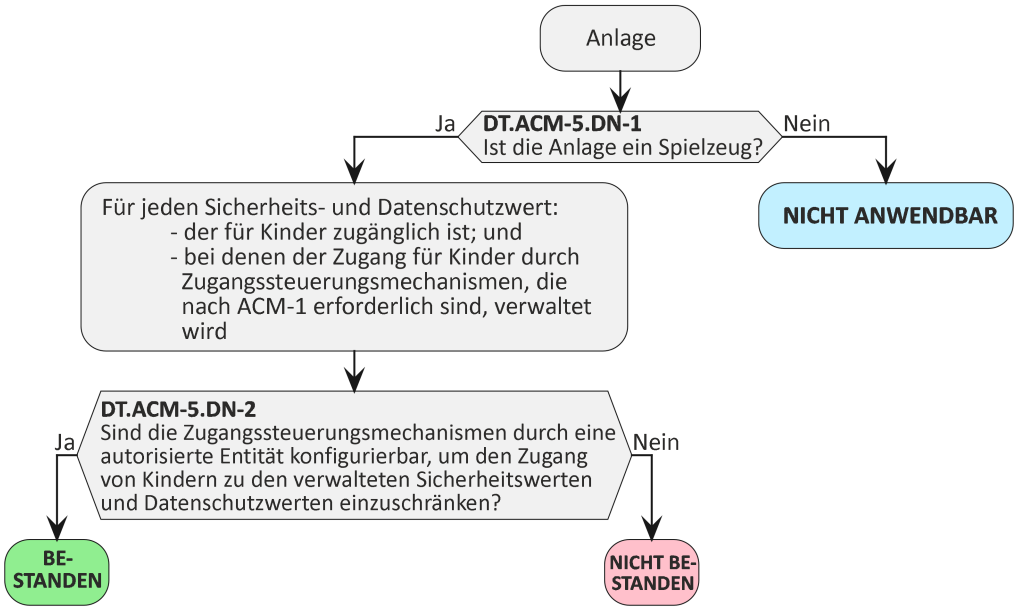



**Bild 5 — Entscheidungsbaum für Anforderung ACM-5**

Für jeden Sicherheitswert und Datenschutzwert, auf den wie in [E.Info.ACM-5.SecurityAsset] und [E.Info.ACM-5.PrivacyAsset] dokumentiert durch Kinder zugegriffen werden kann und bei dem der Zugang durch Zugangssteuerungsmechanismen entsprechend [E.Info.ACM-5.ACM] verwaltet wird, ist zu prüfen, ob der Pfad durch den in [E.Info.DT.ACM-5] dokumentierten Entscheidungsbaum mit „NICHT ANWENDBAR“ oder „BESTANDEN“ endet.

Für jeden in [E.Info.DT.ACM-5] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.ACM-5] dokumentierte Begründung zu untersuchen.

#### 6.1.5.4.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— mindestens ein Pfad durch den in [E.Info.DT.ACM-5] dokumentierten Entscheidungsbaum mit „BESTANDEN“ endet; und

— kein Pfad durch den in [E.Info.DT.ACM-5] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; und

— die in [E.Just.DT.ACM-5] angegebenen Informationen korrekte Begründungen für alle Pfade durch den in [E.Info.DT.ACM-5] dokumentierten Entscheidungsbaum sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— ein Pfad durch den in [E.Info.DT.ACM-5] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; oder

— eine in [E.Just.DT.ACM-5] angegebene Begründung für einen Pfad durch den in [E.Info.DT.ACM-5] dokumentierten Entscheidungsbaum nicht korrekt ist oder fehlt.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

#### 6.1.5.4.5 Beurteilung der funktionalen Vollständigkeit

##### 6.1.5.4.5.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob die Dokumentation der für Kinder zugänglichen Sicherheitswerte und Datenschutzwerte vollständig ist.

##### 6.1.5.4.5.2 Voraussetzungen

Die Anlage befindet sich im Betriebszustand.

##### 6.1.5.4.5.3 Beurteilungseinheiten

Es ist funktional zu beurteilen, ob für Kinder zugängliche Sicherheitswerte existieren, die nicht in [E.Info.ACM-5.SecurityAsset] dokumentiert sind, und ob für Kinder zugängliche Datenschutzwerte existieren, die nicht in [E.Info.ACM-5.PrivacyAsset] dokumentiert sind, indem die folgenden Schritte durchgeführt werden:

1) Alle Sicherheitswerte und Datenschutzwerte sind aufzuführen, die für Kinder zugänglich sind, z. B. durch Untersuchung der installierten Apps, Prüfung der Internet- und Browsereinstellungen, Inspektion des App-Store-Zugangs, Analyse der Kindersicherungseinstellungen, Beurteilung der gemeinsamen Nutzung und Speicherung von Daten.

2) Die Liste aus Schritt 1 ist mit der Liste von [E.Info.ACM-5.SecurityAsset] und [E.Info.ACM-5.PrivacyAsset] zu vergleichen und alle Sicherheitswerte oder Datenschutzwerte auf der Anlage sind zu markieren, die identifiziert/gefunden wurden und die weder in [E.Info.ACM-5.PrivacyAsset] noch in [E.Info.ACM-5.SecurityAsset] aufgeführt sind.

##### 6.1.5.4.5.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn alle gefundenen, für Kinder zugänglichen Sicherheitswerte in [E.Info.ACM-5.SecurityAsset] dokumentiert sind und alle gefundenen, für Kinder zugänglichen Datenschutzwerte in [E.Info.ACM-5.PrivacyAsset] dokumentiert sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn gefundene, für Kinder zugängliche Sicherheitswerte nicht in [E.Info.ACM-5.SecurityAsset] dokumentiert sind oder wenn gefundene, für Kinder zugängliche Datenschutzwerte nicht in [E.Info.ACM-5.PrivacyAsset] dokumentiert sind.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

#### 6.1.5.4.6 Beurteilung der funktionalen Suffizienz

##### 6.1.5.4.6.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob Sicherheitswerte und Datenschutzwerte, die für Kinder zugänglich sind und bei denen der Zugang der Kinder durch Zugangssteuerungsmechanismen verwaltet wird, durch eine autorisierte Entität konfigurierbar sind, um den Zugang der Kinder einzuschränken.

##### 6.1.5.4.6.2 Beurteilungseinheiten

[AU.ACM-5.RBAC]: Wenn die in [E.Info.ACM-5.ACM] dokumentierten Zugangssteuerungsmechanismen zu [IC.ACM-5.RBAC] gehören, ist funktional zu bestätigen, dass

— alle Benutzer den entsprechenden Rollen zugewiesen sind; und

— die wenigsten Privilegien mit den Rollen der Benutzer verbunden sind, so dass nur eine autorisierte Entität in der Lage ist, die rollenbasierten Zugangssteuerungsmechanismen zu konfigurieren, um den

Zugang von Kindern zu den verwalteten Sicherheitswerten und Datenschutzwerten zu beschränken, wie in [E.Just.DT.ACM-5] begründet; und

— Rollenänderungen nur von autorisierten Benutzern vorgenommen werden können.

[AU.ACM-5.DAC]: Wenn die in [E.Info.ACM-5.ACM] dokumentierten Zugangssteuerungsmechanismen zu [IC.ACM-5.DAC] gehören, ist funktional zu bestätigen, dass

— alle Benutzer den entsprechenden Identitäten zugewiesen sind; und

— die wenigsten Privilegien mit den Identitäten der Benutzer verbunden sind, so dass nur eine autorisierte Entität in der Lage ist, die benutzerbestimmbaren Zugangssteuerungsmechanismen zu konfigurieren, um den Zugang von Kindern zu den verwalteten Sicherheitswerten und Datenschutzwerten zu beschränken, wie in [E.Just.DT.ACM-5] begründet; und

— Identitätsänderungen nur von autorisierten Benutzern vorgenommen werden können.

[AU.ACM-5.MAC]: Wenn die in [E.Info.ACM-5.ACM] dokumentierten Zugangssteuerungsmechanismen zu [IC.ACM-5.MAC] gehören, ist funktional zu bestätigen, dass

— allen Benutzern vom Betriebssystem- und/oder Systemadministrator nur dann die Freigabe erteilt wird, die systembestimmte Zugangssteuerung zu konfigurieren, um den Zugang von Kindern zu den verwalteten Sicherheitswerten und Datenschutzwerten zu beschränken, wie in [E.Just.DT.ACM-5] begründet, wenn dieser Benutzer ein autorisierter Benutzer ist; und

— die Erteilung der Freigabe mit dem „Least-Privilege-Prinzip“ verbunden ist; und

— der Wechsel des Betriebssystem- und/oder des Systemadministrators, der für die Freigabe des Benutzers zuständig ist, nur vom autorisierten Systemadministrator vorgenommen werden kann.

[AU.ACM-5.Generic]: Wenn die in [E.Info.ACM-4.ACM] dokumentierten Zugangssteuerungsmechanismen zu [IC.ACM-4.RBAC] gehören, ist funktional zu bestätigen, dass

— Benutzer nur dann Zugangssteuerungsmechanismen konfigurieren dürfen, um den Zugang von Kindern zu den verwalteten Sicherheitswerten und Datenschutzwerten zu beschränken, wenn dieser Benutzer ein autorisierter Benutzer ist; und

— das „Least-Privilege-Prinzip“ für alle Benutzer befolgt wird; und

— die Änderung von Einstellungen, die sich auf den Zugangssteuerungsmechanismus beziehen, oder die Änderung von Privilegien der Benutzer nur von autorisierten Benutzern vorgenommen werden dürfen.

#### 6.1.5.4.6.3 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn für jeden in [E.Info.ACM-5.ACM] dokumentierten Zugangssteuerungsmechanismus die Bestätigungen in der von der Umsetzungskategorie abhängigen Beurteilungseinheit erfolgreich sind.

Die Entscheidung NICHT BESTANDEN für den Beurteilungsfall wird zugewiesen, wenn für einen in [E.Info.ACM-5.ACM] dokumentierten Zugangssteuerungsmechanismus eine Bestätigung in der von der Umsetzungskategorie abhängigen Beurteilungseinheit nicht erfolgreich ist.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

### 6.1.6 [ACM-6] Zugangssteuerung durch Eltern/Erziehungsberechtigte für den Zugang anderer Entitäten auf die verwalteten Datenschutzwerte von Kindern bei Spielzeugen

#### 6.1.6.1 Anforderung

Wenn die Anlage ein Spielzeug ist, muss für jeden Datenschutzwert von Kindern, der für andere Entitäten als die Kinder oder deren Eltern oder Erziehungsberechtigte zugänglich ist und bei dem der Zugang dieser anderen Entitäten über einen nach ACM-1 erforderlichen Zugangssteuerungsmechanismus verwaltet wird, der Zugangssteuerungsmechanismus durch eine autorisierte Entität konfigurierbar sein, um den Zugang anderer Entitäten zu den verwalteten Datenschutzwerten der Kinder einzuschränken.

#### 6.1.6.2 Begründung

Berücksichtigt man das Schutzbedürfnis und die sich entwickelnden Fähigkeiten von Kindern, dann ist es erforderlich, dass Eltern oder Erziehungsberechtigte den Zugang von Entitäten zu den Datenschutzwerten der Kinder einschränken können, um Gefahren für deren Privatsphäre abzuwehren.

#### 6.1.6.3 Leitlinie

Die Anforderung verlangt, dass der Zugang von Entitäten zu Datenschutzwerten von Kindern durch autorisierte Entitäten eingeschränkt werden kann; dies sind üblicherweise die Eltern oder Erziehungsberechtigten des Kindes.

Beispielsweise können Eltern/Erziehungsberechtigte den Zugang Dritter und anderer, potentiell böswilliger Akteure einschränken, die einen Fernzugriff auf die Funktionalität der Anlage zum Zweck der Überwachung, Fernkommunikation oder -kontrolle und anderer, entsprechender Gefährdungen für Kinder durchführen könnten.

Es ist wichtig, dass die Zugangssteuerungskonfiguration durch Erziehungsberechtigte einfach durchzuführen ist.

#### 6.1.6.4 Beurteilungskriterien

##### 6.1.6.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung ACM-6.

##### 6.1.6.4.2 Umsetzungskategorien

[IC.ACM-6.RBAC]: Die Methoden zur Validierung, ob die in [E.Info.ACM-6.ACM] dokumentierten Zugangssteuerungsmechanismen standardmäßig ausschließlich auf einer rollenbasierten Zugangssteuerung beruhen und ob diese zugrundeliegende Zugangssteuerung, die den Zugang zu den Datenschutzwerten von Kindern verwaltet, auf die andere Entitäten als die Kinder oder ihre Eltern oder Erziehungsberechtigten zugreifen können, von einer autorisierten Entität konfigurierbar ist.

[IC.ACM-6.DAC]: Die Methoden zur Validierung, ob die in [E.Info.ACM-6.ACM] dokumentierten Zugangssteuerungsmechanismen standardmäßig ausschließlich auf einer benutzerbestimmbaren Zugangssteuerung beruhen und ob diese zugrundeliegende Zugangssteuerung, die den Zugang zu den Datenschutzwerten von Kindern verwaltet, auf die andere Entitäten als die Kinder oder ihre Eltern oder Erziehungsberechtigten zugreifen können, von einer autorisierten Entität konfigurierbar ist.

[IC.ACM-6.MAC]: Die Methoden zur Validierung, ob die in [E.Info.ACM-6.ACM] dokumentierten Zugangssteuerungsmechanismen standardmäßig ausschließlich auf einer systembestimmten Zugangssteuerung beruhen und ob diese zugrundeliegende Zugangssteuerung, die den Zugang zu den Datenschutzwerten von Kindern verwaltet, auf die andere Entitäten als die Kinder oder ihre Eltern oder Erziehungsberechtigten zugreifen können, von einer autorisierten Entität konfigurierbar ist.

[IC.ACM-6.Generic]: Die Methoden zur Validierung, ob die in [E.Info.ACM-6.ACM] dokumentierten Zugangssteuerungsmechanismen standardmäßig nicht ausschließlich auf einer der in ACM-6-RBAC, ACM-6-DAC oder ACM-6-MAC beschriebenen Methoden beruhen und ob diese zugrundeliegende Zugangssteuerung, die den Zugang zu den Datenschutzwerten von Kindern verwaltet, auf die andere Entitäten als die Kinder oder ihre Eltern oder Erziehungsberechtigten zugreifen können, von einer autorisierten Entität konfigurierbar ist.

#### 6.1.6.4.3 Erforderliche Informationen

[E.Info.ACM-6.PrivacyAsset]: Beschreibung aller Datenschutzwerte von Kindern, auf die durch andere Entitäten als die Kinder oder deren Eltern oder Erziehungsberechtigte zugegriffen werden kann.

[E.Info.ACM-6.ACM]: Beschreibung jedes Zugangssteuerungsmechanismus, der nach ACM-1 erforderlich ist und den Zugang anderer Entitäten als der Kinder oder deren Eltern oder Erziehungsberechtigten zu den in [E.Info.ACM-6.PrivacyAsset] dokumentierten Datenschutzwerten von Kindern verwaltet, einschließlich:

— Beschreibung, wie Entitäten autorisiert sind, den Zugangssteuerungsmechanismus zu konfigurieren, um den Zugang anderer Entitäten zu den verwalteten Datenschutzwerten für Kinder zu beschränken; und

— Beschreibung, wie die Beschränkungen des Zugangs zu den verwalteten Datenschutzwerten für Kinder implementiert werden.

[E.Info.DT.ACM-6]: Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 6 für alle Datenschutzwerte von Kindern, die für andere Entitäten als die Kinder oder deren Eltern oder Erziehungsberechtigte, die in [E.Info.ACM-6.PrivacyAsset] dokumentiert sind, zugänglich sind und bei denen der Zugang der anderen Entitäten durch in [E.Info.ACM-6.ACM] dokumentierten Zugangssteuerungsmechanismen verwaltet wird.

[E.Just.DT.ACM-6]: Begründung für jeden gewählten Pfad durch den in [E.Info.DT.ACM-6] dokumentierten Entscheidungsbaum mit der folgenden Eigenschaft:

— die Begründung für die Entscheidung [DT.ACM-6.DN-2] basiert auf [E.Info.ACM-6.ACM].

#### 6.1.6.4.4 Konzeptuelle Beurteilung

##### 6.1.6.4.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob die Zugangssteuerungsmechanismen durch eine autorisierte Entität konfigurierbar sind, um den Zugang von anderen Entitäten zu den verwalteten Datenschutzwerten von Kindern einzuschränken.

##### 6.1.6.4.4.2 Voraussetzungen

Keine.

#### 6.1.6.4.4.3 Beurteilungseinheiten

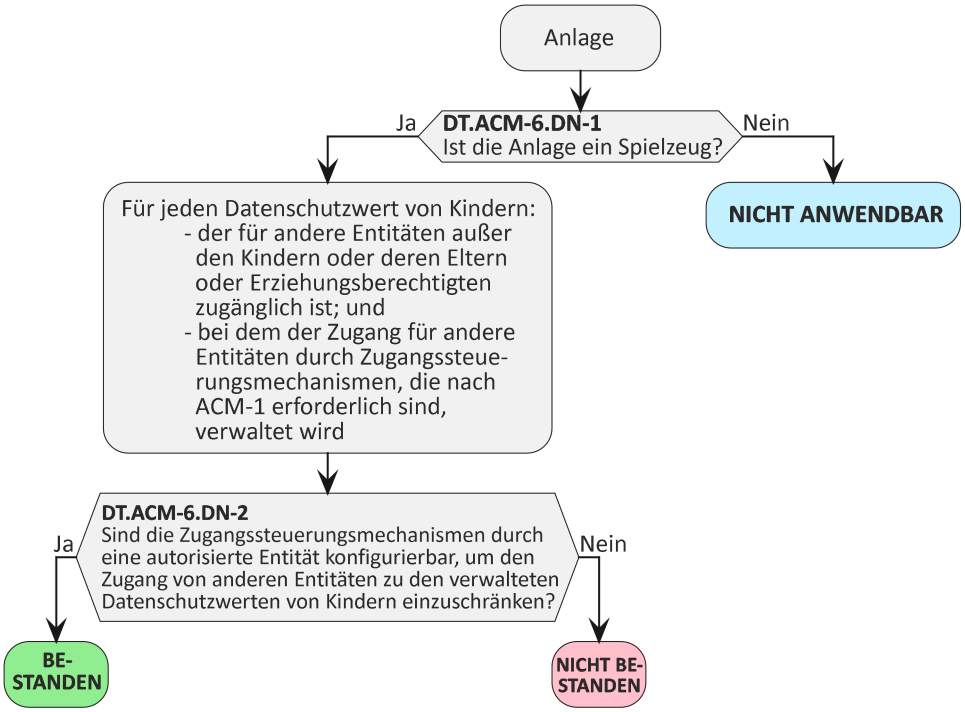



**Bild 6 — Entscheidungsbaum für Anforderung ACM-6**

Für alle in [E.Info.ACM-6.PrivacyAsset] dokumentierten Datenschutzwerte von Kindern, auf die andere Entitäten außer den Kindern oder deren Eltern oder Erziehungsberechtigten zugreifen können und bei denen der Zugang der anderen Entitäten durch Zugangssteuerungsmechanismen entsprechend [E.Info.ACM-6.ACM] verwaltet wird, ist zu prüfen, ob der Pfad durch den in [E.Info.DT.ACM-6] dokumentierten Entscheidungsbaum mit „NICHT ANWENDBAR“ oder „BESTANDEN“ endet.

Für jeden in [E.Info.DT.ACM-6] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.ACM-6] dokumentierte Begründung zu untersuchen.

#### 6.1.6.4.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— mindestens ein Pfad durch den in [E.Info.DT.ACM-6] dokumentierten Entscheidungsbaum mit „BESTANDEN“ endet; und

— kein Pfad durch den in [E.Info.DT.ACM-6] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; und

— die in [E.Just.DT.ACM-6] angegebenen Informationen korrekte Begründungen für alle Pfade durch den in [E.Info.DT.ACM-6] dokumentierten Entscheidungsbaum sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— ein Pfad durch den in [E.Info.DT.ACM-6] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; oder

— eine in [E.Just.DT.ACM-6] angegebene Begründung für einen Pfad durch den in [E.Info.DT.ACM-6] dokumentierten Entscheidungsbaum nicht korrekt ist oder fehlt.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

#### 6.1.6.4.5 Beurteilung der funktionalen Vollständigkeit

##### 6.1.6.4.5.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob die Dokumentation der in [E.Info.ACM-6.PrivacyAsset] dokumentierten Datenschutzwerte von Kindern, die für andere Entitäten als die Kinder oder deren Eltern oder Erziehungsberechtigte zugänglich sind, vollständig ist.

##### 6.1.6.4.5.2 Voraussetzungen

Die Anlage befindet sich im Betriebszustand.

##### 6.1.6.4.5.3 Beurteilungseinheiten

Es ist funktional zu beurteilen, ob es Datenschutzwerte von Kindern gibt, die für Dritte außer den Kindern oder deren Eltern oder Erziehungsberechtigten zugänglich sind und die nicht in [E.Info.ACM-6.PrivacyAsset] dokumentiert sind, indem die folgenden Schritte durchgeführt werden:

1) Alle Datenschutzwerte sind aufzuführen, auf die andere Entitäten als die Kinder oder ihre Eltern oder Erziehungsberechtigten zugreifen können, z. B. durch Untersuchung der App-Berechtigungen und ihrer Bedingungen und Datenschutzrichtlinien, Überprüfung der Netzwerk- und Internetverbindungen, Inspektion der Anlageneinstellungen, Überprüfung des Browserverlaufs und der Einstellungen, Prüfung potentieller Datenzugriffspunkte wie Fotobibliotheken, Standortprotokolle, Kommunikations- und Social-Media-Apps.

2) Die Liste aus Schritt 1 ist mit der Liste von [E.Info.ACM-6.PrivacyAsset] zu vergleichen und alle Datenschutzwerte auf der Anlage zu markieren, die identifiziert/gefunden wurden und die nicht in [E.Info.ACM-6.PrivacyAsset] aufgeführt sind.

##### 6.1.6.4.5.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn alle entdeckten Datenschutzwerte von Kindern, auf die von Dritten außer den Kindern oder deren Eltern oder Erziehungsberechtigten zugegriffen werden kann, in [E.Info.ACM-6.PrivacyAsset] dokumentiert sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn ein entdeckter Datenschutzwert von Kindern, auf den von Dritten außer den Kindern oder deren Eltern oder Erziehungsberechtigten zugegriffen werden kann, nicht in [E.Info.ACM-6.PrivacyAsset] dokumentiert ist.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

#### 6.1.6.4.6 Beurteilung der funktionalen Suffizienz

##### 6.1.6.4.6.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob Datenschutzwerte von Kindern, die für andere Entitäten außer den Kindern oder deren Eltern oder Erziehungsberechtigten zugänglich sind, durch Zugangssteuerungsmechanismen verwaltet werden, die durch eine autorisierte Entität konfigurierbar sind, um den Zugang der anderen Entitäten einzuschränken.

##### 6.1.6.4.6.2 Beurteilungseinheiten

[AU.ACM-6.RBAC]: Wenn die in [E.Info.ACM-6.ACM] dokumentierten Zugangssteuerungsmechanismen zu [IC.ACM-6.RBAC] gehören, ist funktional zu bestätigen, dass

— alle Benutzer den entsprechenden Rollen zugewiesen sind; und

— die geringsten Privilegien mit den Rollen der Benutzer verbunden sind, so dass nur eine autorisierte Entität in der Lage ist, die rollenbasierten Zugangssteuerungsmechanismen zu konfigurieren, um den Zugang der anderen Entitäten zu den verwalteten Datenschutzwerten von Kindern zu beschränken, wie in [E.Just.DT.ACM-6] begründet; und

— Rollenänderungen nur von autorisierten Benutzern vorgenommen werden können.

[AU.ACM-6.DAC]: Wenn die in [E.Info.ACM-6.ACM] dokumentierten Zugangssteuerungsmechanismen zu [IC.ACM-6.DAC] gehören, ist funktional zu bestätigen, dass

— alle Benutzer den entsprechenden Identitäten zugewiesen sind; und

— das Minimum an Zugriffsrechten mit den Identitäten der Benutzer verbunden ist, so dass nur eine autorisierte Entität in der Lage ist, die benutzerbestimmbaren Zugangssteuerungsmechanismen zu konfigurieren, um den Zugang der anderen Entitäten zu den verwalteten Datenschutzwerten von Kindern zu beschränken, wie in [E.Just.DT.ACM-6] begründet; und

— Identitätsänderungen nur von autorisierten Benutzern vorgenommen werden können.

[AU.ACM-6.MAC]: Wenn die in [E.Info.ACM-6.ACM] dokumentierten Zugangssteuerungsmechanismen zu [IC.ACM-6.MAC] gehören, ist funktional zu bestätigen, dass

— Benutzern vom Betriebssystem- und/oder Systemadministrator nur dann die Freigabe erteilt wird, die systembestimmte Zugangssteuerung zu konfigurieren, um den Zugang anderer Entitäten zu den verwalteten Sicherheitswerten und Datenschutzwerten von Kindern zu beschränken, wie in [E.Just.DT.ACM-6] begründet, wenn dieser Benutzer ein autorisierter Benutzer ist; und

— die Erteilung der Freigabe mit dem „Least-Privilege-Prinzip“ verbunden ist; und

— der Wechsel des Betriebssystem- und/oder des Systemadministrators, der für die Freigabe des Benutzers zuständig ist, nur vom autorisierten Systemadministrator vorgenommen werden kann.

[AU.ACM-6.Generic]: Wenn die in [E.Info.ACM-6.ACM] dokumentierten Zugangssteuerungsmechanismen zu [IC.ACM-6.Generic] gehören, ist funktional zu bestätigen, dass

— Benutzer nur dann Zugangssteuerungsmechanismen konfigurieren dürfen, um den Zugang anderer Entitäten zu den verwalteten Sicherheitswerten und Datenschutzwerten von Kindern zu beschränken, wenn dieser Benutzer ein autorisierter Benutzer ist; und

— das „Least-Privilege-Prinzip“ für alle Benutzer befolgt wird; und

— die Änderung von Einstellungen, die sich auf den Zugangssteuerungsmechanismus beziehen, oder die Änderung von Privilegien der Benutzer nur von autorisierten Benutzern vorgenommen werden dürfen.

#### 6.1.6.4.6.3 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn für jeden in [E.Info.ACM-6.ACM] dokumentierten Zugangssteuerungsmechanismus die Bestätigungen in der von der Umsetzungskategorie abhängigen Beurteilungseinheit erfolgreich sind.

Die Entscheidung NICHT BESTANDEN für den Beurteilungsfall wird zugewiesen, wenn für einen in [E.Info.ACM-6.ACM] dokumentierten Zugangssteuerungsmechanismus eine Bestätigung in der von der Umsetzungskategorie abhängigen Beurteilungseinheit nicht erfolgreich ist.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

## 6.2 [AUM] Authentisierungsmechanismus (en: Authentication Mechanism)

### 6.2.1 [AUM-1] Anwendbarkeit von Authentisierungsmechanismen

#### 6.2.1.1 [AUM-1-1] Anforderung Netzwerkschnittstelle

Die nach ACM-1 erforderlichen Zugangssteuerungsmechanismen müssen Authentisierungsmechanismen für die Verwaltung des Zugangs von Entitäten über Netzwerkschnittstellen verwenden, die Folgendes ermöglichen:

— vertrauliche personenbezogene Daten, die Konfiguration vertraulicher Datenschutzfunktionen oder vertrauliche Sicherheitsparameter zu lesen; oder

— die Konfiguration sensibler personenbezogener Daten, sensibler Datenschutzfunktionen oder sensibler Sicherheitsparameter zu ändern; oder

— Datenschutzfunktionen oder Sicherheitsfunktionen zu verwenden,

außer für den Zugang:

— zu personenbezogenen Daten, Datenschutzfunktionen oder die Konfiguration von Datenschutzfunktionen, wenn die fehlende Authentisierung für die vorgesehene Anlagenfunktionalität erforderlich ist; oder

— über Netzwerke, bei denen physische oder logische Maßnahmen in der Zielbetriebsumgebung der Anlage den Zugang für autorisierte Entitäten einschränken.

#### 6.2.1.2 [AUM-1-2] Anforderung Benutzungsschnittstelle

Die nach ACM-1 erforderlichen Zugangssteuerungsmechanismen müssen Authentisierungsmechanismen für die Verwaltung des Zugangs von Entitäten über Benutzungsschnittstellen verwenden, die Folgendes ermöglichen:

— vertrauliche personenbezogene Daten, die Konfiguration vertraulicher Datenschutzfunktionen oder vertrauliche Sicherheitsparameter zu lesen; oder

— die Konfiguration sensibler personenbezogener Daten, sensibler Datenschutzfunktionen oder sensibler Sicherheitsparameter zu ändern; oder

— Datenschutzfunktionen oder Sicherheitsfunktionen zu verwenden,

außer für den Zugang:

— wenn physische oder logische Maßnahmen in der Zielbetriebsumgebung der Anlage den Zugang für autorisierte Entitäten einschränken;

und mit Ausnahme des reinen Lesezugriffs auf personenbezogene Daten, Datenschutzfunktionen oder die Konfiguration von Datenschutzfunktionen, bei denen ein Zugriff ohne Authentisierung erforderlich ist:

— die vorgesehene Anlagenfunktionalität ermöglichen; oder

— weil rechtliche Implikationen keine Authentisierung zulassen.

#### 6.2.1.3 Begründung

Die Anlage muss einen Authentisierungsmechanismus bereitstellen, so dass der entsprechende Zugangssteuerungsmechanismus den unbefugten Zugang zu Sicherheits- und Datenschutzwerten, die für die Privatsphäre des Benutzers maßgeblich sind, von Entitäten verhindert, die nicht sind, wer oder was sie vorgeben zu sein.

#### 6.2.1.4 Leitlinie

Authentisierungsmechanismen können verschiedene Schichten (z. B. Anwendungs- oder Netzwerkschicht) verwenden, um die Gültigkeit der Angaben von Entitäten zu verifizieren. Die Verwaltung der zugehörigen Zugangsrechte für Entitäten wird durch Zugangssteuerungsmechanismen geregelt.

Es gibt verschiedene Arten von Entitäten, die mit der Anlage interagieren können, z. B.:

— eine spezifische Person, der Besitzer eines Benutzerkontos, ein Gerät oder ein Dienst; oder

— ein Mitglied einer spezifischen Gruppe, beispielsweise einer zum Zugang zu einer bestimmten Geräteressource autorisierten Gruppe; oder

— eine Entität, die durch eine andere Entität für den Zugang zu einer spezifischen Geräteressource autorisiert wurde.

Üblicherweise beruht die Verifizierung einer Entität auf der Untersuchung von Nachweisen eines oder mehrerer Elemente der folgenden Kategorien:

— Kenntnis (etwas, das man weiß); und

— Besitz (etwas, das man hat); und

— Inhärenz (etwas, das man ist).

Zur Authentisierung einer Entität kann das Vertrauensverhältnis zu einem Netzwerk genutzt werden (z. B. wenn die Entität ein gemeinsames Geheimnis besitzt, wie beispielsweise WLAN-Anmeldedaten).

Eine Authentisierung ist möglicherweise nicht bei allen Zugriffen auf Sicherheitswerte oder Datenschutzwerte erforderlich.

Beispiele für den Zugang, bei denen eine Authentisierung nicht zwingend erforderlich ist, sind unter anderem:

— das Lesen von Informationen, die eindeutig als öffentlich zugängliche Informationen im Zusammenhang mit der vorgesehenen Anlagenfunktionalität angegeben werden; oder

— Auslesen eines öffentlichen Schlüssels.

Beispiele für physische oder logische Maßnahmen in der angestrebten Umgebung, die das Vertrauen in die Richtigkeit der Angaben einer Entität stärken, könnten unter anderem sein:

— eine physische Zugangssteuerung, die nur den autorisierten Zugang zum Inneren von privaten Straßenfahrzeugen oder Wasserfahrzeugen erlaubt; oder

— physische Zugangssteuerung, die nur autorisierten Zugang z. B. zu einer WPS-Taste eines Home-Gateways erlaubt, um andere Geräte mit einem WLAN-Netzwerk innerhalb eines Privathauses zu verbinden.

#### 6.2.1.5 Beurteilungskriterium Netzwerkschnittstelle

##### 6.2.1.5.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung AUM-1-1.

##### 6.2.1.5.2 Umsetzungskategorien

Nicht anwendbar.

#### 6.2.1.5.3 Erforderliche Informationen

[E.Info.AUM-1-1.ACM]: Beschreibung jedes Zugangssteuerungsmechanismus, der nach ACM-1 für die Verwaltung des Zugangs von Entitäten zu Netzwerkschnittstellen erforderlich ist, die das Lesen vertraulicher personenbezogener Daten, der Konfiguration vertraulicher Datenschutzfunktionen bzw. vertraulicher Sicherheitsparameter oder die Änderung der Konfiguration sensibler Datenschutzfunktionen bzw. sensibler Sicherheitsparameter oder die Nutzung von Datenschutzfunktionen bzw. Sicherheitsfunktionen ermöglichen, einschließlich:

— [E.Info.AUM-1-1.ACM.NetworkInterface]: Beschreibung der Netzwerkschnittstellen für den verwalteten Zugang; und

— [E.Info.AUM-1-1.ACM.ManagedAccessPrivacyAsset]: Beschreibung des verwalteten Zugangs zu Datenschutzwerten über Netzwerkschnittstellen; und

— [E.Info.AUM-1-1.ACM.ManagedAccessSecurityAsset]: Beschreibung des verwalteten Zugangs zu Sicherheitswerten über Netzwerkschnittstellen; und

— (wenn die fehlende Authentisierung für den Zugang zu Datenschutzfunktionen oder die Konfiguration von Datenschutzfunktionen über Netzwerkschnittstellen für die vorgesehene Funktionalität der Anlage erforderlich ist) [E.Info.AUM-1-1.ACM.IntendedFunctionality]: Eine Beschreibung

  — der nicht authentisierten, zugänglichen Datenschutzfunktionen oder der Konfiguration der Datenschutzfunktionen; und

  — der vorgesehenen Funktionalität der Anlage; und

  — dessen Eigenschaften, die eine fehlende Authentisierung für den Zugang zu den Datenschutzfunktionen oder der Konfiguration der Datenschutzfunktionen erfordern, und

— (bei fehlender Authentisierung für den Zugang über Netzwerke, bei denen der Zugang auf autorisierte Entitäten beschränkt ist) [E.Info.AUM-1-1.ACM.AuthorizedEntities]: Beschreibung der Netzwerke und der physischen oder logischen Maßnahmen in der Zielbetriebsumgebung der Anlage, die den Zugang auf autorisierte Entitäten beschränken; und

— (wenn eine Authentifizierung nach AUM-1-1 erforderlich ist) [E.Info.AUM-1-1.ACM.AuthenticationMechanism]: Beschreibung der implementierten Authentisierungsmechanismen.

[E.Info.DT.AUM-1-1]: Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 7 für jeden in [E.Info.AUM-1-1.ACM] dokumentierten Zugangssteuerungsmechanismus.

[E.Just.DT.AUM-1-1]: Begründung für den gewählten Pfad durch den in [E.Info.DT.AUM-1-1] dokumentierten Entscheidungsbaum mit den folgenden Eigenschaften:

— (wenn eine Entscheidung aus [DT.AUM-1-1.DN-1] zu „NICHT ANWENDBAR“ führt) basiert die Begründung für die Entscheidung [DT.AUM-1-1.DN-1] auf [E.Info.AUM-1-1.ACM.IntendedFunctionality]; und

— (wenn eine Entscheidung aus [DT.AUM-1-1.DN-2] zu „NICHT ANWENDBAR“ führt) basiert die Begründung für die Entscheidung [DT.AUM-1-1.DN-2] auf [E.Info.ACM-1-1.ACM.AuthorizedEntities]; und

— die Begründung für die Entscheidung [DT.AUM-1-1.DN-3] basiert auf [E.Info.AUM-1-1.ACM].

#### 6.2.1.5.4 Konzeptuelle Beurteilung

##### 6.2.1.5.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob die Authentisierungsmechanismen implementiert werden, wo sie nach AUM-1-1 erforderlich sind.

#### 6.2.1.5.4.2 Voraussetzungen

Keine.

#### 6.2.1.5.4.3 Beurteilungseinheiten

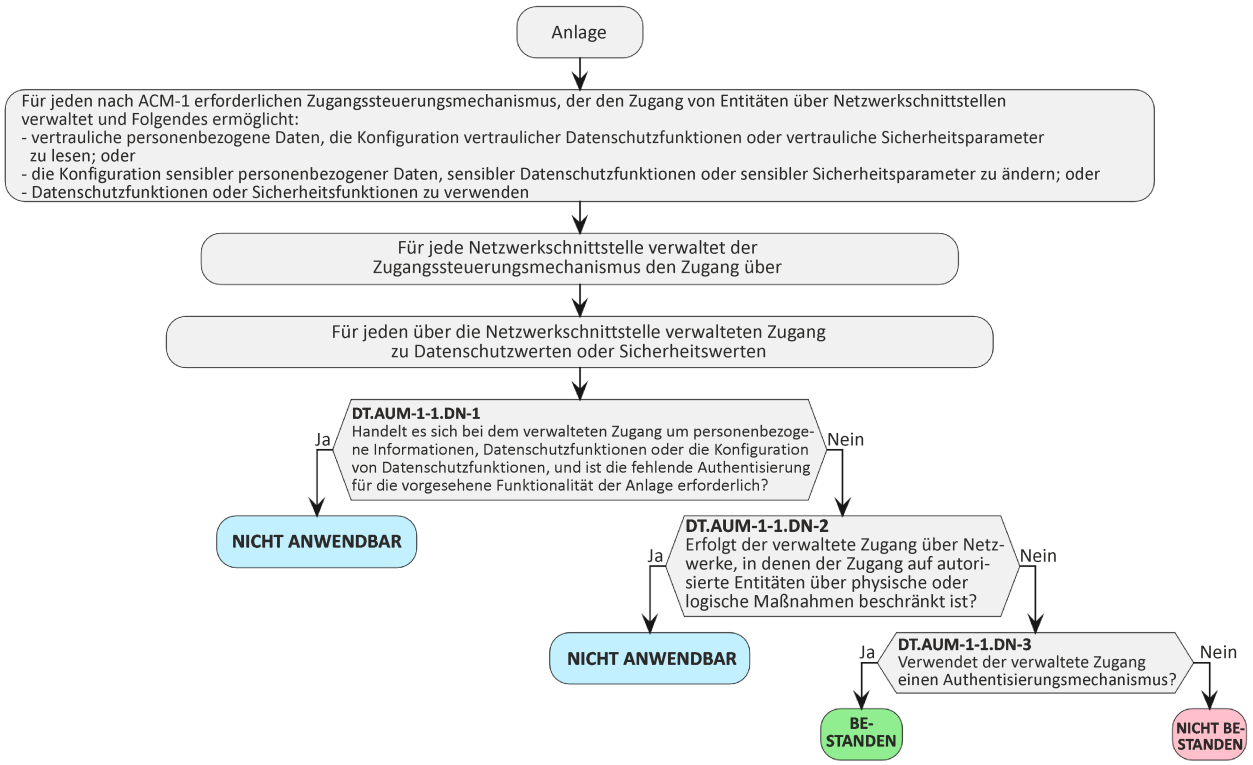



**Bild 7 — Entscheidungsbaum für Anforderung AUM-1-1**

Für jeden in [E.Info.AUM-1-1.ACM] dokumentierten Zugangssteuerungsmechanismus ist zu prüfen, ob der Pfad durch den in [E.Info.DT.AUM-1-1] dokumentierten Entscheidungsbaum mit „NICHT ANWENDBAR“ oder „BESTANDEN“ endet.

Für jeden in [E.Info.DT.AUM-1-1] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.AUM-1-1] dokumentierte Begründung zu untersuchen.

#### 6.2.1.5.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— mindestens ein Pfad durch den in [E.Info.DT.AUM-1-1] dokumentierten Entscheidungsbaum mit „BESTANDEN“ endet; und

— kein Pfad durch den in [E.Info.DT.AUM-1-1] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; und

— die in [E.Just.DT.AUM-1-1] angegebenen Informationen korrekte Begründungen für alle Pfade durch den in [E.Info.DT.AUM-1-1] dokumentierten Entscheidungsbaum sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— ein Pfad durch den in [E.Info.DT.AUM-1-1] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; oder

— eine in [E.Just.DT.AUM-1-1] angegebene Begründung für einen Pfad durch den in [E.Info.DT.AUM-1-1] dokumentierten Entscheidungsbaum nicht korrekt ist oder fehlt.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

#### 6.2.1.5.5 Beurteilung der funktionalen Vollständigkeit

##### 6.2.1.5.5.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob es Zugangssteuerungsmechanismen auf der Anlage für die Verwaltung des Zugangs von Entitäten über Netzwerkschnittstellen gibt, die das Lesen der Konfiguration vertraulicher Netzwerkfunktionen bzw. vertraulicher Sicherheitsparameter oder die Änderung der Konfiguration sensibler Netzwerkfunktionen bzw. sensibler Sicherheitsparameter oder die Nutzung von Netzwerkfunktionen bzw. Sicherheitsfunktionen ermöglichen, die nicht in [E.Info.AUM-1-1.ACM] beschrieben sind.

##### 6.2.1.5.5.2 Voraussetzungen

Die Anlage befindet sich im Betriebszustand.

##### 6.2.1.5.5.3 Beurteilungseinheiten

Es ist funktional zu beurteilen, ob es nach ACM-1 erforderliche Zugangssteuerungsmechanismen für die Verwaltung des Zugangs von Entitäten über Netzwerkschnittstellen gibt, die das Lesen vertraulicher personenbezogener Daten, die Konfiguration vertraulicher Datenschutzfunktionen bzw. vertraulicher Sicherheitsparameter oder die Änderung sensibler personenbezogener Informationen, die Konfiguration sensibler Datenschutzfunktionen bzw. sensibler Sicherheitsparameter oder die Nutzung von Datenschutzfunktionen bzw. Sicherheitsfunktionen ermöglichen, die nicht in [E.Info.AUM-1-1.ACM] beschrieben sind.

##### 6.2.1.5.5.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN für diesen Beurteilungsfall wird zugewiesen, wenn kein Nachweis vorliegt, dass ein nach ACM-1 erforderlicher Zugangssteuerungsmechanismus für die Verwaltung des Zugangs von Entitäten über Netzwerkschnittstellen, die das Lesen vertraulicher personenbezogener Daten, der Konfiguration vertraulicher Datenschutzfunktionen bzw. vertraulicher Sicherheitsparameter oder die Änderung der Konfiguration sensibler Datenschutzfunktionen bzw. sensibler Sicherheitsparameter oder die Nutzung von Datenschutzfunktionen bzw. Sicherheitsfunktionen ermöglichen, gefunden wird, der nicht in [E.Info.AUM-1-1.ACM] dokumentiert ist.

Die Entscheidung NICHT BESTANDEN für diesen Beurteilungsfall wird zugewiesen, wenn ein Nachweis vorliegt, dass ein nach ACM-1 erforderlicher Zugangssteuerungsmechanismus für die Verwaltung des Zugangs von Entitäten über Netzwerkschnittstellen, die das Lesen vertraulicher personenbezogener Daten, der Konfiguration vertraulicher Datenschutzfunktionen bzw. vertraulicher Sicherheitsparameter oder die Änderung der Konfiguration sensibler Datenschutzfunktionen bzw. sensibler Sicherheitsparameter oder die Nutzung von Netzwerkfunktionen bzw. Sicherheitsfunktionen ermöglichen, gefunden wird, der nicht in [E.Info.AUM-1-1.ACM] beschrieben ist.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

#### 6.2.1.5.6 Beurteilung der funktionalen Suffizienz

##### 6.2.1.5.6.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob die nach AUM-1-1 erforderlichen dokumentierten Authentisierungsmechanismen implementiert wurden.

#### 6.2.1.5.6.2 Voraussetzungen

Die Anlage befindet sich im Betriebszustand.

#### 6.2.1.5.6.3 Beurteilungseinheiten

Für jeden in [E.Info.AUM-1-1.ACM] dokumentierten Zugangssteuerungsmechanismus, jeden in [E.Info.AUM-1-1.ACM.ManagedAccessPrivacyAsset] dokumentierten verwalteten Zugang über Netzwerkschnittstellen zu Datenschutzwerten und jeden in [E.Info.AUM-1-1.ACM.ManagedAccessSecurityAsset] dokumentierten verwalteten Zugang über Netzwerkschnittstellen zu Sicherheitswerten ist auf die entsprechenden Werte zuzugreifen und zu prüfen, ob der Authentisierungsmechanismus implementiert ist.

#### 6.2.1.5.6.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn kein Nachweis vorliegt, dass ein in [E.Info.AUM-1-1.ACM.AuthenticationMechanism] dokumentierter Authentisierungsmechanismus nicht implementiert ist.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn ein Nachweis vorliegt, dass ein in [E.Info.AUM-1-1.ACM.AuthenticationMechanism] dokumentierter Authentisierungsmechanismus nicht implementiert ist.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

### 6.2.1.6 Beurteilungskriterium Benutzungsschnittstelle

#### 6.2.1.6.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung AUM-1-2.

#### 6.2.1.6.2 Umsetzungskategorien

Nicht anwendbar.

#### 6.2.1.6.3 Erforderliche Informationen

[E.Info.AUM-1-2.ACM]: Beschreibung jedes Zugangssteuerungsmechanismus, der nach ACM-1 für die Verwaltung des Zugangs von Entitäten zu Benutzungsschnittstellen erforderlich ist, die das Lesen vertraulicher personenbezogener Daten, der Konfiguration vertraulicher Datenschutzfunktionen bzw. vertraulicher Sicherheitsparameter oder die Änderung der Konfiguration sensibler Datenschutzfunktionen bzw. sensibler Sicherheitsparameter oder die Nutzung von Datenschutzfunktionen bzw. Sicherheitsfunktionen ermöglichen, einschließlich:

— [E.Info.AUM-1-2.ACM.UserInterfaces]: eine Beschreibung der Benutzungsschnittstellen für den verwalteten Zugang; und

— [E.Info.AUM-1-2.ACM.ManagedAccessPrivacyAsset]: Beschreibung des verwalteten Zugangs zu Datenschutzwerten über Benutzungsschnittstellen; und

— [E.Info.AUM-1-2.ACM.ManagedAccessSecurityAsset]: Beschreibung des verwalteten Zugangs zu Sicherheitswerten über Benutzungsschnittstellen; und

— (wenn physische oder logische Maßnahmen in der angestrebten Umgebung Vertrauen in die Richtigkeit der Angaben einer Entität schaffen) [E.Info.AUM-1-2.ACM.IntendedEnvironment]: Beschreibung der physischen oder logischen Maßnahmen in der Zielumgebung; und

— (wenn eine Authentisierung nach AUM-1-2 erforderlich ist) [E.Info.AUM-1-2.ACM.AuthenticationMechanism]: Beschreibung der implementierten Authentisierungsmechanismen; und

— (wenn für den reinen Lesezugriff auf personenbezogene Informationen, Datenschutzfunktionen oder die Konfiguration von Datenschutzfunktionen, bei denen der Zugriff ohne Authentisierung erforderlich ist, um die vorgesehene Anlagenfunktionalität zu ermöglichen, keine Authentisierung vorhanden ist) [E.Info.AUM-1-2.ACM.ReadOnlyFunctionality]: Beschreibung der vorgesehenen Anlagenfunktionalität im Hinblick auf die fehlende Authentisierung für den reinen Lesezugriff auf betroffene Werte über Benutzungsschnittstellen; und

— (wenn für den reinen Lesezugriff auf personenbezogene Informationen, Datenschutzfunktionen oder die Konfiguration von Datenschutzfunktionen, bei denen aus rechtlichen Gründen keine Authentisierungsmechanismen zulässig sind, keine Authentisierung vorhanden ist) [E.Info.AUM-1-2.ACM.ReadOnlyLegal]: Verweisungen auf alle entsprechenden Absätze oder Textstellen in sämtlichen maßgeblichen Rechtsdokumenten, einschließlich einer Beschreibung, wie diese auf die Anlage oder den betroffenen Wert anzuwenden sind.

[E.Info.DT.AUM-1-2]: Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 8 für jeden in [E.Info.AUM-1-2.ACM] dokumentierten Zugangssteuerungsmechanismus.

[E.Just.DT.AUM-1-2]: Begründung für den Pfad durch den in [E.Info.DT.AUM-1-2] dokumentierten Entscheidungsbaum mit den folgenden Eigenschaften:

— (wenn eine Entscheidung aus [DT.AUM-1-2.DN-1] zu „NICHT ANWENDBAR“ führt) basiert die Begründung für die Entscheidung [DT.AUM-1-2.DN-1] auf [E.Info.AUM-1-2.ACM.IntendedEnvironment]; und

— (wenn eine Entscheidung aus [DT.AUM-1-2.DN-2] zu „NICHT ANWENDBAR“ führt) basiert die Begründung für die Entscheidung [DT.AUM-1-2.DN-2] auf [E.Info.AUM-1-2.ACM.ReadOnlyFunctionality]; und

— (wenn eine Entscheidung aus [DT.AUM-1-2.DN-3] zu „NICHT ANWENDBAR“ führt) basiert die Begründung für die Entscheidung [DT.AUM-1-2.DN-3] auf [E.Info.AUM-1-2.ACM.ReadOnlyLegal]; und

— die Begründung für die Entscheidung [DT.AUM-1-2.DN-4] basiert auf [E.Info.AUM-1-2.ACM].

#### 6.2.1.6.4 Konzeptuelle Beurteilung

##### 6.2.1.6.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob ein Authentisierungsmechanismus implementiert wurde, wo er nach AUM-1-2 erforderlich ist.

##### 6.2.1.6.4.2 Voraussetzungen

Keine.

#### 6.2.1.6.4.3 Beurteilungseinheiten

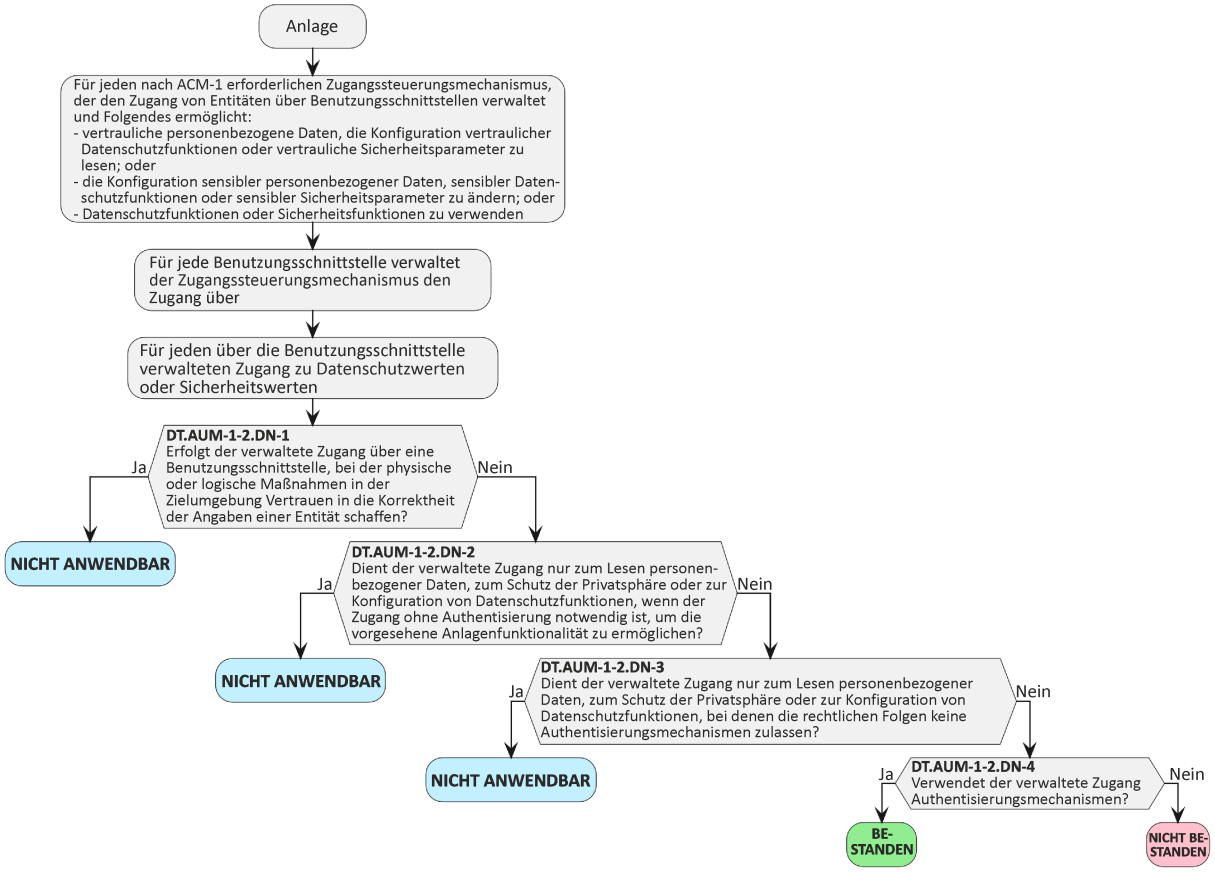



**Bild 8 — Entscheidungsbaum für Anforderung AUM-1-2**

Für jeden in [E.Info.AUM-1-2.ACM] dokumentierten Zugangssteuerungsmechanismus ist zu prüfen, ob der Pfad durch den in [E.Info.DT.AUM-1-2] dokumentierten Entscheidungsbaum mit „NICHT ANWENDBAR“ oder „BESTANDEN“ endet.

Für jeden in [E.Info.DT.AUM-1-2] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.AUM-1-2] dokumentierte Begründung zu untersuchen.

#### 6.2.1.6.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— mindestens ein Pfad durch den in [E.Info.DT.AUM-1-2] dokumentierten Entscheidungsbaum mit „BESTANDEN“ endet; und

— kein Pfad durch den in [E.Info.DT.AUM-1-2] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; und

— die in [E.Just.DT.AUM-1-2] angegebenen Informationen korrekte Begründungen für alle Pfade durch den in [E.Info.DT.AUM-1-2] dokumentierten Entscheidungsbaum sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— ein Pfad durch den in [E.Info.DT.AUM-1-2] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; oder

— eine in [E.Just.DT.AUM-1-2] angegebene Begründung für einen Pfad durch den in [E.Info.DT.AUM-1-2] dokumentierten Entscheidungsbaum nicht korrekt ist oder fehlt.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

#### 6.2.1.6.5 Beurteilung der funktionalen Vollständigkeit

##### 6.2.1.6.5.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob es Zugangssteuerungsmechanismen auf der Anlage für die Verwaltung des Zugangs von Entitäten über Benutzungsschnittstellen gibt, die das Lesen vertraulicher personenbezogener Informationen, der Konfiguration vertraulicher Datenschutzfunktionen bzw. vertraulicher Sicherheitsparameter oder die Änderung sensibler personenbezogener Informationen, der Konfiguration sensibler Datenschutzfunktionen bzw. sensibler Sicherheitsparameter oder die Nutzung von Datenschutzfunktionen bzw. Sicherheitsfunktionen ermöglichen, die nicht in [E.Info.AUM-1-2.ACM] beschrieben sind.

##### 6.2.1.6.5.2 Voraussetzungen

Die Anlage befindet sich im Betriebszustand.

##### 6.2.1.6.5.3 Beurteilungseinheiten

Es ist funktional zu beurteilen, ob es nach ACM-1 erforderliche Zugangssteuerungsmechanismen für die Verwaltung des Zugangs von Entitäten über Benutzungsschnittstellen gibt, die das Lesen vertraulicher personenbezogener Daten, die Konfiguration vertraulicher Datenschutzfunktionen bzw. vertraulicher Sicherheitsparameter oder die Änderung sensibler personenbezogener Informationen, die Konfiguration sensibler Datenschutzfunktionen bzw. sensibler Sicherheitsparameter oder die Nutzung von Datenschutzfunktionen bzw. Sicherheitsfunktionen ermöglichen, die nicht in [E.Info.AUM-1-2.ACM] beschrieben sind.

##### 6.2.1.6.5.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN für diesen Beurteilungsfall wird zugewiesen, wenn kein Nachweis vorliegt, dass ein nach ACM-1 erforderlicher Zugangssteuerungsmechanismus für die Verwaltung des Zugangs von Entitäten über Benutzungsschnittstellen, die das Lesen vertraulicher personenbezogener Daten, der Konfiguration vertraulicher Datenschutzfunktionen bzw. vertraulicher Sicherheitsparameter oder die Änderung der Konfiguration sensibler Datenschutzfunktionen bzw. sensibler Sicherheitsparameter oder die Nutzung von Datenschutzfunktionen bzw. Sicherheitsfunktionen ermöglichen, gefunden wird, der nicht in [E.Info.AUM-1-2.ACM] dokumentiert ist.

Die Entscheidung NICHT BESTANDEN für diesen Beurteilungsfall wird zugewiesen, wenn kein Nachweis vorliegt, dass ein nach ACM-1 erforderlicher Zugangssteuerungsmechanismus für die Verwaltung des Zugangs von Entitäten über Benutzungsschnittstellen, die das Lesen vertraulicher personenbezogener Daten, der Konfiguration vertraulicher Datenschutzfunktionen bzw. vertraulicher Sicherheitsparameter oder die Änderung der Konfiguration sensibler Datenschutzfunktionen bzw. sensibler Sicherheitsparameter oder die Nutzung von Netzwerkfunktionen bzw. Sicherheitsfunktionen ermöglichen, gefunden wird, der nicht in [E.Info.AUM-1-2.ACM] beschrieben ist.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

#### 6.2.1.6.6 Beurteilung der funktionalen Suffizienz

##### 6.2.1.6.6.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob die nach AUM-1-2 erforderlichen dokumentierten Authentisierungsmechanismen implementiert wurden.

#### 6.2.1.6.6.2 Voraussetzungen

Die Anlage befindet sich im Betriebszustand.

#### 6.2.1.6.6.3 Beurteilungseinheiten

Für jeden in [E.Info.AUM-1-2.ACM] dokumentierten Zugangssteuerungsmechanismus, jeden in [E.Info.AUM-1-2.ACM.ManagedAccessPrivacyAsset] dokumentierten verwalteten Zugang über Benutzungsschnittstellen zu Datenschutzwerten und jeden in [E.Info.AUM-1-2.ACM.ManagedAccessSecurityAsset] dokumentierten verwalteten Zugang über Netzwerkschnittstellen zu Sicherheitswerten ist auf die entsprechenden Sicherheitswerte und Netzwerkwerte zuzugreifen und zu prüfen, ob der Authentisierungsmechanismus implementiert ist.

#### 6.2.1.6.6.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn kein Nachweis vorliegt, dass ein in [E.Info.AUM-1-2.ACM.AuthenticationMechanism] dokumentierter Authentisierungsmechanismus nicht implementiert ist.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn ein Nachweis vorliegt, dass ein in [E.Info.AUM-1-2.ACM.AuthenticationMechanism] dokumentierter Authentisierungsmechanismus nicht implementiert ist.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

### 6.2.2 [AUM-2] Angemessene Authentisierungsmechanismen

#### 6.2.2.1 [AUM-2-1] Anforderung Ein-Faktor-Authentisierung

Authentisierungsmechanismen, die nach AUM-1-1 (Netzwerkschnittstelle) oder AUM-1-2 (Benutzungsschnittstelle) erforderlich sind, müssen die Angabe einer Entität verifizieren, indem mindestens ein Element aus den Kategorien Wissen, Besitz und Inhärenz durch mindestens einen Authentisierungsmechanismus geprüft wird (Ein-Faktor-Authentisierung).

#### 6.2.2.2 [AUM-2-2] Anforderung Zwei-Faktor-Authentisierung

Besteht die vorgesehene primäre Funktionalität der Anlage speziell in der Verarbeitung personenbezogener Informationen besonderer Kategorien, so müssen die Authentisierungsmechanismen bei jedem Zugang zu personenbezogenen Informationen besonderer Kategorien mittels Benutzungsschnittstellen über eine Netzwerkschnittstelle die Verifizierung der Angaben einer Entität auf der Grundlage von Nachweisen unterstützen, die aus mindestens zwei verschiedenen Elementen aus den Kategorien Wissen, Besitz und Inhärenz abgeleitet werden (Zwei-Faktor-Authentisierung).

#### 6.2.2.3 Begründung

Die Ein-Faktor-Authentisierung ist geeignet, den unbefugten Zugang zu Sicherheitswerten oder Datenschutzwerten, die für die Privatsphäre des Benutzers maßgeblich sind, von Entitäten zu verhindern, die nicht sind, wer oder was sie vorgeben zu sein. Die Verwaltung der zugehörigen Zugangsrechte für Entitäten wird durch Zugangssteuerungsmechanismen durchgesetzt.

Wenn die vorgesehene primäre Funktionalität der Anlage spezifisch die Verarbeitung personenbezogener Informationen aus speziellen Kategorien ist, könnte die Offenlegung solcher Daten schwerwiegende Auswirkungen haben. In diesem Fall ist die Möglichkeit der Zwei-Faktor-Authentisierung für den Zugang mittels Benutzungsschnittstelle über Netzwerkschnittstellen erforderlich.

#### 6.2.2.4 Leitlinie

Beispiele für die Verifizierung der Angaben einer Entität durch Prüfung von Nachweisen eines Elements aus den Kategorien Wissen, Besitz und Inhärenz:

— PIN-Code, genutzt für die Benutzungsschnittstelle

— 1-Faktor-Authentisierung (z. B. durch Passwort) für jede, an einer Benutzungs- oder Netzwerkschnittstelle eingehende Verbindung;

— biometrische Fingerabdrücke oder Gesichtserkennung für eine Benutzungsschnittstelle;

— Verifizierung des Besitzes eines privaten Schlüssels, der mit einem vertrauenswürdigen Zertifikat übereinstimmt;

— Vertrauensverhältnis zu einem Netzwerk (z. B. aufgrund eines gemeinsamen Geheimnisses), das bei der Verbindungsaufnahme etabliert wurde.

Beispiele für die Verifizierung der Angaben einer Entität auf der Grundlage von Nachweisen, die aus mindestens zwei verschiedenen Elementen aus den Kategorien Wissen, Besitz und Inhärenz abgeleitet werden:

— Passwort + OTP

— PIN + Smartcard

— Passwort + Token

Wenn ein Benutzer über eine Softwareanwendung, die auf einem anderen Gerät läuft, auf die Anlage zugreift, z. B. eine Wartungsanwendung, die auf einem Server oder Laptop läuft, kann dies je nach Architektur als ein Softwareprozess betrachtet werden, der auf die Anlage zugreift. Daher kann die Authentisierung für Softwareprozesse gelten. Für die Authentisierung des Benutzers bei der externen Softwareanwendung kann eine starke Authentisierung, möglicherweise auch eine Multifaktor-Authentisierung, verwendet werden. Es ist auch möglich, durch kryptographische Maßnahmen eine Vertrauensbeziehung zwischen der Anlage und einem anderen Gerät herzustellen, so dass der Besitz des anderen Geräts als ein Authentisierungsfaktor angesehen werden kann. Die Zwei-Faktor-Authentisierung für den Zugang zur Anlage kann durch ein anderes Gerät in der Betriebsumgebung der Anlage sichergestellt werden.

In diesem Fall bedeutet die vorgesehene Funktionalität des Hauptgeräts für die spezifische Verarbeitung personenbezogener Informationen besonderer Kategorien, dass Die Anlage nicht für ihre vorgesehene Funktionalität verwendet werden kann, ohne personenbezogene Informationen besonderer Kategorien zu verarbeiten. Es ist daher speziell für die Verarbeitung solcher Daten konzipiert.

Bei Geräten, deren vorgesehene Funktionalität die Verarbeitung von Daten ist, die nur möglicherweise personenbezogene Informationen aus besonderen Kategorien umfassen könnten, wie beispielsweise Desktop-PCs, Smartphones, Kameras oder Drucker, muss nur ein Schutz der personenbezogenen Daten vorgesehen werden. Allgemein ist es beim Design von Geräten zur Speicherung personenbezogener Daten vernünftig, die Bereitstellung einer Multifaktor-Authentisierung in Betracht zu ziehen.

Ein wichtiger Aspekt bei der Implementation angemessener Authentisierungsmechanismen ist die Berücksichtigung möglicher Einschränkungen von menschlichen Benutzern mit Behinderungen. Zu den Beispielen für Überlegungen bei der Auswahl von Authentisierungsmechanismen gehören:

— Übermittlung der Authentisierungsinformationen an und von einer entsprechenden unterstützenden Technik;

— Ermöglichung einer doppelten oder gemeinsamen Nutzung, wenn die Anlage von einem Benutzer und einem Betreuer (und/oder Eltern und Kind) verwendet wird;

— das Angebot alternativer Authentisierungsmechanismen, so dass sie von Benutzern mit bestimmten Lernschwächen (einschließlich Legasthenie) genutzt werden können und keine negativen Gefühle auslösen (z. B. durch Vermeidung der Angabe familiärer oder persönlicher Informationen, die für den Endbenutzer belastend oder nicht maßgeblich sein können).

Zum Zeitpunkt der Veröffentlichung des vorliegenden Dokuments werden lange Passwörter wie „WeihnachtsmarkTElephanTCarpe2023@Bon(n)“ als stärkere Passwörter angesehen als kurze Passwörter wie „P@ssw0rd!“. Weitere Leitlinien zu aktuellen bewährten Verfahrensweisen für Passwörter sind in der NIST Sonderveröffentlichung 800-63B [10], in ISO/IEC EN 27002:2022 [3], ISO/IEC EN 24760 [4], IEC EN 62443-4-2 [2] und in ETSI EN 303 645 [6] zu finden.

#### 6.2.2.5 Beurteilungskriterien Ein-Faktor-Authentisierung

##### 6.2.2.5.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung AUM-2-1.

##### 6.2.2.5.2 Umsetzungskategorien

Nicht anwendbar.

##### 6.2.2.5.3 Erforderliche Informationen

[E.Info.AUM-2-1.AuthenticationMechanism]: Beschreibung jedes Authentisierungsmechanismus, der nach AUM-1-1 (Netzwerkschnittstelle) oder AUM-1-2 (Benutzungsschnittstelle) erforderlich ist, einschließlich:

— [E.Info.AUM-2-1.AuthenticationMechanism.AuthFactor]: Beschreibung des Authentifikators einschließlich dessen Kategorien (Wissen, Besitz und Inhärenz).

[E.Info.DT.AUM-2-1]: Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 9 für jeden in [E.Info.AUM-2-1.AuthenticationMechanism] dokumentierten Authentisierungsmechanismus.

[E.Just.DT.AUM-2-1]: Begründung für den gewählten Pfad durch den in [E.Info.DT.AUM-2-1] dokumentierten Entscheidungsbaum mit der folgenden Eigenschaft:

— die Begründung für die Entscheidung [DT.AUM-2-1.DN-1] basiert auf [E.Info.AUM-2-1.AuthenticationMechanism.AuthFactor].

##### 6.2.2.5.4 Konzeptuelle Beurteilung

###### 6.2.2.5.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob die Authentisierungsmechanismen, die nach AUM-1-1 (Netzwerkschnittstelle) oder AUM-1-2 (Benutzungsschnittstelle) erforderlich sind, wie nach AUM-2-1 erforderlich implementiert sind.

###### 6.2.2.5.4.2 Voraussetzungen

Keine.

#### 6.2.2.5.4.3 Beurteilungseinheiten

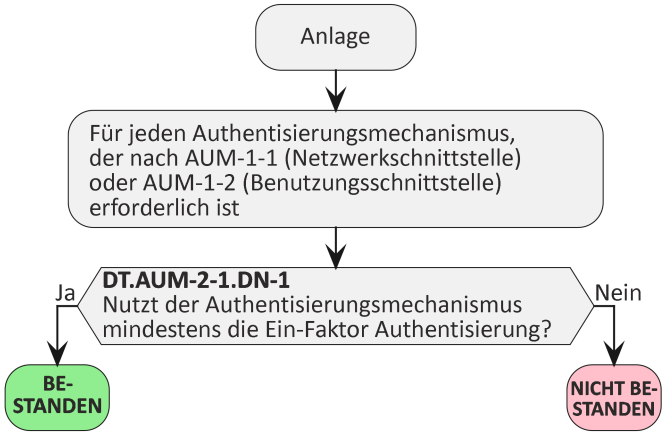



**Bild 9 — Entscheidungsbaum für Anforderung AUM-2-1**

Für jeden in [E.Info.AUM-2-1.AuthenticationMechanism] dokumentierten Authentisierungsmechanismus ist zu prüfen, ob der Pfad durch den in [E.Info.DT.AUM-2-1] dokumentierten Entscheidungsbaum mit „BESTANDEN“ endet.

Für jeden in [E.Info.DT.AUM-2-1] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.AUM-2-1] dokumentierte Begründung zu untersuchen.

#### 6.2.2.5.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— alle Pfade durch den in [E.Info.DT.AUM-2-1] dokumentierten Entscheidungsbaum mit „BESTANDEN“ enden; und

— die in [E.Just.DT.AUM-2-1] angegebenen Informationen korrekte Begründungen für alle Pfade durch den in [E.Info.DT.AUM-2-1] dokumentierten Entscheidungsbaum sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— ein Pfad durch den in [E.Info.DT.AUM-2-1] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; oder

— eine in [E.Just.DT.AUM-2-1] angegebene Begründung für einen Pfad durch den in [E.Info.DT.AUM-2-1] dokumentierten Entscheidungsbaum nicht korrekt ist oder fehlt.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

### 6.2.2.5.5 Beurteilung der funktionalen Vollständigkeit

Die Beurteilung der funktionalen Vollständigkeit wird durch die Beurteilung der funktionalen Suffizienz der Anwendbarkeit des Authentisierungsmechanismus abgedeckt.

Deshalb ist diese Beurteilung der funktionalen Vollständigkeit nicht notwendig.

#### 6.2.2.5.6 Beurteilung der funktionalen Suffizienz

##### 6.2.2.5.6.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob die Authentisierungsmechanismen, die nach AUM-1-1 (Netzwerkschnittstelle) oder AUM-1-2 (Benutzungsschnittstelle) erforderlich sind, wie in [E.Info.AUM-2-1.AuthenticationMechanism.AuthFactor] dokumentiert implementiert sind.

##### 6.2.2.5.6.2 Voraussetzungen

Die Anlage befindet sich im Betriebszustand.

##### 6.2.2.5.6.3 Beurteilungseinheiten

Für jeden in [E.Info.AuthenticationMechanism.AUM-2-1] dokumentierten Authentisierungsmechanismus, der nach AUM-1-1 (Netzwerkschnittstelle) oder AUM-1-2 (Benutzerschnittstelle) erforderlich ist, ist die Authentisierung durchzuführen und zu prüfen, ob der Authentisierungsmechanismus wie dokumentiert implementiert ist.

##### 6.2.2.5.6.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn kein Nachweis vorliegt, dass die Umsetzung eines Authentisierungsmechanismus von [E.Info.AUM-2-1.AuthenticationMechanism] abweicht.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn ein Nachweis vorliegt, dass die Umsetzung eines Authentisierungsmechanismus von [E.Info.AUM-2-1.AuthenticationMechanism] abweicht.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

### 6.2.2.6 Beurteilungskriterien Zwei-Faktor-Authentisierung

#### 6.2.2.6.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung AUM-2-2.

#### 6.2.2.6.2 Umsetzungskategorien

Nicht anwendbar.

#### 6.2.2.6.3 Erforderliche Informationen

(Wenn die vorgesehene Funktionalität des Hauptgeräts spezifisch die Verarbeitung personenbezogener Informationen aus speziellen Kategorien ist) [E.Info.AUM-2-2.AuthenticationMechanism]: Beschreibung jedes nach AUM-1-1 (Netzwerkschnittstelle) oder AUM-1-2 (Benutzungsschnittstelle) erforderlichen Authentisierungsmechanismus und für den Zugriff auf personenbezogene Informationen besonderer Kategorien mittels Benutzungsschnittstellen über Netzwerkschnittstellen verwendet, einschließlich:

— [E.Info.AUM-2-2.AuthenticationMechanism.AuthFactor]: Beschreibung des Authentifikators einschließlich dessen Kategorien (Wissen, Besitz und Inhärenz).

[E.Info.DT.AUM-2-2]: Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 10 für jeden in [E.Info.AUM-2-2.AuthenticationMechanism] dokumentierten Authentisierungsmechanismus.

[E.Just.DT.AUM-2-2]: Begründung für den gewählten Pfad durch den in [E.Info.DT.AUM-2-2] dokumentierten Entscheidungsbaum mit der folgenden Eigenschaft:

— die Begründung für die Entscheidung [DT.AUM-2-2.DN-2] basiert auf [E.Info.AUM-2-2.AuthenticationMechanism] oder [E.Info.AUM-2-2.AuthenticationMechanism.AuthFactor].

#### 6.2.2.6.4 Konzeptuelle Beurteilung

##### 6.2.2.6.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob der Authentisierungsmechanismus, der nach AUM-1-1 (Netzwerkschnittstelle) oder AUM-1-2 (Benutzungsschnittstelle) erforderlich ist, wie nach AUM-2-2 erforderlich implementiert ist.

##### 6.2.2.6.4.2 Voraussetzungen

Keine.

##### 6.2.2.6.4.3 Beurteilungseinheiten

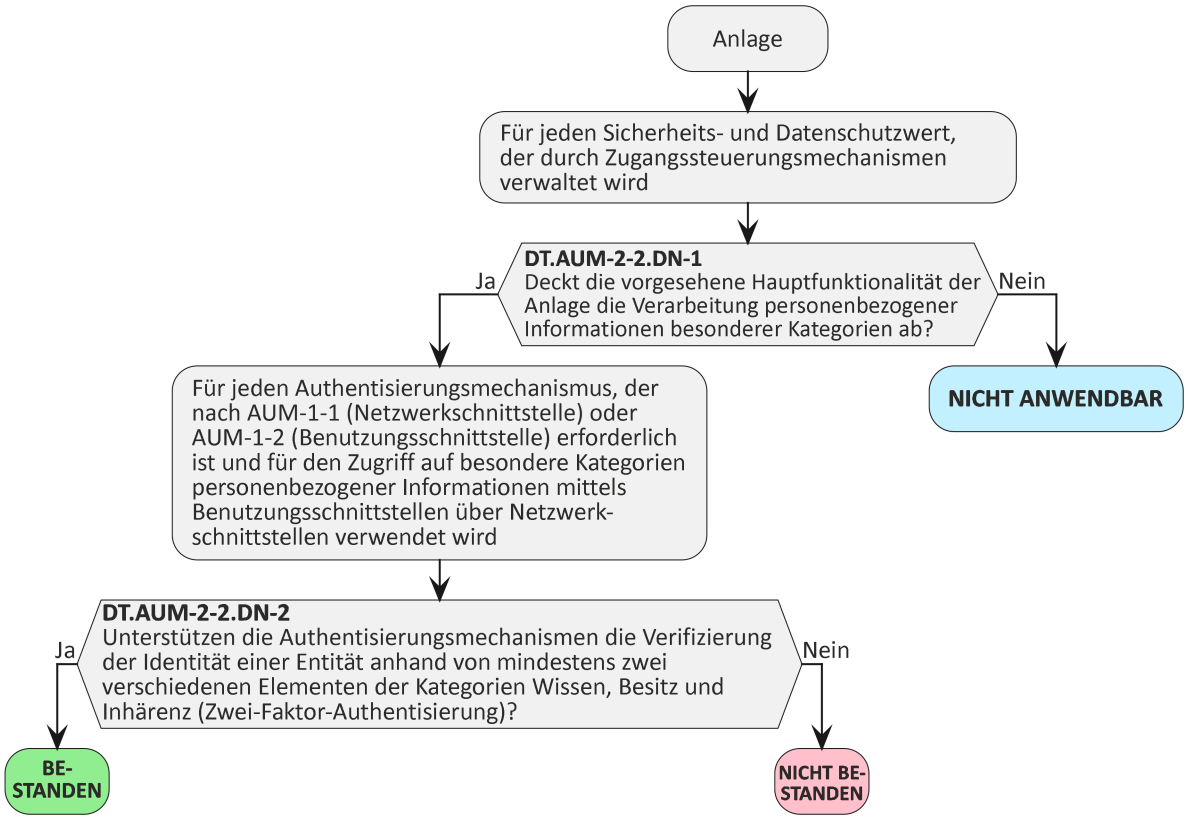



**Bild 10 — Entscheidungsbaum für Anforderung AUM-2-2**

Für jeden in [E.Info.AUM-2-2.AuthenticationMechanism] dokumentierten Authentisierungsmechanismus ist zu prüfen, ob der Pfad durch den in [E.Info.DT.AUM-2-2] dokumentierten Entscheidungsbaum mit „BESTANDEN“ endet.

Für jeden in [E.Info.DT.AUM-2-2] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.AUM-2-2] dokumentierte Begründung zu untersuchen.

#### 6.2.2.6.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— mindestens ein Pfad durch den in [E.Info.DT.AUM-2-2] dokumentierten Entscheidungsbaum mit „BESTANDEN“ endet; und

— kein Pfad durch den in [E.Info.DT.AUM-2-2] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; und

— die in [E.Just.DT.AUM-2-2] angegebenen Informationen korrekte Begründungen für alle Pfade durch den in [E.Info.DT.AUM-2-2] dokumentierten Entscheidungsbaum sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— ein Pfad durch den in [E.Info.DT.AUM-2-2] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; oder

— eine in [E.Just.DT.AUM-2-2] angegebene Begründung für einen Pfad durch den in [E.Info.DT.AUM-2-2] dokumentierten Entscheidungsbaum nicht korrekt ist oder fehlt.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

#### 6.2.2.6.5 Beurteilung der funktionalen Vollständigkeit

Die Beurteilung der funktionalen Vollständigkeit wird durch die Beurteilung der funktionalen Suffizienz der Anwendbarkeit des Authentisierungsmechanismus abgedeckt.

Deshalb ist diese Beurteilung der funktionalen Vollständigkeit nicht notwendig.

#### 6.2.2.6.6 Beurteilung der funktionalen Suffizienz

##### 6.2.2.6.6.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob die Authentisierungsmechanismen, die nach AUM-1-1 (Netzwerkschnittstelle) oder AUM-1-2 (Benutzungsschnittstelle) erforderlich sind, wie in [E.Info.AUM-2-2.AuthenticationMechanism.AuthFactor] dokumentiert implementiert sind.

##### 6.2.2.6.6.2 Voraussetzungen

Die Anlage befindet sich im Betriebszustand.

##### 6.2.2.6.6.3 Beurteilungseinheiten

Für jeden in [E.Info.AUM-2-2.AuthenticationMechanism] dokumentierten Authentisierungsmechanismus, der nach AUM-1-1 (Netzwerkschnittstelle) oder AUM-1-2 (Benutzerschnittstelle) erforderlich ist, ist die Zwei-Faktor-Authentisierung zu aktivieren, die Authentisierung durchzuführen und zu prüfen, ob der Authentisierungsmechanismus wie dokumentiert implementiert ist.

##### 6.2.2.6.6.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn kein Nachweis vorliegt, dass die Umsetzung eines Authentisierungsmechanismus von [E.Info.AUM-2-2.AuthenticationMechanism] abweicht.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn ein Nachweis vorliegt, dass die Umsetzung eines Authentisierungsmechanismus von [E.Info.AUM-2-2.AuthenticationMechanism] abweicht.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

### 6.2.3 [AUM-3] Authentifikator-Validierung

#### 6.2.3.1 Anforderung

Authentisierungsmechanismen, die nach AUM-1-1 (Netzwerkschnittstelle) oder AUM-1-2 (Benutzungsschnittstelle) erforderlich sind, müssen, abhängig von den in der verwendeten Betriebsumgebung verfügbaren Informationen, alle relevanten Eigenschaften der verwendeten Authentifikatoren validieren.

#### 6.2.3.2 Begründung

Auch wenn die Anlage einen Authentisierungsmechanismus bereitstellt, besteht das Risiko, dass ein Angreifer typische Design-Schwachstellen zu dessen Überwindung nutzt. Ein Angriff gegen solche Mechanismen beruht häufig auf der Nutzung gefälschter oder teilweise gefälschter Authentifikatoren. Daher sind beim Sicherheitsdesign von Mechanismen Techniken erforderlich, um gefälschten Authentifikatoren, beispielsweise manipulierten PKI-Zertifikaten, zu widerstehen.

#### 6.2.3.3 Leitlinie

Der Authentifikator und seine Attribute unterscheiden sich je nach Authentisierungsmechanismus. Für die Validierung des Authentifikators sollten bewährte Verfahrensweisen für den entsprechenden Authentisierungsmechanismus angewendet werden. Dies ist erforderlich, um die Verwendung eines ungültigen Authentifikators zu erkennen und zu verhindern. Wenn ein Gerät beispielsweise nur den gemeinsamen Namen eines PKI-Zertifikats validiert, ohne zusätzlich die vollständigen Zertifikatinformationen zu validieren, würde ein entsprechend gefälschter Authentifikator akzeptiert. In diesem Beispiel sind die maßgeblichen Eigenschaften des Authentifikators die Signaturen und öffentlichen Schlüssel der Vertrauenskette, der Widerrufsstatus und in vielen Fällen auch die Validität des Zertifikats. Der Satz maßgeblicher Eigenschaften kann sich abhängig davon unterscheiden, ob die Anlage tatsächlich mit dem Internet verbunden ist oder nicht. Beispielsweise hat ein Offline-Gerät wahrscheinlich keinen Zugang zu einer zuverlässigen Zeitquelle oder zu Informationen zum Widerruf von Zertifikaten.

Ein weiteres Beispiel für eine unzureichende Validierung von Authentifikatoren liegt vor, wenn nur Teile des Passworts überprüft werden. Dies würde die Passwortstärke schwächen und so Brute-Force-Angriffe auf den entsprechenden Authentisierungsmechanismus erleichtern.

#### 6.2.3.4 Beurteilungskriterien

##### 6.2.3.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung AUM-3.

##### 6.2.3.4.2 Umsetzungskategorien

[IC.AUM-3.Password]: Der Authentifikator ist ein Passwort.

[IC.AUM-3.CertificatePrivateKey]: Der Authentifikator ist ein privater Schlüssel, der mit einem vom Gerät als vertrauenswürdig eingestuften Zertifikat verbunden ist.

ANMERKUNG Einem Zertifikat kann die Anlage z. B. über eine Vertrauenskette zu einem vorinstallierten Stammzertifikat einer PKI oder durch Zertifikatsanbindung vertrauen.

[IC.AUM-3.Generic]: Der Authentifikator unterscheidet sich von [IC.AUM-3.Password] oder [IC.AUM-3.CertificatePrivateKey].

BEISPIEL Biometrie, Secure Shell (SSH)-Schlüssel, symmetrische Schlüssel

#### 6.2.3.4.3 Erforderliche Informationen

[E.Info.AUM-3.AUM]: Beschreibung jedes Authentisierungsmechanismus, der nach AUM-1-1 (Netzwerkschnittstelle) oder AUM-1-2 (Benutzungsschnittstelle) erforderlich ist, einschließlich:

— [E.Info.AUM-3.AUM.AuthVal]: Beschreibung, wie die Validierung des Authentifikators durchgeführt wird, einschließlich seiner Umsetzungskategorie und der maßgeblichen Eigenschaften; und

— [E.Info.AUM-3.AUM.AuthEnv]: Beschreibung der verfügbaren Informationen über den Authentifikator in der genutzten Betriebsumgebung.

[E.Info.DT.AUM-3]: Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 11 für jeden in [E.Info.AUM-3.AUM] dokumentierten Authentisierungsmechanismus.

[E.Just.DT.AUM-3]: Begründung für den gewählten Pfad durch den in [E.Info.DT.AUM-3] dokumentierten Entscheidungsbaum mit der folgenden Eigenschaft:

— die Begründung für die Entscheidung [DT.AUM-3.DN-1] basiert auf [E.Info.AUM-3.AUM.AuthVal] und [E.Info.AUM-3.AUM.AuthEnv].

#### 6.2.3.4.4 Konzeptuelle Beurteilung

##### 6.2.3.4.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob Authentisierungsmechanismen alle maßgeblichen Eigenschaften des Authentifikators validieren, wie in [E.Info.AUM-3.AUM] dokumentiert. Diese Beurteilung wird für jeden Pfad zu Sicherheitswerten und/oder Datenschutzwerten durchgeführt, die nach AUM-1-1 oder AUM-1-2 erforderlich sind.

##### 6.2.3.4.4.2 Voraussetzungen

Keine.

##### 6.2.3.4.4.3 Beurteilungseinheiten

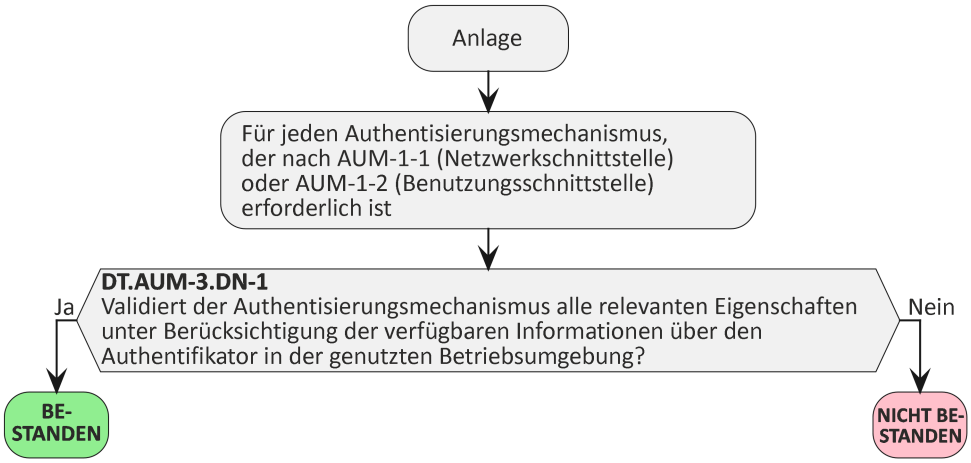



**Bild 11 — Entscheidungsbaum für Anforderung AUM-3**

Für jeden in [E.Info.AUM-3.AUM] dokumentierten Authentisierungsmechanismus ist zu prüfen, ob der Pfad durch den in [E.Info.DT.AUM-3] dokumentierten Entscheidungsbaum mit „BESTANDEN“ endet.

Für jeden in [E.Info.DT.AUM-3] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.AUM-3] dokumentierte Begründung zu untersuchen.

#### 6.2.3.4.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— alle Pfade durch den in [E.Info.DT.AUM-3] dokumentierten Entscheidungsbaum mit „BESTANDEN“ enden; und

— die in [E.Just.DT.AUM-3] angegebenen Informationen korrekte Begründungen für alle Pfade durch den in [E.Info.DT.AUM-3] dokumentierten Entscheidungsbaum sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— ein Pfad durch den in [E.Info.DT.AUM-3] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; oder

— eine in [E.Just.DT.AUM-3] angegebene Begründung für einen Pfad durch den in [E.Info.DT.AUM-3] dokumentierten Entscheidungsbaum nicht korrekt ist oder fehlt.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

#### 6.2.3.4.5 Beurteilung der funktionalen Vollständigkeit

Die Beurteilung der funktionalen Vollständigkeit wird durch die Beurteilung der funktionalen Suffizienz der Anwendbarkeit des Authentisierungsmechanismus abgedeckt.

Deshalb ist diese Beurteilung der funktionalen Vollständigkeit nicht notwendig.

#### 6.2.3.4.6 Beurteilung der funktionalen Suffizienz

##### 6.2.3.4.6.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob der nach AUM-1-1 oder AUM-1-2 geforderte Authentisierungsmechanismus alle erforderlichen Eigenschaften validiert.

##### 6.2.3.4.6.2 Voraussetzungen

Die Anlage befindet sich im Betriebszustand.

##### 6.2.3.4.6.3 Beurteilungseinheiten

Für jeden in [E.Info.AUM-3.AUM] dokumentierten Authentisierungsmechanismus:

[AU.AUM-3.Password]: Wenn der Authentifikator zu [IC.AUM-3.Password] gehört, ist die Validierung der in [E.Info.AUM-3.AUM.AuthVal] dokumentierten maßgeblichen Eigenschaften des Authentifikators funktional zu bestätigen, indem geprüft wird, ob:

— falsche Passwörter für eine erfolgreiche Authentisierung verwendet werden können; und

— (wenn die Vertraulichkeit der während der Authentisierung über Netzwerkschnittstellen ausgetauschten Nachrichten nicht geschützt ist) eine Wiederholung eines aufgezeichneten erfolgreichen Authentisierungsversuchs für eine erfolgreiche Authentisierung verwendet werden kann; und

— Teile des richtigen Passwortes für eine Authentisierung verwendet werden können; und

— (wenn verschiedene Benutzerkonten existieren oder erstellt werden können) Passwörter anderer Entitäten zur Authentisierung verwendet werden können.

[AU.AUM-3.CertificatePrivateKey]: Wenn der Authentifikator zu [IC.AUM-3.CertificatePrivateKey] gehört, ist die Validierung der in [E.Info.AUM-3.AUM.AuthVal] dokumentierten maßgeblichen Eigenschaften des Authentifikators funktional zu bestätigen, indem geprüft wird, ob:

— falsche private Schlüssel zu einem vertrauenswürdigen Zertifikat für eine erfolgreiche Authentisierung verwendet werden können; und

— (wenn die Vertraulichkeit der während der Authentisierung über Netzwerkschnittstellen ausgetauschten Nachrichten nicht geschützt ist) eine Wiederholung eines aufgezeichneten erfolgreichen Authentisierungsversuchs für eine erfolgreiche Authentisierung verwendet werden kann; und

— gültige private Schlüssel zu nicht vertrauenswürdigen oder ungültigen Zertifikaten für eine erfolgreiche Authentisierung verwendet werden können; und

ANMERKUNG Bei nicht vertrauenswürdigen oder ungültigen Zertifikaten kann es sich um Zertifikate handeln, die von der Zertifizierungsstelle widerrufen wurden, um abgelaufene Zertifikate oder um Zertifikate mit einer ungültigen Vertrauenskette, die z. B. von einer nicht vertrauenswürdigen Entität erstellt wurden und einen erwarteten Eintrag eines „gemeinsamen Namens“ (CN, en: Common Name) enthalten.

— (wenn verschiedene Benutzerkonten existieren oder erstellt werden können) private Schlüssel eines vertrauenswürdigen Zertifikats anderer Entitäten zur Authentisierung verwendet werden können.

[AU.AUM-3.Generic]: Wenn der Authentifikator zu [IC.AUM-3.Generic] gehört, ist die Validierung der in [E.Info.AUM-3.AUM.AuthVal] dokumentierten maßgeblichen Eigenschaften des Authentifikators funktional zu bestätigen, indem geprüft wird, ob:

— falsche Authentifikatoren für eine erfolgreiche Authentisierung verwendet werden können; und

— (wenn die Vertraulichkeit der während der Authentisierung über Netzwerkschnittstellen ausgetauschten Nachrichten nicht geschützt ist) eine Wiederholung eines aufgezeichneten erfolgreichen Authentisierungsversuchs für eine erfolgreiche Authentisierung verwendet werden kann; und

— (wenn verschiedene Benutzerkonten existieren oder erstellt werden können) Authentifikatoren anderer Entitäten zur Authentisierung verwendet werden können.

#### 6.2.3.4.6.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn für jeden in [E.Info.AUM-3.AUM] dokumentierten Authentisierungsmechanismus die Bestätigungen in der von der Umsetzungskategorie abhängigen Beurteilungseinheit erfolgreich sind.

Die Entscheidung NICHT BESTANDEN für den Beurteilungsfall wird zugewiesen, wenn für einen in [E.Info.AUM-3.AUM] dokumentierten Authentisierungsmechanismus eine Bestätigung in der von der Umsetzungskategorie abhängigen Beurteilungseinheit nicht erfolgreich ist.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

### 6.2.4 [AUM-4] Änderung von Authentifikatoren

#### 6.2.4.1 Anforderung

Authentisierungsmechanismen, die nach AUM-1-1 oder AUM-1-2 erforderlich sind, müssen eine Änderung des Authentifikators zulassen, außer bei Authentifikatoren, bei denen widersprechende Sicherheitsziele keine Änderung erlauben.

#### 6.2.4.2 Begründung

Statische Authentifikatoren können ein Sicherheitsrisiko für die Anlagen darstellen, z. B. erhöhte Anfälligkeit für Brute-Force- und Abhörangriffe. Daher ist als Gegenmaßnahme eine Unterstützung zur Änderung der Authentifikatoren auf der Anlage erforderlich.

#### 6.2.4.3 Leitlinie

Eine autorisierte Einheit muss eine Möglichkeit zur Änderung des Authentifikators haben. Das Verfahren kann sich je nach Authentisierungsmechanismus unterscheiden.

— Die Anlage stellt der autorisierten Entität, z. B. dem Benutzer, eine Funktionalität zur Änderung des Authentifikators auf der Anlage zur Verfügung.

— Der Authentifikator, z. B. der Token, wird vom Hersteller erneuert oder ausgetauscht, und die Anlage akzeptiert den geänderten Authentifikator, weil die Vertrauenskette nach wie vor gültig ist.

— Der Authentifikator wird mithilfe eines sicheren Aktualisierungsmechanismus aktualisiert.

Bei Maschinenschnittstellen kann eine neue Kopplung notwendig sein. Die Integration der Änderung des Authentifikators in den üblichen Arbeitsablauf vereinfacht das Verfahren für den Benutzer. Dieses Verfahren hängt vom gewählten Authentifikator ab (z. B. Fingerabdruck, Passwort oder Token)

Es kann Anwendungsfälle geben, bei denen ein statischer Authentifikator zulässig ist, beispielsweise eine Vertrauensgrundlage, bei der die Vertraulichkeit des entsprechenden kryptographischen Schlüssels durch den Hersteller sichergestellt wird. In solchen Fällen stellt der Hersteller üblicherweise Tokens für autorisierte Entitäten zur Verfügung, die alle mit der gleichen Vertrauensgrundlage verbunden sind.

Es kann auch Ausnahmen geben, bei denen das Gesamtrisiko der Änderung eines Authentifikators, z. B. aufgrund der Komplexität, das mit den Sicherheitswerten oder Datenschutzwerten verbundene Risiko überwiegt, wenn statische Authentifikatoren verwendet werden. In solchen Fällen ist es wichtig, bewährte Verfahrensweisen für Sicherheits-Design-Grundsätze zu berücksichtigen, um das mit dem statischen Authentifikator verbundene Risiko möglichst gering zu halten, indem z. B. die Verwendung globaler Authentifikatoren vermieden wird.

Je nach der beabsichtigten Anlagenfunktionalität kann es erforderlich sein, die Anlagenfunktionalität durch eine Rückstellungsmöglichkeit sicherzustellen, indem z. B. keine Passwortaktualisierung während der Autofahrt erzwungen wird.

#### 6.2.4.4 Beurteilungskriterien

##### 6.2.4.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung AUM-4.

##### 6.2.4.4.2 Umsetzungskategorien

Nicht anwendbar.

##### 6.2.4.4.3 Erforderliche Informationen

[E.Info.AUM-4.AUM]: Beschreibung jedes Authentisierungsmechanismus, der nach AUM-1-1 (Netzwerkschnittstelle) und AUM-1-2 (Benutzungsschnittstelle) erforderlich ist, einschließlich:

— (wenn widersprechende Sicherheitsziele keine Änderung erlauben) [E.Info.AUM-4.AUM.ConfSecGoals]: Beschreibung der widersprechenden Sicherheitsziele aus dem Sicherheitskonzept der Anlage bezüglich der Änderung des Authentifikators; und

— [E.Info.AUM-4.AUM.AuthChange]: Beschreibung, wie die Änderung des Authentifikators bei jedem in [E.Info.AUM-4.AUM] dokumentierten Authentisierungsmechanismus durchgeführt wird, unter Berücksichtigung des Sicherheitskonzepts der Anlage.

[E.Info.DT.AUM-4]: Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 12 für jede in [E.Info.AUM-4.AUM.AuthChange] dokumentierte Authentifikator-Änderungsfunktionalität.

[E.Just.DT.AUM-4]: Begründung für den gewählten Pfad durch den in [E.Info.DT.AUM-4] dokumentierten Entscheidungsbaum mit den folgenden Eigenschaften:

— die Begründung für die Entscheidung [DT.AUM-4.DN-1] basiert auf [E.Info.AUM-4.AUM.ConfSecGoals]; und

— die Begründung für die Entscheidung [DT.AUM-4.DN-2] basiert auf [E.Info.AUM-4.AUM.AuthChange].

#### 6.2.4.4.4 Konzeptuelle Beurteilung

##### 6.2.4.4.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob der Authentifikator, der von den in [E.Info.AUM-4.AUM] dokumentierten Authentifizierungsmechanismen verwendet wird, geändert werden kann.

##### 6.2.4.4.4.2 Voraussetzungen

Keine.

##### 6.2.4.4.4.3 Beurteilungseinheiten

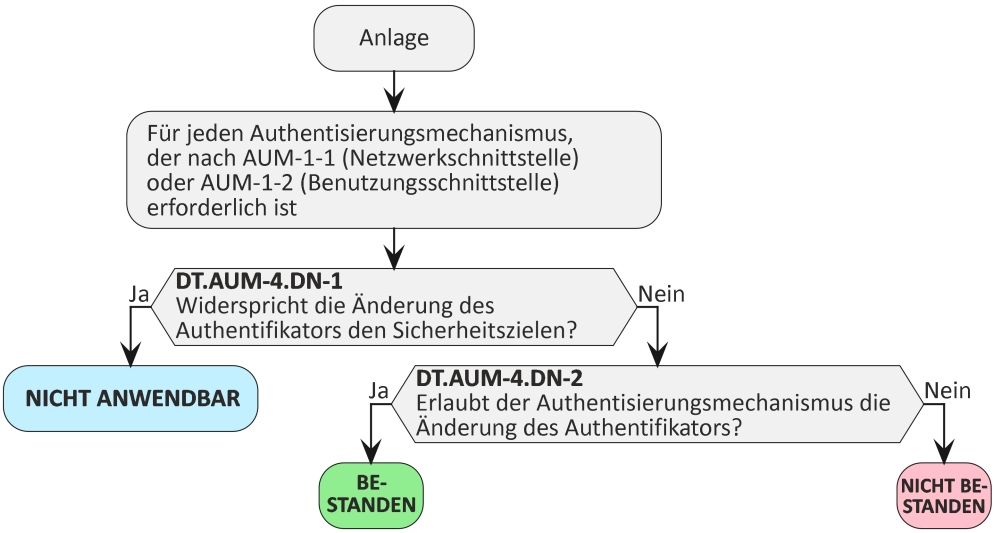



**Bild 12 — Entscheidungsbaum für Anforderung AUM-4**

Für jede in [E.Info.AUM-4.AUM] dokumentierte Authentifikator-Änderungsfunktionalität ist zu prüfen, ob der Pfad durch den in [E.Info.DT.AUM-4] dokumentierten Entscheidungsbaum mit „NICHT ANWENDBAR“ oder „BESTANDEN“ endet.

Für jeden in [E.Info.DT.AUM-4] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.AUM-4] dokumentierte Begründung zu untersuchen.

#### 6.2.4.4.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— mindestens ein Pfad durch den in [E.Info.DT.AUM-4] dokumentierten Entscheidungsbaum mit „BESTANDEN“ endet; und

— kein Pfad durch den in [E.Info.DT.AUM-4] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; und

— die in [E.Just.DT.AUM-4] angegebenen Informationen korrekte Begründungen für alle Pfade durch den in [E.Info.DT.AUM-4] dokumentierten Entscheidungsbaum sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— ein Pfad durch den in [E.Info.DT.AUM-4] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; oder

— eine in [E.Just.DT.AUM-4] angegebene Begründung für einen Pfad durch den in [E.Info.DT.AUM-4] dokumentierten Entscheidungsbaum nicht korrekt ist oder fehlt.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

#### 6.2.4.4.5 Beurteilung der funktionalen Vollständigkeit

Die Beurteilung der funktionalen Vollständigkeit wird durch die Beurteilung der funktionalen Suffizienz der Anwendbarkeit des Authentisierungsmechanismus abgedeckt.

Deshalb ist diese Beurteilung der funktionalen Vollständigkeit nicht notwendig.

#### 6.2.4.4.6 Beurteilung der funktionalen Suffizienz

##### 6.2.4.4.6.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob die dokumentierten Authentisierungsmechanismen, die nach AUM-1-1 (Netzwerkschnittstelle) oder AUM-1-2 (Benutzungsschnittstelle) erforderlich sind, eine Änderung des Authentifikators, wie in [E.Info.AUM-4.AUM.AuthChange] dokumentiert, erlauben.

##### 6.2.4.4.6.2 Voraussetzungen

Die Anlage befindet sich im Betriebszustand.

##### 6.2.4.4.6.3 Beurteilungseinheiten

Für jeden Authentisierungsmechanismus, der nach AUM-1-1 (Netzwerkschnittstelle) oder AUM-1-2 (Benutzungsschnittstelle), dokumentiert in [E.Info.AUM-4.AUM], erforderlich ist, ist die Fähigkeit, den Authentifikator zu ändern, wie in [E.Info.AUM-4.AUM.AuthChange] dokumentiert, funktional zu bestätigen durch

— Prüfen, ob der neu zugewiesene Authentifikator auf jedem Pfad Zugang zu Sicherheitswerten und/oder Datenschutzwerten gewährt; und

— Prüfen, ob der bisherige Authentifikator auf keinem Pfad mehr Zugang zu Sicherheitswerten und/oder Datenschutzwerten gewährt

nach Änderung des Authentifikators.

#### 6.2.4.4.6.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn kein Nachweis vorliegt, dass eine Umsetzung der Änderung eines Authentifikators von [E.Info.AUM-4.AUM.AuthChange] abweicht.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn ein Nachweis vorliegt, dass eine Umsetzung der Änderung eines Authentifikators von [E.Info.AUM-4.AUM.AuthChange] abweicht.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

### 6.2.5 [AUM-5] Passwortstärke

#### 6.2.5.1 [AUM-5-1] Anforderung an werkseitig voreingestellte Passwörter

Wenn ein nach AUM-1-1 oder AUM-1-2 geforderter Authentisierungsmechanismus werkseitig voreingestellte Passwörter verwendet, müssen diese:

— für jedes Gerät eindeutig sein; und

— bezüglich der Stärke bewährte Verfahrensweisen einhalten;

oder

— vom Benutzer vor oder bei der ersten Nutzung geändert werden.

ANMERKUNG Der Benutzer kann sich dafür entscheiden, kein Passwort zu verwenden.

#### 6.2.5.2 [AUM-5-2] Anforderung an nicht werkseitig voreingestellte Passwörter

Wenn ein nach AUM-1-1 oder AUM-1-2 geforderter Authentisierungsmechanismus andere als werkseitig voreingestellte Passwörter verwendet, müssen diese:

— vom Benutzer vor oder bei der ersten Nutzung und vor dem logischen Anschluss der Anlage an ein Netz eingestellt werden; oder

— von einer autorisierten Entität innerhalb eines Netzwerks definiert werden, in dem der Zugang auf autorisierte Entitäten beschränkt ist; oder

— von den Anlagen unter Anwendung bewährter Praktiken in Bezug auf die Stärke erzeugt und nur an eine autorisierte Entität innerhalb eines Netzwerks übermittelt werden, in dem der Zugang auf autorisierte Entitäten beschränkt ist.

ANMERKUNG Der Benutzer kann sich dafür entscheiden, kein Passwort zu verwenden.

#### 6.2.5.3 Begründung

Schwache Passwörter wie universelle Passwörter stellen einen der am meisten ausgenutzten Angriffsvektoren bei Anlagen dar. Es existiert ein breites Spektrum an Schadsoftware, die solche Passwörter zur automatischen Kompromittierung von Anlagen nutzt. Daher ist es zwingend erforderlich, dass für jedes Gerät bei der Ersteinrichtung ein eigenes Passwort festgelegt oder ein benutzer- bzw. organisationsdefiniertes Passwort verwendet wird.

#### 6.2.5.4 Leitlinie

Es gibt unterschiedliche Techniken, um universelle Passwörter zu vermeiden, Beispiele sind:

— Das vom Werk voreingestellte Passwort der Anlage ist auf einen Aufkleber unten am Gerätegehäuse aufgedruckt. Das Passwort wird durch einen echten Zufallsgenerator oder eine andere kryptographisch sichere Implementation eines Pseudo-Zufallszahlengenerators (CSPRNG) erzeugt.

— Die Anlage fordert den Benutzer auf, bei der ersten Benutzung ein Passwort zu erstellen.

Es wird dringend empfohlen, etablierte Normen für die sichere Generierung von Zufallszahlen zu befolgen, die zur Generierung sicherer Passwörter verwendet werden. Es gibt zahlreiche anerkannte, öffentlich zugängliche Normen für Zufallszahlengenerierungsmechanismen, die von Fachkollegen geprüft wurden. Gängige Beispiele für solche Normen sind NIST SP 800-90A Rev.1 [11], NIST SP 800-90B [12], NIST SP 800-90C [13], BSI AIS31 [18].

Leitlinien zu bewährten Verfahrensweisen für Passwörter sind in NIST SP 800-63B [10], in ISO/IEC EN 27002:2022 [3], ISO/IEC EN 24760 [4], in IEC EN 62443-4-2 [2] und in ETSI EN 303 645 [6] zu finden.

Eindeutig bedeutet, dass das Passwort nicht systematisch wiederverwendet wird oder für ein anderes Gerät des gleichen Produkttyps abgeleitet werden kann, und dass es nicht einfach von den Eigenschaften der Anlage (z. B. dem Herstellernamen, dem Modellnamen oder der Media Access Control-(MAC-)Adresse) abgeleitet werden kann. Ein gängiger Zufallsgenerator kann verwendet werden, um faktisch eindeutige Passwörter zu erzeugen.

Bei der Erzwingung einer Passwortänderung sind auch Sicherheitsaspekte von Bedeutung, z. B. dass eine Passwortänderung nicht während des Autofahrens erzwungen wird.

#### 6.2.5.5 Beurteilungskriterien für werkseitig voreingestellte Passwörter

##### 6.2.5.5.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung AUM-5-1.

##### 6.2.5.5.1 Umsetzungskategorien

[IC.AUM-5-1.UniqueBestPractice]: Der Benutzer ist nicht gezwungen, das werkseitig voreingestellte Passwort bei oder vor der ersten Nutzung zu ändern, und das Passwort ist für jedes Gerät eindeutig und entspricht der bewährten Verfahrensweise hinsichtlich der Stärke.

[IC.AUM-5-1.EnforceSettingFirstUse]: Der Benutzer ist gezwungen, das werkseitig voreingestellte Passwort bei oder vor der ersten Nutzung zu ändern.

##### 6.2.5.5.2 Erforderliche Informationen

[E.Info.AUM-5-1.AUM]: Beschreibung jedes Authentisierungsmechanismus, der nach AUM-1-1 (Netzwerkschnittstelle) erforderlich ist oder AUM-1-2 (Benutzungsschnittstelle), werkseitig voreingestellte Passwörter verwendet, einschließlich:

— [E.Info.AUM-5-1.AUM.PwdProperty]: Beschreibung für das werkseitig voreingestellte Passwort jedes Authentisierungsmechanismus:

— (wenn die Implementation auf [IC.AUM-5-1.UniqueBestPractice] basiert), wie die Eindeutigkeit und die bewährte Verfahrensweise in Bezug auf Passwortstärken für das Passwort im Hinblick auf den zugrunde liegenden Anwendungsfall der Authentisierung implementiert wird; und

— (wenn die Implementation auf [IC.AUM-5-1.EnforceSettingFirstUse] basiert), wie die Änderung des Passworts bei oder vor der ersten Nutzung erzwungen wird.

[E.Info.DT.AUM-5-1]: Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 13 für jeden in [E.Info.AUM-5-1.AUM] dokumentierten Authentisierungsmechanismus.

[E.Just.DT.AUM-5-1]: Begründung für den gewählten Pfad durch den in [E.Info.DT.AUM-5-1] dokumentierten Entscheidungsbaum mit den folgenden Eigenschaften:

— die Begründung für die Entscheidungen [DT.AUM-5-1.DN-1], [DT.AUM-5-1.DN-2] und [DT.AUM-5-1.DN-3] basieren auf [E.Info.AUM-5-1.AUM.PwdProperty].

#### 6.2.5.5.3 Konzeptuelle Beurteilung

##### 6.2.5.5.3.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob die Authentisierungsmechanismen, die durch AUM-1-1 oder AUM-1-2 erforderlich sind, wie nach AUM-5-1 erforderlich implementiert sind.

##### 6.2.5.5.3.2 Voraussetzungen

Keine.

##### 6.2.5.5.3.3 Beurteilungseinheiten

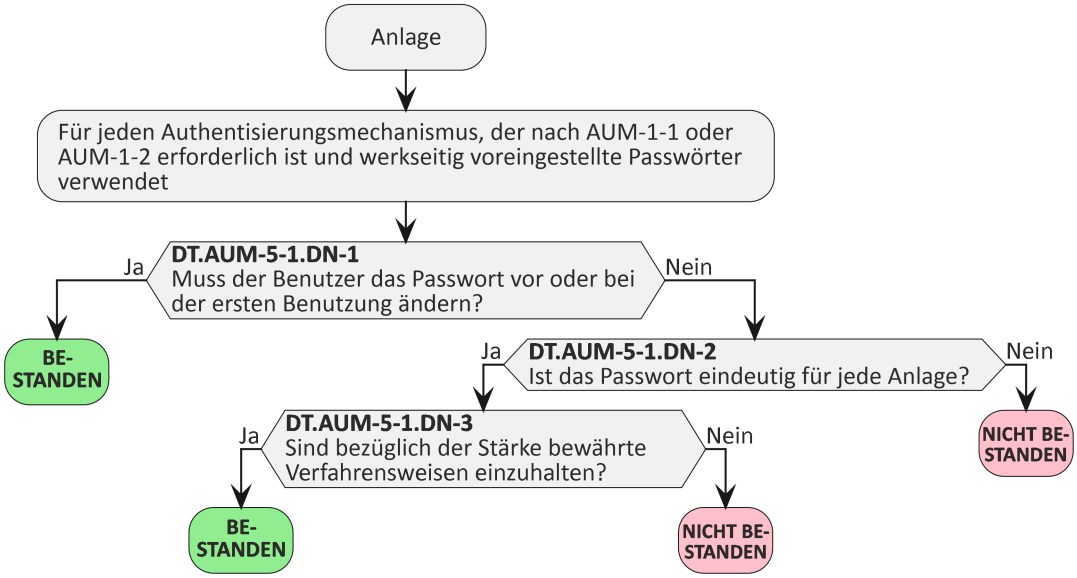



**Bild 13 — Entscheidungsbaum für Anforderung AUM-5-1**

Für jeden in [E.Info.AUM-5-1.AUM] dokumentierten Authentisierungsmechanismus ist zu prüfen, ob der Pfad durch den in [E.Info.DT.AUM-5-1] dokumentierten Entscheidungsbaum mit „BESTANDEN“ endet.

Für jeden in [E.Info.DT.AUM-5-1] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.AUM-5-1] dokumentierte Begründung zu untersuchen.

##### 6.2.5.5.3.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— alle Pfade durch den in [E.Info.DT.AUM-5-1] dokumentierten Entscheidungsbaum mit „BESTANDEN“ enden; und

— die in [E.Just.DT.AUM-5-1] angegebenen Informationen korrekte Begründungen für alle Pfade durch den in [E.Info.DT.AUM-5-1] dokumentierten Entscheidungsbaum sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— ein Pfad durch den in [E.Info.DT.AUM-5-1] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; oder

— eine in [E.Just.DT.AUM-5-1] angegebene Begründung für einen Pfad durch den in [E.Info.DT.AUM-5-1] dokumentierten Entscheidungsbaum nicht korrekt ist oder fehlt.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

#### 6.2.5.5.4 Beurteilung der funktionalen Vollständigkeit

Die Beurteilung der funktionalen Vollständigkeit wird durch die Beurteilung der funktionalen Suffizienz der Anwendbarkeit des Authentisierungsmechanismus abgedeckt.

Deshalb ist diese Beurteilung der funktionalen Vollständigkeit nicht notwendig.

#### 6.2.5.5.5 Beurteilung der funktionalen Suffizienz

##### 6.2.5.5.5.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob die Authentisierungsmechanismen, die nach AUM-1-1 oder AUM-1-2 erforderlich sind, wie nach AUM-5-1 erforderlich implementiert sind.

##### 6.2.5.5.5.2 Voraussetzungen

Die Anlage befindet sich in Werksvoreinstellung und ist nicht in Betrieb genommen.

(Wenn die in [E.Info.AUM-5-1.AUM.PwdProperty] dokumentierte Methode zu [IC.AUM-5-1.UniqueBestPractice] gehört) Das tatsächliche werkseitig voreingestellte Passwort der Anlage ist verfügbar.

##### 6.2.5.5.5.3 Beurteilungseinheiten

Für jeden in [E.Info.AUM-5-1.AUM] dokumentierten Authentisierungsmechanismus:

[AU.AUM-5-1.UniqueBestPractice]: Wenn die in [E.Info.AUM-5-1.AUM.PwdProperty] dokumentierte Methode zu [IC.AUM-5-1.UniqueBestPractice] gehört, ist die Umsetzung der in [E.Info.AUM-5-1.AUM.PwdProperty] dokumentierten Methoden funktional zu bestätigen durch:

— Vergleich der tatsächlichen werkseitig voreingestellten Passwörter mit der in [E.Info.AUM-5-1.AUM.Pwd-Property] enthaltenen Beschreibung der Umsetzung; und

— Inbetriebnahme der Anlage nach der Installationsanweisung und Verifizierung der Gültigkeit der werkseitig voreingestellten Passwörter.

[AU.AUM-5-1.EnforceSettingFirstUse]: Wenn die in [E.Info.AUM-5-1.AUM.PwdProperty] dokumentierte Methode zu [IC.AUM-5-1.EnforceSettingFirstUse] gehört, ist die Umsetzung der in [E.Info.AUM-5-1.AUM.Pwd-Property] dokumentierten Methoden funktional zu bestätigen durch:

— Inbetriebnahme der Anlage nach der Installationsanweisung; und

— Nutzung der werkseitig voreingestellten Passwörter.

##### 6.2.5.5.5.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn kein Nachweis vorliegt, dass eine Umsetzung eines Authentifizierungsmechanismus mit einem werkseitig voreingestellten Passwort von [E.Info.AUM-5-1.AUM.PwdProperty] abweicht.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn ein Nachweis vorliegt, dass eine Umsetzung eines Authentifizierungsmechanismus mit einem werkseitig voreingestellten Passwort von [E.Info.AUM-5-1.AUM.PwdProperty] abweicht.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

#### 6.2.5.6 Beurteilungskriterien für nicht werkseitig voreingestellte Passwörter

##### 6.2.5.6.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung AUM-5-2.

##### 6.2.5.6.1 Umsetzungskategorien

[IC.AUM-5-2.SettingFirstUse]: Der Benutzer ist gezwungen, bei oder vor der ersten Nutzung ein nicht werkseitig voreingestelltes Passwort festzulegen, bevor die Anlage logisch mit einem Netzwerk verbunden wird.

[IC.AUM-5-2.DefinedAuthEntity]: Eine autorisierte Entität definiert ein nicht werkseitig voreingestelltes Passwort innerhalb eines Netzwerks, in dem der Zugang auf autorisierte Entitäten beschränkt ist.

[IC.AUM-5-2.EquipmentGenerated]: Ein nicht werkseitig voreingestelltes Passwort wird von den Anlagen unter Anwendung bewährter Verfahrensweisen in Bezug auf die Stärke erzeugt und nur an eine autorisierte Entität innerhalb eines Netzwerks übermittelt, in dem der Zugang auf autorisierte Entitäten beschränkt ist.

##### 6.2.5.6.2 Erforderliche Informationen

[E.Info.AUM-5-2.AUM]: Beschreibung jedes nach AUM-1-1 (Netzwerkschnittstelle) oder AUM-1-2 (Benutzungsschnittstelle) erforderlichen Authentisierungsmechanismus, der nicht werkseitig voreingestellte Passwörter verwendet, einschließlich:

— [E.Info.AUM-5-2.AUM.PwdProperty]: Beschreibung für das nicht werkseitig voreingestellte Passwort jedes Authentifizierungsmechanismus:

  — (wenn die Implementation auf [IC.AUM-5-2.SettingFirstUse] basiert), wie die Festlegung des Passworts erzwungen wird und die Mittel, um eine logische Netzwerkverbindung vor der Festlegung des Passworts zu verhindern; und

  — (wenn die Implementation auf [IC.AUM-5-2.DefinedAuthEntity] basiert), wie die Festlegung des Passworts auf autorisierte Entitäten beschränkt wird und die Mittel, um eine Festlegung innerhalb eines Netzwerks zu verhindern, in dem der Zugang nicht auf autorisierte Entitäten beschränkt ist; und

  — (wenn die Implementation auf [IC.AUM-5-2.EquipmentGenerated] basiert), wie bewährte Verfahrensweisen in Bezug auf die Passwortstärke hinsichtlich des zugrundeliegenden Anwendungsfalls der Authentisierung und der Mittel zur Verhinderung ihrer Weitergabe an nicht autorisierte Entitäten oder innerhalb eines Netzwerks, in dem der Zugang nicht auf autorisierte Entitäten beschränkt ist, umgesetzt werden.

[E.Info.DT.AUM-5-2]: Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 14 für jeden in [E.Info.AUM-5-2.AUM] dokumentierten Authentisierungsmechanismus.

[E.Just.DT.AUM-5-2]: Begründung für den gewählten Pfad durch den in [E.Info.DT.AUM-5-2] dokumentierten Entscheidungsbaum mit der folgenden Eigenschaft:

— die Begründung für die Entscheidungen [DT.AUM-5-2.DN-1], [DT.AUM-5-2.DN-2] und [DT.AUM-5-2.DN-3] basieren auf [E.Info.AUM-5-2.AUM.PwdProperty].

#### 6.2.5.6.3 Konzeptuelle Beurteilung

##### 6.2.5.6.3.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob die Authentisierungsmechanismen, die nach AUM-1-1 oder AUM-1-2 erforderlich sind, wie nach AUM-5-2 erforderlich implementiert sind.

##### 6.2.5.6.3.2 Voraussetzungen

Keine.

##### 6.2.5.6.3.3 Beurteilungseinheiten

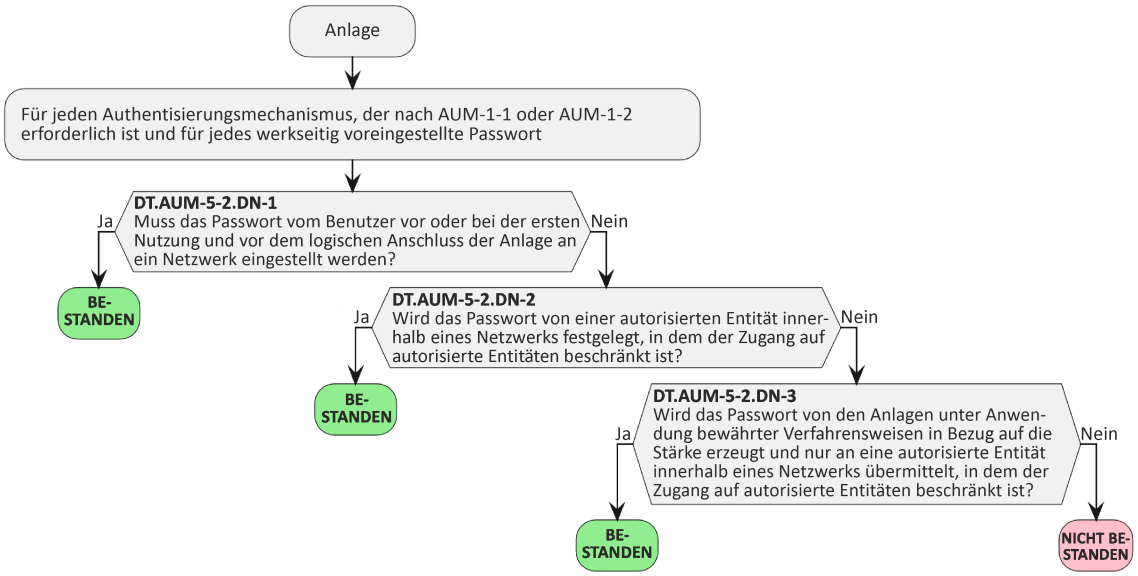



**Bild 14 — Entscheidungsbaum für Anforderung AUM-5-2**

Für jeden in [E.Info.AUM-5-2.AUM] dokumentierten Authentisierungsmechanismus ist zu prüfen, ob der Pfad durch den in [E.Info.DT.AUM-5-2] dokumentierten Entscheidungsbaum mit „BESTANDEN“ endet.

Für jeden in [E.Info.DT.AUM-5-2] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.AUM-5-2] dokumentierte Begründung zu untersuchen.

##### 6.2.5.6.3.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— alle Pfade durch den in [E.Info.DT.AUM-5-2] dokumentierten Entscheidungsbaum mit „BESTANDEN“ enden; und

— die in [E.Just.DT.AUM-5-2] angegebenen Informationen korrekte Begründungen für alle Pfade durch den in [E.Info.DT.AUM-5-2] dokumentierten Entscheidungsbaum sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— ein Pfad durch den in [E.Info.DT.AUM-5-2] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; oder

— eine in [E.Just.DT.AUM-5-2] angegebene Begründung für einen Pfad durch den in [E.Info.DT.AUM-5-2] dokumentierten Entscheidungsbaum nicht korrekt ist oder fehlt.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

#### 6.2.5.6.4 Beurteilung der funktionalen Vollständigkeit

Die Beurteilung der funktionalen Vollständigkeit wird durch die Beurteilung der funktionalen Suffizienz der Anwendbarkeit des Authentisierungsmechanismus abgedeckt.

Deshalb ist diese Beurteilung der funktionalen Vollständigkeit nicht notwendig.

#### 6.2.5.6.5 Beurteilung der funktionalen Suffizienz

##### 6.2.5.6.5.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob die Authentisierungsmechanismen, die nach AUM-1-1 oder AUM-1-2 erforderlich sind, wie nach AUM-5-2 erforderlich implementiert sind.

##### 6.2.5.6.5.2 Voraussetzungen

Die Anlage befindet sich in Werksvoreinstellung und ist nicht in Betrieb genommen.

##### 6.2.5.6.5.3 Beurteilungseinheiten

Für jeden in [E.Info.AUM-5-2.AUM] dokumentierten Authentisierungsmechanismus:

[AU.AUM-5-2.SettingFirstUse]: Wenn die in [E.Info.AUM-5-2.AUM.PwdProperty] dokumentierte Methode zu [IC.AUM-5-2.SettingFirstUse] gehört, ist die Umsetzung der in [E.Info.AUM-5-2.AUM.PwdProperty] dokumentierten Methoden funktional zu bestätigen durch:

— Beobachtung der logischen Konnektivität des Netzwerks der Anlage; und

— Inbetriebnahme der Anlage nach der Installationsanweisung; und

— Nutzung der nicht werkseitig voreingestellten Passwörter.

[AU.AUM-5-2.DefinedAuthEntity]: Wenn die in [E.Info.AUM-5-2.AUM.PwdProperty] dokumentierte Methode zu [IC.AUM-5-2.DefinedAuthEntity] gehört, ist die Umsetzung der in [E.Info.AUM-5-2.AUM.PwdProperty] dokumentierten Methoden funktional zu bestätigen durch:

— Inbetriebnahme der Anlage nach der Installationsanweisung; und

— (wenn die Anlage mit einem Netzwerk verbunden werden kann, dessen Zugang nicht auf autorisierte Entitäten beschränkt ist) die Festlegung der nicht werkseitig voreingestellten Passwörter als autorisierte Entität über ein Netzwerk, dessen Zugang nicht auf autorisierte Entitäten beschränkt ist; und

— Festlegung der nicht werksseitig voreingestellten Passwörter als nicht autorisierte Entität; und

— Festlegung der nicht werkseitig voreingestellten Passwörter als autorisierte Entität über ein Netzwerk, bei dem der Zugang auf autorisierte Entitäten beschränkt ist, oder über eine nicht netzwerkgebundene Schnittstelle.

[AU.AUM-5-2.EquipmentGenerated]: Wenn die in [E.Info.AUM-5-2.AUM.PwdProperty] dokumentierte Methode zu [IC.AUM-5-2.EquipmentGenerated] gehört, ist die Umsetzung der in [E.Info.AUM-5-2.AUM.Pwd-Property] dokumentierten Methoden funktional zu bestätigen durch:

— Inbetriebnahme der Anlage nach der Installationsanweisung; und

— Initialisierung der Generierung von Passwörtern; und

— Erhalt des Passworts als nicht autorisierte Entität; und

— (wenn die Anlage mit einem Netzwerk verbunden werden kann, dessen Zugang nicht auf autorisierte Entitäten beschränkt ist) den Erhalt des Passworts als autorisierte Entität über ein Netzwerk, dessen Zugang nicht auf autorisierte Entitäten beschränkt ist; und

— Festlegung der nicht werkseitig voreingestellten Passwörter als autorisierte Entität über ein Netzwerk, bei dem der Zugang auf autorisierte Entitäten beschränkt ist, oder über eine nicht netzwerkgebundene Schnittstelle.

— Vergleich der erzeugten Passwörter mit der in [E.Info.AUM-5-2.AUM.PwdProperty] enthaltenen Beschreibung der Umsetzung.

#### 6.2.5.6.5.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn kein Nachweis vorliegt, dass eine Umsetzung eines Authentifizierungsmechanismus mit einem nicht werkseitig voreingestellten Passwort von [E.Info.AUM-5-2.AUM.PwdProperty] abweicht.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn ein Nachweis vorliegt, dass eine Umsetzung eines Authentifizierungsmechanismus mit einem nicht werkseitig voreingestellten Passwort von [E.Info.AUM-5-2.AUM.PwdProperty] abweicht.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

### 6.2.6 [AUM-6] Schutz vor Brute-Force-Angriffen

#### 6.2.6.1 Anforderung

Authentisierungsmechanismen, die nach AUM-1-1 oder AUM-1-2 erforderlich sind, müssen gegen Brute-Force-Angriffe resilient sein.

#### 6.2.6.2 Begründung

Ein Angreifer kann versuchen, Massenauthentisierungsversuche zu nutzen, um einen Authentisierungsmechanismus zu überwinden oder um die Geräteverfügbarkeit zu beeinträchtigen. Daher sind Techniken erforderlich, um die Auswirkungen eines solchen Angriffs einzudämmen.

#### 6.2.6.3 Leitlinie

Zu den Techniken für den Brute-Force-Schutz von Authentifizierungsmechanismen gehören z. B.:

— Zeitverzögerungen zwischen aufeinanderfolgenden fehlgeschlagenen Authentisierungsversuchen;

— eine begrenzte Anzahl fehlgeschlagener Authentisierungsversuche, gefolgt von einer Sperrzeit, während der keine Anmeldung zulässig ist;

— Multifaktor-Authentisierung;

— eine angemessene Stärke für Authentisierungswerte auf der Grundlage bewährter Verfahrensweisen für Kryptographie;

— Bei der Machine-to-Machine-Authentifizierung können Maßnahmen zur Risikominderung eingesetzt werden, z. B.:

— langes Passwort (mehr als 16 Zeichen und hohe Komplexität);

— Liste der zulässigen IP-Adressen;

— Warn-/Protokollierungsmechanismus in der Maschine-Maschine-Schnittstelle.

— Abhängig von den implementierten Techniken sind Risiken in Bezug auf das „Aufbrauchen von Ressourcen“ und „Denial-of-Service“ zu berücksichtigen.

Auch ist die Eindämmung von Auswirkungen wiederholter Versuche zum Erlangen einer rechtswidrigen Authentisierung und die Eindämmung des Blockierens von legitimen Zugriffen durch das Auslösen vorgeschalteter Abwehrmechanismen zu berücksichtigen.

Siehe NIST 800-63 Reihe [9].

#### 6.2.6.4 Beurteilungskriterien

##### 6.2.6.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung AUM-6.

##### 6.2.6.4.2 Umsetzungskategorien

[IC.AUM-6.TimeDelay]: Die Methoden zur Resilienz gegenüber Brute-Force-Angriffen beruhen auf Zeitverzögerungen zwischen den Authentisierungsversuchen.

[IC.AUM-6.LimitedAttemps]: Die Methoden zur Resilienz gegenüber Brute-Force-Angriffen beruhen auf einer begrenzten Anzahl von Authentisierungsversuchen.

[IC.AUM-6.AuthenticatorComplexity]: Die Methoden zur Resilienz gegenüber Brute-Force-Angriffen beruhen auf der Komplexität des Authentifikators.

BEISPIEL obligatorische Multifaktor-Authentisierung, CCK mit einer Mindestsicherheitsstufe von 112 Bits wird durchgesetzt

[IC.AUM-6.Generic]: Die Methoden zur Resilienz gegenüber Brute-Force-Angriffen beruhen auf anderen Methoden als [IC.AUM-6.TimeDelay], [IC.AUM-6.LimitedAttemps] oder [IC.AUM-6.AuthenticatorComplexity].

##### 6.2.6.4.3 Erforderliche Informationen

[E.Info.AUM-6.AUM]: Beschreibung jedes Authentisierungsmechanismus, der nach AUM-1-1 (Netzwerkschnittstelle) oder AUM-1-2 (Benutzungsschnittstelle) erforderlich ist, einschließlich:

— [E.Info.AUM-6.AUM.BFProtection]: Beschreibung, wie die Resilienz gegenüber Brute-Force-Angriffen unter Berücksichtigung der Umsetzungskategorien sichergestellt wird.

[E.Info.DT.AUM-6]: Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 15 für jeden in [E.Info.AUM-6.AUM] dokumentierten Authentisierungsmechanismus.

[E.Just.DT.AUM-6]: Begründung für den gewählten Pfad durch den in [E.Info.DT.AUM-6] dokumentierten Entscheidungsbaum mit der folgenden Eigenschaft:

— die Begründung für die Entscheidung [DT.AUM-6.DN-1] basiert auf [E.Info.AUM-6.AUM.BFProtection].

##### 6.2.6.4.4 Konzeptuelle Beurteilung

###### 6.2.6.4.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob die Authentisierungsmechanismen, die nach AUM-1-1 oder AUM-1-2 erforderlich sind, die nach AUM-6 erforderlichen Fähigkeiten besitzen.

#### 6.2.6.4.4.2 Voraussetzungen

Keine.

#### 6.2.6.4.4.3 Beurteilungseinheiten

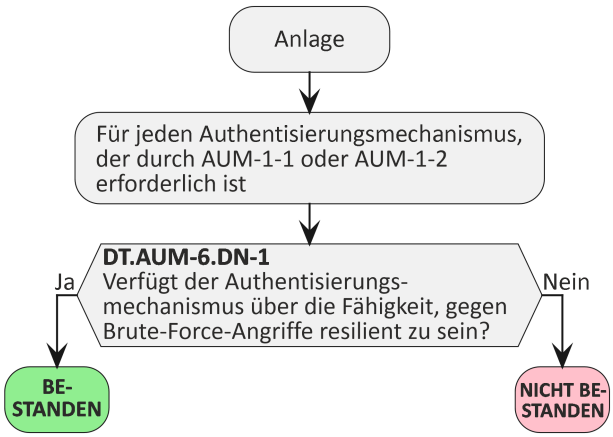



**Bild 15 — Entscheidungsbaum für Anforderung AUM-6**

Für jeden in [E.Info.AUM-6.AUM] dokumentierten Authentisierungsmechanismus ist zu prüfen, ob der Pfad durch den in [E.Info.DT.AUM-6] dokumentierten Entscheidungsbaum mit „BESTANDEN“ endet.

Für jeden in [E.Info.DT.AUM-6] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.AUM-6] dokumentierte Begründung zu untersuchen.

#### 6.2.6.4.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— alle Pfade durch den in [E.Info.DT.AUM-6] dokumentierten Entscheidungsbaum mit „BESTANDEN“ enden; und

— die in [E.Just.DT.AUM-6] angegebenen Informationen korrekte Begründungen für alle Pfade durch den in [E.Info.DT.AUM-6] dokumentierten Entscheidungsbaum sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— ein Pfad durch den in [E.Info.DT.AUM-6] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; oder

— eine in [E.Just.DT.AUM-6] angegebene Begründung für einen Pfad durch den in [E.Info.DT.AUM-6] dokumentierten Entscheidungsbaum nicht korrekt ist oder fehlt.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

#### 6.2.6.4.5 Beurteilung der funktionalen Vollständigkeit

Die Beurteilung der funktionalen Vollständigkeit wird durch die Beurteilung der funktionalen Suffizienz der Anwendbarkeit des Authentisierungsmechanismus abgedeckt.

Deshalb ist diese Beurteilung der funktionalen Vollständigkeit nicht notwendig.

#### 6.2.6.4.6 Beurteilung der funktionalen Suffizienz

##### 6.2.6.4.6.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob die Authentisierungsmechanismen, die nach AUM-1-1 oder AUM-1-2 erforderlich sind, die Anforderung an AUM-6 erfüllen.

##### 6.2.6.4.6.2 Voraussetzungen

Die Anlage befindet sich im Betriebszustand.

##### 6.2.6.4.6.3 Beurteilungseinheiten

Für jeden in [E.Info.AUM-6.AUM] dokumentierten Authentisierungsmechanismus:

[AU.AUM-6.TimeDelay]: Wenn die in [E.Info.AUM-6.AUM.BFProtection] dokumentierte Methode zu [IC.AUM-6.TimeDelay] gehört, ist die Umsetzung der in [E.Info.AUM-6.AUM.BFProtection] dokumentierten Methoden funktional zu bestätigen durch:

— wiederholte Authentifizierungsversuche unter Verwendung falscher Authentifikatoren; und

— Messung der vom Gerät erzwungenen Zeitverzögerungen zwischen aufeinanderfolgenden fehlgeschlagenen Versuchen.

[AU.AUM-6.LimitedAttemps]: Wenn die in [E.Info.AUM-6.AUM.BFProtection] dokumentierte Methode zu [IC.AUM-6.LimitedAttemps] gehört, ist die Umsetzung der in [E.Info.AUM-6.AUM.BFProtection] dokumentierten Methoden funktional zu bestätigen durch:

— wiederholte Authentifizierungsversuche unter Verwendung falscher Authentifikatoren; und

— Zählung der Anzahl an aufeinanderfolgenden fehlgeschlagenen Versuchen, bevor die Anlage weitere Versuche verhindert.

[AU.AUM-6.AuthenticatorComplexity]: Wenn die in [E.Info.AUM-6.AUM.BFProtection] dokumentierte Methode zu [IC.AUM-6.AuthenticatorComplexity] gehört, ist die Umsetzung der in [E.Info.AUM-6.AUM.BFProtection] dokumentierten Methoden funktional zu bestätigen durch:

— Versuch, einen Authentifikator zuzuweisen, der die in [E.Info.AUM-6.AUM.BFProtection] dokumentierten Komplexitätskriterien nicht erfüllt; und

— Durchführung eines Brute-Force-Angriffs auf den Authentisierungsmechanismus.

[AU.AUM-6.Generic]: Wenn die in [E.Info.AUM-6.AUM.BFProtection] dokumentierte Methode zu [IC.AUM-6.Generic] gehört, ist die Umsetzung der in [E.Info.AUM-6.AUM.BFProtection] dokumentierten Methoden funktional zu bestätigen durch:

— Durchführung eines Brute-Force-Angriffs auf den Authentisierungsmechanismus.

##### 6.2.6.4.6.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn für jeden in [E.Info.AUM-6.AUM] dokumentierten Authentisierungsmechanismus die Bestätigungen in der von der Umsetzungskategorie abhängigen Beurteilungseinheit erfolgreich sind.

Die Entscheidung NICHT BESTANDEN für den Beurteilungsfall wird zugewiesen, wenn für einen in [E.Info.AUM-6.AUM] dokumentierten Authentisierungsmechanismus eine Bestätigung in der von der Umsetzungskategorie abhängigen Beurteilungseinheit nicht erfolgreich ist.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

## 6.3 [SUM] Sicherer Aktualisierungsmechanismus (en: Secure Update Mechanism)

### 6.3.1 [SUM-1] Anwendbarkeit von Aktualisierungsmechanismen

#### 6.3.1.1 Anforderung

Die Anlage muss über mindestens einen Aktualisierungsmechanismus für die Aktualisierung von Software, einschließlich Firmware, verfügen, der die Sicherheitswerte und/oder Datenschutzwerte betrifft, außer für Software:

— bei der die Auswirkungen auf die funktionale Sicherheit keine Aktualisierungsfähigkeit erlauben; oder

— die unveränderlich ist; oder

— bei der alternative Maßnahmen die betroffenen Sicherheitswerte und/oder Datenschutzwerte während des gesamten Lebenszyklus der Anlage schützen.

#### 6.3.1.2 Begründung

Die Möglichkeit, Softwareaktualisierungen über einen Aktualisierungsmechanismus bereitzustellen und zu verteilen, ist eine wesentliche Fähigkeit. Er hilft bei der Wartung der Anlagen, bei der Behebung von Sicherheitsschwachstellen und bei der Vorbeugung gegen potentielle Angriffe, die die Anlagen gefährden könnten. Solche Kompromittierungen können das Netzwerk gefährden, seinen Betrieb stören oder zu einer missbräuchlichen Nutzung von Netzwerkressourcen führen, was eine unzumutbare Beeinträchtigung der Dienste zur Folge hat.

Allerdings können manche Softwareteile aus Technologiegründen unveränderlich und somit nicht aktualisierbar sein, oder Auswirkungen auf die funktionale Sicherheit erlauben keine Aktualisierbarkeit. Schwachstellen können auch durch andere Maßnahmen eingedämmt werden, beispielsweise durch den Austausch von anfälligen Geräten während des gesamten Lebenszyklus oder durch die sichere Eindämmung mittels anderer Anlagen, die den Schutz der Sicherheitswerte und Datenschutzwerte sicherstellen.

#### 6.3.1.3 Leitlinie

Es darf mehr als ein Aktualisierungsmechanismus für Teile der Software vorhanden sein. Diese Anforderung verlangt jedoch mindestens einen Aktualisierungsmechanismus für jede Software, der die Sicherheitswerte und/oder Netzwerkwerte betrifft, für die keine Ausnahmekriterien gelten.

Nicht die gesamte Software der Anlage kann aktualisierbar sein. Dazu kann Software gehören, die technologiebedingt oder zur Erfüllung von funktionalen Sicherheitsanforderungen bzw. rechtlichen Anforderungen in einem nicht aktualisierbaren Speicher abgelegt ist.

In manchen Fällen sind alternative Maßnahmen zur Verhinderung von Schäden durch potentielle, öffentlich bekannte ausnutzbare Schwachstellen in Teilen der Software vorhanden, oder eine ausnutzbare Software-Schwachstelle gefährdet die zu schützenden Sicherheitswerte oder Datenschutzwerte möglicherweise nicht. Zum Beispiel:

— Anlagen, für die eine Austauschstrategie vorhanden ist, z. B. Anlagen mit begrenzten Ressourcen (beispielsweise Sensoren, die viele Jahre batteriebetrieben laufen müssen); oder

— Anlagen oder Software-Bestandteile, die sicher isoliert werden können und voraussichtlich werden; oder

— das System, zu dem die Anlage gehört, die Ausnutzung von Schwachstellen eindämmt.

Falls möglich, entspricht es bewährten Verfahren, einen Software-Aktualisierungsmechanismus zu implementieren, der eine Trennung zwischen sicherheitsbezogenen Software-Aktualisierungen und Anwendungssoftware-Aktualisierungen ermöglicht.

#### 6.3.1.4 Beurteilungskriterien

##### 6.3.1.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung SUM-1.

##### 6.3.1.4.2 Umsetzungskategorien

Nicht anwendbar.

##### 6.3.1.4.3 Erforderliche Informationen

[E.Info.SUM-1.PartOfSoftw]: Beschreibung jedes Softwareteils, von dem die Sicherheitswerte und/oder Datenschutzwerte betroffen sind, einschließlich:

— (wenn der Softwareteil aus Gründen der funktionalen Sicherheit nicht aktualisierbar ist) [E.Info.SUM-1.PartOfSoftw.FuncSaftyImp]: Beschreibung:

  — der funktionalen Sicherheitsanforderungen und deren Quelle; und

  — der Funktion der Software in Bezug auf die funktionalen Sicherheitsanforderungen

— (wenn der Teil der Software nicht aktualisierbar ist, weil er unveränderlich ist) [E.Info.SUM-1.PartOfSoftw.Immutable]: Beschreibung der Methoden, die sicherstellen, dass der Softwareteil unveränderlich ist; und

— (wenn der Teil der Software nicht aktualisierbar ist, weil alternative Maßnahmen existieren) [E.Info.SUM-1.PartOfSoftw.AltMeasures]: Beschreibung:

  — der Sicherheitswerte und/oder Datenschutzwerte, die den Softwareteil betrifft; und

  — der alternativen Maßnahmen, die die betroffenen Sicherheitswerte und/oder Datenschutzwerte schützen, insbesondere für den Fall, dass eine öffentlich bekannte ausnutzbare Schwachstelle die Sicherheitswerte und/oder Datenschutzwerte betrifft; und

  — des erwarteten Lebenszyklus der Anlage

— (wenn der Softwareteil aktualisierbar ist) [E.Info.SUM-1.PartOfSoftw.SUM]: Beschreibung der Aktualisierungsmechanismen, die den Softwareteil aktualisieren können.

ANMERKUNG Das vorliegende Dokument legt nicht die Granularität fest, mit der die Software untergliedert wird. Eine in Bezug auf den Dokumentationsaufwand geeignete Untergliederung berücksichtigt die Abdeckung der Softwareteile durch bestimmte Aktualisierungsmechanismen.

[E.Info.DT.SUM-1]: Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 16 für jeden in [E.Info.SUM-1.PartOfSoftw] dokumentierten Softwareteil.

[E.Just.DT.SUM-1]: Begründung für den gewählten Pfad durch den in [E.Info.DT.SUM-1] dokumentierten Entscheidungsbaum mit den folgenden Eigenschaften:

— (wenn eine Entscheidung aus [DT.SUM-1.DN-1] zu „NICHT ANWENDBAR“ führt) basiert die Begründung für die Entscheidung [DT.SUM-1.DN-1] auf [E.Info.SUM-1.PartOfSoftw.FuncSaftyImp]; und

— (wenn eine Entscheidung aus [DT.SUM-1.DN-2] zu „NICHT ANWENDBAR“ führt) basiert die Begründung für die Entscheidung [DT.SUM-1.DN-2] auf [E.Info.SUM-1.PartOfSoftw.Immutable]; und

— (wenn eine Entscheidung aus [DT.SUM-1.DN-3] zu „NICHT ANWENDBAR“ führt) basiert die Begründung für die Entscheidung [DT.SUM-1.DN-3] auf [E.Info.SUM-1PartOfSoftw.AltMeasures].

#### 6.3.1.4.4 Konzeptuelle Beurteilung

##### 6.3.1.4.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob ein Aktualisierungsmechanismus implementiert wurde, wo er nach SUM-1 erforderlich ist.

##### 6.3.1.4.4.2 Voraussetzungen

Keine.

##### 6.3.1.4.4.3 Beurteilungseinheiten

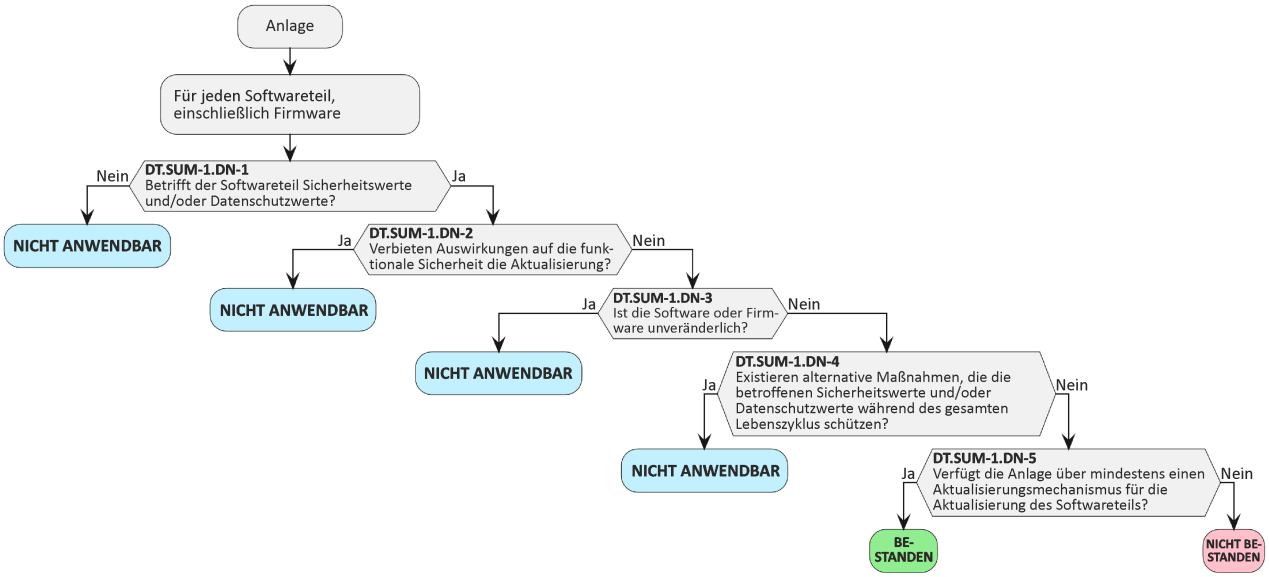



**Bild 16 — Entscheidungsbaum für Anforderung SUM-1**

Für jeden Teil der in [E.Info.SUM-1.PartOfSoftw] dokumentierten Software ist zu prüfen, ob der Pfad durch den in [E.Info.DT.SUM-1] dokumentierten Entscheidungsbaum mit „NICHT ANWENDBAR“ oder „BESTANDEN“ endet.

Für jeden Pfad durch den in [E.Info.DT.SUM-1] dokumentierten Entscheidungsbaum ist zu überprüfen, ob die in [E.Just.DT.SUM-1] dokumentierte Begründung die von der Software betroffenen Sicherheitswerte und/oder Datenschutzwerte beschreibt und ob die Software aktualisierbar ist, und wenn nicht, die Gründe dafür.

##### 6.3.1.4.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— mindestens ein Pfad durch den in [E.Info.DT.SUM-1] dokumentierten Entscheidungsbaum mit „BESTANDEN“ endet; und

— kein Pfad durch den in [E.Info.DT.SUM-1] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; und

— die in [E.Just.DT.SUM-1] angegebenen Informationen korrekte Begründungen für alle Pfade durch den in [E.Info.DT.SUM-1] dokumentierten Entscheidungsbaum sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— ein Pfad durch den in [E.Info.DT.SUM-1] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; oder

— eine in [E.Just.DT.SUM-1] angegebene Begründung für einen Pfad durch den in [E.Info.DT.SUM-1] dokumentierten Entscheidungsbaum nicht korrekt ist oder fehlt.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

#### 6.3.1.4.5 Beurteilung der funktionalen Vollständigkeit

Keine.

#### 6.3.1.4.6 Beurteilung der funktionalen Suffizienz

##### 6.3.1.4.6.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob die Anlage Aktualisierungsmechanismen für Teile der Software unterstützt, von denen Sicherheitswerte und/oder Datenschutzwerte betroffen sind, wie in [E.Info.SUM-1.PartOfSoftw.SUM] dokumentiert.

##### 6.3.1.4.6.2 Voraussetzungen

Die Anlage befindet sich im Betriebszustand.

Für jeden in [E.Info.SUM-1.PartOfSoftw.SUM] beschriebenen Aktualisierungsmechanismus stellt der Hersteller aktualisierte Software zur Verfügung (im Folgenden: SW-a), deren Integrität und Authentizität durch einen Mechanismus geschützt ist, den die Anlage von Haus aus unterstützt.

##### 6.3.1.4.6.3 Beurteilungseinheiten

Für jeden in [E.Info.SUM-1.PartOfSoftw.SUM] dokumentierten Aktualisierungsmechanismus, der in der konzeptuellen Beurteilung von SUM-1 mit der Entscheidung BESTANDEN endet, ist SW-a auf der Anlage zu installieren.

##### 6.3.1.4.6.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn kein Nachweis vorliegt, dass eine Installation von SW-a für einen in [E.Info.SUM-1.PartOfSoftw.SUM] dokumentierten Aktualisierungsmechanismus nicht erfolgreich ist.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn ein Nachweis vorliegt, dass eine Installation von SW-a für einen in [E.Info.SUM-1.PartOfSoftw.SUM] dokumentierten Aktualisierungsmechanismus nicht erfolgreich ist.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

### 6.3.2 [SUM-2] Sichere Aktualisierungen

#### 6.3.2.1 Anforderung

Jeder Aktualisierungsmechanismus nach den Anforderungen von SUM-1 darf nur Software installieren, deren Integrität und Authentizität zum Zeitpunkt der Installation gültig ist.

#### 6.3.2.2 Begründung

Ein sicherer Software-Aktualisierungsmechanismus stellt sicher, dass die Software zur Kontrolle der Anlage nicht über Angriffe des Aktualisierungsmechanismus manipuliert wird.

#### 6.3.2.3 Leitlinie

Ein häufiger Ansatz zur Bestätigung, dass eine Aktualisierung gültig ist, soll kryptographisch deren Integrität und Authentizität anhand eines Vertrauensankers verifizieren. Dies kann auf der Anlage geschehen oder durch ein anderes vertrauenswürdiges Gerät, das die Verifizierung durchführt. Im letzteren Fall wird die verifizierte Aktualisierung üblicherweise über einen sicheren Kanal an das auf der Anlage sicher installierte Gerät gesendet.

ANMERKUNG Ein „sicherer Kanal“ erhält üblicherweise die Sicherheitseigenschaften der übertragenen Informationen und kann auch beinhalten, dass autorisierte und authentifizierte Personen die validierte Software-Aktualisierung lokal bereitstellen (Beispiel für technische oder organisatorische Maßnahmen).

Ein Hersteller kann ein sicheres Verfahren zur Installation alternativer, nicht vom Hersteller selbst bereitgestellter Software anbieten; beispielsweise kann es einem Benutzer erlaubt sein, auf einem Home-Router eine alternative Software zu installieren.

Es entspricht bewährten Verfahrensweisen für Sicherheit, den Downgrade von Software auf eine ältere Version zu verhindern.

Aufgrund einiger Sicherheitsaktualisierungen kehrt das Produkt möglicherweise zu den Standardeinstellungen zurück und erfordert die erneute Eingabe von Anmeldedaten und Konfigurationsdaten.

Die Nutzung von SCM-3 ist angemessen, wenn eine Softwareaktualisierung vertrauliche kryptographische Schlüssel enthält.

#### 6.3.2.4 Beurteilungskriterien

##### 6.3.2.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung SUM-2.

##### 6.3.2.4.2 Umsetzungskategorien

[IC.SUM-2.AuthIntVal.Sign]: Die Methoden zur Validierung der Integrität und Authentizität der Software beruhen ausschließlich auf digitalen Signaturen für Softwareaktualisierungen durch autorisierte Entitäten.

[IC.SUM-2.AuthIntVal.SecChan]: Die Methoden zur Validierung der Integrität und Authentizität der Software beruhen ausschließlich auf einem sicheren Kommunikationsmechanismus zur Quelle der autorisierten Softwareaktualisierung, wie in SCM-1 und SCM-2 gefordert.

[IC.SUM-2.AuthIntVal.AccContMech]: Die Methoden zur Validierung der Integrität und Authentizität der Software beruhen ausschließlich auf Zugangssteuerungsmechanismen, die nur Aktualisierungen durch autorisierte Entitäten nach den Anforderungen von ACM-1 in Kombination mit einer Hash-geschützten Softwareaktualisierung zulassen.

[IC.SUM-2.AuthIntVal.Generic]: Die Methoden zur Validierung der Integrität und Authentizität der Software unterscheiden sich von [IC.SUM-2.AuthIntVal.Sign], [IC.SUM-2.AuthIntVal.SecChan] oder [IC.SUM-2.AuthIntVal.AccContMech].

##### 6.3.2.4.3 Erforderliche Informationen

[E.Info.SUM-2.SUM]: Beschreibung jedes Aktualisierungsmechanismus, der einen Teil der in [E.Info.SUM-1.PartOfSoftw] dokumentierten Software aktualisieren kann, einschließlich:

— (wenn die Implementation auf [IC.SUM-2.AuthIntVal.Sign] basiert) [E.Info.SUM-2.SUM.Sign]: Beschreibung des verwendeten digitalen Signaturverfahrens mit einer Beschreibung der zugrunde liegenden bewährten Kryptographie nach [E.Info.CRY-1.Assets.Cryptography]; und

— (wenn die Implementation auf [IC.SUM-2.AuthIntVal.SecChan] basiert) [E.Info.SUM-2.SUM.SecChan]: Beschreibung des sicheren Kommunikationsmechanismus nach [E.Info.SCM-1.SCM] mit einer Beschreibung der zugrunde liegenden bewährten Kryptographie nach [E.Info.CRY-1.Assets.Cryptography]; und

— (wenn die Implementation auf [IC.SUM-2.AuthIntVal.AccContMech] basiert) [E.Info.SUM-2.SUM.AccContMech]: Beschreibung des Zugangssteuerungsmechanismus nach [E.Info.ACM-2.SecurityAsset.ACM] und der Hash-Funktion nach [E.Info.CRY-1.Assets.Cryptography]; und

— (wenn die Implementation auf [IC.SUM-2.AuthIntVal.Generic] basiert) [E.Info.SUM-2.SUM.Generic]: Beschreibung der Methoden zur Validierung der Integrität und Authentizität der Software.

[E.Info.DT.SUM-2]: Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 17 für jeden in [E.Info.SUM-2.SUM] dokumentierten Aktualisierungsmechanismus.

[E.Just.DT.SUM-2]: Begründung für den gewählten Pfad durch den in [E.Info.DT.SUM-2] dokumentierten Entscheidungsbaum mit den folgenden Eigenschaften:

— (wenn die Implementation auf [IC.SUM-2.AuthIntVal.Sign] basiert) die Begründung für die Entscheidung [DT.SUM-2.DN-1] auf [E.Info.SUM-2.SUM.Sign] basiert; und

— (wenn die Implementation auf [IC.SUM-2.AuthIntVal.SecChan] basiert) die Begründung für die Entscheidung [DT.SUM-2.DN-1] auf [E.Info.SUM-2.SUM.SecChan] basiert; und

— (wenn die Implementation auf [IC.SUM-2.AuthIntVal.AccContMech] basiert) die Begründung für die Entscheidung [DT.SUM-2.DN-1] auf [E.Info.SUM-2.SUM.AccContMech] basiert; und

— (wenn die Implementation auf [IC.SUM-2.AuthIntVal.Generic] basiert) die Begründung für die Entscheidung [DT.SUM-2.DN-1] auf [E.Info.SUM-2.SUM.Generic] basiert.

#### 6.3.2.4.4 Konzeptuelle Beurteilung

##### 6.3.2.4.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob die Aktualisierungsmechanismen nach SUM-1 nur die nach SUM-2 geforderte Software installieren.

##### 6.3.2.4.4.2 Voraussetzungen

Keine.

#### 6.3.2.4.4.3 Beurteilungseinheiten

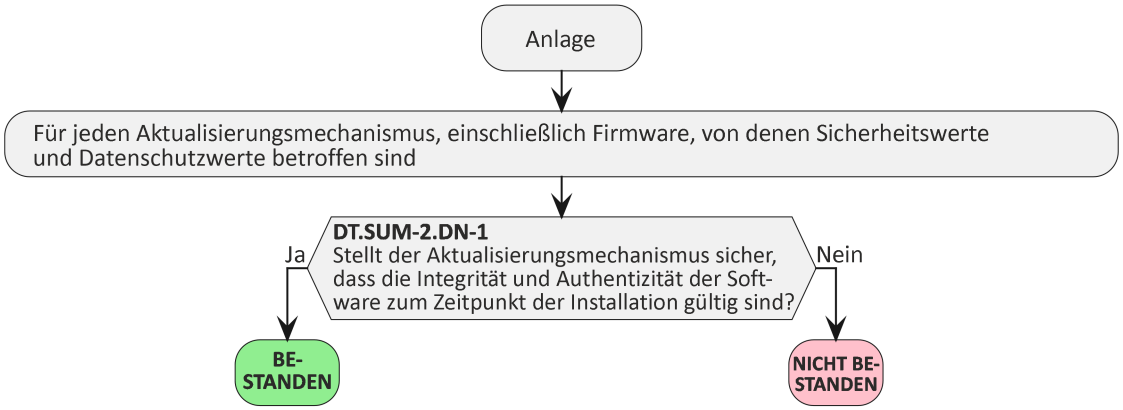



**Bild 17 — Entscheidungsbaum für Anforderung SUM-2**

Für jeden in [E.Info.SUM-2.SUM] dokumentierten Aktualisierungsmechanismus ist zu prüfen, ob der Pfad durch den in [E.Just.DT.SUM-2] dokumentierten Entscheidungsbaum mit „BESTANDEN“ endet.

Für jeden Pfad durch den in [E.Info.DT.SUM-2] dokumentierten Entscheidungsbaum ist zu überprüfen, ob die in [E.Just.DT.SUM-2] dokumentierte Begründung anhand von Verweisungen auf [E.Info.SUM-2.SUM.Sign] die Methoden zur Sicherstellung der Gültigkeit der Integrität und Authentizität der Software zum Zeitpunkt der Installation beschreibt.

#### 6.3.2.4.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— alle Pfade durch den in [E.Info.DT.SUM-2] dokumentierten Entscheidungsbaum mit „BESTANDEN“ enden; und

— die in [E.Just.DT.SUM-2] angegebenen Informationen korrekte Begründungen für alle Pfade durch den in [E.Info.DT.SUM-2] dokumentierten Entscheidungsbaum sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— ein Pfad durch den in [E.Info.DT.SUM-2] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; oder

— eine in [E.Just.DT.SUM-2] angegebene Begründung für einen Pfad durch den in [E.Info.DT.SUM-2] dokumentierten Entscheidungsbaum nicht korrekt ist oder fehlt.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

#### 6.3.2.4.5 Beurteilung der funktionalen Vollständigkeit

Die Beurteilung der funktionalen Vollständigkeit wird durch die Beurteilung der funktionalen Suffizienz der Anwendbarkeit des sicheren Aktualisierungsmechanismus abgedeckt.

Deshalb ist diese Beurteilung der funktionalen Vollständigkeit nicht notwendig.

#### 6.3.2.4.6 Beurteilung der funktionalen Suffizienz

##### 6.3.2.4.6.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob die Aktualisierungsmechanismen für Softwareteile, von denen Sicherheitswerte und/oder Datenschutzwerte betroffen sind, nur Software installieren, deren Integrität und Authentizität zum Zeitpunkt der Installation gültig sind, wie in [E.Info.SUM-2.SUM] dokumentiert.

##### 6.3.2.4.6.2 Voraussetzungen

Die Anlage befindet sich im Betriebszustand.

##### 6.3.2.4.6.3 Beurteilungseinheiten

Für jeden in [E.Info.SUM-2.SUM] dokumentierten Aktualisierungsmechanismus:

[AU.SUM-2.Sign]: Wenn die Umsetzung auf [IC.SUM-2.AuthIntVal.Sign] basiert, ist funktional zu bestätigen, dass:

— es unter Verwendung der bewährten Verfahrensweisen für Kryptographie nach CRY-1 implementiert wird; und

— eine unsignierte Softwareaktualisierung nicht installiert wird; und

— eine Softwareaktualisierung mit einer geänderten Signatur nicht installiert wird; und

— eine geänderte Softwareaktualisierung mit einer gültigen Signatur für die unveränderte Softwareaktualisierung nicht installiert wird; und

— eine Softwareaktualisierung mit einer Signatur von einer nicht autorisierten Entität nicht installiert wird.

[AU.SUM-2.SecChan]: Wenn die Umsetzung auf [IC.SUM-2.AuthIntVal.SecChan] basiert, ist funktional zu bestätigen, dass:

— es unter Verwendung des sicheren Kommunikationsmechanismus nach SCM implementiert wird; und

— eine Softwareaktualisierung von einer unbefugten Quelle nicht installiert wird; und

— der sichere Kommunikationskanal es nicht zulässt, sich über einen Man-in-the-Middle-Angriff als die autorisierte Softwareaktualisierungsquelle auszugeben; und

— eine Softwareaktualisierung, die während der Kommunikation modifiziert wird, nicht installiert wird.

[AU.SUM-2.AccContMech]: Wenn die Umsetzung auf [IC.SUM-2.AuthIntVal.AccContMech] basiert, ist funktional zu bestätigen, dass:

— es unter Verwendung des Zugangssteuerungsmechanismus nach ACM implementiert wird; und

— eine geänderte Softwareaktualisierung mit einem gültigen Hash für die unveränderte Softwareaktualisierung nicht installiert wird; und

— eine Softwareaktualisierung mit einem Hash, der mit einer nicht unterstützten Hash-Funktion erzeugt wurde, nicht installiert wird; und

— eine von einer nicht autorisierten Entität bereitgestellten Softwareaktualisierung nicht installiert wird.

[AU.SUM-2.Generic]: Wenn die Umsetzung auf [IC.SUM-2.AuthIntVal.Generic] basiert, ist funktional zu bestätigen, dass:

— eine Softwareaktualisierung, deren Integrität nicht gültig ist, nicht installiert wird und

— eine Softwareaktualisierung, deren Authentizität nicht gültig ist, nicht installiert wird.

#### 6.3.2.4.6.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn für jeden in [E.Info.SUM-2.SUM] dokumentierten Aktualisierungsmechanismus die Bestätigungen in der von der Umsetzungskategorie abhängigen Beurteilungseinheit erfolgreich sind.

Die Entscheidung NICHT BESTANDEN für den Beurteilungsfall wird zugewiesen, wenn für einen in [E.Info.SUM-2.SUM] dokumentierten Aktualisierungsmechanismus eine Bestätigung in der von der Umsetzungskategorie abhängigen Beurteilungseinheit nicht erfolgreich ist.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

### 6.3.3 [SUM-3] Automatisierte Aktualisierungen

#### 6.3.3.1 Anforderung

Wenn die Anlage internetfähig ist, muss jeder Aktualisierungsmechanismus, der nach SUM-1 erforderlich ist, in der Lage sein, die Software zu aktualisieren:

— ohne menschlichen Eingriff am Gerät; oder

— durch Zeitsteuerung der Installation einer Aktualisierung mit menschlicher Zustimmung; oder

— durch Auslösung der Installation einer Aktualisierung mit menschlicher Zustimmung oder Aufsicht, wenn unerwartete Schäden in der Betriebsumgebung vermieden werden müssen.

#### 6.3.3.2 Begründung

Falls eine öffentlich bekannte ausnutzbare Schwachstelle der Anlage vorhanden ist, durch die Sicherheitswerte und Datenschutzwerte kompromittiert werden können, kann durch einen automatisierten Aktualisierungsmechanismus sichergestellt werden, dass eine verfügbare, diese Schwachstelle betreffende Sicherheitsaktualisierung ohne oder mit minimalem menschlichen Eingriff installiert wird und so die Ausnutzung der Schwachstelle verhindert.

#### 6.3.3.3 Leitlinie

Diese Anforderung verlangt mindestens einen automatisierten Aktualisierungsmechanismus für jede Software, bei der SUM-1 einen Aktualisierungsmechanismus erfordert.

ANMERKUNG 1 Ein automatisierter Aktualisierungsmechanismus kann für die Aktualisierung mehrerer Teile der Software verwendet werden.

Automatisierte Aktualisierungen werden von Maschinen durchgeführt, die keine oder nur eine minimale menschliche Kontrolle oder Eingriffe benötigen.

Automatisierte Aktualisierungen sind ein weiterer Schritt, bei dem die Anlage selbständig Entscheidungen trifft und Aktualisierungen ohne menschliches Eingreifen durchführt.

In spezifischen Fällen, in denen sicherheits- oder zeitkritische Aspekte bzw. die Abhängigkeit von der Kompatibilität der Aktualisierungen in einem Netzwerk betroffen sind, können vor dem Anstoßen der Aktualisierung unter Umständen einige Vorsichtsmaßnahmen und/oder Verifizierungen vor Ort erforderlich sein, und diese

kann daher nicht automatisiert durchgeführt werden, um den Betrieb der Anwendung nicht zu beeinträchtigen. In solchen Fällen ist ein menschliches Eingreifen zum Auslösen oder Planen der Aktualisierung erforderlich.

Falls die Installation der neuen Softwareversion fehlschlägt, d. h. die Validierung des/der Software-Images nicht erfolgreich ist, ist eine bewährte Verfahrensweise die Anwendung eines Rollback-Verfahrens, um die vorherige Softwareversion wieder zu aktivieren, es sei denn, es steht nicht genügend Speicherplatz zur Verfügung, um die Aktualisierung abzuspeichern.

Das Auslösen der Installation einer Aktualisierung mit menschlicher Zustimmung kann beispielsweise darin bestehen, dass eine Meldung angezeigt wird, dass eine Aktualisierung verfügbar ist, und der Benutzer aufgefordert wird, die Aktualisierung über einen sicheren Aktualisierungsmechanismus zu installieren.

Aus Benutzersicht einfache automatisierte Aktualisierungen verbessern die Verteilungsrate von Sicherheitsaktualisierungen.

ANMERKUNG 2 „Einfach aus Benutzersicht“ kann Folgendes einschließen:

— eine einfache Konfiguration von Mitteilungen bezüglich des sicheren Aktualisierungsmechanismus,

— eine einfache Konfiguration des Aktualisierungsmechanismus

— die einfache Erteilung einer Zustimmung zu vollständig automatischen Aktualisierungen

Wenn vollständig automatisierte Aktualisierungsmechanismen möglich sind, verbessert das Einholen der Zustimmung des Benutzers bei der Inbetriebnahme der Anlage die Verteilungsrate von Sicherheitsaktualisierungen.

Die Prüfung der Verfügbarkeit neuer Sicherheitsaktualisierungen nach der Initialisierung und in regelmäßigen Abständen verbessert die Verteilungsrate von Sicherheitsaktualisierungen.

#### 6.3.3.4 Beurteilungskriterien

##### 6.3.3.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung SUM-3.

##### 6.3.3.4.2 Umsetzungskategorien

Nicht anwendbar.

##### 6.3.3.4.3 Erforderliche Informationen

[E.Info.SUM-3.SUM]: Beschreibung jedes nach SUM-1 erforderlichen Aktualisierungsmechanismus, einschließlich:

— [E.Info.SUM-3.SUM.Automation]: Beschreibung des Mittels zur Automatisierung des Aktualisierungsmechanismus.

[E.Info.DT.SUM-3]: Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 18 für jeden in [E.Info.SUM-3.SUM] dokumentierten Aktualisierungsmechanismus.

[E.Just.DT.SUM-3]: Begründung für den gewählten Pfad durch den in [E.Info.DT.SUM-3] dokumentierten Entscheidungsbaum mit den folgenden Eigenschaften:

— die Begründung für die Entscheidung [DT.SUM-3.DN-2], [DT.SUM-3.DN-3] und [DT.SUM-3.DN-4] basiert auf [E.Info.SUM-3.SUM.Automation].

#### 6.3.3.4.4 Konzeptuelle Beurteilung

##### 6.3.3.4.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die Vorgabe, ob jeder Aktualisierungsmechanismus automatisierte Aktualisierungen unterstützt, wie dokumentiert in [E.Info.SUM-3.SUM.Automation] nach den Anforderungen von SUM-3.

##### 6.3.3.4.4.2 Voraussetzungen

Keine.

##### 6.3.3.4.4.3 Beurteilungseinheiten

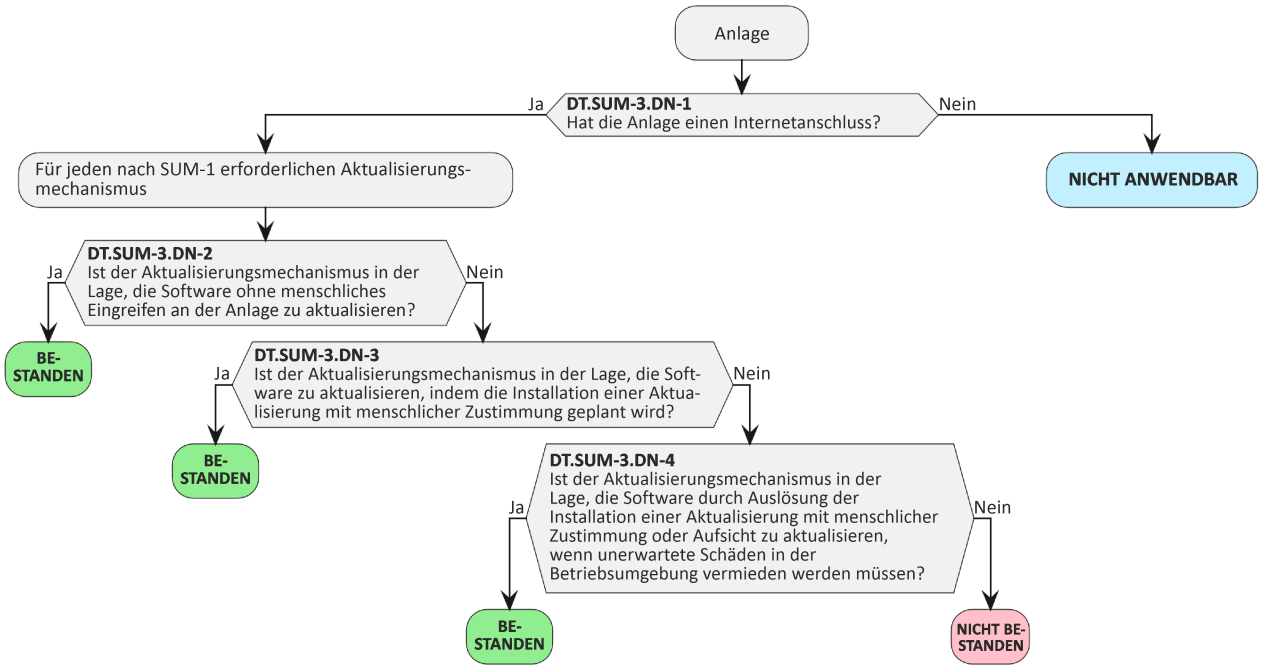



**Bild 18 — Entscheidungsbaum für Anforderung SUM-3**

Für jeden Aktualisierungsmechanismus ist zu prüfen, ob der Pfad durch den in [E.Info.DT.SUM-3] dokumentierten Entscheidungsbaum mit „BESTANDEN“ oder „NICHT BESTANDEN“ endet.

Für jeden in [E.Info.DT.SUM-3] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.SUM-3] dokumentierte Begründung zu untersuchen.

##### 6.3.3.4.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— alle Pfade durch den in [E.Info.DT.SUM-3] dokumentierten Entscheidungsbaum mit „BESTANDEN“ enden; und

— die in [E.Just.DT.SUM-3] angegebenen Informationen korrekte Begründungen für alle Pfade durch den in [E.Info.DT.SUM-3] dokumentierten Entscheidungsbaum sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— ein Pfad durch den in [E.Info.DT.SUM-3] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; oder

— eine in [E.Just.DT.SUM-3] angegebene Begründung für einen Pfad durch den in [E.Info.DT.SUM-3] dokumentierten Entscheidungsbaum nicht korrekt ist oder fehlt.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

#### 6.3.3.4.5 Beurteilung der funktionalen Vollständigkeit

Die Beurteilung der funktionalen Vollständigkeit wird durch die Beurteilung der funktionalen Suffizienz der Anwendbarkeit des sicheren Aktualisierungsmechanismus abgedeckt.

Deshalb ist diese Beurteilung der funktionalen Vollständigkeit nicht notwendig.

#### 6.3.3.4.6 Beurteilung der funktionalen Suffizienz

##### 6.3.3.4.6.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob die Aktualisierungsmechanismen für Teile der Software, von denen Sicherheitswerte und/oder Datenschutzwerte betroffen sind, automatisiert sind, wie in [E.Info.SUM-3.SUM.Automation] dokumentiert.

##### 6.3.3.4.6.2 Voraussetzungen

Die Anlage befindet sich im Betriebszustand.

Der Hersteller bietet das Mittel zur Durchführung automatisierter Aktualisierungen.

##### 6.3.3.4.6.3 Beurteilungseinheiten

Für jeden in [E.Info.SUM-3.SUM] dokumentierten Aktualisierungsmechanismus ist funktional zu beurteilen, ob die Umsetzung der Automatisierung von [E.Info.SUM-3.SUM.Automation] abweicht durch:

— Prüfung der Softwareversion auf der Anlage; und

— Bereitstellung einer Softwareaktualisierung an der Quelle, die Sicherheitsaktualisierungen bereithält; und

— Prüfung, ob die Anlage die Softwareaktualisierung durchführt:

  — ohne menschlichen Eingriff an der Anlage; oder

  — durch Zeitsteuerung der Installation einer Aktualisierung mit menschlicher Zustimmung; oder

  — durch Auslösung der Installation einer Aktualisierung mit menschlicher Zustimmung; und

— Prüfung auf der Anlage, ob die Softwareversion auf eine neue Versionsnummer aktualisiert wurde.

##### 6.3.3.4.6.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn kein Nachweis vorliegt, dass die Umsetzung eines nach SUM-1 erforderlichen Aktualisierungsmechanismus von [E.Info.SUM-3.SUM] abweicht.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn ein Nachweis vorliegt, dass die Umsetzung eines nach SUM-1 erforderlichen Aktualisierungsmechanismus von [E.Info.SUM-3.SUM] abweicht.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

## 6.4 [SSM] Sicherer Speichermechanismus (en: Secure Storage Mechanism)

### 6.4.1 [SSM-1] Anwendbarkeit von sicheren Speichermechanismen

#### 6.4.1.1 Anforderung

Die Anlage muss immer sichere Speichermechanismen nutzen, um die dauerhaft auf der Anlage gespeicherten Sicherheitswerte und Datenschutzwerte zu schützen, mit Ausnahme von dauerhaft gespeicherten Sicherheitswerten und Datenschutzwerten, bei denen:

— die physischen oder logischen Maßnahmen in der Zielumgebung sicherstellen, dass nur autorisierten Entitäten die Zugänglichkeit zu den auf der Anlage gespeicherten Sicherheitswerten oder Datenschutzwerten ermöglicht wird.

#### 6.4.1.2 Begründung

Sichere Speichermechanismen schützen Sicherheitswerte und Datenschutzwerte gegen unbefugten Zugriff. Wenn Sicherheitswerte oder Datenschutzwerte nicht angemessen gesichert werden, kann ein Angreifer auf die Werte zugreifen, sie manipulieren oder löschen und die Anlage kompromittieren, was zu einer Offenlegung personenbezogener Informationen führen könnte.

#### 6.4.1.3 Leitlinie

Die Sicherheitswerte und Datenschutzwerte können beispielsweise folgendermaßen geschützt werden:

— durch kryptographische Maßnahmen wie Verschlüsselung, um die Vertraulichkeit sicherzustellen,

— durch kryptographische Maßnahmen wie digitale Signaturen, um die Integrität und Authentizität sicherzustellen,

— durch Zugangssteuerung mithilfe von Authentisierung oder Autorisierung,

— durch Hardware-Schutzmaßnahmen,

— durch physische Schutzmaßnahmen.

Der angemessene Schutzmechanismus hängt vom Risiko in Verbindung mit den zu speichernden Sicherheitswerten und Datenschutzwerten ab; dieses kann abhängen von:

— der Kritikalität der Sicherheitswerte und Datenschutzwerte;

— der Anzahl der Sicherheitswerte und Datenschutzwerte;

— der Zeitspanne, während der die Sicherheitswerte und Datenschutzwerte gespeichert werden müssen;

— der für die Nutzung vorgesehenen Betriebsumgebung.

Ein Wechselspeicher, der zum Zeitpunkt des Inverkehrbringens nicht Teil der Anlage ist, wird nicht als dauerhafter Speicher betrachtet, sondern als ein Speicher, der dazu dient, Sicherheitswerte oder Datenschutzwerte zwischen verschiedenen Anlagen zu verschieben. Um einen solchen Speicher aus der Anlage zu entfernen, ist ein physischer Zugang zum Gerät erforderlich. Dadurch wird sichergestellt, dass nur autorisierte Entitäten, die physischen Zugang zu den Anlagen haben, Zugriff auf die gespeicherten Sicherheitswerte oder Datenschutzwerte haben.

Dauerhaft gespeicherte Daten, die nicht als Sicherheitswerte oder Datenschutzwerte aufgeführt sind, sind möglicherweise durch den sicheren Speichermechanismus geschützt, fallen aber nicht in den Anwendungsbereich dieser Anforderung.

#### 6.4.1.4 Beurteilungskriterien

##### 6.4.1.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung SSM-1.

##### 6.4.1.4.2 Umsetzungskategorien

Nicht anwendbar.

##### 6.4.1.4.3 Erforderliche Informationen

[E.Info.SSM-1.SecurityAsset]: Beschreibung jedes Sicherheitswertes, der dauerhaft auf der Anlage gespeichert ist, einschließlich für jeden seiner dauerhaften Speicher:

— (wenn angegeben wird, dass ein sicherer Speichermechanismus nicht erforderlich ist, weil physische oder logische Maßnahmen in der Zielbetriebsumgebung der Umgebung sicherstellen, dass der Zugriff auf den gespeicherten Sicherheitswert auf autorisierte Entitäten beschränkt ist) [E.Info.SSM-1.SecurityAsset.Environment]: Beschreibung:

  — der physischen oder logischen Maßnahmen in der Zielbetriebsumgebung der Anlage; und

  — der Art und Weise der Authentisierung/Autorisierung von Entitäten in der Zielbetriebsumgebung der Anlage; und

— (wenn der dauerhafte Speicher durch einen sicheren Speichermechanismus bereitgestellt wird) [E.Info.SSM-1.SecurityAsset.SSM]: Beschreibung des sicheren Speichermechanismus.

[E.Info.SSM-1.PrivacyAsset]: Beschreibung jedes Datenschutzwertes, der dauerhaft auf der Anlage gespeichert ist, einschließlich für jeden seiner dauerhaften Speicher:

— (wenn angegeben wird, dass ein sicherer Speichermechanismus nicht erforderlich ist, weil physische oder logische Maßnahmen in der Zielbetriebsumgebung der Umgebung sicherstellen, dass der Zugriff auf den gespeicherten Datenschutzwert auf autorisierte Entitäten beschränkt ist) [E.Info.SSM-1.PrivacyAsset.Environment]: Beschreibung:

  — der physischen oder logischen Maßnahmen in der Zielbetriebsumgebung der Anlage; und

  — der Art und Weise der Authentisierung/Autorisierung von Entitäten in der Zielbetriebsumgebung der Anlage; und

— (wenn angegeben wird, dass der dauerhafte Speicher durch einen sicheren Speichermechanismus erforderlich ist) [E.Info.SSM-1.PrivacyAsset.SSM]: Beschreibung des sicheren Speichermechanismus.

[E.Info.DT.SSM-1]: Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 19 für jeden in [E.Info.SSM-1.SecurityAsset] und [E.Info.SSM-1.PrivacyAsset] dokumentierten Sicherheitswert und Datenschutzwert.

[E.Just.DT.SSM-1]: Begründung für den gewählten Pfad durch den in [E.Info.DT.SSM-1] dokumentierten Entscheidungsbaum mit den folgenden Eigenschaften:

— (wenn eine Entscheidung aus [DT.SSM-1.DN-1 zu „NICHT ANWENDBAR“ führt) basiert die Begründung für die Entscheidung [DT.SSM-1.DN-1] auf [E.Info.SSM-1.SecurityAsset.Environment] oder [E.Info.SSM-1.PrivacyAsset.Environment]; und

— die Begründung für die Entscheidung [DT.SSM-1.DN-2] basiert auf [E.Info.SSM-1.SecurityAsset.ACM] oder [E.Info.SSM-1.PrivacyAsset.SSM].

#### 6.4.1.4.4 Konzeptuelle Beurteilung

##### 6.4.1.4.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob sichere Speichermechanismen implementiert wurden, wo sie nach SSM-1 erforderlich sind.

##### 6.4.1.4.4.2 Voraussetzungen

Keine.

##### 6.4.1.4.4.3 Beurteilungseinheiten

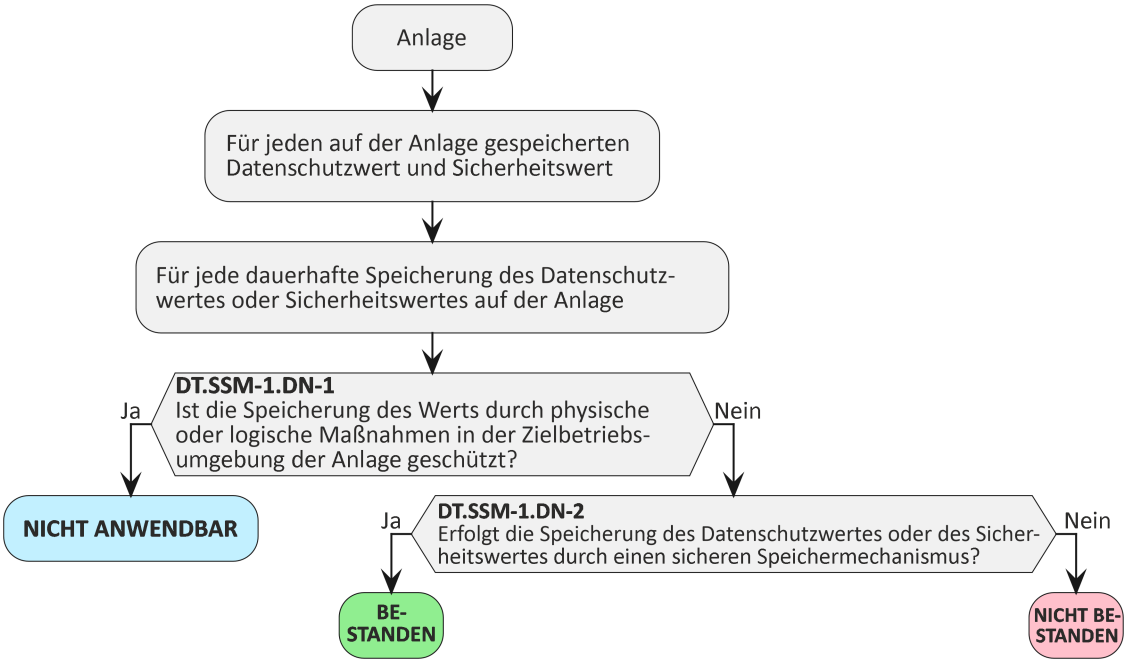



**Bild 19 — Entscheidungsbaum für Anforderung SSM-1**

Für jeden in [E.Info.SSM-1.SecurityAsset] und [E.Info.SSM-1.PrivacyAsset] dokumentierten Sicherheitswert und Datenschutzwert ist zu prüfen, ob der Pfad durch den in [E.Info.DT.SSM-1] dokumentierten Entscheidungsbaum mit „NICHT ANWENDBAR“ oder „BESTANDEN“ endet.

Für jeden in [E.Info.DT.SSM-1] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.SSM-1] dokumentierte Begründung zu untersuchen.

##### 6.4.1.4.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— mindestens ein Pfad durch den in [E.Info.DT.SSM-1] dokumentierten Entscheidungsbaum mit „BESTANDEN“ endet; und

— kein Pfad durch den in [E.Info.DT.SSM-1] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; und

— die in [E.Just.DT.SSM-1] angegebenen Informationen korrekte Begründungen für alle Pfade durch den in [E.Info.DT.SSM-1] dokumentierten Entscheidungsbaum sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— ein Pfad durch den in [E.Info.DT.SSM-1] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; oder

— eine in [E.Just.DT.SSM-1] angegebene Begründung für einen Pfad durch den in [E.Info.DT.SSM-1] dokumentierten Entscheidungsbaum nicht korrekt ist oder fehlt.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

#### 6.4.1.4.5 Beurteilung der funktionalen Vollständigkeit

##### 6.4.1.4.5.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob die in [E.Info.SSM-1.SecurityAsset] dokumentierten Sicherheitswerte und die in [E.Info.SSM-1.PrivacyAsset] dokumentierten Netzwerkwerte vollständig sind.

##### 6.4.1.4.5.2 Voraussetzungen

Die Anlage befindet sich im Betriebszustand.

##### 6.4.1.4.5.3 Beurteilungseinheiten

Es ist funktional zu beurteilen, ob Sicherheitswerte dauerhaft auf der Anlage gespeichert sind, die nicht in [E.Info.SSM-1.SecurityAsset] aufgeführt sind.

Es ist funktional zu beurteilen, ob Datenschutzwerte dauerhaft auf der Anlage gespeichert sind, die nicht in [E.Info.SSM-1.PrivacyAsset] aufgeführt sind.

##### 6.4.1.4.5.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn alle gefundenen dauerhaft gespeicherten Sicherheitswerte in [E.Info.SSM-1.SecurityAsset] dokumentiert sind und alle gefundenen dauerhaft gespeicherten Datenschutzwerte in [E.Info.SSM-1.PrivacyAsset] dokumentiert sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn ein dauerhaft gespeicherter Sicherheitswert gefunden wird, der nicht in [E.Info.SSM-1.SecurityAsset] dokumentiert ist, oder wenn ein dauerhaft gespeicherter Datenschutzwert gefunden wird, der nicht in [E.Info.SSM-1.PrivacyAsset] dokumentiert ist.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

#### 6.4.1.4.6 Beurteilung der funktionalen Suffizienz

##### 6.4.1.4.6.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob sichere Speichermechanismen implementiert wurden, wo sie nach SSM-1 erforderlich sind.

##### 6.4.1.4.6.2 Voraussetzungen

Die Anlage befindet sich im Betriebszustand.

#### 6.4.1.4.6.3 Beurteilungseinheiten

Für jeden in [E.Info.SSM-1.SecurityAsset] dokumentierten Sicherheitswert ist funktional zu bestätigen, dass er ausschließlich über die in [E.Info.SSM-1.SecurityAsset.SSM] dokumentierten sicheren Speichermechanismen dauerhaft gespeichert wird.

Für jeden in [E.Info.SSM-1.PrivacyAsset] dokumentierten Datenschutzwert ist funktional zu bestätigen, dass er ausschließlich über die in [E.Info.SSM-1.PrivacyAsset.SSM] dokumentierten sicheren Speichermechanismen dauerhaft gespeichert wird.

#### 6.4.1.4.6.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn kein Nachweis vorliegt, dass:

— ein Sicherheitswert auf andere Weise als über die in [E.Info.SSM-1.SecurityAsset.SSM] dokumentierten sicheren Speichermechanismen dauerhaft gespeichert wird; und

— ein Datenschutzwert auf andere Weise als über sichere Speichermechanismen, die in einem [E.Info.SSM-1.PrivacyAsset.SSM] dokumentiert sind, dauerhaft gespeichert wird.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn ein Nachweis vorliegt, dass:

— ein Sicherheitswert auf andere Weise als über die in [E.Info.SSM-1.SecurityAsset.SSM] dokumentierten sicheren Speichermechanismen dauerhaft gespeichert wird; oder

— ein Datenschutzwert auf andere Weise als über sichere Speichermechanismen, die in einem [E.Info.SSM-1.PrivacyAsset.SSM] dokumentiert sind, dauerhaft gespeichert wird.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

### 6.4.2 [SSM-2] Angemessener Integritätsschutz für sichere Speichermechanismen

#### 6.4.2.1 Anforderung

Jeder sichere Speichermechanismus, der nach SSM-1 erforderlich ist, muss die Integrität von Sicherheitswerten und Datenschutzwerten, die er dauerhaft speichert, schützen.

#### 6.4.2.2 Begründung

Sicherheitswerte und Datenschutzwerte müssen während der Speicherung gegen Manipulation geschützt werden. Wenn die Integrität der gespeicherten Sicherheitswerte oder Datenschutzwerte nicht angemessen gesichert wird, kann ein Angreifer diese Werte manipulieren, was zur Verletzung von Persönlichkeitsrechten führen kann, z. B. durch Missbrauch von personenbezogenen Informationen, falsche Zuschreibung usw.

Der Integritätsschutz gilt sowohl für die verschlüsselte als auch für die nicht verschlüsselte Speicherung.

#### 6.4.2.3 Leitlinie

Daten können unter anderem folgendermaßen gegen Manipulation geschützt werden:

— durch kryptographische Maßnahmen wie digitale Signaturen,

— durch Zugangssteuerung,

— durch Hardware-Schutzmaßnahmen,

— durch physische Schutzmaßnahmen.

#### 6.4.2.4 Beurteilungskriterien

##### 6.4.2.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung SSM-2.

##### 6.4.2.4.2 Umsetzungskategorien

[IC.SSM-2.DigitalSignature]: Die Methode zur Sicherstellung der Integrität gespeicherter Sicherheitswerte oder Datenschutzwerte basiert auf digitalen Signaturen, die mit Hilfe eines kryptographischen Geheimnisses, das während der Herstellung, der Inbetriebnahme oder des Normalbetriebs eines Geräts bereitgestellt wird, abgeleitet werden.

[IC.SSM-2.AccessControl]: Die Methode zur Sicherstellung der Integrität gespeicherter Sicherheitswerte oder Datenschutzwerte ist die Verwendung von Zugangssteuerungsmechanismen, die eine unbefugte Änderung verhindern.

[IC.SSM-2.OTProgrammable]: Die Methode zur Sicherstellung der Integrität gespeicherter Sicherheitswerte oder Datenschutzwerte basiert auf einem einmalig programmierbaren Speicher.

[IC.SSM-2.HardwareProtection]: Die Methode zur Sicherstellung der Integrität gespeicherter Sicherheitswerte oder Datenschutzwerte basiert auf Hardware zum Schutz des Speichers.

[IC.SSM-2.Generic]: Die Methoden zur Sicherstellung der Integrität gespeicherter Sicherheitswerte und Datenschutzwerte beruhen nicht ausschließlich auf [IC.SSM-2.DigitalSignature], [IC.SSM-2.AccessControl], [IC.SSM-2.OTProgrammable] oder [IC.SSM-2.HardwareProtection].

##### 6.4.2.4.3 Erforderliche Informationen

[E.Info.SSM-2.SSM]: Beschreibung des sicheren Speichermechanismus, einschließlich

— [IC.SSM-2.SSM.Asset]: Liste aller Sicherheitswerte und Datenschutzwerte, die er dauerhaft speichert; und

— (wenn die SSM-Umsetzung auf [IC.SSM-2.DigitalSignature] basiert) [E.Info.SSM-2.SSM.DigitalSignature]: Beschreibung, wie der Integritätsschutz mit Hilfe der digitalen Signatur erreicht wird, einschließlich:

  — einer Beschreibung des Mechanismus der digitalen Signatur und der Kryptographie für die Sicherheitswerte und Datenschutzwerte, die er dauerhaft speichert; und

  — einer Beschreibung der Art und Weise, wie das zur Ableitung der Signatur verwendete kryptographische Geheimnis in die Anlage eingespeist oder von diesem erzeugt wird; und

— (wenn die SSM-Umsetzung auf [IC.SSM-2.AccessControl] basiert) [E.Info.SSM-2.SSM.AccessControl]: Beschreibung, wie der Integritätsschutz mit Hilfe des Zugangssteuerungsmechanismus erreicht wird, einschließlich:

  — einer Beschreibung des Zugangssteuerungsmechanismus und der entsprechenden Zugangsrechte für die Sicherheitswerte und Datenschutzwerte, die er dauerhaft speichert; und

— (wenn die SSM-Umsetzung auf [IC.SSM-2.OTProgrammable] basiert) [E.Info.SSM-2.SSM.OTProgrammable]: Beschreibung, wie der Integritätsschutz mit Hilfe des einmalig programmierbaren Speichers erreicht wird, einschließlich:

  — einer Beschreibung des Typs des einmalig programmierbaren Speichers, der verwendet wird für die Sicherheitswerte und Datenschutzwerte, die er dauerhaft speichert; und

— (wenn die SSM-Umsetzung auf [IC.SSM-2.HardwareProtection] basiert) [E.Info.SSM-2.Hardware-Protection]: Beschreibung, wie der Integritätsschutz mit Hilfe des Hardwareschutzes erreicht wird, einschließlich:

  — einer Beschreibung, welcher Hardwareschutz für die dauerhaft gespeicherten Sicherheitswerte und Datenschutzwerte verwendet wird; und

— (wenn die SSM-Umsetzung auf [IC.SSM-2.Generic] basiert) [E.Info.SSM-2.SSM.Generic]: Beschreibung des Integritätsschutzmechanismus, der zum Schutz der Sicherheitswerte oder Datenschutzwerte verwendet wird; und

— (wenn angegeben wird, dass die sicheren Speichermechanismen anerkannten Sicherheitsnormen oder Zertifizierungsprogrammen entsprechen), [IC.SSM-2.SSM.ComplianceEvidence]: Bietet Nachweise über die anerkannten Sicherheitsnormen oder Zertifizierungsprogramme vorzulegen, denen die sicheren Speichermechanismen entsprechen.

ANMERKUNG Die oben genannten Informationen stehen dem Hersteller möglicherweise nicht immer zur Verfügung, wenn der Mechanismus für die sichere Speicherung von einem Anbieter bereitgestellt wird, der diese Informationen aus Sicherheitsgründen nicht preisgibt, jedoch alle notwendigen Sicherheitsanweisungen zur Verwendung des Mechanismus für die sichere Speicherung bereitstellt.

[E.Info.DT.SSM-2]: Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 20 für jeden in [E.Info.SSM-2.SSM] beschriebenen sicheren Speichermechanismus.

[E.Just.DT.SSM-2]: Begründung für den gewählten Pfad durch den in [E.Info.DT.SSM-2] dokumentierten Entscheidungsbaum mit den folgenden Eigenschaften:

— (wenn die Implementation auf [IC.SSM-2.DigitalSignature] basiert) die Begründung für die Entscheidung [DT.SSM-2.DN-1] auf [E.Info.SSM-2.DigitalSignature] basiert; und

— (wenn die Implementation auf [IC.SSM-2.AccessControl] basiert) die Begründung für die Entscheidung [DT.SSM-2.DN-1] auf [E.Info.SSM-2.SSM.AccessControl] basiert; und

— (wenn die Implementation auf [IC.SSM-2.OTProgrammable] basiert) die Begründung für die Entscheidung [DT.SSM-2.DN-1] auf [E.Info.SSM-2.SSM.OTProgrammable] basiert; und

— (wenn die Implementation auf [IC.SSM-2.HardwareProtection] basiert) die Begründung für die Entscheidung [DT.SSM-2.DN-1] auf [E.Info.SSM-2.SSM.HardwareProtection] basiert; und

— (wenn die Implementation auf [IC.SSM-2.Generic] basiert) die Begründung für die Entscheidung [DT.SSM-2.DN-1] auf [E.Info.SSM-2.SSM.Generic] basiert.

#### 6.4.2.4.4 Konzeptuelle Beurteilung

##### 6.4.2.4.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob durch SSM-1 erforderliche sichere Speichermechanismen implementiert wurden, wie nach SSM-2 erforderlich.

##### 6.4.2.4.4.2 Voraussetzungen

Keine.

#### 6.4.2.4.4.3 Beurteilungseinheiten

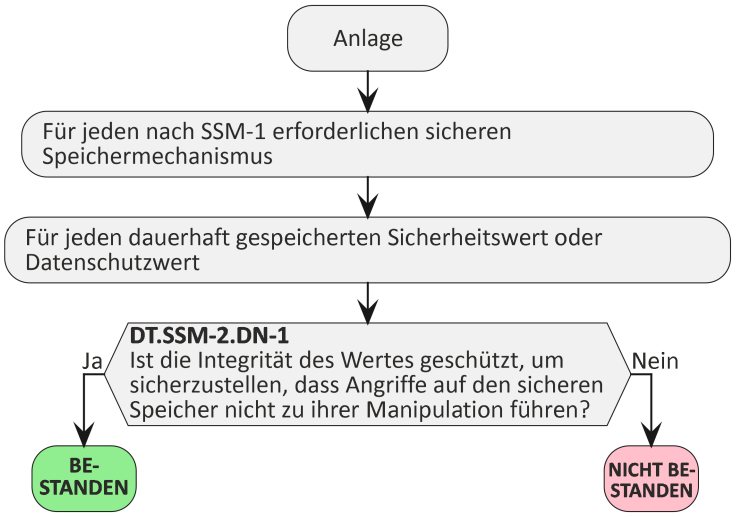



**Bild 20 — Entscheidungsbaum für Anforderung SSM-2**

Für jeden sicheren Speichermechanismus in [E.Info.SSM-2.SSM] ist zu prüfen, ob der Pfad durch den in [E.Info.DT.SSM-2] dokumentierten Entscheidungsbaum mit „BESTANDEN“ endet.

Für jeden in [E.Info.DT.SSM-2] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.SSM-2] dokumentierte Begründung zu untersuchen.

#### 6.4.2.4.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— alle Pfade durch den in [E.Info.DT.SSM-2] dokumentierten Entscheidungsbaum mit „BESTANDEN“ enden; und

— die in [E.Just.DT.SSM-2] angegebenen Informationen korrekte Begründungen für alle Pfade durch den in [E.Info.DT.SSM-2] dokumentierten Entscheidungsbaum sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— ein Pfad durch den in [E.Info.DT.SSM-2] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; oder

— eine in [E.Just.DT.SSM-2] angegebene Begründung für einen Pfad durch den in [E.Info.DT.SSM-2] dokumentierten Entscheidungsbaum nicht korrekt ist oder fehlt.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

#### 6.4.2.4.5 Beurteilung der funktionalen Vollständigkeit

Die Beurteilung der funktionalen Vollständigkeit wird durch die Beurteilung der funktionalen Suffizienz der Anwendbarkeit des sicheren Speichermechanismus abgedeckt.

Deshalb ist diese Beurteilung der funktionalen Vollständigkeit nicht notwendig.

#### 6.4.2.4.6 Beurteilung der funktionalen Suffizienz

##### 6.4.2.4.6.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob die nach SSM-1 erforderlichen sicheren Speichermechanismen den erforderlichen Integritätsschutz bieten.

##### 6.4.2.4.6.2 Voraussetzungen

Die Anlage befindet sich im Betriebszustand.

##### 6.4.2.4.6.3 Beurteilungseinheiten

Für jeden in [E.Info.SSM-2.SSM] dokumentierten sicheren Speichermechanismus:

[AU.SSM-2.DigitalSignature]: Wenn die Umsetzung des sicheren Speichermechanismus auf [IC.SSM-2.DigitalSignature] basiert, ist funktional zu bestätigen, dass:

— er nach [E.Info.SSM-2.SSM.DigitalSignature] implementiert wird; und

— das zur digitalen Signatur der Sicherheitswerte oder Datenschutzwerte verwendete Geheimnis nicht abgefangen, abgeleitet oder extrahiert werden kann; und

— eine Änderung der Sicherheitswerte und Datenschutzwerte ohne gültige Signatur durch den sicheren Speichermechanismus erkannt wird.

[AU.SSM-2.AccessControl]: Wenn die Umsetzung des sicheren Speichermechanismus auf [IC.SSM-2.AccessControl] basiert, ist funktional zu bestätigen, dass:

— er nach [E.Info.SSM-2.SSM.AccessControl] implementiert wird; und

— eine unbefugte Änderung der gespeicherten Sicherheitswerte und Datenschutzwerte verweigert wird.

[AU.SSM-2.OTProgrammable]: Wenn die Umsetzung des sicheren Speichermechanismus auf [IC.SSM-2.OTProgrammable] basiert, ist funktional zu bestätigen, dass:

— er nach [E.Info.SSM-2.SSM.OTProgrammable] implementiert wird; und

— eine Änderung der gespeicherten Sicherheitswerte und Datenschutzwerte nicht möglich ist.

[AU.SSM-2.HardwareProtection]: Wenn die Umsetzung des sicheren Speichermechanismus auf [IC.SSM-2.HardwareProtection] basiert, ist funktional zu bestätigen, dass:

— er nach [E.Info.SSM-2.SSM.HardwareProtection] implementiert wird; und

— eine unbefugte Änderung der Sicherheitswerte und Datenschutzwerte nicht möglich ist oder durch den sicheren Speichermechanismus erkannt werden kann.

[AU.SSM-2.Generic]: Wenn die Umsetzung des sicheren Speichermechanismus auf [IC.SSM-2.Generic] basiert, ist funktional zu bestätigen, dass:

— er nach [E.Info.SSM-2.SSM.Generic] implementiert wird; und

— eine unbefugte Änderung der Sicherheitswerte oder Datenschutzwerte nicht möglich ist oder durch den sicheren Speichermechanismus erkannt werden kann.

#### 6.4.2.4.6.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn für jeden in [E.Info.SSM-2.SSM] dokumentierten sicheren Speichermechanismus die Bestätigungen in den von der Umsetzungskategorie abhängigen Beurteilungseinheiten erfolgreich sind.

Die Entscheidung NICHT BESTANDEN für den Beurteilungsfall wird zugewiesen, wenn für jeden in [E.Info.SSM-2.SSM] dokumentierten sicheren Speichermechanismus eine Bestätigung in den von der Umsetzungskategorie abhängigen Beurteilungseinheiten nicht erfolgreich ist.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

### 6.4.3 [SSM-3] Angemessener Vertraulichkeitsschutz für sichere Speichermechanismen

#### 6.4.3.1 Anforderung

Jeder sichere Speichermechanismus, der nach SSM-1 erforderlich ist, muss die Geheimhaltung vertraulicher personenbezogener Informationen, vertraulicher Datenschutzfunktionskonfigurationen und der vertraulichen Sicherheitsparameter, die dauerhaft auf der Anlage gespeichert sind, schützen.

#### 6.4.3.2 Begründung

Vertrauliche personenbezogene Informationen, die Konfiguration vertraulicher Datenschutzfunktionen und vertrauliche Sicherheitsparameter benötigen während der Speicherung einen Schutz vor Offenlegung. Wenn solche Informationen nicht angemessen gesichert sind, kann ein Angreifer auf die Anlage und die gespeicherten Daten zugreifen und diese missbrauchen, was zur Offenlegung personenbezogener Informationen führen kann.

#### 6.4.3.3 Leitlinie

Daten können unter anderem folgendermaßen vor Offenlegung geschützt werden:

— durch kryptographische Maßnahmen wie Verschlüsselung,

— durch Zugangssteuerung,

— durch Hardware-Schutzmaßnahmen.

#### 6.4.3.4 Beurteilungskriterien

##### 6.4.3.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung SSM-3.

##### 6.4.3.4.2 Umsetzungskategorien

[IC.SSM-3.Encryption]: Die Methode zur Sicherstellung der Geheimhaltung gespeicherter vertraulicher personenbezogener Informationen, vertraulicher Datenschutzfunktionskonfigurationen und vertraulicher Sicherheitsparameter basiert auf der Verschlüsselung unter Verwendung eines Geheimnisses, das während der Herstellung, der Inbetriebnahme oder des Normalbetriebs eines Geräts bereitgestellt wird.

[IC.SSM-3.AccessControl]: Die Methode der Geheimhaltung gespeicherter vertraulicher personenbezogener Informationen, vertraulicher Datenschutzfunktionskonfigurationen und vertraulicher Sicherheitsparameter wird durch Zugangssteuerungsmechanismen sichergestellt, die ein unbefugtes Lesen verweigern.

[IC.SSM-3.HardwareProtection]: Die Methode zur Sicherstellung der Geheimhaltung gespeicherter vertraulicher personenbezogener Informationen, der Konfiguration vertraulicher Datenschutzfunktionen und vertraulicher Sicherheitsparameter auf der Grundlage von Hardwareschutz (z. B. Verschlüsselung, Verschleierung usw.).

[IC.SSM-3.Generic]: Die Methoden zur Sicherstellung der Geheimhaltung gespeicherter vertraulicher personenbezogener Informationen, der Konfiguration vertraulicher Datenschutzfunktionen und vertraulicher Sicherheitsparameter beruhen nicht ausschließlich auf [IC.SSM-3.Encryption], [IC.SSM-3.AccessControl] oder [IC.SSM-3.HardwareProtection].

#### 6.4.3.4.3 Erforderliche Informationen

[E.Info.SSM-3.SSM]: Beschreibung jedes sicheren Speichermechanismus, der vertrauliche personenbezogene Informationen, vertrauliche Datenschutzfunktionskonfigurationen oder vertrauliche Sicherheitsparameter dauerhaft speichert, einschließlich:

— [E.Info.SSM-3.SSM.Asset]: Liste aller vertraulichen personenbezogenen Informationen, der vertraulichen Konfiguration der Datenschutzfunktionen und der vertraulichen Sicherheitsparameter, die dauerhaft gespeichert werden; und

— (wenn die SSM-Umsetzung auf [IC.SSM-3.Encryption] basiert) [E.Info.SSM-3.SSM.Encryption]: Beschreibung, wie die Geheimhaltung mit Hilfe der Verschlüsselung erreicht wird, einschließlich:

  — des Verschlüsselungsmechanismus und der Kryptographie, die zum Schutz der Vertraulichkeit der vertraulichen personenbezogenen Informationen, der Konfiguration der vertraulichen Datenschutzfunktion und der vertraulichen Sicherheitsparameter, die dauerhaft gespeichert werden, verwendet werden; und

  — wie das zur Verschlüsselung des Wertes verwendete Geheimnis beschafft oder abgeleitet wurde; und

— (wenn die SSM-Umsetzung auf [IC.SSM-3.AccessControl] basiert) [E.Info.SSM-3.SSM.AccessControl]: Beschreibung, wie die Geheimhaltung mit Hilfe des Zugangssteuerungsmechanismus erreicht wird, einschließlich:

  — einer Beschreibung des Zugangssteuerungsmechanismus einschließlich der entsprechenden Zugangsrechte für die vertraulichen personenbezogenen Informationen, die Konfiguration der vertraulichen Datenschutzfunktion und die vertraulichen Sicherheitsparameter, die er dauerhaft speichert; und

— (wenn die SSM-Umsetzung auf [IC.SSM-3.HardwareProtection] basiert) [E.Info.SSM-3.SSM.HardwareProtection]: Beschreibung, wie die Geheimhaltung mit Hilfe des Hardwareschutzes erreicht wird, einschließlich:

  — einer Beschreibung, welche Hardware zum Schutz der vertraulichen personenbezogenen Informationen, der Konfiguration der vertraulichen Datenschutzfunktion und der vertraulichen Sicherheitsparameter, die er dauerhaft speichert, verwendet wird; und

— (wenn die SSM-Umsetzung auf [IC.SSM-3.Generic] basiert) [E.Info.SSM-3.SSM.Generic]: Beschreibung des Vertraulichkeitsschutzmechanismus zur Wahrung der Geheimhaltung vertraulicher personenbezogener Informationen, der Konfiguration vertraulicher Datenschutzfunktionen oder vertraulicher Sicherheitsparameter, die dauerhaft gespeichert werden; und

— (wenn angegeben wird, dass die sicheren Speichermechanismen anerkannten Sicherheitsnormen oder Zertifizierungsprogrammen entsprechen), [IC.SSM-3.SSM.ComplianceEvidence]: Bietet Nachweise über die anerkannten Sicherheitsnormen oder Zertifizierungsprogramme vorzulegen, denen die sicheren Speichermechanismen entsprechen.

ANMERKUNG Die oben genannten Informationen stehen dem Hersteller möglicherweise nicht immer zur Verfügung, wenn der sichere Speichermechanismus von einem Anbieter bereitgestellt wird, der diese Informationen aus Sicherheitsgründen nicht preisgibt, jedoch alle notwendigen Sicherheitsanweisungen zur Verwendung des Erzeugungsmechanismus bereitstellt.

[E.Info.DT.SSM-3]: Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 21 für jeden in [E.Info.SSM-3.SSM] beschriebenen sicheren Speichermechanismus.

[E.Just.DT.SSM-3]: Begründung für den gewählten Pfad durch den in [E.Info.DT.SSM-3] dokumentierten Entscheidungsbaum mit den folgenden Eigenschaften:

— (wenn die Implementation auf [IC.SSM-3.Encryption] basiert) die Begründung für die Entscheidung [DT.SSM-3.DN-1] auf [E.Info.SSM-3.SSM.Encryption] basiert; und

— (wenn die Implementation auf [IC.SSM-3.AccessControl] basiert) die Begründung für die Entscheidung [DT.SSM-3.DN-1] auf [E.Info.SSM-3.SSM.AccessControl] basiert; und

— (wenn die Implementation auf [IC.SSM-3.HardwareProtection] basiert) die Begründung für die Entscheidung [DT.SSM-3.DN-1] auf [E.Info.SSM-3.SSM.HardwareProtection] basiert; und

— (wenn die Implementation auf [IC.SSM-3.Generic] basiert) die Begründung für die Entscheidung [DT.SSM-3.DN-1] auf [E.Info.SSM-3.SSM.Generic] basiert.

#### 6.4.3.4.4 Konzeptuelle Beurteilung

##### 6.4.3.4.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob durch SSM-1 erforderliche sichere Speichermechanismen, die dauerhaft vertrauliche personenbezogene Informationen, die Konfiguration vertraulicher Datenschutzfunktionen oder vertrauliche Sicherheitsparameter speichern, implementiert werden, wie nach SSM-3 erforderlich.

##### 6.4.3.4.4.2 Voraussetzungen

Keine.

#### 6.4.3.4.4.3 Beurteilungseinheiten

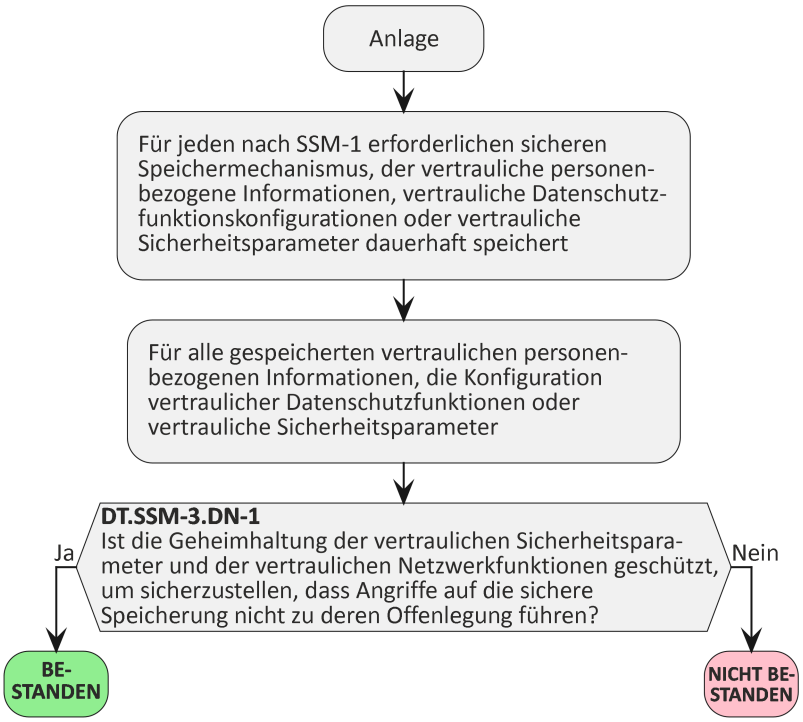



**Bild 21 — Entscheidungsbaum für Anforderung SSM-3**

Für jeden sicheren Speichermechanismus in [E.Info.SSM-3.SSM] ist zu prüfen, ob der Pfad durch den in [E.Info.DT.SSM-3] dokumentierten Entscheidungsbaum mit „BESTANDEN“ endet.

Für jeden in [E.Info.DT.SSM-3] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.SSM-3] dokumentierte Begründung zu untersuchen.

#### 6.4.3.4.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— alle Pfade durch den in [E.Info.DT.SSM-3] dokumentierten Entscheidungsbaum mit „BESTANDEN“ enden; und

— die in [E.Just.DT.SSM-3] angegebenen Informationen korrekte Begründungen für alle Pfade durch den in [E.Info.DT.SSM-3] dokumentierten Entscheidungsbaum sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— ein Pfad durch den in [E.Info.DT.SSM-3] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; oder

— eine in [E.Just.DT.SSM-3] angegebene Begründung für einen Pfad durch den in [E.Info.DT.SSM-3] dokumentierten Entscheidungsbaum nicht korrekt ist oder fehlt.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

#### 6.4.3.4.5 Beurteilung der funktionalen Vollständigkeit

##### 6.4.3.4.5.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob die in [E.Info.SSM-3.SSM.Asset] dokumentierten Werte vollständig sind.

##### 6.4.3.4.5.2 Voraussetzungen

Die Anlage befindet sich im Betriebszustand.

##### 6.4.3.4.5.3 Beurteilungseinheiten

Es ist funktional zu beurteilen, ob vertrauliche Sicherheitsparameter, vertrauliche personenbezogene Informationen oder Konfigurationen vertraulicher Datenschutzfunktionen dauerhaft auf der Anlage gespeichert sind, die nicht in [E.Info.SSM-3.SSM.Asset] aufgeführt sind.

##### 6.4.3.4.5.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn alle gefundenen dauerhaft gespeicherten vertraulichen Sicherheitsparameter, alle gefundenen dauerhaft gespeicherten vertraulichen personenbezogenen Informationen und alle gefundenen dauerhaft gespeicherten Konfigurationen vertraulicher Datenschutzfunktionen in [E.Info.SSM-3.SSM.Asset] dokumentiert sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn ein dauerhaft gespeicherter vertraulicher Sicherheitsparameter gefunden wird, wenn dauerhaft gespeicherte vertrauliche personenbezogene Informationen gefunden werden oder wenn eine dauerhaft gespeicherte Konfiguration vertraulicher Datenschutzfunktionen gefunden wird, die nicht in [E.Info.SSM-3.SSM.Asset] dokumentiert ist/sind.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

#### 6.4.3.4.6 Beurteilung der funktionalen Suffizienz

##### 6.4.3.4.6.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob die durch SSM-1 erforderlichen sicheren Speichermechanismen, die dauerhaft vertrauliche Sicherheitsparameter, vertrauliche personenbezogene Informationen oder die Konfiguration vertraulicher Datenschutzfunktionen speichern, den erforderlichen Vertraulichkeitsschutz bereitstellen.

##### 6.4.3.4.6.2 Voraussetzungen

Die Anlage befindet sich im Betriebszustand.

##### 6.4.3.4.6.3 Beurteilungseinheiten

Für jeden in [E.Info.SSM-3.SSM] dokumentierten sicheren Speichermechanismus:

[AU.SSM-3.Encryption]: Wenn die Umsetzung des sicheren Speichermechanismus auf [IC.SSM-3.Encryption] basiert, ist funktional zu bestätigen, dass:

— er nach [E.Info.SSM-3.SSM.Encryption] implementiert wird; und

— das zur Verschlüsselung der vertraulichen Sicherheitsparameter, der vertraulichen personenbezogenen Informationen oder der Konfiguration der vertraulichen Datenschutzfunktion verwendete Geheimnis nicht abgefangen, abgeleitet oder extrahiert werden kann; und

— das Auslesen vertraulicher Sicherheitsparameter, vertraulicher personenbezogener Informationen und der Konfiguration der vertraulichen Datenschutzfunktionen ohne Zugriff auf das für die Entschlüsselung verwendete Geheimnis nicht möglich ist.

[AU.SSM-3.AccessControl]: Wenn die Umsetzung des sicheren Speichermechanismus auf [IC.SSM-3.AccessControl] basiert, ist funktional zu bestätigen, dass:

— er nach [E.Info.SSM-3.SSM.AccessControl] implementiert wird; und

— ein unbefugtes Auslesen der gespeicherten vertraulichen Sicherheitsparameter, vertraulichen personenbezogenen Informationen und der Konfiguration vertraulicher Datenschutzfunktionen verweigert wird.

[AU.SSM-3.HardwareProtection]: Wenn die Umsetzung des sicheren Speichermechanismus auf [IC.SSM-3.HardwareProtection] basiert, ist funktional zu bestätigen, dass:

— er nach [E.Info.SSM-3.SSM.HardwareProtection] implementiert wird; und

— der Mechanismus, der zum Schutz der Vertraulichkeit der gespeicherten vertraulichen Sicherheitsparameter, vertraulichen personenbezogenen Informationen und der Konfiguration der vertraulichen Datenschutzfunktionen verwendet wird, nicht gebrochen oder umgangen werden kann; und

— ein unbefugtes Auslesen der gespeicherten vertraulichen Sicherheitsparameter, vertraulichen personenbezogenen Informationen und der Konfiguration vertraulicher Datenschutzfunktionen nicht möglich ist.

[AU.SSM-3.Generic]: Wenn die Umsetzung des sicheren Speichermechanismus auf [IC.SSM-3.Generic] basiert, ist funktional zu bestätigen, dass:

— er nach [E.Info.SSM-3.SSM.Generic] implementiert wird; und

— ein unbefugtes Auslesen der gespeicherten vertraulichen Sicherheitsparameter, vertraulichen personenbezogenen Informationen und der Konfiguration vertraulicher Datenschutzfunktionen nicht möglich ist.

#### 6.4.3.4.6.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn für jeden in [E.Info.SSM-3.SSM] dokumentierten sicheren Speichermechanismus die Bestätigungen in den von der Umsetzungskategorie abhängigen Beurteilungseinheiten erfolgreich sind.

Die Entscheidung NICHT BESTANDEN für den Beurteilungsfall wird zugewiesen, wenn für jeden in [E.Info.SSM-3.SSM] dokumentierten sicheren Speichermechanismus eine Bestätigung in den von der Umsetzungskategorie abhängigen Beurteilungseinheiten nicht erfolgreich ist.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

## 6.5 [SCM] Sicherer Kommunikationsmechanismus (en: Secure Communication Mechanism)

### 6.5.1 [SCM-1] Anwendbarkeit von sicheren Kommunikationsmechanismen

#### 6.5.1.1 Anforderung

Die Anlage muss immer sichere Kommunikationsmechanismen nutzen, um Sicherheitswerte und Datenschutzwerte mit anderen Entitäten über Netzwerkschnittstellen auszutauschen, mit Ausnahme

— der Übermittlung von Sicherheitswerten oder Datenschutzwerten, deren Übertragung durch physische oder logische Maßnahmen in der Zielumgebung geschützt ist, die sicherstellen, dass Sicherheitswerte oder Datenschutzwerte nicht für unbefugte Entitäten zugänglich sind; oder

— Kommunikation von Sicherheitswerten, deren Offenlegung Teil des Aufbaus oder der Verwaltung einer Verbindung ist, kombiniert mit zusätzlichen Maßnahmen zur Authentisierung der Verbindung oder der Vertrauensbeziehung.

#### 6.5.1.2 Begründung

Die Sicherheitswerte oder Datenschutzwerte der Anlage können an andere Kommunikationspartner übertragen werden, z. B. bei der Verwendung von Webdiensten. Die laufende Kommunikation ermöglicht es einem Angreifer, der Zugriff auf die Kommunikation hat, diese abzuhören, zu manipulieren oder wiederzugeben, insbesondere bei Verwendung drahtloser Technologien. Die Anlage muss sicherstellen, dass die Kommunikation gegen diese Angriffe durch sichere Kommunikationsmechanismen geschützt ist.

#### 6.5.1.3 Leitlinie

Es gibt unterschiedliche Technologien, die zur Sicherung der Kommunikation der Anlage verwendet werden können (siehe auch CRY-1). Die entsprechenden verwendeten Konfigurationen sollten bewährten Verfahrensweisen für Kommunikationsprotokolle entsprechen, um die Kommunikation gegen Abhören, Manipulation und Wiederholung zu schützen. Übliche Maßnahmen sind daher eine Kombination aus Authentisierung, Integritätsschutz, Verschlüsselung und Wiedergabeschutz. Die Maßnahmen können beispielsweise auf den Kommunikationskanal angewendet oder für den Ende-zu-Ende-Schutz verwendet werden. Die Anlage muss anderen Kommunikationspartnern als Vorgabe bewährte Verfahrensweisen für Kommunikationsprotokolle anbieten. Die Art und Weise, wie das anfängliche Vertrauensverhältnis zwischen der Anlage und einer anderen Entität hergestellt wird, ist entscheidend für die Sicherheit der nachfolgenden Kommunikation.

Es wird dringend davon abgeraten, Protokolle ohne oder mit schwacher Sicherheitsfunktionalität für die Kommunikation zu verwenden. Aus unvermeidlichen Gründen der Interoperabilität könnte eine Abweichung hiervon erforderlich sein. Bei der Nutzung solcher Protokolle muss für den Hersteller vorhersehbar sein, dass z. B. zusätzliche Sicherheitsmaßnahmen angewendet werden:

— Die Zielumgebung der Anlage ist ein Bereich, der nur für befugte Personen zugänglich ist, und die Funkreichweite ist kurz genug, um Verbindungsversuche von außerhalb des Gebäudes zu unterbinden. Übliche Beispiele für solche Bereiche sind Industriestandorte oder abgeschlossene Haustechnikräume in Mietshäusern.

— Die Zielumgebung der Anlage ist eine bestimmte Netzwerkinfrastruktur, die ein virtuelles privates Netzwerk verwendet, das das unsichere Protokoll der Anlage tunnelt.

Im Allgemeinen wird empfohlen, dass die Anlage den Benutzer benachrichtigt, wenn eine unsichere Kommunikation durchgeführt wird.

Bei Anlagen in lokalen oder persönlichen Netzwerken (z. B. Wearables) mit begrenzter Benutzungsschnittstelle, die keine komplexeren Kopplungsverfahren zulässt, könnten Kopplungsprotokolle für Man-in-the-Middle-Angriffe anfällig sein. Hier muss der Angriffsvektor durch zusätzliche Maßnahmen (Besitz, Wissen oder Inhärenz) für den Verbindungsaufbau reduziert werden, z. B. durch ein begrenztes Zeitfenster für eine Benutzerinteraktion, die für den Abschluss der Kopplung erforderlich ist.

Eine Netzwerkadresse, die von einem Protokoll offengelegt wird, ist ein Beispiel für Daten, die personenbezogene Informationen enthalten könnten, die nicht auf Netzwerkebene geschützt werden können.

#### 6.5.1.4 Beurteilungskriterien

##### 6.5.1.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung SCM-1.

##### 6.5.1.4.2 Umsetzungskategorien

Nicht anwendbar.

#### 6.5.1.4.3 Erforderliche Informationen

[E.Info.SCM-1.NetworkInterface]: Beschreibung jeder Netzwerkschnittstelle, einschließlich:

— der Beschreibung der physikalischen Merkmale, einschließlich:

  — (im Falle einer Funkschnittstelle) [E.Info.SCM-1.NetworkInterface.Radio]: die verwendete Technologie, das belegte Funkspektrum, die auf der Funkschnittstelle verwendete Sendeleistung und die implementierten Betriebsarten; oder

  — (im Falle einer kabelgebundenen Schnittstelle) [E.Info.SCM-1.NetworkInterface.Wired]: elektrische Merkmale, die auf der kabelgebundenen Schnittstelle verwendet werden, und die implementierten Betriebsarten; oder

  — (im Falle einer optischen Schnittstelle) [E.Info.SCM-1.NetworkInterface.Optical]: die auf der Schnittstelle verwendete optische Technologie und die implementierten Betriebsarten; oder

  — (im Falle einer akustischen Schnittstelle) [E.Info.SCM-1.NetworkInterface.Acoustic]: akustische Technologie, die auf der Schnittstelle verwendet wird, und die implementierten Betriebsarten; und

— der Beschreibung der logischen Merkmale, einschließlich:

  — [E.Info.SCM-1.NetworkInterface.Protocol]: Beschreibung aller Kommunikationsprotokolle, die auf der in [E.Info.SCM-1.NetworkInterface.Radio], [E.Info.SCM-1.NetworkInterface.Wired], [E.Info.SCM-1.NetworkInterface.Optical] oder [E.Info.SCM-1.NetworkInterface.Acoustic] dokumentierten Schnittstelle implementiert sind, sowie der implementierten Betriebsarten, der Version des Protokolls und gegebenenfalls der SW-Bibliothek, die für die Implementation verwendet wird; und

— der Beschreibung der Konfiguration, einschließlich

  — die für die Anlage angewandte Konfiguration und die verfügbaren Optionen zur Änderung des physischen oder logischen Verhaltens der Schnittstelle.

[E.Info.SCM-1.SecurityAsset]: Beschreibung jedes gespeicherten Sicherheitswertes, der über die in [E.Info.SCM-1.NetworkInterface] dokumentierten Netzwerkschnittstellen kommuniziert wird und für den Vertraulichkeit, Integrität oder Authentizität erforderlich ist, um die Datenschutzwerte der Anlage zu schützen, einschließlich:

— (wenn eine Klassifizierung der Sicherheitswerte anwendbar ist) [E.Info.SCM-1.SecurityAsset.Class]: Klassifizierung von Sicherheitswerten (z. B. Root-Schlüssel, Master-Schlüssel, Wrapper-Schlüssel oder öffentliche Schlüssel), wobei Sicherheitswerte in Gruppen als eine einzige Kategorie aufgeführt werden dürfen, wenn sie Teil desselben Anwendungsfalls und derselben Sicherheitsstufe sind; und

— [E.Info.SCM-1.SecurityAsset.Com]: Beschreibung des Anwendungsfalls, in dem der Wert über eine in [E.Info.SCM-1.NetworkInterface] dokumentierte Netzwerkschnittstelle kommuniziert wird (z. B. Kopplung mit einer Basisstation); und

— [E.Info.SCM-1.SecurityAsset.NetworkInterface]: Netzwerkschnittstelle, die für die Kommunikation des Sicherheitswertes verwendet wird (aus [E.Info.SCM-1.NetworkInterface]); und

— (wenn die Übertragung durch physische und logische Maßnahmen in der Zielumgebung geschützt ist) [E.Info.SCM-1.SecurityAsset.TrustedEnv]: Beschreibung der physischen oder logischen Maßnahmen in der Zielbetriebsumgebung der Anlage, die sicherstellen, dass die Werte nicht für unbefugte Entitäten zugänglich sind; und

— (wenn die Werte Teil der Herstellung oder Verwaltung der Verbindung sind) [E.Info.SCM-1.SecurityAssets.AddMeasures]: Beschreibung der implementierten zusätzlichen Maßnahmen zur Authentisierung der Verbindung oder der Vertrauensbeziehung.

[E.Info.SSM-1.PrivacyAsset]: Beschreibung jedes Datenschutzwertes, der über die in [E.Info.SCM-1.NetworkInterface] dokumentierten Netzwerkschnittstellen kommuniziert wird und für den Vertraulichkeits-, Integritäts- oder Authentizitätsschutz erforderlich ist, einschließlich

— (wenn eine Klassifizierung der Datenschutzwerte anwendbar ist) [E.Info.SCM-1.PrivacyAsset.Class]: Klassifizierung von Datenschutzwerten (z. B. personenbezogene Informationen, Standort, sensible personenbezogene Informationen), Datenschutzwerte dürfen in Gruppen als eine einzige Kategorie aufgeführt werden, wenn sie Teil desselben Anwendungsfalls und derselben Sicherheitsstufe sind; und

— [E.Info.SCM-1.PrivacyAsset.Com]: Beschreibung des Anwendungsfalls, in dem der Wert über eine in [E.Info.SCM-1.NetworkInterface] dokumentierte Netzwerkschnittstelle kommuniziert wird (z. B. Kopplung mit einer Basisstation); und

— [E.Info.SCM-1.PrivacyAsset.NetInterface]: Netzwerkschnittstelle, die für die Kommunikation des Datenschutzwertes verwendet wird (aus [E.Info.SCM-1.NetworkInterface]); und

— (wenn die Übertragung durch physische und logische Maßnahmen in der Zielumgebung geschützt ist) [E.Info.SCM-1.PrivacyAsset.TrustedEnv]: Beschreibung der physischen oder logischen Maßnahmen in der Zielbetriebsumgebung der Anlage, die sicherstellt, dass die Werte nicht für unbefugte Entitäten zugänglich sind; und

— (wenn die Werte Teil der Herstellung oder Verwaltung der Verbindung sind) [E.Info.SCM-1.PrivacyAssets.AddMeasures]: Beschreibung der implementierten zusätzlichen Maßnahmen zur Authentisierung der Verbindung oder der Vertrauensbeziehung.

[E.Info.SCM-1.SCM]: Beschreibung jedes sicheren Kommunikationsmechanismus, der zur Kommunikation von in [E.Info.SCM-1.SecurityAsset] dokumentierten Sicherheitswerten und in [E.Info.SCM-1.PrivacyAsset] dokumentierten Datenschutzwerten über die in [E.Info.SCM-1.NetworkInterface] dokumentierten Netzwerkschnittstellen verwendet wird, einschließlich:

— [E.Info.SCM-1.SCM.Protocol]: Kommunikationsprotokolle, bei denen der Mechanismus (aus [E.Info.SCM-1.NetworkInterface.Protocol]) angewendet wird; und

— [E.Info.SCM-1.SCM.States]: Gerätezustände, in denen die Kommunikation der in [E.Info.SCM-1.SecurityAsset] dokumentierten Sicherheitswerte und der in [E.Info.SCM-1.PrivacyAsset] dokumentierten Datenschutzwerte stattfindet; und

— [E.Info.SCM-1.SCM.SecObjectives]: Sicherheitszielsetzungen unter Berücksichtigung der vorgesehenen Funktionalität der Anlage und der analysierten Bedrohungen und potentiell erfolgreichen Angriffsszenarien (z. B. Offenlegung von Daten, Manipulation von Daten, unbefugte Kontrolle über die Anlage); und

— (wenn die Anlage den Aufbau oder die Verwaltung einer Verbindung unterstützt) [E.Info.SCM-1.SCM.Manage]: Einzelheiten zum Aufbau oder zum Verwaltungsverfahren.

[E.Info.DT.SCM-1]: Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 22 für jede der in [E.Info.SCM-1.NetworkInterface] dokumentierten maßgeblichen Netzwerkschnittstellen.

ANMERKUNG Aufgrund der Klassifizierung von Sicherheitswerten oder Datenschutzwerten und der in [E.Info.SCM-1.SCM.States] dokumentierten Gerätezustände müssen möglicherweise mehrere gültige Pfade dokumentiert werden.

[E.Just.DT.SCM-1]: Begründung für den gewählten Pfad durch den in [E.Info.DT.SCM-1] dokumentierten Entscheidungsbaum mit den folgenden Eigenschaften:

— (wenn eine Entscheidung aus [DT.SCM-1.DN-2] zu „NICHT ANWENDBAR“ führt) basiert die Begründung für die Entscheidung [DT.SCM-1.DN-2] auf [E.Info.SCM-1.SecurityAsset.TrustedEnv] und [E.Info.SCM-1.PrivacyAsset.TrustedEnv]; und

— (wenn eine Entscheidung aus [DT.SCM-1.DN-3] zu „NICHT ANWENDBAR“ führt) basiert die Begründung für die Entscheidung [DT.SCM-1.DN-3] auf [E.Info.SCM-1.SecurityAssets.AddMeasures] und [E.Info.SCM-1.NetworkAssets.AddMeasures].

#### 6.5.1.4.4 Konzeptuelle Beurteilung

##### 6.5.1.4.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob sichere Kommunikationsmechanismen implementiert sind, wenn es erforderlich ist, die in [E.Info.SCM-1.SecurityAsset] dokumentierten Sicherheitswerte oder die in [E.Info.SCM-1.PrivacyAsset] dokumentierten Datenschutzwerte zu schützen, wenn sie über Netzwerkschnittstellen wie nach SCM-1 erforderlich kommuniziert werden.

##### 6.5.1.4.4.2 Voraussetzungen

Keine.

##### 6.5.1.4.4.3 Beurteilungseinheiten

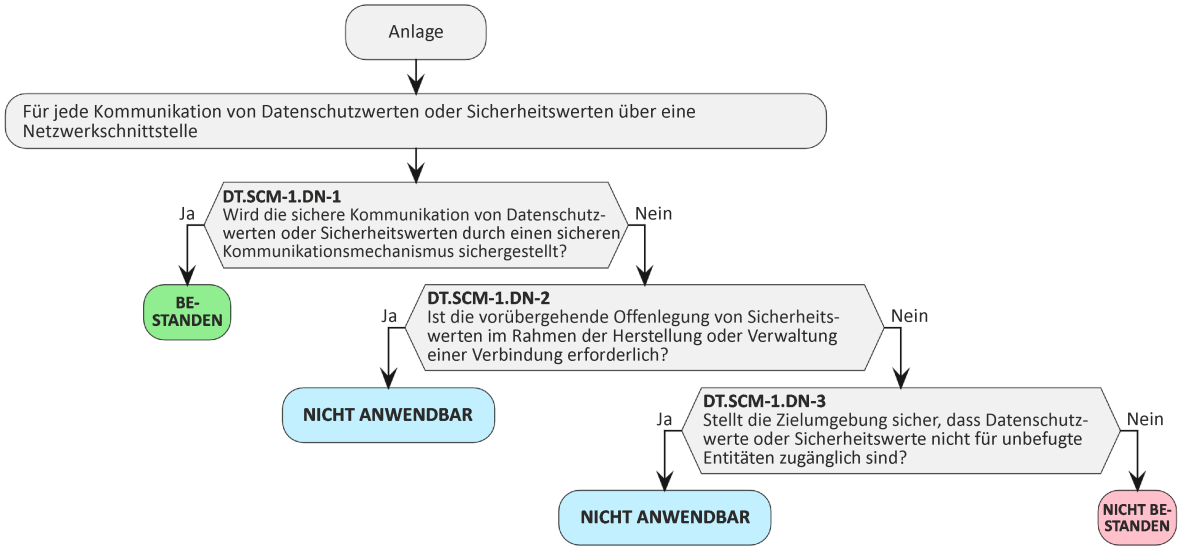



**Bild 22 — Entscheidungsbaum für Anforderung SCM-1**

Für jede in [E.Info.SCM-1.NetworkInterface] dokumentierte Netzwerkschnittstelle ist zu prüfen, ob der Pfad durch den in [E.Info.DT.SCM-1] dokumentierten Entscheidungsbaum mit „NICHT ANWENDBAR“ oder „BESTANDEN“ endet.

Für jeden in [E.Info.DT.SCM-1] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.SCM-1] dokumentierte Begründung zu untersuchen.

#### 6.5.1.4.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— mindestens ein Pfad durch den in [E.Info.DT.SCM-1] dokumentierten Entscheidungsbaum mit „BESTANDEN“ endet; und

— kein Pfad durch den in [E.Info.DT.SCM-1] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; und

— die in [E.Just.DT.SCM-1] angegebenen Informationen korrekte Begründungen für alle Pfade durch den in [E.Info.DT.SCM-1] dokumentierten Entscheidungsbaum sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— ein Pfad durch den in [E.Info.DT.SCM-1] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; oder

— eine in [E.Just.DT.SCM-1] angegebene Begründung für einen Pfad durch den in [E.Info.DT.SCM-1] dokumentierten Entscheidungsbaum nicht korrekt ist oder fehlt.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

#### 6.5.1.4.5 Beurteilung der funktionalen Vollständigkeit

##### 6.5.1.4.5.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob die Dokumentation vollständig ist.

##### 6.5.1.4.5.2 Voraussetzungen

Die Anlage befindet sich im Betriebszustand.

##### 6.5.1.4.5.3 Beurteilungseinheiten

Durch die Anwendung aktueller Bewertungsmethoden ist funktional zu beurteilen, ob gespeicherte Sicherheitswerte kommuniziert werden, die nicht in [E.Info.SCM-1.SecurityAsset] aufgeführt sind.

Durch die Anwendung aktueller Bewertungsmethoden ist funktional zu beurteilen, ob Datenschutzwerte kommuniziert werden, die nicht in [E.Info.SCM-1.PrivacyAsset] aufgeführt sind.

##### 6.5.1.4.5.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn alle gefundenen kommunizierten und gespeicherten Sicherheitswerte in [E.Info.SCM-1.SecurityAsset] dokumentiert sind und alle gefundenen Datenschutzwerte in [E.Info.SCM-1.PrivacyAsset] dokumentiert sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn ein übertragener gespeicherter Sicherheitswert gefunden wird, der nicht in [E.Info.SCM-1.SecurityAsset] dokumentiert ist, oder wenn ein Datenschutzwert gefunden wird, der nicht in [E.Info.SCM-1.PrivacyAsset] dokumentiert ist.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

#### 6.5.1.4.6 Beurteilung der funktionalen Suffizienz

##### 6.5.1.4.6.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob sichere Kommunikationsmechanismen implementiert wurden, wo sie erforderlich sind.

#### 6.5.1.4.6.2 Voraussetzungen

Die Anlage befindet sich im Betriebszustand.

#### 6.5.1.4.6.3 Beurteilungseinheiten

Für jeden in [E.Info.SCM-1.SecurityAsset] dokumentierten Sicherheitswert und für jeden in [E.Info.SCM-1.PrivacyAsset] dokumentierten Datenschutzwert ist funktional durch die Anwendung aktueller Bewertungsmethoden das Vorhandensein von sicheren Kommunikationsmechanismen entsprechend [E.Info.SCM-1.SCM] zu bestätigen.

#### 6.5.1.4.6.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn kein Nachweis vorliegt, dass ein in [E.Info.SCM-1.SCM] dokumentierter sicherer Kommunikationsmechanismus nicht implementiert ist.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn ein Nachweis vorliegt, dass ein in [E.Info.SCM-1.SCM] dokumentierter sicherer Kommunikationsmechanismus nicht implementiert ist.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

### 6.5.2 [SCM-2] Angemessener Integritäts- und Authentizitätsschutz für sichere Kommunikationsmechanismen

#### 6.5.2.1 Anforderung

Jeder sichere Kommunikationsmechanismus, der nach SCM-1 erforderlich ist, muss bewährte Verfahrensweisen zum Schutz der Integrität und Authentizität der kommunizierten Sicherheitswerte und Datenschutzwerte anwenden, mit Ausnahme der Kommunikation von Sicherheitswerten oder Datenschutzwerten, bei denen:

— eine Abweichung von der bewährten Verfahrensweise zum Schutz der Integrität oder Authentizität aus Gründen der Interoperabilität erforderlich ist.

#### 6.5.2.2 Begründung

Sicherheitswerte und Datenschutzwerte benötigen während der Kommunikation einen Schutz gegen Manipulation. Ein Angreifer, der sich Zugang zum Netzwerk verschafft hat, könnte die Kommunikation abfangen und manipulieren (Man-in-the-Middle-Angriff). Die Anlage muss sicherstellen, dass die Kommunikation gegen diese Angriffe durch den Einsatz von Integritäts- und Authentizitätsschutzmechanismen geschützt ist. Der Schutz könnte durch das Protokoll, das für die Kommunikation der Sicherheitswerte oder Datenschutzwerte verwendet wird, oder durch ein zusätzliches Protokoll/zusätzliche Maßnahmen erreicht werden.

Der Integritäts- und Authentizitätsschutz gilt sowohl für die verschlüsselte als auch für die nicht verschlüsselte Kommunikation.

#### 6.5.2.3 Leitlinie

Im Zusammenhang mit sicherer Kommunikation bezieht sich die „bewährte Verfahrensweise“ darauf, dass zugelassene Protokolle mit entsprechender Konfiguration (siehe auch CRY-1) verwendet werden und dass die Implementation des Protokolls regelmäßig auf Schwachstellen überprüft wird (siehe GEC-1).

Ziel ist es, die Kommunikation vor Manipulationen zu schützen. Übliche Maßnahmen sind eine Kombination von Authentisierung und Integritätsschutz. Die Art und Weise, wie das anfängliche Vertrauensverhältnis zwischen der Anlage und einer anderen Entität hergestellt wird, ist entscheidend für die Sicherheit der Kommunikation. Die Maßnahmen können beispielsweise auf den Kommunikationskanal angewendet oder für den „Ende-zu-Ende“-Schutz verwendet werden. Der weitere Schutz der Integrität und

Authentizität kommunizierter Daten wird üblicherweise durch auf Verschlüsselung basierende Mitteilungsauthentisierungscode-(MAC-)Techniken erreicht.

Eine Abweichung von der bewährten Verfahrensweise ist nur aus Gründen der Interoperabilität im Rahmen der vorgesehenen Anlagenfunktionalität möglich. In diesem Fall müssen kompensierende logische oder physische Maßnahmen erwogen werden, um eine vergleichbare Sicherheitsstufe sicherzustellen.

Die Anlage muss anderen Kommunikationspartnern als Vorgabe bewährte Verfahrensweisen anbieten, selbst wenn aus Gründen der Interoperabilität auch andere Protokolle erforderlich sein könnten. Die angemessenen Maßnahmen dürfen sich abhängig von den der Kommunikation zugrundeliegenden Anwendungsfällen unterscheiden, um die vorgesehene Funktionalität der Anlage zu erfüllen.

Beispiele für zugelassene Protokolle, die zur Umsetzung einer sicheren Kommunikation verwendet werden können, wenn eine Konfiguration nach bewährten Verfahrensweisen (siehe auch CRY-1) vorgenommen wird, sind:

— Transportschichtsicherheit (TLS, en: Transport Layer Security)

— geschützter WLAN-Zugang (WPA, en: Wi-Fi Protected Access)

— passwortauthentifizierter Verbindungsaufbau (PACE, en: Password Authenticated Connection Establishment)

— symmetrische Verschlüsselungsverfahren (z. B. Advanced Encryption Standard – AES)

Unsichere Kommunikation wird oft nicht durch Mängel im Protokoll, sondern durch Fehler in der Implementation verursacht. Daher ist die Anforderung GEC-1 wichtig.

#### 6.5.2.4 Beurteilungskriterien

##### 6.5.2.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung SCM-2.

##### 6.5.2.4.2 Umsetzungskategorien

[IC.SCM-2.ManufSecret]: Die Methode besteht darin, das (anfängliche) Geheimnis einzuführen, das verwendet wird, um die Integrität und Authentizität der kommunizierten Datenschutzwerte und Sicherheitswerte bei der Herstellung der Anlagen sicherzustellen. Das Geheimnis ist individuell für ein Gerät und wird nur innerhalb dieses Gerätes verwendet. Der Schutz der Integrität und Authentizität selbst wird kanal- oder nachrichtenbasiert mit einem auf dem Geheimnis basierenden Nachrichtenauthentisierungscode realisiert.

[IC.SCM-2.SecChanExchange]: Die Methode zum Austausch der anfänglichen Geheimnisse stützt sich auf einen unabhängigen Kanal: Das (anfängliche) Geheimnis, das zur Sicherstellung der Integrität und Authentizität der übermittelten Datenschutzwerte und Sicherheitswerte verwendet wird, wird ausschließlich über einen zweiten Kanal ausgetauscht, der vom Kommunikationsmechanismus unabhängig ist. Der Schutz der Integrität und Authentizität selbst wird kanal- oder nachrichtenbasiert mit einem auf dem Geheimnis basierenden Nachrichtenauthentisierungscode realisiert.

BEISPIEL Eingabe eines gemeinsam genutzten Schlüssels über einen QR-Code oder manuelle Eingabe eines Geheimnisses

[IC.SCM-2.PKI-based]: Die Methode zur Authentisierung des Zertifikats, das zur Sicherstellung der Integrität und Authentizität der kommunizierten Datenschutzwerte und Sicherheitswerte verwendet wird, basiert ausschließlich auf der Signatur des von einer vertrauenswürdigen PKI ausgestellten Zertifikats. Der Schutz der Integrität und Authentizität selbst wird kanal- oder nachrichtenbasiert mit einem auf dem Geheimnis basierenden Nachrichtenauthentisierungscode realisiert.

BEISPIEL Nutzung von X.509-PKI-Zertifikaten für TLS

[IC.SCM-2.ThirdPartyTrust]: Die Methode zur Authentisierung des (anfänglichen) Geheimnisses, das verwendet wird, um die Integrität und Authentizität der kommunizierten Datenschutzwerte und Sicherheitswerte sicherzustellen, basiert ausschließlich auf einer bestehenden Vertrauensbeziehung zu einer Drittpartei, die die Authentizität des Geheimnisses bestätigt. Der Schutz der Integrität und Authentizität selbst wird kanal- oder nachrichtenbasiert mit einem auf dem Geheimnis basierenden Nachrichtenauthentisierungscode realisiert.

BEISPIEL Kerberos-Protokoll

[IC.SCM-2.Generic]: Die Methoden zur Sicherstellung der Integrität und Authentizität der (in [E.Info.SCM-2.PrivacyAsset] dokumentierten) kommunizierten Datenschutzwerte und Sicherheitswerte stützen sich nicht nur auf eine der in diesem Abschnitt beschriebenen Methoden.

#### 6.5.2.4.3 Erforderliche Informationen

[E.Info.SCM-2.SecurityAsset]: Beschreibung jedes gespeicherten Sicherheitswertes, der über die in [E.Info.SCM-2.NetworkInterface] dokumentierten Netzwerkschnittstellen kommuniziert wird und für den Integritäts- oder Authentizitätsschutz erforderlich ist, um die Datenschutzwerte der Anlage zu schützen, einschließlich:

— [E.Info.SCM-2.SecurityAsset.Com]: Beschreibung des Anwendungsfalls, in dem der Wert über eine in [E.Info.SCM-2.NetworkInterface] dokumentierte Netzwerkschnittstelle kommuniziert wird (z. B. Kopplung mit einer Basisstation).

ANMERKUNG 1 Die Informationen von [E.Info.SCM-2.SecurityAsset] sind eine Teilmenge von [E.Info.SCM-1.SecurityAsset].

[E.Info.SCM-2.PrivacyAsset]: Beschreibung jedes Datenschutzwertes, der über die in [E.Info.SCM-2.NetworkInterface] dokumentierten Netzwerkschnittstellen kommuniziert wird und für den Integritäts- oder Authentizitätsschutz erforderlich ist:

— [E.Info.SCM-2.PrivacyAsset.Com]: Beschreibung des Anwendungsfalls, in dem der Wert über eine in [E.Info.SCM-2.NetworkInterface] dokumentierte Netzwerkschnittstelle kommuniziert wird (z. B. Registrierung bei einem bestimmten Webdienst).

ANMERKUNG 2 Diese Informationen von [E.Info.SCM-2.PrivacyAsset] sind eine Teilmenge von [E.Info.SCM-1.PrivacyAsset].

[E.Info.SCM-2.NetworkInterface]: Beschreibung aller Netzwerkschnittstellen der Anlagen, einschließlich

— [E.Info.SCM-2.NetworkInterface.Protocol]: Alle implementierten Kommunikationsprotokolle und die implementierten Betriebsarten, die Version des Protokolls und gegebenenfalls die SW-Bibliothek, die für die Implementation verwendet wird.

[E.Info.SCM-2.SCM]: Beschreibung jedes sicheren Kommunikationsmechanismus, der nach SCM-1 für den Integritäts- und Authentizitätsschutz der in [E.Info.SCM-2.PrivacyAsset] dokumentierten kommunizierten Datenschutzwerte oder der in [E.Info.SCM-2.SecurityAsset] dokumentierten Sicherheitswerte erforderlich ist, einschließlich

— [E.Info.SCM-2.SCM.Capabilities]: Beschreibung der Sicherheitsmechanismen und kryptographischen Modi, die zum Schutz der Integrität und Authentizität der in [E.Info.SCM-2.SecurityAsset] dokumentierten Sicherheitswerte oder der in [E.Info.SCM-2.PrivacyAsset] dokumentierten Datenschutzwerte bei der Kommunikation über sichere Netzwerkschnittstellen verwendet werden; und

— (wenn die SCM-Umsetzung auf [IC.SCM-2.ManufSecret] basiert) [E.Info.SCM-2.SCM.ManufSecret]: Beschreibung, wie das anfängliche Vertrauen für den Integritäts- und Authentizitätsschutz erreicht wird

und wie es in dem in [E.Info.SCM-2.NetworkInterface.Protocol] dokumentierten Protokoll implementiert ist; und

— (wenn die SCM-Umsetzung auf [IC.SCM-2.SecChanExchange] basiert) [E.Info.SCM-2.SCM.SecChanExchange]: Beschreibung, wie der zweite Kanal realisiert und wie das Geheimnis für den Integritäts- und Authentizitätsschutz verwendet wird und wie es in dem in [E.Info.SCM-2.NetworkInterface.Protocol] dokumentierten Protokoll implementiert ist; und

— (wenn die SCM-Umsetzung auf [IC.SCM-2.PKI-based] basiert) [E.Info.SCM-2.SCM.PKI-based]: Beschreibung, wie die PKI-Zertifikate validiert werden und wie dies zum Integritäts- und Authentizitätsschutz in dem in [E.Info.SCM-2.NetworkInterface.Protocol] dokumentierten Protokoll implementiert ist; und

— (wenn die SCM-Umsetzung auf [IC.SCM-2.ThirdPartyTrust] basiert) [E.Info.SCM-2.SCM.ThirdPartyTrust]: Beschreibung, wie die bestehende Vertrauensbeziehung zu einer Drittpartei, die die Authentizität des Geheimnisses bestätigt, realisiert wird und wie dies für den Integritäts- und Authentizitätsschutz in dem in [E.Info.SCM-2.NetworkInterface.Protocol] dokumentierten Protokoll umgesetzt wird; und

— (wenn die SCM-Umsetzung auf [IC.SCM-2.Generic] basiert) [E.Info.SCM-2.SCM.Generic]: Beschreibung, wie der Integritäts- und Authentizitätsschutz in dem in [E.Info.SCM-2.NetworkInterface.Protocol] dokumentierten Protokoll realisiert wird; und

— (falls vorhanden) [E.Info.SCM-2.SCM.ImplDetail]: Verweisung auf versionierte Normen oder Spezifikationen, in denen die gewählte Umsetzungskategorie definiert ist, und gegebenenfalls auf die SW-Bibliothek, die für die Umsetzung verwendet wird; und

— [E.Info.SCM-2.SCM.CCK]: die Beschreibung der Eigenschaften der vertraulichen kryptographischen Schlüssel, die für den Integritäts- und Authentizitätsschutz verwendet werden (siehe CRY-1); und

— [E.Info.SCM-2.SCM.ThreatProtection]: die Beschreibung, wie der Mechanismus vor den folgenden Sicherheitsbedrohungen schützt:

  — Spoofing; und

  — Manipulation.

[E.Info.DT.SCM-2]: Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 23 für jeden in [E.Info.SCM-2.SCM] dokumentierten sicheren Kommunikationsmechanismus.

ANMERKUNG 3 Aufgrund der Klassifizierung von Sicherheitswerten oder Datenschutzwerten und der in [E.Info.SCM-2.SCM] dokumentierten Gerätezustände benötigen möglicherweise mehrere gültige Pfade eine Dokumentation.

[E.Just.DT.SCM-2]: Begründung für den gewählten Pfad durch den in [E.Info.DT.SCM-2] dokumentierten Entscheidungsbaum mit den folgenden Eigenschaften:

— die Begründung für die Entscheidung [DT.SCM-2.DN-1] basiert auf [E.Info.SCM-2 SecurityAsset.Com], [E.Info.SCM-2.PrivacyAsset.Com], [E.Info.SCM-2.SCM.ThreatProtection] und [E.Info.SCM-2.SCM.Capabilities]; und

— (wenn eine Entscheidung aus [DT.SCM-2.DN-2] zu „NICHT ANWENDBAR“ führt) basiert die Begründung für die Entscheidung [DT.SCM-2.DN-2] besonders auf [E.Info.SCM-2.SecurityAsset.Com], [E.Info.SCM-2.PrivacyAsset.Com] und [E.Info.SCM-2.SCM.Capabilities].

#### 6.5.2.4.4 Konzeptuelle Beurteilung

##### 6.5.2.4.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob alle sicheren Kommunikationsmechanismen der Anlage die Integrität und Authentizität der Sicherheitswerte und Datenschutzwerte wie nach SCM-2 erforderlich schützen.

##### 6.5.2.4.4.2 Voraussetzungen

Keine.

##### 6.5.2.4.4.3 Beurteilungseinheiten

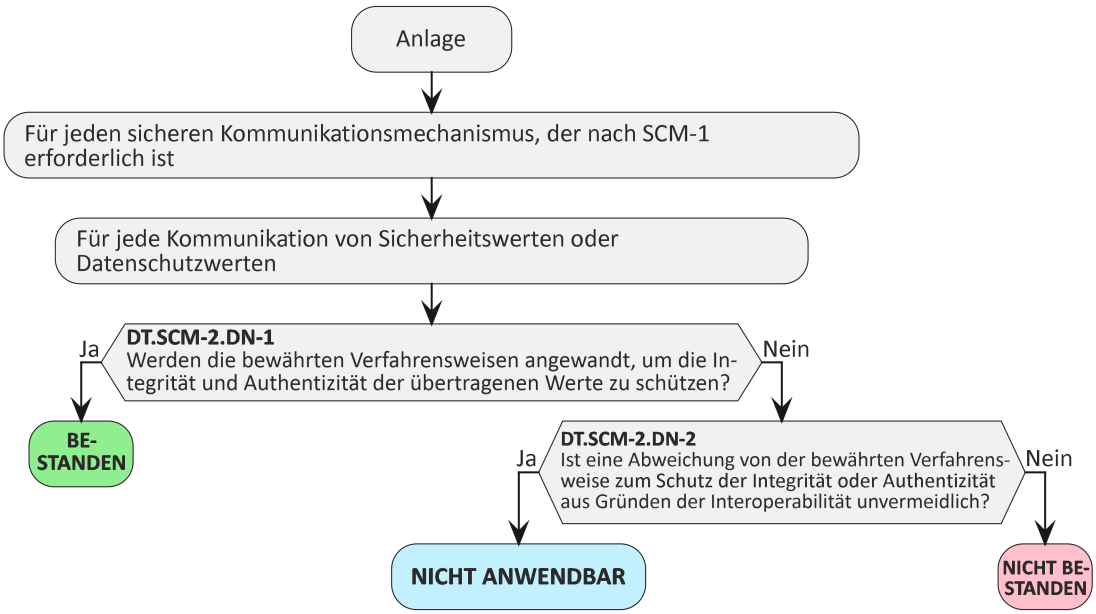



**Bild 23 — Entscheidungsbaum für Anforderung SCM-2**

Für jeden sicheren Kommunikationsmechanismus in [E.Info.SCM-2.SCM] und für jeden dokumentierten Gerätezustand ist zu prüfen, ob der Pfad durch den in [E.Info.DT.SCM-2] dokumentierten Entscheidungsbaum mit „BESTANDEN“ endet.

Für jeden in [E.Info.DT.SCM-2] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.SCM-2] dokumentierte Begründung zu untersuchen.

##### 6.5.2.4.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— mindestens ein Pfad durch den in [E.Info.DT.SCM-2] dokumentierten Entscheidungsbaum mit „BESTANDEN“ endet; und

— kein Pfad durch den in [E.Info.DT.SCM-2] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; und

— die in [E.Just.DT.SCM-2] angegebenen Informationen korrekte Begründungen für alle Pfade durch den in [E.Info.DT.SCM-2] dokumentierten Entscheidungsbaum sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— ein Pfad durch den in [E.Info.DT.SCM-2] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; oder

— eine in [E.Just.DT.SCM-2] angegebene Begründung für einen Pfad durch den in [E.Info.DT.SCM-2] dokumentierten Entscheidungsbaum nicht korrekt ist oder fehlt.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

#### 6.5.2.4.5 Beurteilung der funktionalen Vollständigkeit

Die Beurteilung der funktionalen Vollständigkeit wird durch die Beurteilung der funktionalen Suffizienz der Anwendbarkeit des sicheren Kommunikationsmechanismus abgedeckt.

Deshalb ist diese Beurteilung der funktionalen Vollständigkeit nicht notwendig.

#### 6.5.2.4.6 Beurteilung der funktionalen Suffizienz

##### 6.5.2.4.6.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob die kommunizierten Sicherheitswerte und Datenschutzwerte vor unbemerkter Manipulation geschützt sind.

##### 6.5.2.4.6.2 Voraussetzungen

Die Anlage befindet sich im Betriebszustand.

##### 6.5.2.4.6.3 Beurteilungseinheiten

Für jeden in [E.Info.SCM-2.SecurityAsset] dokumentierten Sicherheitswert und für jeden in [E.Info.SCM-2.PrivacyAsset] dokumentierten Datenschutzwert ist funktional zu bestätigen, dass der Integritäts- und Authentizitätsschutz durch die Kommunikationsmechanismen nach [E.Info.SCM-2.SCM] unter Berücksichtigung der dokumentierten Gerätezustände und unter Anwendung der dokumentierten Umsetzungskategorien sichergestellt ist:

[AU.SCM-2.ManufSecret]: Für [IC.SCM-2.ManufSecret] ist, wie in [E.Info.SCM-2.SCM.ManufSecret] dokumentiert, funktional zu bestätigen, dass:

— das bei der Produktion eingebrachte Geheimnis nicht abgefangen werden kann, während die Anlage über das Netzwerk kommuniziert; und

— eine manipulierte Nachricht nicht als integer akzeptiert wird; und

— eine unautorisierte Nachricht nicht als authentisch akzeptiert wird; und

— ein erfolgreicher MitM-Angriff nicht möglich ist, wenn eine kanalbasierte Kommunikation verwendet wird.

[AU.SCM-2.SecChanExchange]: Für [IC.SCM-2.SecChanExchange] ist, wie in [E.Info.SCM-2.SCM.SecChanExchange] dokumentiert, funktional zu bestätigen, dass:

— das Geheimnis mit Hilfe des beurteilten Kommunikationsmechanismus nicht abgefangen werden kann; und

— eine manipulierte Nachricht nicht als integer akzeptiert wird; und

— eine unautorisierte Nachricht nicht als authentisch akzeptiert wird; und

— ein erfolgreicher MitM-Angriff nicht möglich ist, wenn eine kanalbasierte Kommunikation verwendet wird.

[AU.SCM-2.PKI-based]: Für [IC.SCM-2.PKI-based] ist, wie in [E.Info.SCM-2.SCM.PKI-based] dokumentiert, funktional zu bestätigen, dass:

— ein gefälschtes Zertifikat nicht akzeptiert wird; und

— eine manipulierte Nachricht nicht als integer akzeptiert wird; und

— eine unautorisierte Nachricht nicht als authentisch akzeptiert wird; und

— ein erfolgreicher MitM-Angriff nicht möglich ist, wenn eine kanalbasierte Kommunikation verwendet wird.

[AU.SCM-2.ThirdPartyTrust]: Für [IC.SCM-2.ThirdPartyTrust] ist, wie in [E.Info.SCM-2.SCM.ThirdPartyTrust] dokumentiert, funktional zu bestätigen, dass:

— die Antwort der dritten Partei nicht manipuliert werden kann; und

— eine manipulierte Nachricht nicht als integer akzeptiert wird; und

— eine unautorisierte Nachricht nicht als authentisch akzeptiert wird; und

— ein erfolgreicher MitM-Angriff nicht möglich ist, wenn eine kanalbasierte Kommunikation verwendet wird.

[AU.SCM-2.Generic]: Für [IC.SCM-2.Generic] ist funktional zu bestätigen, dass:

— die zum Schutz der Authentizität und Integrität verwendeten Geheimnisse nicht abgefangen und missbraucht werden können; und

— eine manipulierte Nachricht nicht als integer akzeptiert wird; und

— eine unautorisierte Nachricht nicht als authentisch akzeptiert wird; und

— ein erfolgreicher MitM-Angriff nicht möglich ist, wenn eine kanalbasierte Kommunikation verwendet wird.

#### 6.5.2.4.6.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn für jeden in [E.Info.SCM-2.SCM] dokumentierten sicheren Kommunikationsmechanismus die Bestätigungen in der von der Umsetzungskategorie abhängigen Beurteilungseinheit erfolgreich sind.

Die Entscheidung NICHT BESTANDEN für den Beurteilungsfall wird zugewiesen, wenn für einen in [E.Info.SCM-2.SCM] dokumentierten sicheren Kommunikationsmechanismus eine Bestätigung in der von der Umsetzungskategorie abhängigen Beurteilungseinheit nicht erfolgreich ist.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

### 6.5.3 [SCM-3] Angemessener Vertraulichkeitsschutz für sichere Kommunikationsmechanismen

#### 6.5.3.1 Anforderung

Jeder sichere Kommunikationsmechanismus, der nach SCM-1 erforderlich ist, muss bewährte Verfahrensweisen zum Schutz der Vertraulichkeit der kommunizierten Datenschutzwerte und Sicherheitswerte anwenden, mit Ausnahme der Kommunikation von Sicherheitswerten oder Datenschutzwerten, bei denen:

— eine Abweichung von der bewährten Verfahrensweise zum Schutz der Vertraulichkeit aus Gründen der Interoperabilität erforderlich ist.

#### 6.5.3.2 Begründung

Sicherheitswerte und Datenschutzwerte benötigen während der Kommunikation im Allgemeinen einen Schutz gegen Abhören. Ein Angreifer, der sich Zugang zum Netzwerk verschafft hat, über das die Anlagen Sicherheitswerte oder Datenschutzwerte kommunizieren, könnte die Kommunikation überwachen. Die Anlage muss sicherstellen, dass die Kommunikation gegen diese Angriffe geschützt ist, indem Vertraulichkeit hergestellt wird.

#### 6.5.3.3 Leitlinie

Im Zusammenhang mit sicherer Kommunikation bezieht sich die „bewährte Verfahrensweise“ darauf, dass zugelassene Protokolle mit entsprechender Konfiguration (insbesondere hinsichtlich der integrierten Kryptographie, siehe CRY-1) verwendet werden und dass die Implementation des Protokolls regelmäßig auf Schwachstellen überprüft wird (siehe GEC-1).

Es gibt unterschiedliche Sicherheitsmechanismen, die zur Sicherung der Vertraulichkeit der Kommunikation der Anlage angewendet werden können (siehe auch CRY-1). Es sollten bewährte Verfahrensweisen für die Konfiguration verwendet werden, um die Kommunikation vor Abhören zu schützen. Dies wird üblicherweise durch symmetrische Verschlüsselungsverfahren erreicht. Die Verfahren können auf den Kommunikationskanal angewendet oder für den „Ende-zu-Ende“-Schutz verwendet werden. Es wird empfohlen, standardmäßig für Vertraulichkeit zwischen den kommunizierenden Entitäten zu sorgen und bewährte Verfahrensweisen für Kryptographie einzusetzen. Wenn die Notwendigkeit besteht, von bewährten Verfahrensweisen abzuweichen (z. B. aus Gründen der Interoperabilität), sollten die sich daraus ergebenden Risiken für die „bewährten Verfahrensweisen für Sicherheit“ beurteilt werden. Die angemessenen Maßnahmen können sich abhängig von den der Kommunikation zugrundeliegenden Anwendungsfällen unterscheiden, um die vorgesehene Funktionalität der Anlage zu erfüllen.

Eine Abweichung von der bewährten Verfahrensweise ist nur aus Gründen der Interoperabilität im Rahmen der vorgesehenen Anlagenfunktionalität möglich. In diesem Fall müssen kompensierende logische oder physische Maßnahmen erwogen werden, um eine vergleichbare Sicherheitsstufe sicherzustellen.

Wenn die Vertraulichkeit über eine lange Zeitspanne gewahrt werden muss, empfiehlt sich die Verwendung von Kryptographie und kryptographischen Protokollen, die eine perfekte Geheimhaltung der kommunizierten Datenschutzwerte und Sicherheitswerte durchsetzen.

Die Verschlüsselungsverfahren, die zum Schutz der Vertraulichkeit der übertragenen Daten verwendet werden, sind in der Anforderung CRY-1 festgelegt.

ANMERKUNG Authentisierte Verschlüsselung (en: Authenticated Encryption, AE) kann eingesetzt werden, um die Vertraulichkeit und Authentizität der Daten mit einem einzigen Verschlüsselungsverfahren sicherzustellen. Diese Verfahren können auch verwendet werden, um die Anforderung SCM-2 zu erfüllen.

#### 6.5.3.4 Beurteilungskriterien

##### 6.5.3.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung SCM-3.

##### 6.5.3.4.2 Umsetzungskategorien

[IC.SCM-3.MessageEnc]: Die sendende und die empfangende Entität haben bereits ein Geheimnis über eine Vertrauensbeziehung ausgetauscht, die die Grundlage für die Verschlüsselung bildet. Die Methode besteht darin, dass jede Nachricht den Schlüssel für die Inhaltsverschlüsselung kapselt, um die Nutzdaten der Nachricht zu entschlüsseln. Dieser Schlüssel wird symmetrisch oder asymmetrisch mit dem bestehenden Geheimnis verschlüsselt. Eine autorisierte empfangende Entität kann die Nutzdaten nur dann entschlüsseln, wenn sie im Besitz des Schlüssels ist, mit dem sie zuvor den Verschlüsselungscode für den Inhalt dechiffriert hat.

[IC.SCM-3.ChannelEnc]: Die sendende und die empfangende Entität haben bereits ein Geheimnis über eine Vertrauensbeziehung ausgetauscht, die die Grundlage für die Verschlüsselung bildet. Die Methode besteht darin, dass die Anlage und die empfangende Entität über denselben symmetrischen Schlüssel verfügen, der zur Ent- und Verschlüsselung der Nutzdaten der kommunizierten Nachrichten verwendet wird.

[IC.SCM-3.Generic]: Die Methoden zur Sicherstellung der Vertraulichkeit der übertragenen Datenschutzwerte und Sicherheitswerte stützen sich nicht nur auf eine der in diesem Abschnitt beschriebenen Methoden.

#### 6.5.3.4.3 Erforderliche Informationen

[E.Info.SCM-3.SecurityAsset]: Beschreibung jedes gespeicherten Sicherheitswertes, der über die in [E.Info.SCM-3.NetworkInterface] dokumentierten Netzwerkschnittstellen kommuniziert wird und für den Vertraulichkeit erforderlich ist, um die Datenschutzwerte der Anlage zu schützen, einschließlich:

— [E.Info.SCM-3.SecurityAsset.Com]: Beschreibung des Anwendungsfalls, in dem der Wert über eine in [E.Info.SCM-3.NetworkInterface] dokumentierte Netzwerkschnittstelle kommuniziert wird (z. B. Kopplung mit einer Basisstation).

ANMERKUNG 1 Die Informationen von [E.Info.SCM-3.SecurityAsset] sind eine Teilmenge von [E.Info.SCM-1.SecurityAsset].

[E.Info.SCM-3.PrivacyAsset]: Beschreibung aller Datenschutzwerte, die über in [E.Info.SCM-3.NetworkInterface] dokumentierten Netzwerkschnittstellen übertragen werden und für die Vertraulichkeit erforderlich ist, einschließlich

— [E.Info.SCM-3.PrivacyAsset.Com]: Beschreibung des Anwendungsfalls, in dem der Wert über eine in [E.Info.SCM-3.NetworkInterface] dokumentierte Netzwerkschnittstelle kommuniziert wird (z. B. Registrierung bei einem bestimmten Webdienst).

ANMERKUNG 2 Diese Informationen von [E.Info.SCM-3.PrivacyAsset] sind eine Teilmenge von [E.Info.SCM-1.PrivacyAsset].

[E.Info.SCM-3.NetworkInterface]: Beschreibung aller Netzwerkschnittstellen der Anlagen, einschließlich

— [E.Info.SCM-3.NetworkInterface.Protocol]: Alle implementierten Kommunikationsprotokolle und die implementierten Betriebsarten, die Version des Protokolls und gegebenenfalls die SW-Bibliothek, die für die Implementierung verwendet wird.

[E.Info.SCM-3.SCM]: Beschreibung jedes sicheren Kommunikationsmechanismus, der nach SCM-1 für den Vertraulichkeitsschutz der in [E.Info.SCM-3.PrivacyAsset] dokumentierten Datenschutzwerte oder der in [E.Info.SCM-3.PrivacyAsset] dokumentierten Datenschutzwerte erforderlich ist, einschließlich

— [E.Info.SCM-3.SCM.Capabilities]: Beschreibung der Sicherheitsmechanismen und kryptographischen Modi, die zum Schutz der Vertraulichkeit der in [E.Info.SCM-3.SecurityAsset] dokumentierten Sicherheitswerte oder der in [E.Info.SCM-3.PrivacyAsset] dokumentierten Datenschutzwerte bei der Kommunikation über Netzwerkschnittstellen verwendet werden; und

— (wenn die SCM-Umsetzung auf [IC.SCM-3.MessageEnc] basiert) [E.Info.SCM-3.SCM.MessageEnc]: Beschreibung, wie der Inhaltsverschlüsselungscode für den Vertraulichkeitsschutz erzeugt und verschlüsselt wird und wie es in dem in [E.Info.SCM-3.NetworkInterface.Protocol] dokumentierten Protokoll implementiert ist; und

— (wenn die SCM-Umsetzung auf [IC.SCM-3.ChannelEnc] basiert) [E.Info.SCM-3.SCM.ChannelEnc]: Beschreibung, wie der Sitzungsschlüssel für den Vertraulichkeitsschutz erzeugt und verwendet wird und wie es in dem in [E.Info.SCM-3.NetworkInterface.Protocol] dokumentierten Protokoll implementiert ist; und

— (wenn die SCM-Umsetzung auf [IC.SCM-3.Generic] basiert) [E.Info.SCM-3.SCM.Generic]: Beschreibung, wie der Vertraulichkeitsschutz in dem in [E.Info.SCM-3.NetworkInterface.Protocol] dokumentierten Protokoll realisiert wird; und

— (falls vorhanden) [E.Info.SCM-3.SCM.ImplDetail]: Verweisung auf versionierte Normen oder Spezifikationen, in denen die gewählte Umsetzungskategorie definiert ist, und gegebenenfalls auf die SW-Bibliothek, die für die Umsetzung verwendet wird; und

— [E.Info.SCM-3.SCM.CCK]: die Eigenschaften der vertraulichen kryptographischen Schlüssel, die für den Vertraulichkeitsschutz verwendet werden (siehe CRY-1); und

— [E.Info.SCM-3.SCM.ThreatProtection]: Wie der Mechanismus mindestens vor den folgenden Sicherheitsbedrohungen schützt:

  — Informationsoffenlegung; und

  — Ausweitung der Privilegien.

[E.Info.DT.SCM-3]: Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 24 für jeden in [E.Info.SCM-3.SCM] dokumentierten sicheren Kommunikationsmechanismus.

ANMERKUNG 3 Aufgrund der Klassifizierung von Sicherheitswerten oder Datenschutzwerten und der in [E.Info.SCM-3.SCM] dokumentierten Gerätezustände müssen möglicherweise mehrere gültige Pfade dokumentiert werden.

[E.Just.DT.SCM-3]: Begründung für den gewählten Pfad durch den in [E.Info.DT.SCM-3] dokumentierten Entscheidungsbaum mit den folgenden Eigenschaften:

— Die Begründung für die Entscheidung [DT.SCM-3.DN-1] basiert auf [E.Info.SCM-3 SecurityAsset.Com], [E.Info.SCM-3.PrivacyAsset.Com], [E.Info.SCM-3.SCM.ThreatProtection] und [E.Info.SCM-3.SCM.Capabilities]; und

— (wenn eine Entscheidung aus [DT.SCM-3.DN-2 zu „NICHT ANWENDBAR“ führt) basiert die Begründung für die Entscheidung [DT.SCM-3.DN-2] besonders auf [E.Info.SCM-3.SecurityAsset.Com], [E.Info.SCM-3.PrivacyAsset.Com] und [E.Info.SCM-3.SCM.Capabilities].

#### 6.5.3.4.4 Konzeptuelle Beurteilung

##### 6.5.3.4.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob alle sicheren Kommunikationsmechanismen der Anlage die Vertraulichkeit der (in [E.Info.SCM-3.PrivacyAsset] dokumentierten) Datenschutzwerte und (in [E.Info.SCM-3.SecurityAsset] dokumentierten) Sicherheitswerte wie nach SCM-3 erforderlich schützen.

**Voraussetzungen**

Keine.

#### 6.5.3.4.4.2 Beurteilungseinheiten

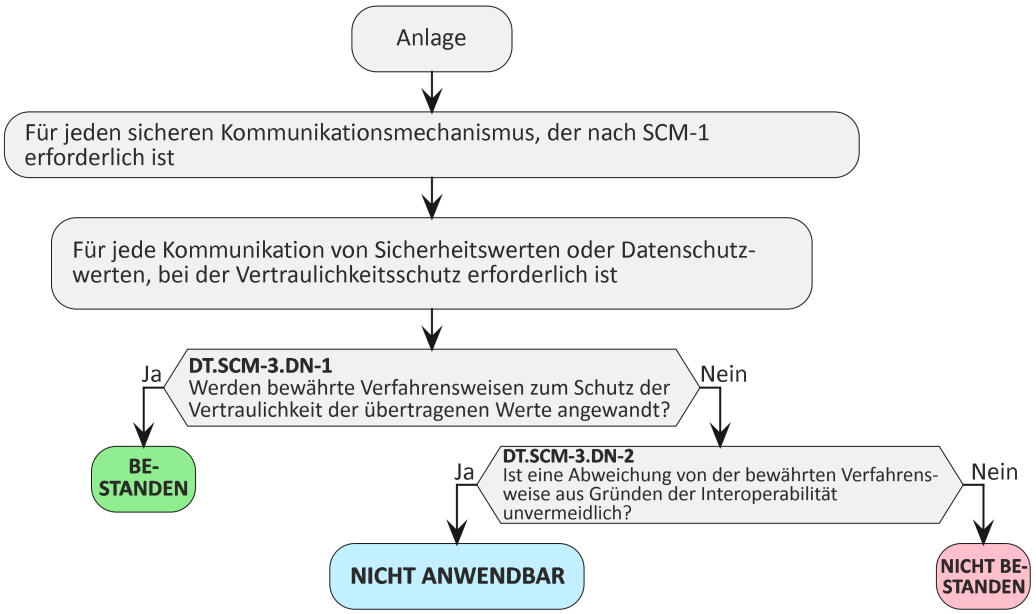



**Bild 24 — Entscheidungsbaum für Anforderung SCM-3**

Für jeden sicheren in [E.Info.SCM-3.SCM] dokumentierten Kommunikationsmechanismus und für jeden dokumentierten Gerätezustand ist zu prüfen, ob der Pfad durch den in [E.Info.DT.SCM-3] dokumentierten Entscheidungsbaum mit „BESTANDEN“ endet.

Für jeden in [E.Info.DT.SCM-3] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.SCM-3] dokumentierte Begründung zu untersuchen.

#### 6.5.3.4.4.3 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— mindestens ein Pfad durch den in [E.Info.DT.SCM-3] dokumentierten Entscheidungsbaum mit „BESTANDEN“ endet; und

— kein Pfad durch den in [E.Info.DT.SCM-3] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; und

— die in [E.Just.DT.SCM-3] angegebenen Informationen korrekte Begründungen für alle Pfade durch den in [E.Info.DT.SCM-3] dokumentierten Entscheidungsbaum sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— ein Pfad durch den in [E.Info.DT.SCM-3] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; oder

— eine in [E.Just.DT.SCM-3] angegebene Begründung für einen Pfad durch den in [E.Info.DT.SCM-3] dokumentierten Entscheidungsbaum nicht korrekt ist oder fehlt.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

#### 6.5.3.4.5 Beurteilung der funktionalen Vollständigkeit

Die Beurteilung der funktionalen Vollständigkeit wird durch die Beurteilung der funktionalen Suffizienz der Anwendbarkeit des sicheren Kommunikationsmechanismus abgedeckt.

Deshalb ist diese Beurteilung der funktionalen Vollständigkeit nicht notwendig.

#### 6.5.3.4.6 Beurteilung der funktionalen Suffizienz

##### 6.5.3.4.6.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob die kommunizierten Sicherheitswerte und Datenschutzwerte vor Abhören geschützt sind.

##### 6.5.3.4.6.2 Voraussetzungen

Die Anlage befindet sich im Betriebszustand.

##### 6.5.3.4.6.3 Beurteilungseinheiten

Für jeden in [E.Info.SCM-3.SecurityAsset] dokumentierten Sicherheitswert und jeden in [E.Info.SCM-3.PrivacyAsset] dokumentierten Datenschutzwert ist eine rechtmäßige Kommunikation zwischen der Anlage und einem autorisierten Kommunikationsendpunkt durchzuführen. Es ist funktional zu bestätigen, dass der Vertraulichkeitsschutz durch die Kommunikationsmechanismen nach [E.Info.SCM-3.SCM] unter Berücksichtigung der dokumentierten Gerätezustände und unter Anwendung der dokumentierten Umsetzungskategorien sichergestellt ist:

[AU.SCM-3.MessageEnc]: Für [IC.SCM-3.MessageEnc] ist, wie in [E.Info.SCM-3.SCM.MessageEnc] dokumentiert, funktional zu bestätigen, dass:

— der Schlüssel innerhalb der Nachricht, der zur Verschlüsselung der Nutzdaten verwendet wird, nicht offengelegt werden kann; und

— die kommunizierten Sicherheitswerte und Datenschutzwerte nicht abgehört werden können.

[AU.SCM-3.ChannelEnc]: Für [IC.SCM-3.ChannelEnc] ist, wie in [E.Info.SCM-3.SCM.ChannelEnc] dokumentiert, funktional zu bestätigen, dass:

— der Schlüssel, der zur Verschlüsselung der Nachrichten innerhalb des Kommunikationskanals verwendet wird, nicht abgefangen werden kann; und

— die kommunizierten Sicherheitswerte und Datenschutzwerte nicht abgehört werden können.

[AU.SCM-3.Generic]: Für [IC.SCM-3.Generic] ist, wie in [E.Info.SCM-3.SCM.Generic] dokumentiert, funktional zu bestätigen, dass:

— das zur Verschlüsselung der Nachricht verwendete Geheimnis nicht abgefangen oder abgehört werden kann; und

— der verschlüsselte Inhalt der Nachricht nicht abgehört oder offengelegt werden kann.

##### 6.5.3.4.6.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn für jeden in [E.Info.SCM-3.SCM] dokumentierten sicheren Kommunikationsmechanismus die Bestätigungen in der von der Umsetzungskategorie abhängigen Beurteilungseinheit erfolgreich sind.

Die Entscheidung NICHT BESTANDEN für den Beurteilungsfall wird zugewiesen, wenn für einen in [E.Info.SCM-3.SCM] dokumentierten sicheren Kommunikationsmechanismus eine Bestätigung in der von der Umsetzungskategorie abhängigen Beurteilungseinheit nicht erfolgreich ist.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

### 6.5.4 [SCM-4] Angemessener Replay-Schutz für sichere Kommunikationsmechanismen

#### 6.5.4.1 Anforderung

Jeder sichere Kommunikationsmechanismus, der nach SCM-1 erforderlich ist, muss bewährte Verfahrensweisen zum Schutz der gegen Replay-Angriffe übertragenen Sicherheitswerte und Datenschutzwerte anwenden, mit Ausnahme der Kommunikation von Sicherheitswerten oder Datenschutzwerten, bei denen:

— eine zweifache Übertragung keine Bedrohung durch einen Replay-Angriff verursacht; oder

— eine Abweichung von der bewährten Verfahrensweise zum Replay-Schutz aus Gründen der Interoperabilität erforderlich ist.

#### 6.5.4.2 Begründung

Ein Replay-Angriff ist eine Netzwerkangriffsart, bei der eine gültige Datenübertragung böswillig wiederholt wird. Ein Angreifer, der sich Zugang zum Netzwerk verschafft hat, könnte die Kommunikation aufzeichnen und unverändert wieder abspielen, was zu unerwünschten Auswirkungen bei der empfangenden Entität führen kann. Ein Replay-Angriff stellt insbesondere dann eine Bedrohung dar, wenn die Authentisierung unterlaufen werden kann oder nicht autorisierte Steuerbefehle übermittelt werden können.

Wird beispielsweise während eines Benutzer-Anmeldevorgangs das Passwort verschlüsselt, aber ohne Replay-Schutz (insbesondere Schutz vor Session Hijacking) übertragen, könnte ein Angreifer in der Lage sein, den Teil der Kommunikation mit der verschlüsselten Anmeldung zu wiederholen und so böswillig einen autorisierten Zugang zum Gerät zu erhalten. Ein Session-Hijacking-Angriff besteht in der Ausnutzung des Web-Sitzungssteuerungsmechanismus, der üblicherweise für ein Sitzungstoken verwaltet wird.

Die Anlage muss die Kommunikation vor dieser Klasse von Angriffen schützen.

Auf der Grundlage einer Gefährdungseinschätzung könnten Anwendungsfälle identifiziert werden, für die möglicherweise kein Replay-Schutz erforderlich ist, z. B. wenn die übertragenen Daten nicht zu einer Zustandsänderung bei der empfangenden Entität führen. So stellt beispielsweise die Anforderung, ein X.509-Zertifikat von einem Server abzurufen, möglicherweise kein Risiko für einen Replay-Angriff dar.

#### 6.5.4.3 Leitlinie

Replay-Angriffe können üblicherweise verhindert werden, indem jede Nachricht einer Kommunikationssitzung mit einer Sitzungs-ID und einem Zähler gekennzeichnet wird. Die Sitzungs-ID verhindert Replay-Angriffe der gesamten Kommunikation, während der Zähler die Wiederholung einer spezifischen Nachricht innerhalb einer Kommunikationssitzung verhindert. Außerdem können Zeitstempel oder eine einmalige Verschlüsselungstechnik verwendet werden, um Replay-Angriffe zu verhindern. Dennoch ist die Umsetzung des Schutzes vor Replay-Angriffen komplex. Daher muss zunächst die Nutzung zugelassener Protokolle in Betracht gezogen werden, die bereits einen Schutz vor Replay-Angriffen bieten. Beispiele für zugelassene Protokolle, die zur Umsetzung einer sicheren Kommunikation verwendet werden können, wenn eine Konfiguration nach bewährten Verfahrensweisen (siehe auch CRY-1) vorgenommen wird, sind:

— Transportschichtsicherheit (TLS, en: Transport Layer Security)

— Secure Socket Shell (SSH)

— Sicherheitsprotokolle im Internet (IPsec, en: Internet Protocol Security)

#### 6.5.4.4 Beurteilungskriterien

##### 6.5.4.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung SCM-4.

##### 6.5.4.4.2 Umsetzungskategorien

[IC.SCM-4.SeqNumb]: Die sendende und die empfangende Entität haben bereits ein Geheimnis über eine Vertrauensbeziehung ausgetauscht, die die Grundlage für den Mitteilungsauthentisierungscode zur Sicherstellung der Integrität der Kommunikation bildet. Die Methode besteht darin, dass jeder übermittelten Nachricht eine eindeutige Sequenznummer zugewiesen wird. Wenn der Empfänger eine Nachricht empfängt, prüft er die Sequenznummer, um sicherzustellen, dass er die Nachricht noch nicht erhalten hat. Wurde die Sequenznummer bereits gesehen, wird die Nachricht als Replay-Angriff verworfen.

ANMERKUNG 1 Zum Schutz vor MitM-Angriffen kann die Authentizität der Sequenznummer sichergestellt werden, indem sie als Eingabe für die Funktion verwendet wird, die den Mitteilungsauthentisierungscode (MAC, en: message authentication code) erzeugt.

[IC.SCM-4.TimeStamp]: Die sendende und die empfangende Entität haben bereits ein Geheimnis über eine Vertrauensbeziehung ausgetauscht, die die Grundlage für den Mitteilungsauthentisierungscode zur Sicherstellung der Integrität der Kommunikation bildet. Die Methode besteht darin, dass die Anlage Zeitstempel in die Nachrichten integriert, um sicherzustellen, dass sie nicht zu einem späteren Zeitpunkt erneut übertragen werden. Der Empfänger prüft den Zeitstempel, um sicherzustellen, dass die Nachricht nicht zu weit in der Vergangenheit oder in der Zukunft erstellt wurde.

ANMERKUNG 2 Zum Schutz vor MitM-Angriffen kann die Authentizität des Zeitstempels sichergestellt werden, indem sie als Eingabe für die Funktion verwendet wird, die den Mitteilungsauthentisierungscode (MAC) erzeugt.

[IC.SCM-4.OneTimeEncKey]: Die sendende und die empfangende Entität haben bereits ein Geheimnis über eine Vertrauensbeziehung ausgetauscht, die die Grundlage für den Mitteilungsauthentisierungscode zur Sicherstellung der Integrität der Kommunikation bildet. Die Methode besteht darin, dass die Anlage und der Empfänger einen völlig zufälligen Sitzungsschlüssel erstellen, eine Art Code, der nur für eine Transaktion gültig ist und nicht wiederverwendet werden kann.

[IC.SCM-4.Generic]: Die Methoden zur Vermeidung von Replay-Angriffen in Bezug auf übertragene Datenschutzwerte und Sicherheitswerte stützen sich nicht nur auf eine der in diesem Abschnitt beschriebenen Methoden.

##### 6.5.4.4.3 Erforderliche Informationen

[E.Info.SCM-4.SecurityAsset]: Beschreibung jedes gespeicherten Sicherheitswertes, der über die in [E.Info.SCM-4.NetworkInterface] dokumentierten Netzwerkschnittstellen kommuniziert wird und für den Replay-Schutz erforderlich ist, um die Datenschutzwerte der Anlage zu schützen, einschließlich:

— [E.Info.SCM-4.SecurityAsset.Com]: Beschreibung des Anwendungsfalls, in dem der Wert über eine in [E.Info.SCM-4.NetworkInterface] dokumentierte Netzwerkschnittstelle kommuniziert wird (z. B. Kopplung mit einer Basisstation).

ANMERKUNG 3 Die Informationen von [E.Info.SCM-4.SecurityAsset] sind eine Teilmenge von [E.Info.SCM-1.SecurityAsset].

[E.Info.SCM-4.PrivacyAsset]: Beschreibung jedes Datenschutzwertes, der über die in [E.Info.SCM-4.NetworkInterface] dokumentierten Netzwerkschnittstellen kommuniziert wird und für den Replay-Schutz erforderlich ist, einschließlich

— [E.Info.SCM-4.PrivacyAsset.Com]: Beschreibung des Anwendungsfalls, in dem der Wert über eine in [E.Info.SCM-4.NetworkInterface] dokumentierte Netzwerkschnittstelle kommuniziert wird (z. B. Kopplung mit einer Basisstation).

ANMERKUNG 4 Diese Informationen von [E.Info.SCM-4.PrivacyAsset] sind eine Teilmenge von [E.Info.SCM-1.PrivacyAsset].

[E.Info.SCM-4.NetworkInterface]: Beschreibung jeder Netzwerkschnittstelle der Anlagen, einschließlich

— [E.Info.SCM-4.NetworkInterface.Protocol]: Alle implementierten Kommunikationsprotokolle und die implementierten Betriebsarten, die Version des Protokolls und gegebenenfalls die SW-Bibliothek, die für die Implementation verwendet wird.

[E.Info.SCM-4.SCM]: Beschreibung jedes sicheren Kommunikationsmechanismus, der nach SCM-1 für den Replay-Schutz der in [E.Info.SCM-4.PrivacyAsset] dokumentierten kommunizierten Datenschutzwerte oder der in [E.Info.SCM-4.SecurityAsset] dokumentierten Sicherheitswerte erforderlich ist, einschließlich

— [E.Info.SCM-4.SCM.Capabilities]: Beschreibung der Sicherheitsmechanismen und kryptographischen Modi, die zur Vermeidung von Replay-Angriffen auf die Kommunikation mit in [E.Info.SCM-4.SecurityAsset] dokumentierten Sicherheitswerten oder die in [E.Info.SCM-4.PrivacyAsset] dokumentierten Datenschutzwerte verwendet werden; und

— (wenn die SCM-Umsetzung auf [IC.SCM-4.SeqNumb] basiert) [E.Info.SCM-4.SCM.SeqNumb]: Beschreibung, wie die Sequenznummern verwendet und in den Mitteilungsauthentisierungscode für den Replay-Schutz integriert werden und wie es in dem in [E.Info.SCM-4.NetworkInterface.Protocol] dokumentierten Protokoll implementiert ist; und

— (wenn die SCM-Umsetzung auf [IC.SCM-4.TimeStamp] basiert) [E.Info.SCM-4.SCM.TimeStamp]: Beschreibung, wie die Zeitstempel verwendet und in den Mitteilungsauthentisierungscode für den Replay-Schutz integriert werden und wie dies in dem in [E.Info.SCM-4.NetworkInterface.Protocol] dokumentierten Protokoll implementiert ist; und

— (wenn die SCM-Umsetzung auf [IC.SCM-4.OneTimeEncKey] basiert) [E.Info.SCM-4.SCM.OneTimeEncKey]: Beschreibung, wie der einmalige Verschlüsselungscode generiert und für den Replay-Schutz verwendet wird und wie er in dem in [E.Info.SCM-4.NetworkInterface.Protocol] dokumentierten Protokoll implementiert ist; und

— (wenn die SCM-Umsetzung auf [IC.SCM-4.Generic] basiert) [E.Info.SCM-4.SCM.Generic]: Beschreibung, wie der Replay-Schutz in dem in [E.Info.SCM-4.NetworkInterface.Protocol] dokumentierten Protokoll realisiert wird; und

— (wenn Normen oder Spezifikationen verfügbar sind, in denen die ausgewählte Umsetzungskategorie definiert ist) [E.Info.SCM-4.SCM.ImplDetail]: Verweisung auf versionierte Normen oder Spezifikationen, in denen die gewählte Umsetzungskategorie definiert ist, und gegebenenfalls auf die SW-Bibliothek, die für die Umsetzung verwendet wird; und

— [E.Info.SCM-4.SCM.Repudiation]: Beschreibung, wie der Mechanismus mindestens gegen die Sicherheitsbedrohung „Ablehnung“ schützt.

[E.Info.DT.SCM-4]: Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 25 für jeden in [E.Info.SCM-4.SCM] dokumentierten Kommunikationsmechanismus.

ANMERKUNG 5 Aufgrund der Klassifizierung von Sicherheitswerten oder Datenschutzwerten und der in [E.Info.SCM-4.SCM] dokumentierten Gerätezustände müssen möglicherweise mehrere gültige Pfade dokumentiert werden.

[E.Just.DT.SCM-4]: Begründung für den gewählten Pfad durch den in [E.Info.DT.SCM-4] dokumentierten Entscheidungsbaum mit den folgenden Eigenschaften:

— (wenn eine Entscheidung aus [DT.SCM-4.DN-1 zu „NICHT ANWENDBAR“ führt) basiert die Begründung für die Entscheidung [DT.SCM-4.DN-1] auf [E.Info.SCM-4.SecurityAsset.Com], [E.Info.SCM-4.PrivacyAsset.Com], [E.Info.SCM-4.SCM.Capabilities] und [E.Info.SCM-4.SCM.Repudiation]; und

— (wenn eine Entscheidung aus [DT.SCM-4.DN-3] zu „NICHT ANWENDBAR“ führt) basiert die Begründung für die Entscheidung [DT.SCM-4.DN-3] besonders auf [E.Info.SCM-4.SecurityAsset.Com], [E.Info.SCM-4.PrivacyAsset.Com] und [E.Info.SCM-4.SCM.Capabilities].

#### 6.5.4.4.4 Konzeptuelle Beurteilung

##### 6.5.4.4.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob alle sicheren Kommunikationsmechanismen der Anlage die Kommunikation der übertragenen Sicherheitswerte und Datenschutzwerte vor Replay-Angriffen wie nach SCM-4 erforderlich schützen.

##### 6.5.4.4.4.2 Voraussetzungen

Keine.

##### 6.5.4.4.4.3 Beurteilungseinheiten

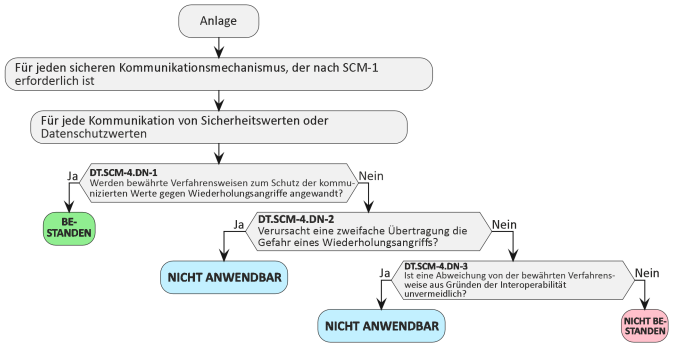



**Bild 25 — Entscheidungsbaum für Anforderung SCM-4**

Für jeden sicheren Kommunikationsmechanismus in [E.Info.SCM-4.SCM] und für jeden dokumentierten Gerätezustand ist zu prüfen, ob der Pfad durch den in [E.Info.DT.SCM-4] dokumentierten Entscheidungsbaum mit „NICHT ANWENDBAR“ oder „BESTANDEN“ endet.

Für jeden in [E.Info.DT.SCM-4] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.SCM-4] dokumentierte Begründung zu untersuchen.

##### 6.5.4.4.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— mindestens ein Pfad durch den in [E.Info.DT.SCM-4] dokumentierten Entscheidungsbaum mit „BESTANDEN“ endet; und

— kein Pfad durch den in [E.Info.DT.SCM-4] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; und

— die in [E.Just.DT.SCM-4] angegebenen Informationen korrekte Begründungen für alle Pfade durch den in [E.Info.DT.SCM-4] dokumentierten Entscheidungsbaum sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— ein Pfad durch den in [E.Info.DT.SCM-4] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN" endet; oder

— eine in [E.Just.DT.SCM-4] angegebene Begründung für einen Pfad durch den in [E.Info.DT.SCM-4] dokumentierten Entscheidungsbaum nicht korrekt ist oder fehlt.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

#### 6.5.4.4.5 Beurteilung der funktionalen Vollständigkeit

Die Beurteilung der funktionalen Vollständigkeit wird durch die Beurteilung der funktionalen Suffizienz der Anwendbarkeit des sicheren Kommunikationsmechanismus abgedeckt.

Deshalb ist diese Beurteilung der funktionalen Vollständigkeit nicht notwendig.

#### 6.5.4.4.6 Beurteilung der funktionalen Suffizienz

##### 6.5.4.4.6.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob die kommunizierten Sicherheitswerte und Datenschutzwerte vor Replay-Angriffen geschützt sind.

##### 6.5.4.4.6.2 Voraussetzungen

Die Anlage befindet sich im Betriebszustand.

##### 6.5.4.4.6.3 Beurteilungseinheiten

Für jeden in [E.Info.SCM-4.SecurityAsset] dokumentierten Sicherheitswert und jeden in [E.Info.SCM-4.PrivacyAsset] dokumentierten Datenschutzwert ist eine rechtmäßige Kommunikation zwischen der Anlage und einem autorisierten Kommunikationsendpunkt durchzuführen. Die Kommunikationssequenzen werden aufgezeichnet. Es ist funktional zu bestätigen, dass der Replay-Schutz durch die Kommunikationsmechanismen nach [E.Info.SCM-4.SCM] unter Berücksichtigung der dokumentierten Gerätezustände und unter Anwendung der dokumentierten Umsetzungskategorien sichergestellt ist:

[AU.SCM-4.SeqNumb]: Für [IC.SCM-4.SeqNumb] ist, wie in [E.Info.SCM-4.SCM.SeqNumb] dokumentiert, funktional zu bestätigen, dass:

— die eingehende Nachricht (Teil der Kommunikation von Sicherheitswerten und Datenschutzwerten) mit einer sich wiederholenden Sequenznummer wird nicht akzeptiert.

[AU.SCM-4.TimeStamp]: Für [IC.SCM-4.TimeStamp] ist, wie in [E.Info.SCM-4.SCM.TimeStamp] dokumentiert, funktional zu bestätigen, dass:

— die eingehende Nachricht (Teil der Kommunikation von Sicherheitswerten und Datenschutzwerten) mit unregelmäßigen Zeitstempeln wird nicht akzeptiert.

[AU.SCM-4.OneTimeEncKey]: Für [IC.SCM-4.OneTimeEncKey] ist, wie in [E.Info.SCM-4.SCM.OneTimeEncKey] dokumentiert, funktional zu bestätigen, dass:

— der Verschlüsselungscode nicht abgefangen werden kann; und

— dass das Duplikat (binäre Kopie) einer bereits akzeptierten Nachricht (Teil der Kommunikation von Sicherheitswerten und Datenschutzwerten) nicht erneut akzeptiert wird.

[AU.SCM-4.Generic]: Für [IC.SCM-4.Generic] ist, wie in [E.Info.SCM-4.SCM.Generic] dokumentiert, funktional zu bestätigen, dass:

— dass das Duplikat (binäre Kopie) einer bereits akzeptierten Nachricht (Teil der Kommunikation von Sicherheitswerten und Datenschutzwerten) nicht erneut akzeptiert wird.

#### 6.5.4.4.6.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn für jeden in [E.Info.SCM-4.SCM] dokumentierten sicheren Kommunikationsmechanismus mit den entsprechenden Methoden zur Sicherstellung des Replay-Schutzes für die Kommunikation von Sicherheitswerten und Datenschutzwerten die Bestätigungen in der von der Umsetzungskategorie abhängigen Beurteilungseinheit erfolgreich sind.

Die Entscheidung NICHT BESTANDEN für den Beurteilungsfall wird zugewiesen, wenn für einen in [E.Info.SCM-4.SCM] dokumentierten sicheren Kommunikationsmechanismus mit den entsprechenden Methoden zur Sicherstellung des Replay-Schutzes für die Kommunikation von Sicherheitswerten und Datenschutzwerten eine Bestätigung in der von der Umsetzungskategorie abhängigen Beurteilungseinheit nicht erfolgreich ist.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

## 6.6 [LGM] Protokollierungsmechanismus (en: Logging Mechanism)

### 6.6.1 [LGM-1] Anwendbarkeit von Protokollierungsmechanismen

#### 6.6.1.1 Anforderung

Die Anlage muss Protokollierungsmechanismen für interne Aktivitäten verwenden, die für die Datenschutzwerte und deren Schutz maßgeblich sind (als Ereignisse bezeichnet), außer für:

— interne Aktivitäten, bei denen eine gesetzliche Verpflichtung die Protokollierung verbietet.

#### 6.6.1.2 Begründung

Um Informationen über solche Ereignisse bereitzustellen, erstellt die Anlage entsprechende Protokolle. Solche Protokollinformationen können beispielsweise bei der Identifizierung von möglichem ungewöhnlichem Verhalten der Anlage und von Sicherheits- bzw. Datenschutzverletzungen hilfreich sein.

#### 6.6.1.3 Leitlinie

Der Hersteller legt fest, zu welchem Zweck (und für welche Zielgruppe) Protokolle erstellt werden können, welche Daten gesammelt und protokolliert werden können und welche protokollspezifischen Anforderungen zum Schutz und zur Handhabung der Protokolldaten bestehen, z. B. die Bereitstellung der Daten an ein SIEM (Security Information and Event Management).

Eine Untermenge der identifizierten Ereignisse wird üblicherweise so konfiguriert, dass sie standardmäßig erfasst wird. Der Hersteller kann dem Endbenutzer erlauben, diese Protokollierungskonfiguration zu ändern.

Im Folgenden sind Beispiele für übliche, zu protokollierende Ereignisse aufgeführt:

— Aktivitäten in Bezug auf den Datenschutz wie Hinzufügen, Bearbeiten, Kombinieren, Entfernen/ Archivieren, Löschen, Ändern des Passworts, erlaubte oder verweigerte Zugriffsversuche,

— Änderungen von Einstellungen, die den Datenschutz verschlechtern oder verbessern können,

— Aktivierung oder Deaktivierung von sicherheitsrelevanten Sensoren.

Beispiele für Protokollierungsereignisse sind:

— die Datenschutzwerte betreffende Aktivitäten, wie beispielsweise Zugriff, Hinzufügen, Bearbeiten, Entfernen/Archivieren, Löschen,

— nicht autorisierte Zugangsversuche.

Die in den Protokollen erfassten personenbezogenen Daten sind auf solche zu beschränken, die absolut notwendig sind, um Untersucher bei der Untersuchung von Sicherheitsverletzungen zu unterstützen.

Produkte können so gestaltet werden, dass Versuche von Angreifern, eine nicht autorisierte physische Aktion durchzuführen, verhindert werden. Dennoch ist die Erkennung, Protokollierung und Antwort beim Auftreten von Manipulationsereignissen von grundlegender Bedeutung.

Weitere Einzelheiten zur Protokollierung sind in Normen wie beispielsweise ISO/IEC 27002 [3], Dritte Ausgabe, 2022-02, Unterabschnitt 8.15 zu finden.

ANMERKUNG 1 Die folgenden Ereignisse können protokolliert werden: erfolgreiche und abgelehnte Systemzugriffsereignisse, Änderungen von personenbezogenen Daten, Verkehrsdaten oder Ortsdaten, Dateien, auf die zugegriffen wurde, und die Art des Zugriffs, einschließlich des Löschens wichtiger Dateien.

ANMERKUNG 2 Ereignisprotokolle können gegebenenfalls Benutzerkennungen, Systemaktivitäten, Zeitstempel und Einzelheiten relevanter Ereignisse, Gerätekennung, Systemkennung sowie Standorte, Netzwerkadressen und Protokolle enthalten.

#### 6.6.1.4 Beurteilungskriterien

##### 6.6.1.4.1 Beurteilungsziel

Die Beurteilung betrifft den Anforderungsabschnitt LGM-1.

##### 6.6.1.4.2 Umsetzungskategorien

Nicht anwendbar.

##### 6.6.1.4.3 Erforderliche Informationen

[E.Info.LGM-1.PrivacyAssetEvent]: Beschreibung jeder internen Aktivität, die für die Datenschutzwerte und deren Schutz maßgeblich ist, einschließlich:

— (wenn eine gesetzliche Verpflichtung die Protokollierung der internen Aktivität verbietet) [E.Info.LGM-1.PrivacyAssetEvent.Legal]: Verweisungen auf alle entsprechenden Absätze oder Textstellen in allen maßgeblichen Rechtsdokumenten, einschließlich einer Beschreibung, wie diese auf die interne Aktivität der Anlage anzuwenden sind; und

— (wenn eine gesetzliche Verpflichtung die Protokollierung der internen Aktivität verbietet) [E.Info.LGM-1.PrivacyAssetEvent.LGM]: Beschreibung des Protokollierungsmechanismus, der zur Protokollierung des Ereignisses verwendet wird.

[E.Info.DT.LGM-1]: Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 26 für jedes in [E.Info.LGM-1.PrivacyAssetEvent] dokumentiertes Ereignis.

[E.Just.DT.LGM-1]: Begründung für jeden gewählten Pfad durch den in [E.Info.DT.LGM-1] dokumentierten Entscheidungsbaum mit den folgenden Eigenschaften:

— (wenn eine Entscheidung aus [DT.LGM-1.DN-1] zu „NICHT ANWENDBAR“ führt) basiert die Begründung für die Entscheidung [DT.LGM-1.DN-1] auf [E.Info.LGM-1.PrivacyAssetEvent.Legal]; und

— die Begründung für die Entscheidung [DT.LGM-1.DN-2] basiert auf [E.Info.LGM-1.PrivacyAssetEvent.LGM].

#### 6.6.1.4.4 Konzeptuelle Beurteilung

##### 6.6.1.4.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob ein Protokollierungsmechanismus implementiert wurde, wo er nach LGM-1 erforderlich ist.

##### 6.6.1.4.4.2 Voraussetzungen

Keine.

##### 6.6.1.4.4.3 Beurteilungseinheiten

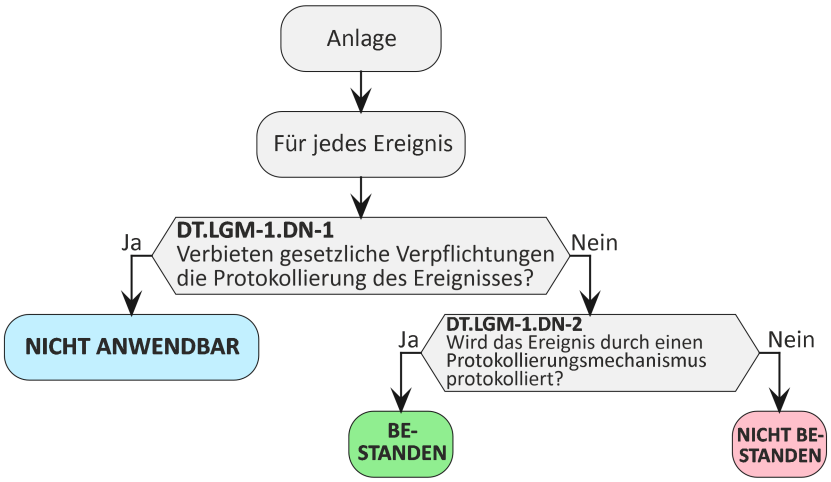



**Bild 26 — Entscheidungsbaum für Anforderung LGM-1**

Für jedes in [E.Info.LGM-1.PrivacyAssetEvent] dokumentierte Ereignis ist zu prüfen, ob der Pfad durch den in [E.Info.DT.LGM-1] dokumentierten Entscheidungsbaum mit „NICHT ANWENDBAR“ oder „BESTANDEN“ endet.

Für jeden in [E.Info.DT.LGM-1] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.LGM-1] dokumentierte Begründung zu untersuchen.

##### 6.6.1.4.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— mindestens ein Pfad durch den in [E.Info.DT.LGM-1] dokumentierten Entscheidungsbaum mit „BESTANDEN“ endet; und

— kein Pfad durch den in [E.Info.DT.LGM-1] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; und

— die in [E.Just.DT.LGM-1] angegebenen Informationen korrekte Begründungen für alle Pfade durch den in [E.Info.DT.LGM-1] dokumentierten Entscheidungsbaum sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— ein Pfad durch den in [E.Info.DT.LGM-1] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; oder

— eine in [E.Just.DT.LGM-1] angegebene Begründung für einen Pfad durch den in [E.Info.DT.LGM-1] dokumentierten Entscheidungsbaum nicht korrekt ist oder fehlt.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

#### 6.6.1.4.5 Beurteilung der funktionalen Vollständigkeit

Keine.

#### 6.6.1.4.6 Beurteilung der funktionalen Suffizienz

##### 6.6.1.4.6.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob Protokollierungsmechanismen implementiert wurden, wo sie nach LGM-1 erforderlich sind.

##### 6.6.1.4.6.2 Voraussetzungen

Die Anlage befindet sich im Betriebszustand.

##### 6.6.1.4.6.3 Beurteilungseinheiten

Für jedes in [E.Info.LGM-1.PrivacyAssetEvent] dokumentierte Ereignis ist funktionell zu bestätigen, ob die Ereignisse durch die in [E.Info.LGM-1.PrivacyAssetEvent.LGM] dokumentierten Protokollierungsmechanismen protokolliert werden durch:

— Generierung des Ereignisses; und

— Zugriff auf zugehörige Protokolldaten.

##### 6.6.1.4.6.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn kein Nachweis vorliegt, dass ein in [E.Info.LGM-1.PrivacyAssetEvent.LGM] dokumentierter Protokollierungsmechanismus nicht implementiert ist.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn ein Nachweis vorliegt, dass ein in [E.Info.LGM-1.PrivacyAssetEvent.LGM] dokumentierter Protokollierungsmechanismus nicht implementiert ist.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

### 6.6.2 [LGM-2] Dauerhafte Speicherung von Protokolldaten

#### 6.6.2.1 Anforderung

Protokollierungsmechanismen, die nach LGM-1 erforderlich sind, müssen Protokolldaten für entsprechende Ereignisse im dauerhaften Speicher der Anlage speichern, außer für Ereignisse, bei denen:

— zugehörige Protokolldaten außerhalb der Anlage gespeichert werden.

#### 6.6.2.2 Begründung

Ereignisprotokolle müssen nach dem Aus- und Einschalten der Anlage bestehen bleiben, um ihre versehentliche oder absichtliche Löschung zu verhindern.

#### 6.6.2.3 Leitlinie

Keine.

#### 6.6.2.4 Beurteilungskriterien

##### 6.6.2.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung LGM-2.

##### 6.6.2.4.2 Umsetzungskategorien

Nicht anwendbar.

##### 6.6.2.4.3 Erforderliche Informationen

[E.Info.LGM-2.LGM]: Beschreibung jedes nach LGM-1 erforderlichen Protokollierungsmechanismus, einschließlich:

— einer Beschreibung der protokollierten Ereignisse, einschließlich:

  — (wenn die Speicherung von Protokolldaten im dauerhaften Speicher der Anlage als erforderlich erachtet wird) [E.Info.LGM-2.LGM.InternalStorage]: Der Speicherort der Protokolldaten für damit zusammenhängende Ereignisse auf der Anlage und eine Beschreibung, wie die Persistenz der gespeicherten Protokolldaten sichergestellt wird; und

  — (wenn die Speicherung von Protokolldaten im dauerhaften Speicher der Anlage als nicht erforderlich erachtet wird, weil die Speicherung außerhalb der Anlage stattfindet) [E.Info.LGM-2.LGM.ExternalStorage]: Beschreibung der Funktionalität der Anlage zur Unterstützung der Speicherung von Protokolldaten außerhalb der Anlage.

[E.Info.DT.LGM-2]: Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 27 für jeden in [E.Info.LGM-2.LGM] dokumentierten Protokollierungsmechanismus.

[E.Just.DT.LGM-2]: Begründung für jeden gewählten Pfad durch den in [E.Info.DT.LGM-2] dokumentierten Entscheidungsbaum mit den folgenden Eigenschaften:

— (wenn eine Entscheidung aus [DT.LGM-2.DN-1] zu „NICHT ANWENDBAR“ führt) basiert die Begründung für die Entscheidung [DT.LGM-2.DN-1] auf [E.Info.LGM-2.LGM.ExternalStorage]; und

— die Begründung für die Entscheidung [DT.LGM-2.DN-2] basiert auf [E.Info.LGM-2.LGM.InternalStorage].

##### 6.6.2.4.4 Konzeptuelle Beurteilung

###### 6.6.2.4.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob die Protokollierungsmechanismen, die nach LGM-1 erforderlich sind, wie nach LGM-2 erforderlich Protokolldaten dauerhaft speichern.

###### 6.6.2.4.4.2 Voraussetzungen

Keine.

#### 6.6.2.4.4.3 Beurteilungseinheiten

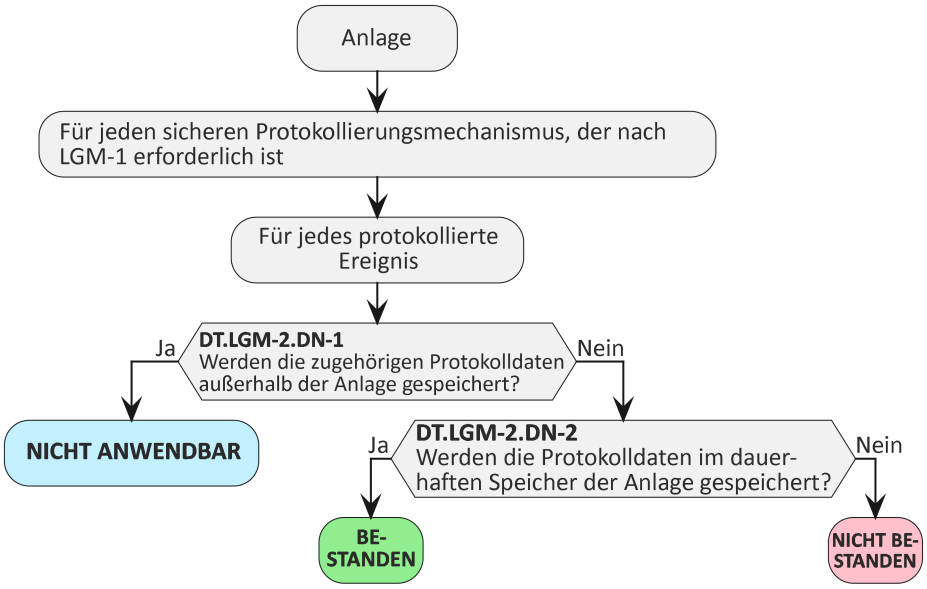



**Bild 27 — Entscheidungsbaum für Anforderung LGM-2**

Für jeden in [E.Info.LGM-2.LGM] dokumentierten Protokollierungsmechanismus ist zu prüfen, ob der Pfad durch den in [E.Info.DT.LGM-2] dokumentierten Entscheidungsbaum mit „NICHT ANWENDBAR“ oder „BESTANDEN“ endet.

Für jeden in [E.Info.DT.LGM-2] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.LGM-2] dokumentierte Begründung zu untersuchen.

#### 6.6.2.4.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— mindestens ein Pfad durch den in [E.Info.DT.LGM-2] dokumentierten Entscheidungsbaum mit „BESTANDEN“ endet; und

— kein Pfad durch den in [E.Info.DT.LGM-2] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; und

— die in [E.Just.DT.LGM-2] angegebenen Informationen korrekte Begründungen für alle Pfade durch den in [E.Info.DT.LGM-2] dokumentierten Entscheidungsbaum sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— ein Pfad durch den in [E.Info.DT.LGM-2] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; oder

— eine in [E.Just.DT.LGM-2] angegebene Begründung für einen Pfad durch den in [E.Info.DT.LGM-2] dokumentierten Entscheidungsbaum nicht korrekt ist oder fehlt.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

#### 6.6.2.4.5 Beurteilung der funktionalen Vollständigkeit

Die Beurteilung der funktionalen Vollständigkeit wird durch die Beurteilung der funktionalen Suffizienz der Anwendbarkeit des Protokollierungsmechanismus abgedeckt.

Deshalb ist diese Beurteilung der funktionalen Vollständigkeit nicht notwendig.

#### 6.6.2.4.6 Beurteilung der funktionalen Suffizienz

##### 6.6.2.4.6.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob Protokollierungsmechanismen implementiert wurden, wie in [E.Info.LGM-2.LGM] dokumentiert erforderlich sind.

##### 6.6.2.4.6.2 Voraussetzungen

Die Anlage befindet sich im Betriebszustand.

##### 6.6.2.4.6.3 Beurteilungseinheiten

Für jeden in [E.Info.LGM-2.LGM] dokumentierten Protokollierungsmechanismus, bei dem [E.Info.LGM-2.LGM.InternalStorage] angibt, dass Protokolldaten für zugehörige Ereignisse im dauerhaften Speicher der Anlage gespeichert werden, ist funktional zu bestätigen, dass die Protokolldaten für die zugehörigen Ereignisse im dauerhaften Speicher der Anlage gespeichert werden durch:

— Generierung der Ereignisse; und

— Zugriff auf den Speicherort der entsprechenden Protokolldaten der Anlage und Prüfung, ob die Protokolldaten vorhanden sind.

##### 6.6.2.4.6.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn kein Nachweis vorliegt, dass die Verarbeitung von Protokolldaten für die zugehörigen Ereignisse von [E.Info.LGM-2.LGM.InternalStorage] abweichen.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn ein Nachweis vorliegt, dass die Verarbeitung von Protokolldaten für die zugehörigen Ereignisse von [E.Info.LGM-2.LGM.InternalStorage] abweichen.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

### 6.6.3 [LGM-3] Mindestanzahl an dauerhaft gespeicherten Ereignissen

#### 6.6.3.1 Anforderung

Alle Protokolldaten, die im dauerhaften Speicher der Anlage durch Protokollierungsmechanismen gespeichert werden, die nach LGM-1 erforderlich sind, müssen immer Folgendes enthalten:

— eine Mindestanzahl jüngster Ereignisse; und

— das neueste Ereignis.

#### 6.6.3.2 Begründung

Es ist eine Mindestanzahl von gespeicherten Ereignissen erforderlich, um sicherzustellen, dass ein ausreichender Prüfpfad vorhanden ist, um Untersuchungen effektiv durchführen zu können.

#### 6.6.3.3 Leitlinie

Die Mindestanzahl auf der Anlage gespeicherter Ereignisse wird abhängig von der vorgesehenen Funktionalität der Anlage üblicherweise der Benutzerdokumentation entnommen.

Rechtliche Verpflichtungen hinsichtlich der Aufbewahrungsfristen und der Mindestanzahl der gespeicherten Ereignisse müssen eingehalten werden.

#### 6.6.3.4 Beurteilungskriterien

##### 6.6.3.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung LGM-3.

##### 6.6.3.4.2 Umsetzungskategorien

Nicht anwendbar.

##### 6.6.3.4.3 Erforderliche Informationen

[E.Info.LGM-3.Events]: Beschreibung der protokollierten Ereignisse, wobei die zugehörigen Protokolldaten dauerhaft auf der Anlage gespeichert werden.

[E.Info.LGM-3.Quantity]: Mindestanzahl der jüngsten Ereignisse, für die gleichzeitig Protokolldaten auf der Anlage dauerhaft gespeichert werden können, und eine Beschreibung der Speicherorte der Protokolldaten.

[E.Info.DT.LGM-3]: Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 28.

[E.Just.DT.LGM-3]: Begründung für den gewählten Pfad durch den in [E.Info.DT.LGM-3] dokumentierten Entscheidungsbaum mit der folgenden Eigenschaft:

— die Begründung für die Entscheidung [DT.LGM-3.DN-1] basiert auf [E.Info.LGM-3.Quantity].

##### 6.6.3.4.4 Konzeptuelle Beurteilung

###### 6.6.3.4.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob die Mindestanzahl dauerhaft gespeicherter protokollierter Ereignisse wie nach LGM-3 erforderlich festgelegt ist.

###### 6.6.3.4.4.2 Voraussetzungen

Keine.

#### 6.6.3.4.4.3 Beurteilungseinheiten

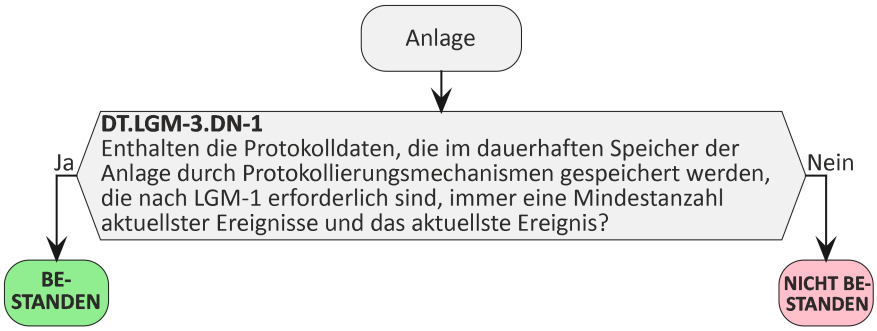



**Bild 28 — Entscheidungsbaum für Anforderung LGM-3**

Es ist zu prüfen, ob der Pfad durch den in [E.Info.DT.LGM-3] dokumentierten Entscheidungsbaum mit „BESTANDEN“ endet.

Für den in [E.Info.DT.LGM-3] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.LGM-3] dokumentierte Begründung zu untersuchen.

#### 6.6.3.4.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— alle Pfade durch den in [E.Info.DT.LGM-3] dokumentierten Entscheidungsbaum mit „BESTANDEN“ enden; und

— die in [E.Just.DT.LGM-3] angegebenen Informationen korrekte Begründungen für alle Pfade durch den in [E.Info.DT.LGM-3] dokumentierten Entscheidungsbaum sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— ein Pfad durch den in [E.Info.DT.LGM-3] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; oder

— eine in [E.Just.DT.LGM-3] angegebene Begründung für einen Pfad durch den in [E.Info.DT.LGM-3] dokumentierten Entscheidungsbaum nicht korrekt ist oder fehlt.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

### 6.6.3.4.5 Beurteilung der funktionalen Vollständigkeit

Die Beurteilung der funktionalen Vollständigkeit wird durch die Beurteilung der funktionalen Suffizienz der Anwendbarkeit des Protokollierungsmechanismus abgedeckt.

Deshalb ist diese Beurteilung der funktionalen Vollständigkeit nicht notwendig.

### 6.6.3.4.6 Beurteilung der funktionalen Suffizienz

#### 6.6.3.4.6.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob die Anzahl der jüngsten Ereignisse, für die gleichzeitig in [E.Info.LGM-3.Quantity] dokumentierte Protokolldaten auf der Anlage dauerhaft gespeichert werden können, vom Gerät dauerhaft gespeichert werden können.

#### 6.6.3.4.6.2 Voraussetzungen

Die Anlage befindet sich im Betriebszustand.

#### 6.6.3.4.6.3 Beurteilungseinheiten

Die in [E.Info.LGM-3.Quantity] dokumentierte Mindestanzahl von protokollierten Ereignissen ist funktional zu bestätigen durch

— Generierung der in [E.Info.LGM-3.Events] dokumentierten Ereignisse, um die in [E.Info.LGM-3.Quantity] dokumentierte Mindestanzahl an protokollierten Ereignissen zu erreichen; und

— Zugriff auf den Speicherort der entsprechenden Protokolldaten der Anlage und Zählen der protokollierten Ereignisse.

#### 6.6.3.4.6.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn kein Nachweis vorliegt, dass die Anzahl der protokollierten Ereignisse, die gleichzeitig auf der Anlage dauerhaft gespeichert werden, geringer sein kann als in [E.Info.LGM-3.Quantity] dokumentiert.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn ein Nachweis vorliegt, dass die Anzahl der protokollierten Ereignisse, die gleichzeitig auf der Anlage dauerhaft gespeichert werden, geringer sein kann als in [E.Info.LGM-3.Quantity] dokumentiert.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

### 6.6.4 [LGM-4] Zeitbezogene Informationen der dauerhaft gespeicherten Protokolldaten

#### 6.6.4.1 Anforderung

Alle Protokolldaten, die im dauerhaften Speicher der Anlage durch Protokollierungsmechanismen gespeichert werden, die nach LGM-1 erforderlich sind, müssen Folgendes enthalten:

— einen Zeitstempel, wenn auf der Anlage Echtzeit verfügbar ist; und

— zeitbezogene Informationen, wenn die Anlage nicht über Echtzeit verfügt.

#### 6.6.4.2 Begründung

Ein Zeitstempel oder eine Zeitinformation, die das zeitliche Auftreten jedes Ereignisses einschließt, ist erforderlich, um Untersuchungen zu unterstützen, die dem Verständnis der zeitlichen Ereignisabfolge und dem Vergleich mit Protokollen auf anderen Anlagen dienen.

#### 6.6.4.3 Leitlinie

Bei den zeitbezogenen Informationen kann es sich um die Zeitspanne in Sekunden seit dem Einschalten der Anlage oder einfach um die Abfolge der Ereignisse handeln.

#### 6.6.4.4 Beurteilungskriterien

#### 6.6.4.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung LGM-4.

#### 6.6.4.4.2 Umsetzungskategorien

Nicht anwendbar.

#### 6.6.4.4.3 Erforderliche Informationen

[E.Info.LGM-4.Events]: Beschreibung der protokollierten Ereignisse, wobei die zugehörigen Protokolldaten dauerhaft auf der Anlage gespeichert werden.

[E.Info.LGM-4.LGM]: Beschreibung jedes nach LGM-1 erforderlichen Protokollierungsmechanismus, der Protokolldaten erzeugt, die im dauerhaften Speicher der Anlage gespeichert werden, einschließlich:

— (wenn Echtzeitinformationen auf der Anlage verfügbar sind) [E.Info.LGM-4.LGM.Timestamp]: Beschreibung jeder Echtzeitquelle und des entsprechenden Zeitstempels, der in den dauerhaft gespeicherten Protokolldaten enthalten ist; und

— (wenn Echtzeitinformationen nicht zuverlässig über die Anlage verfügbar sind) [E.Info.LGM-4.LGM.Timerelated]: Beschreibung der zeitbezogenen Informationen, die in den dauerhaft gespeicherten Protokolldaten enthalten sind.

[E.Info.DT.LGM-4]: Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 29 für jeden in [E.Info.LGM-4.LGM] dokumentierten Protokollierungsmechanismus.

[E.Just.DT.LGM-4]: Begründung für jeden gewählten Pfad durch den in [E.Info.DT.LGM-4] dokumentierten Entscheidungsbaum mit den folgenden Eigenschaften:

— die Begründung für die Entscheidung [DT.LGM-4.DN-1] basiert auf [E.Info.LGM-4.LGM.Timestamp]; und

— die Begründung für die Entscheidung [DT.LGM-4.DN-2] basiert auf [E.Info.LGM-4.LGM.Timerelated].

#### 6.6.4.4.4 Konzeptuelle Beurteilung

##### 6.6.4.4.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob die protokollierten Ereignisse über die nach LGM-4 erforderlichen Informationen verfügen.

##### 6.6.4.4.4.2 Voraussetzungen

Keine.

#### 6.6.4.4.4.3 Beurteilungseinheiten

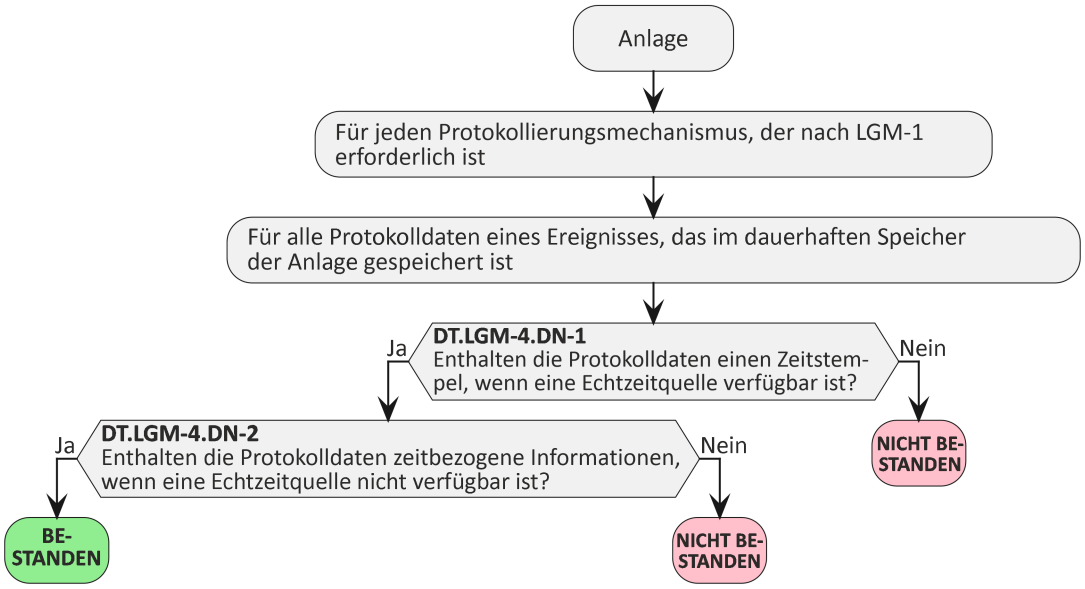



**Bild 29 — Entscheidungsbaum für Anforderung LGM-4**

Für jeden in [E.Info.LGM-4.LGM] dokumentierten Protokollierungsmechanismus ist zu prüfen, ob der Pfad durch den in [E.Info.DT.LGM-4] dokumentierten Entscheidungsbaum mit „BESTANDEN“ endet.

Für jeden in [E.Info.DT.LGM-4] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.LGM-4] dokumentierte Begründung zu untersuchen.

#### 6.6.4.4.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— alle Pfade durch den in [E.Info.DT.LGM-4] dokumentierten Entscheidungsbaum mit „BESTANDEN“ enden; und

— die in [E.Just.DT.LGM-4] angegebenen Informationen korrekte Begründungen für alle Pfade durch den in [E.Info.DT.LGM-4] dokumentierten Entscheidungsbaum sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— ein Pfad durch den in [E.Info.DT.LGM-4] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; oder

— eine in [E.Just.DT.LGM-4] angegebene Begründung für einen Pfad durch den in [E.Info.DT.LGM-4] dokumentierten Entscheidungsbaum nicht korrekt ist oder fehlt.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

#### 6.6.4.4.5 Beurteilung der funktionalen Vollständigkeit

Die Beurteilung der funktionalen Vollständigkeit wird durch die Beurteilung der funktionalen Suffizienz der Anwendbarkeit des Protokollierungsmechanismus abgedeckt.

Deshalb ist diese Beurteilung der funktionalen Vollständigkeit nicht notwendig.

#### 6.6.4.4.6 Beurteilung der funktionalen Suffizienz

##### 6.6.4.4.6.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob Protokollierungsmechanismen implementiert wurden, wie in [E.Info.LGM-4.LGM] in Bezug auf die Zeitstempel und zeitbezogenen Informationen dokumentiert implementiert sind.

##### 6.6.4.4.6.2 Voraussetzungen

Die Anlage befindet sich im Betriebszustand.

##### 6.6.4.4.6.3 Beurteilungseinheiten

(Wenn die Anlage mit verfügbaren Echtzeitinformationen betrieben werden kann) Für jeden in [E.Info.LGM-4.LGM] dokumentierten Protokollierungsmechanismus ist funktionell zu bestätigen, dass die dauerhaft im Gerät gespeicherten Protokolldaten Zeitstempel nach [E.Info.LGM-4.LGM.Timestamp] enthalten, wenn Echtzeitinformationen verfügbar sind durch:

— Sicherstellung, dass den Anlagen Echtzeitinformationen zur Verfügung stehen; und

— Erzeugung von Ereignissen, die in [E.Info.LGM-4.Events] dokumentiert sind; und

— Zugriff auf den Speicherort der entsprechenden Protokolldaten der Anlage und Prüfung, ob Zeitstempel vorhanden sind.

(Wenn die Anlage auch bei nicht verfügbaren Echtzeitinformationen betrieben werden kann) Für jeden in [E.Info.LGM-4.LGM] dokumentierten Protokollierungsmechanismus ist funktionell zu bestätigen, dass die dauerhaft im Gerät gespeicherten Protokolldaten zeitbezogene Informationen nach [E.Info.LGM-4.LGM.Timerelated] enthalten, wenn Echtzeitinformationen nicht verfügbar sind durch:

— Sicherstellung, dass den Anlagen Echtzeitinformationen nicht zur Verfügung stehen; und

— Erzeugung von Ereignissen, die in [E.Info.LGM-4.Events] dokumentiert sind; und

— Zugriff auf den Speicherort der entsprechenden Protokolldaten der Anlage und Prüfung, ob zeitbezogene Informationen vorhanden sind.

##### 6.6.4.4.6.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn für jeden in [E.Info.LGM-4.LGM] dokumentierten Protokollierungsmechanismus kein Nachweis vorliegt, dass:

— dauerhaft gespeicherte Protokolldaten keinen Zeitstempel enthalten, wenn Informationen in Echtzeit verfügbar sind; und

— dauerhaft gespeicherte Protokolldaten keine zeitbezogenen Informationen enthalten, wenn Informationen in Echtzeit nicht verfügbar sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn für einen in [E.Info.LGM-4.LGM] dokumentierten Protokollierungsmechanismus ein Nachweis vorliegt, dass:

— dauerhaft gespeicherte Protokolldaten keinen Zeitstempel enthalten, wenn Informationen in Echtzeit verfügbar sind; oder

— dauerhaft gespeicherte Protokolldaten keine zeitbezogenen Informationen enthalten, wenn Informationen in Echtzeit nicht verfügbar sind.

## 6.7 [DLM] Löschungsmechanismus (en: Deletion Mechanism)

### 6.7.1 [DLM-1] Anwendbarkeit von Löschungsmechanismen

#### 6.7.1.1 Anforderung

Die Anlage muss einen Löschungsmechanismus bieten, der es dem Benutzer ermöglicht, seine personenbezogenen Daten und sensiblen Sicherheitsparameter, die auf der Anlage gespeichert sind, zu löschen.

#### 6.7.1.2 Begründung

Diese Anforderung ist notwendig, um das Risiko der Offenlegung personenbezogener Daten im Zusammenhang mit der Entsorgung oder dem Austausch der Anlage zu vermeiden.

#### 6.7.1.3 Leitlinie

Der Benutzer ist in der Regel die Person, die die Anlage nutzt. Ein Benutzer löscht seine eigenen personenbezogenen Daten.

Ein autorisierter Benutzer ist jemand, dem von einem Benutzer Zugriff auf die Anlage gewährt wurde. Ein autorisierter Benutzer löscht personenbezogene Daten, auf die er Zugriff hat.

Es gibt aber Fälle, in denen ein anderer Benutzer mit Administratorrechten für die Benutzerverwaltung der Anlage verantwortlich ist, der nicht mit dem Benutzer übereinstimmt, dessen personenbezogene Daten auf der Anlage gespeichert sind. In diesen Fällen hat der Benutzer mit Administratorrechten die Aufsichtsverantwortung für Löschung der personenbezogenen Informationen des Benutzers im Namen des Benutzers. Ein Benutzer mit Administratorrechten löscht personenbezogene Daten, auf die er Zugriff hat.

In manchen Fällen ist der Benutzer mit Administratorrechten nicht der Benutzer, aber der Benutzer mit Administratorrechten hat die Verantwortung, den Schutz der personenbezogenen Informationen des Benutzers sicherzustellen. In diesen Fällen sollte der Löschungsmechanismus so implementiert werden, dass nur der Benutzer mit Administratorrechten den Löschungsmechanismus nutzen kann.

Wenn es mehrere Benutzer gibt, kann ein Benutzer seine eigenen Daten löschen und ein Benutzer mit Administratorrechten kann die Daten aller Benutzer löschen.

Ein Einschaltzyklus kann verwendet werden, um sicherzustellen, dass die personenbezogenen Daten dauerhaft gelöscht sind.

Jede unnötige Verzögerung bei der Löschung oder bei der Beendigung einer teilweisen (z. B. zuvor unterbrochenen) Löschung könnte zu einem Risiko der Wiederherstellbarkeit der personenbezogenen Informationen des Benutzers führen.

Im Kontext dieser Regelung bedeutet der Ausdruck „löschen“, dass je nach den Risiken verschiedene technische Lösungen eingesetzt werden können, um die Wiederherstellung der personenbezogenen Informationen dauerhaft zu verhindern.

ANMERKUNG 1 Dabei könnte es sich um eine Softwarefunktion handeln, die das Gerät auf die Werkeinstellungen zurücksetzt und den Verschlüsselungscode sicher löscht und einen neuen generiert, um sicherzustellen, dass alle personenbezogenen Informationen gelöscht werden.

Ziel des Löschungsmechanismus ist es, dass er:

— resilient gegen Unterbrechungen ist; und

ANMERKUNG 2 Resilienz bedeutet, dass der Löschungsmechanismus der Anlage bei Wiederaufnahme nach der Unterbrechung abgeschlossen ist.

— Manipulationen, beispielsweise nicht autorisierten Versuchen, eine nicht autorisierte Löschung durchzuführen, oder nicht autorisierten Versuchen, die autorisierte Löschung zu verhindern, widersteht; und

— vor einer unbeabsichtigten Auslösung durch den Benutzer schützt; und

— für den Benutzer entsprechend einfach zu finden und zu aktivieren ist.

Beispiele für Anwendungsfälle, in denen ein Benutzer mit Administratorrechten erforderlich ist, der kein Benutzer eines Geräts ist:

— eine getrennte Entität könnte erforderlich sein, um die angeforderte Löschung der personenbezogenen Informationen des Benutzers zu starten;

— die Löschung könnte erfordern, dass für die Zustimmung zur Löschung die Autorisierung des Gerätebesitzers erforderlich ist;

— Anwendungsfälle, bei denen zum Löschen personenbezogener Daten eine spezielle Autorisierung erforderlich ist;

— Anwendungsfälle, bei denen die Löschung nicht durch den Eigentümer der personenbezogenen Daten durchgeführt werden darf, wenn diese Daten aus Betriebsgründen grundlegend wichtig sind (z. B. im industriellen Kontext).

Beispiele für sonstige Normen:

ETSI EN 303 645 [6] und ETSI TS 103 701 [7] beziehen sich auf einfaches Löschen/Löschen von Daten, wobei TS 103 701 „einfach“ als „auf eine Weise, die für einen Benutzer mit begrenztem technischen Wissen verständlich ist“, beschreibt.

ANMERKUNG 3 „Angemessen“ bezieht sich auf den Wissensstand des Benutzers, die Sensibilität der Daten und auf andere Faktoren, die den Zugang zur Auslösung des Löschungsmechanismus beeinflussen.

ANMERKUNG 4 ISO/IEC 27555:2021 [5] E-Guidelines on personally identifiable information deletion (Projekt 1.27.142) kann zusätzliche nützliche Informationen enthalten.

#### 6.7.1.4 Beurteilungskriterien

##### 6.7.1.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung DLM-1.

##### 6.7.1.4.2 Umsetzungskategorien

Nicht anwendbar.

##### 6.7.1.4.3 Erforderliche Informationen

[E.Info.DLM-1.PersonalData]: Beschreibung der auf der Anlage gespeicherten personenbezogenen Daten.

[E.Info.DLM-1.SenSecParam]: Beschreibung der sensiblen Sicherheitsparameter, die auf der Anlage gespeichert werden können.

[E.Info.DLM-1.DLM]: Beschreibung jedes Löschungsmechanismus, einschließlich einer Beschreibung, ob der Löschungsmechanismus sicherstellt, dass auf der Anlage gespeicherte personenbezogene Daten und/oder sensible Sicherheitsparameter zum Zweck der Entsorgung oder des Ersatzes der Anlage gelöscht werden können, und zwar:

— durch Benutzer; oder

— wenn eine autorisierte Entität die Aufsichtsverantwortung zur Löschung der personenbezogenen Daten und/oder sensibler Sicherheitsparameter im Namen des Benutzers hat, durch diese Entität.

[E.Info.DT.DLM-1]: Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 30 für jede personenbezogene Information, die auf dem in [E.Info.DLM-1.PersonalData] dokumentierten Gerät gespeichert ist.

[E.Just.DT.DLM-1]: Begründung für den gewählten Pfad durch den in [E.Info.DT.DLM-1] dokumentierten Entscheidungsbaum mit der folgenden Eigenschaft:

— die Begründung für die Entscheidung [DT.DLM-1.DN-1] basiert auf [E.Info.DLM-1.DLM].

#### 6.7.1.4.4 Konzeptuelle Beurteilung

##### 6.7.1.4.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob ein Löschungsmechanismus implementiert wurde, wo er nach DLM-1 erforderlich ist.

##### 6.7.1.4.4.2 Voraussetzungen

Keine.

##### 6.7.1.4.4.3 Beurteilungseinheiten

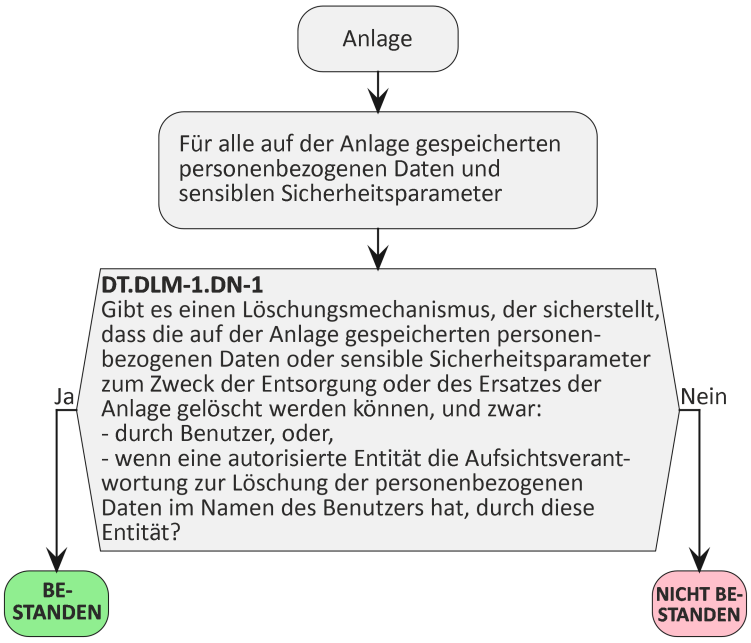



**Bild 30 — Entscheidungsbaum für Anforderung DLM-1**

Für jede in [E.Info.DLM-1.PersonalData] dokumentierte personenbezogene Information und für jeden in [E.Info.DLM-1.SenSecParam] dokumentierten sensiblen Sicherheitsparameter ist zu prüfen, ob der Pfad durch den in [E.Info.DT.DLM-1] dokumentierten Entscheidungsbaum mit „BESTANDEN“ endet.

Für jeden in [E.Info.DT.DLM-1] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.DLM-1] dokumentierte Begründung zu untersuchen.

#### 6.7.1.4.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— alle Pfade durch den in [E.Info.DT.DLM-1] dokumentierten Entscheidungsbaum mit „BESTANDEN“ enden; und

— die in [E.Just.DT.DLM-1] angegebenen Informationen korrekte Begründungen für alle Pfade durch den in [E.Info.DT.DLM-1] dokumentierten Entscheidungsbaum sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— ein Pfad durch den in [E.Info.DT.DLM-1] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; oder

— eine in [E.Just.DT.DLM-1] angegebene Begründung für einen Pfad durch den in [E.Info.DT.DLM-1] dokumentierten Entscheidungsbaum nicht korrekt ist oder fehlt.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

### 6.7.1.4.5 Beurteilung der funktionalen Vollständigkeit

#### 6.7.1.4.5.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob die in [E.Info.DLM-1.PersonalData] dokumentierten personenbezogene Daten oder die in [E.Info.DLM-1.SenSecParam] dokumentierten sensiblen Sicherheitsparameter vollständig sind.

#### 6.7.1.4.5.2 Voraussetzungen

Die Anlage befindet sich im Betriebszustand.

#### 6.7.1.4.5.3 Beurteilungseinheiten

Es ist funktional zu beurteilen, ob personenbezogene Daten vorhanden sind und ob es auf der Anlage Orte zur Speicherung personenbezogener Daten gibt, die nicht in [E.Info.DLM-1.PersonalData] beschrieben sind.

Es ist funktional zu beurteilen, ob es sensible Sicherheitsparameter gibt und ob es Orte für die Speicherung sensibler Sicherheitsparameter auf der Anlage gibt, die nicht in [E.Info.DLM-1.SenSecParam] beschrieben sind.

#### 6.7.1.4.5.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn alle gefundenen personenbezogenen Daten in [E.Info.DLM-1.PersonalData] dokumentiert sind und alle gefundenen sensiblen Sicherheitsparameter in [E.Info.DLM-1.SenSecParam] dokumentiert sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn sich personenbezogene Daten auf der Anlage befinden, die nicht in [E.Info.DLM-1.PersonalData] dokumentiert sind, oder wenn sich ein sensibler Sicherheitsparameter auf der Anlage befindet, der nicht in [E.Info.DLM-1.SenSecParam] dokumentiert ist.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

#### 6.7.1.4.6 Beurteilung der funktionalen Suffizienz

##### 6.7.1.4.6.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob Löschungsmechanismen implementiert wurden, wo sie nach DLM-1 erforderlich sind.

##### 6.7.1.4.6.2 Voraussetzungen

Die Anlage befindet sich im Betriebszustand.

##### 6.7.1.4.6.3 Beurteilungseinheiten

Für jeden in [E.Info.DLM-1.DLM] dokumentierten Löschungsmechanismus ist funktional zu bestätigen, dass der Löschungsmechanismus auf der Anlage verwendet wird.

##### 6.7.1.4.6.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn kein Nachweis vorliegt, dass ein in [E.Info.DLM-1.DLM] dokumentierter Löschungsmechanismus nicht verwendet wird.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn ein Nachweis vorliegt, dass ein in [E.Info.DLM-1.DLM] dokumentierter Löschungsmechanismus nicht verwendet wird.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

## 6.8 [UNM] Benutzer-Benachrichtigungsmechanismus (en: User Notification Mechanism)

### 6.8.1 [UNM-1] Anwendbarkeit von Benutzer-Benachrichtigungsmechanismen

#### 6.8.1.1 Anforderung

Die Anlage muss einen oder mehrere Mechanismen zur Benachrichtigung des Benutzers über Änderungen enthalten, die sich auf die Privatsphäre und den Schutz von personenbezogenen Daten auswirken, es sei denn, es handelt sich um Änderungen:

— andere, nicht mit der Anlage in Zusammenhang stehende Verfahren, um den Benutzer zu informieren.

#### 6.8.1.2 Begründung

Das Ziel ist die Sicherstellung der Transparenz für den Benutzer der Anlage, wenn Änderungen beim Datenschutz und beim Schutz der vom Gerät erfassten, gespeicherten oder verarbeiteten personenbezogenen Informationen auftreten.

Die Transparenz ermöglicht es dem Benutzer der Anlage, weitere Aktionen oder Aktualisierungen in Betracht zu ziehen.

Die rechtzeitige Benachrichtigung eines Benutzers ermöglicht es ihm, eine fundierte Entscheidung darüber zu treffen, wie er mit diesen Änderungen umgehen sollte.

#### 6.8.1.3 Leitlinie

Der Benutzer ist in der Regel die Person, die die Anlage nutzt.

Bei einer vom Benachrichtigungsmechanismus gesendeten oder angezeigten Meldung kann es sich um eine Textmeldung, eine Sprachmeldung, einen Link oder eine andere entsprechende Mitteilung an den Benutzer handeln; die Informationen über das Benachrichtigungsverfahren könnte auch vorab in der Benutzerdokumentation bereitgestellt werden.

Mit „Benutzer“ wird in dieser Anforderung eine natürliche Person bezeichnet, die entweder der Bediener oder der Eigentümer der Anlage sein kann.

Folgende Änderungen könnten den Datenschutz und den Schutz personenbezogener Daten betreffen:

— die Erfassung und Verarbeitung zusätzlicher Kategorien von personenbezogenen Informationen im Vergleich zum Zustand vor der Änderung,

— zusätzliche Bearbeitungsvorgänge, die personenbezogene Informationen betreffen,

— Deaktivierung oder wesentliche Änderungen der Sicherheitskontrollen oder der Protokollierungseinstellungen, die zum Schutz personenbezogener Informationen gedacht sind,

— Änderungen der Art und der Parameter der Verarbeitung personenbezogener Informationen, wenn dadurch die durch die genannte Verarbeitung und die Parameter bereitgestellte Schutzstufe für personenbezogene Daten beeinflusst wird.

Die rechtzeitige Bereitstellung von Benachrichtigungen ist von den Fähigkeiten und vom Status der Anlage abhängig, wobei die Bedeutung von „rechtzeitig“ in Abhängigkeit von der Wichtigkeit der Änderung und dem Benachrichtigungsmechanismus der Anlage sowie von anderen Faktoren variieren kann. Wenn die Anlage beispielsweise nicht mit dem Netzwerk verbunden ist, kann sie möglicherweise keine Benachrichtigung für Fernbenutzer bereitstellen, und die Benachrichtigung erfolgt nach bestmöglichem Bemühen.

#### 6.8.1.4 Beurteilungskriterien

##### 6.8.1.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung UNM-1.

##### 6.8.1.4.2 Umsetzungskategorien

Nicht anwendbar.

##### 6.8.1.4.3 Erforderliche Informationen

[E.Info.UNM-1.PersonalInformation]: Beschreibung aller auf der Anlage gespeicherten personenbezogenen Daten, einschließlich:

— [E.Info.UNM-1.PersonalInformation.UseCase]: Beschreibung jedes Anwendungsfalls, bei dem sich Änderungen auf die Privatsphäre oder den Schutz der personenbezogenen Daten auswirken können, einschließlich:

  — [E.Info.UNM-1.PersonalInformation.UseCase.Notification]: Beschreibung des Benachrichtigungsmechanismus, der den Benutzer über diese Änderung benachrichtigt; oder

  — (wenn es eine andere Methode zur Information des Benutzers gibt, die nicht die Anlage betrifft) [E.Info.UNM-1.PersonalInformation.UseCase.OtherInfo]: Beschreibung anderer Methoden zur Information des Benutzers, die nicht die Anlage betreffen.

[E.Info.DT.UNM-1]: Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 31 für die Beurteilung von UNM-1 für jeden in [E.Info.UNM-1.PersonalInformation.UseCase.Notification] dokumentierten Benutzerbenachrichtigungsmechanismus.

[E.Just.DT.UNM-1]: Begründung für den gewählten Pfad durch den in [E.Info.DT.UNM-1] dokumentierten Entscheidungsbaum mit den folgenden Eigenschaften:

— (wenn eine Entscheidung aus [DT.UNM-1.DN-1] zu „NICHT ANWENDBAR“ führt) basiert die Begründung für die Entscheidung [DT.UNM-1.DN-1] auf [E.Info.UNM-1.PersonalInformation.UseCase.OtherInfo]; und

— die Begründung für die Entscheidung [DT.UNM-1.DN-2] basiert auf [E.Info.UNM-1.PersonalInformation.UseCase.Notification].

#### 6.8.1.4.4 Konzeptuelle Beurteilung

##### 6.8.1.4.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob einer oder mehrere Benachrichtigungsmechanismen implementiert wurden, wo sie nach UNM-1 erforderlich sind.

##### 6.8.1.4.4.2 Voraussetzungen

Keine.

##### 6.8.1.4.4.3 Beurteilungseinheiten

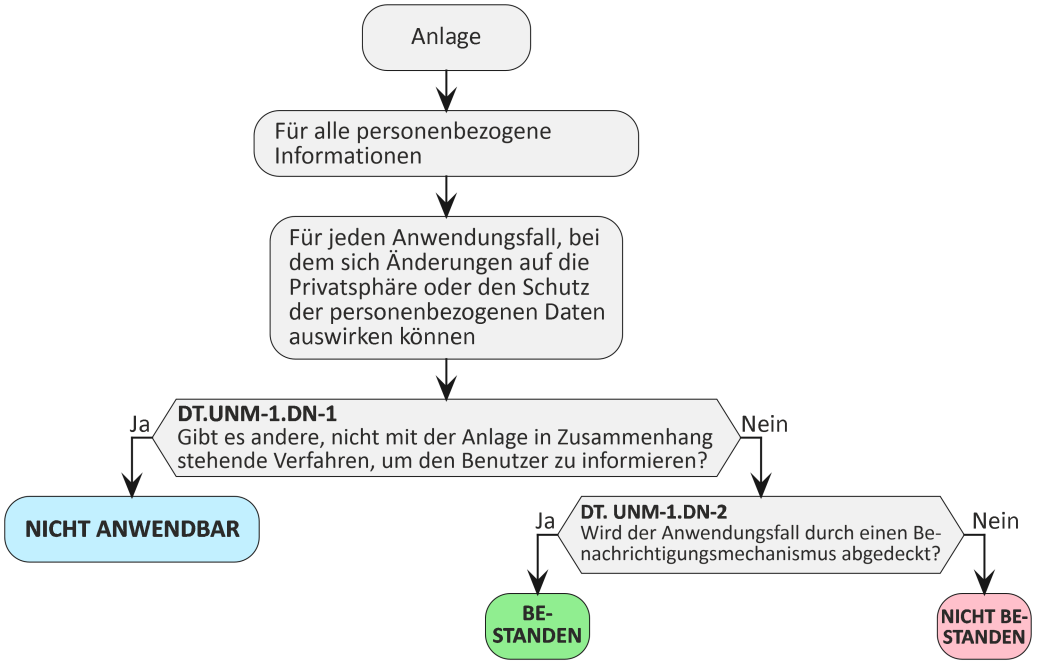



**Bild 31 — Entscheidungsbaum für Anforderung UNM-1**

Für jede in [E.Info.UNM-1.PersonalInformation.UseCase] dokumentierte Netzwerkschnittstelle ist zu prüfen, ob der Pfad durch den in [E.Info.DT.UNM-1] dokumentierten Entscheidungsbaum mit „NICHT ANWENDBAR“ oder „BESTANDEN“ endet.

Für jeden in [E.Info.DT.UNM-1] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.UNM-1] dokumentierte Begründung zu untersuchen.

##### 6.8.1.4.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— mindestens ein Pfad durch den in [E.Info.DT.UNM-1] dokumentierten Entscheidungsbaum mit „BESTANDEN“ endet; und

— kein Pfad durch den in [E.Info.DT.UNM-1] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; und

— die in [E.Just.DT.UNM-1] angegebenen Informationen korrekte Begründungen für alle Pfade durch den in [E.Info.DT.UNM-1] dokumentierten Entscheidungsbaum sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— ein Pfad durch den in [E.Info.DT.UNM-1] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN" endet; oder

— eine in [E.Just.DT.UNM-1] angegebene Begründung für einen Pfad durch den in [E.Info.DT.UNM-1] dokumentierten Entscheidungsbaum nicht korrekt ist oder fehlt.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

#### 6.8.1.4.5 Beurteilung der funktionalen Vollständigkeit

##### 6.8.1.4.5.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob die in [E.Info.UNM-1.PersonalInformation.UseCase] dokumentierte Liste der Anwendungsfälle und die in [E.Info.UNM-1.PersonalInformation] dokumentierte Liste der personenbezogenen Informationen, die auf der Anlage gespeichert werden können, vollständig ist.

##### 6.8.1.4.5.2 Voraussetzungen

Die Anlage befindet sich im Betriebszustand.

##### 6.8.1.4.5.3 Beurteilungseinheiten

Es ist funktional zu beurteilen, ob sich auf der Anlage personenbezogene Informationen befinden, die nicht in [E.Info.UNM-1.PersonalInformation] beschrieben sind.

Es ist funktional zu beurteilen, ob es einen Anwendungsfall für die Änderung personenbezogener Informationen auf der Anlage gibt, der nicht in [E.Info.UNM-1.PersonalInformation.UseCase] beschrieben ist.

##### 6.8.1.4.5.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn alle gefundenen personenbezogenen Informationen in [E.Info.UNM-1.PersonalInformation] dokumentiert sind und alle gefundenen Anwendungsfälle in [E.Info.UNM-1.PersonalInformation.UseCase] dokumentiert sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn sich personenbezogene Informationen auf der Anlage befinden, die nicht in [E.Info.UNM-1.PersonalInformation] dokumentiert sind, oder wenn ein Anwendungsfall gefunden wird, der nicht in [E.Info.UNM-1.PersonalInformation.UseCase] dokumentiert ist.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

#### 6.8.1.4.6 Beurteilung der funktionalen Suffizienz

##### 6.8.1.4.6.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob die Benachrichtigung für jede Änderung implementiert wurde, wo sie nach UNM-1 erforderlich ist.

##### 6.8.1.4.6.2 Voraussetzungen

Die Anlage befindet sich im Betriebszustand.

#### 6.8.1.4.6.3 Beurteilungseinheiten

Es ist funktional zu bestätigen, dass mindestens ein in [E.Info.UNM-1.PersonalInformation.UseCase.Notification] dokumentierter Benutzer-Benachrichtigungsmechanismus für jeden in [E.Info.UNM-1.PersonalInformation.UseCase] dokumentierten Anwendungsfall vorhanden ist/genutzt wird.].

#### 6.8.1.4.6.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn kein Nachweis vorliegt, dass ein in [E.Info.UNM-1.PersonalInformation.UseCase] dokumentierter Anwendungsfall nicht durch einen in [E.Info.UNM-1.PersonalInformation.UseCase.Notification] dokumentierten Benachrichtigungsmechanismus für den Benutzer abgedeckt ist.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn ein Nachweis vorliegt, dass ein in [E.Info.UNM-1.PersonalInformation.UseCase] dokumentierter Anwendungsfall nicht durch einen in [E.Info.UNM-1.PersonalInformation.UseCase.Notification] dokumentierten Benachrichtigungsmechanismus für den Benutzer abgedeckt ist.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

### 6.8.2 [UNM-2] Angemessener Inhalt der Benutzerbenachrichtigung

#### 6.8.2.1 Anforderung

Der Inhalt einer Benachrichtigung, die von einem Benutzer-Benachrichtigungsmechanismus bereitgestellt wird, der nach UNM-1 vorgeschrieben ist, muss mindestens Folgendes umfassen:

— eine Beschreibung einer Änderung; und

— eine Beschreibung, wie sich eine Änderung auf die Privatsphäre und den Schutz personenbezogener Informationen auswirken wird.

#### 6.8.2.2 Begründung

Die transparente und verständliche Information ermöglicht es dem Benutzer der Anlage zu verstehen, welche Änderungen den Datenschutz und den Schutz der personenbezogenen Informationen beeinflussen.

#### 6.8.2.3 Leitlinie

Mit „Reflektieren des Inhalts einer Benachrichtigung“ ist gemeint, dass dem Benutzer der Anlage erläutert wird, wie die Änderungen den Datenschutz und den Schutz der personenbezogenen Informationen beeinflussen.

Der Inhalt einer Benachrichtigung muss in präziser, transparenter, verständlicher und leicht zugänglicher Form abgefasst sein.

Alle Informationen für Kinder müssen prägnant, gut sichtbar und in einer dem Alter der Kinder angemessenen, klaren Sprache bereitgestellt werden.

#### 6.8.2.4 Beurteilungskriterien

#### 6.8.2.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung UNM-2.

#### 6.8.2.4.2 Umsetzungskategorien

Nicht anwendbar.

#### 6.8.2.4.3 Erforderliche Informationen

[E.Info.UNM-2.Notifications]: Beschreibung jedes nach UNM-1 erforderlichen Benutzer-Benachrichtigungsmechanismus, einschließlich:

— [E.Info.UNM-2.Notifications.UseCase]: Beschreibung jedes Anwendungsfalls, in dem Benachrichtigungen durch die Benutzer-Benachrichtigungsmechanismen bereitgestellt werden, einschließlich:

  — [E.Info.UNM-2.Notifications.UseCase.Content]: Beschreibung des Inhalts der Benachrichtigungen für den Anwendungsfall.

[E.Info.DT.UNM-2]: Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 32 für jeden in [E.Info.UNM-2.Notifications] dokumentierten Benutzer-Benachrichtigungsmechanismus.

[E.Just.DT.UNM-2]: Begründung für den gewählten Pfad durch den in [E.Info.DT.UNM-2] dokumentierten Entscheidungsbaum mit der folgenden Eigenschaft:

— die Begründung für die Entscheidung [DT.UNM-2.DN-1] basiert auf [E.Info.UNM-2.Notifications.UseCase.Content].

#### 6.8.2.4.4 Konzeptuelle Beurteilung

##### 6.8.2.4.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist eine konzeptuelle Beurteilung, ob eine Benachrichtigung den in [E.Info.UNM-2.Notifications.UseCase.Content] dokumentierten erforderlichen Inhalt wie nach UNM-2 erforderlich enthält.

##### 6.8.2.4.4.2 Voraussetzungen

Keine.

##### 6.8.2.4.4.3 Beurteilungseinheiten

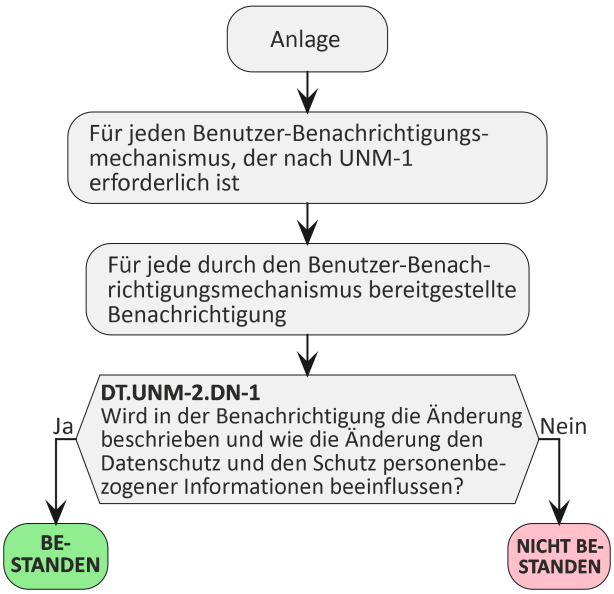



**Bild 32 — Entscheidungsbaum für Anforderung UNM-2**

Für jeden in [E.Info.UNM-2.Notifications] dokumentierten Benutzer-Benachrichtigungsmechanismus ist zu prüfen, ob der Pfad durch den in [E.Info.DT.UNM-2] dokumentierten Entscheidungsbaum mit „BESTANDEN“ endet.

Für jeden in [E.Info.DT.UNM-2] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.UNM-2] dokumentierte Begründung zu untersuchen.

#### 6.8.2.4.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— alle Pfade durch den in [E.Info.DT.UNM-2] dokumentierten Entscheidungsbaum mit „BESTANDEN“ enden; und

— die in [E.Just.DT.UNM-2] angegebenen Informationen korrekte Begründungen für alle Pfade durch den in [E.Info.DT.UNM-2] dokumentierten Entscheidungsbaum sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— ein Pfad durch den in [E.Info.DT.UNM-2] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; oder

— eine in [E.Just.DT.UNM-2] angegebene Begründung für einen Pfad durch den in [E.Info.DT.UNM-2] dokumentierten Entscheidungsbaum nicht korrekt ist oder fehlt.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

### 6.8.2.4.5 Beurteilung der funktionalen Vollständigkeit

Die Beurteilung der funktionalen Vollständigkeit wird durch die Beurteilung der funktionalen Suffizienz der Anwendbarkeit des Benutzer-Benachrichtigungsmechanismus abgedeckt.

Deshalb ist diese Beurteilung der funktionalen Vollständigkeit nicht notwendig.

### 6.8.2.4.6 Beurteilung der funktionalen Suffizienz

#### 6.8.2.4.6.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob eine Benachrichtigung den Inhalt wie nach UNM-2 erforderlich enthält.

#### 6.8.2.4.6.2 Voraussetzungen

Die Anlage befindet sich im Betriebszustand.

#### 6.8.2.4.6.3 Beurteilungseinheiten

Es ist funktional zu bestätigen, dass der Inhalt jedes in [E.Info.UNM-2.Notifications] dokumentierten Benutzer-Benachrichtigungsmechanismus den in UNM-2 erforderlichen Inhalt enthält.

#### 6.8.2.4.6.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn kein Nachweis vorliegt, dass die Umsetzung eines Benutzer-Benachrichtigungsmechanismus von [E.Info.UNM-2.Notifications] abweicht.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn ein Nachweis vorliegt, dass die Umsetzung eines Benutzer-Benachrichtigungsmechanismus von [E.Info.UNM-2.Notifications] abweicht.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

## 6.9 [CCK] Vertrauliche kryptographische Schlüssel (en: Confidential Cryptographic Keys)

### 6.9.1 [CCK-1] Angemessene CCKs

#### 6.9.1.1 Anforderung

Vertrauliche kryptographische Schlüssel, die auf der Anlage vorinstalliert sind oder von ihm während seiner Nutzung erzeugt werden, müssen eine Sicherheitsstufe von mindestens 112 Bits aufweisen, außer:

— CCKs, die ausschließlich von einem bestimmten Sicherheitsmechanismus verwendet werden, bei dem eine Abweichung nach den Vorgaben der Abschnitte ACM, AUM, SCM, SUM oder SSM festgestellt und begründet wird.

ANMERKUNG 1 Vertraulicher kryptographischer Schlüssel ist ein definierter Begriff. Andere Sicherheitsinformationen, deren Offenlegung nicht dazu verwendet werden kann, den Schutz der Daten des Benutzers oder Teilnehmers zu kompromittieren, wie Sicherheitsinformationen, die ausschließlich dem Schutz des geistigen Eigentums dienen, fallen nicht unter die Definition des vertraulichen kryptographischen Schlüssels.

ANMERKUNG 2 Die Anforderung bezieht sich auf alle vertraulichen kryptographischen Schlüssel, die vom Gerätehersteller entweder direkt gewählt oder durch ein Protokoll vorgeschrieben werden. So wählt/konfiguriert der Hersteller beispielsweise direkt die vom Gerät zu verwendende Chiffriersuite des TLS-Protokolls, während andere Protokolle nur eine einzige Option für kryptographische Algorithmen und ihre jeweiligen Schlüssel vorschreiben können.

#### 6.9.1.2 Begründung

Die Anlagen können Kryptographie und damit CCKs für viele und unterschiedliche Zwecke nutzen, wie beispielsweise zur Authentisierung, um eine Zugangssteuerung zu Sicherheitswerten oder Datenschutzwerten zu erzwingen, zum Schutz der Vertraulichkeit oder Integrität von Sicherheitswerten oder Datenschutzwerten während der Speicherung oder während der Übertragung zu einer anderen Entität, oder zur Ableitung anderer CCKs. Wenn die Vertraulichkeit eines CCK kompromittiert wird, können die vom CCK geschützten Sicherheitswerte und Datenschutzwerte ebenfalls kompromittiert werden. Ein CCK eines Geräts, der für einen kryptographischen Schutzalgorithmus generiert wurde, ist angemessen, wenn von einem erfolgreichen Angriff auf den CCK keine anderen, von diesem oder einem anderen Gerät verwendeten oder generierten CCKs betroffen sind und der Algorithmus bei Verwendung dieses CCK ausreichend stark ist, um bei seiner Nutzung auftretenden Angriffen zu widerstehen, deren Ziel die Zerstörung der Vertraulichkeit ist.

#### 6.9.1.3 Leitlinie

Die von einem CCK unterstützte Sicherheitsstufe hängt hauptsächlich von 3 Parametern ab:

— die Entropie des für ihre Erzeugung verwendeten RNG; und

— dessen effektive Länge (siehe BSI TR-02102-1 [20]); und

— vom kryptographischen Algorithmus, mit dem er verwendet wird.

Ein weiterer wichtiger Aspekt, der mit der von einem CCK unterstützten erforderlichen Sicherheitsstufe zusammenhängt, ist die Lebensdauer des CCK. Langfristige CCKs, die über lange Zeitspannen gespeichert und wiederholt genutzt werden, würden im Vergleich zu kurzfristigen CCKs, die üblicherweise auf der Anlage erzeugt und nur für kurze Zeit genutzt werden, eine zeitlich längere Widerstandsfähigkeit gegen Angriffe benötigen. Typische Beispiele für kurzfristige Schlüssel sind z. B. Sitzungsschlüssel, die zur Verschlüsselung der während einer einzigen Kommunikationssitzung übertragenen Sicherheitswerte oder Datenschutzwerte verwendet werden. Perfekte Folgenlosigkeit ist jedoch ein Aspekt, der in der Regel für die Sicherheit von Sitzungsschlüsseln berücksichtigt wird, und so werden diese in der Regel mit angemessenen kryptographischen Mechanismen erzeugt/abgeleitet, damit Sitzungsschlüssel vergangener Sitzungen nicht kompromittiert werden können.

Siehe CRY-1 als Orientierungshilfe zur bewährten Verfahrensweise.

Weitere bewährte Sicherheitsverfahren müssen ebenfalls berücksichtigt werden. Beispielsweise entspricht es bewährten Sicherheitsverfahren, einen CCK nur für einen Zweck zu verwenden. Besondere Sorgfalt ist bei CCKs geboten, die nicht mehr verwendet werden; diese sind beispielsweise zu löschen. Es wird empfohlen, hierbei bewährte Verfahrensweisen zu befolgen, siehe Anforderung CRY-1. Es wird auch empfohlen, den gleichen CCK nicht zu replizieren und auf anderen Ausführungen/Einheiten dieses Geräts zu verwenden.

Es kann Fälle geben, in denen Abweichungen von der Sicherheitsstufe von mindestens 112 Bit der CCKs gerechtfertigt sind. Zum Beispiel können CCKs, die aus von Menschen generierten Passwörtern abgeleitet sind, keine 112 Bit Sicherheitsstufe bieten. Die Ableitung von Passwortschlüsseln wird in Anwendungen und Protokollen verwendet, weil sie praktisch sind und für den jeweiligen Anwendungsfall angemessene Sicherheit bieten. Es könnte auch Fälle geben, in denen aus Gründen der Interoperabilität Sicherheitsmaßnahmen eine Abweichung von der Sicherheitsstufe von mindestens 112 Bit vorschreiben, die von CCKs bereitgestellt werden muss. Dies kann auf den Bedarf an „Interoperabilitätsunterstützung“ (siehe z. B. SCM-1) oder auf die notwendige Nutzung von standardisierten und weit verbreiteten Kommunikationsprotokollen zurückzuführen sein, die von den bewährten Verfahrensweisen abweichen.

Bei solchen Abweichungen müssen die sich daraus ergebenden Risiken für „den Schutz der Datenschutzwerte und/oder Sicherheitswerte“ beurteilt werden.

#### 6.9.1.4 Beurteilungskriterien

##### 6.9.1.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung CCK-1.

##### 6.9.1.4.2 Umsetzungskategorien

Nicht anwendbar.

##### 6.9.1.4.3 Erforderliche Informationen

[E.Info.CCK-1.CCK]: Für jeden vertraulichen kryptographischen Schlüssel (ob er vorinstalliert ist oder vom Gerät während seiner Verwendung erzeugt wird) ist Folgendes zu beschreiben:

— die kryptographischen Algorithmen für den vertraulichen kryptographischen Schlüssel und die Schlüssellänge der Umsetzung des vertraulichen kryptographischen Schlüssels; und

— (wird der vertrauliche kryptographische Schlüssel ausschließlich von einem bestimmten Sicherheitsmechanismus verwendet, bei dem eine Abweichung nach den Vorgaben der Abschnitte ACM, AUM, SCM, SUM oder SSM festgestellt und begründet wird) [E.Info.CCK-1.CCK.Deviation]: Verweisung auf die entsprechende Begründung und auf die erforderlichen Informationen, auf die sich die Begründung stützt; und

— [E.Info.CCK-1.CCK.SecurityStrength]: Die Sicherheitsstufe und die Verweisung auf die bei der Beurteilung verwendeten Nachschlagetabellen.

ANMERKUNG Z. B. unter Bezugnahme auf die Definitionen der Sicherheitsstufe in SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms [24] oder NIST Special Publications 800-57 [8] oder 800-131A [15].

[E.Info.DT.CCK-1]: Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 33 für jeden in [E.Info.CCK-1.CCK] dokumentierten vertraulichen kryptographischen Schlüssel.

[E.Just.DT.CCK-1]: Begründung für den gewählten Pfad durch den in [E.Info.DT.CCK-1] dokumentierten Entscheidungsbaum mit den folgenden Eigenschaften:

— (wenn eine Entscheidung aus [DT.CCK-1.DN-2] zu „NICHT ANWENDBAR“ führt) basiert die Begründung für die Entscheidung [DT.CCK-1.DN-2] auf [E.Info.CCK-1.CCK.Deviation]; und

— die Begründung für die Entscheidung [DT.CCK-1.DN-1] basiert auf [E.Info.CCK-1.CCK] und [E.Info.CCK-1.CCK.SecurityStrength].

#### 6.9.1.4.4 Konzeptuelle Beurteilung

##### 6.9.1.4.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob die vertraulichen kryptographischen Schlüssel wie nach CCK-1 erforderlich implementiert sind.

##### 6.9.1.4.4.2 Voraussetzungen

Keine.

##### 6.9.1.4.4.3 Beurteilungseinheiten

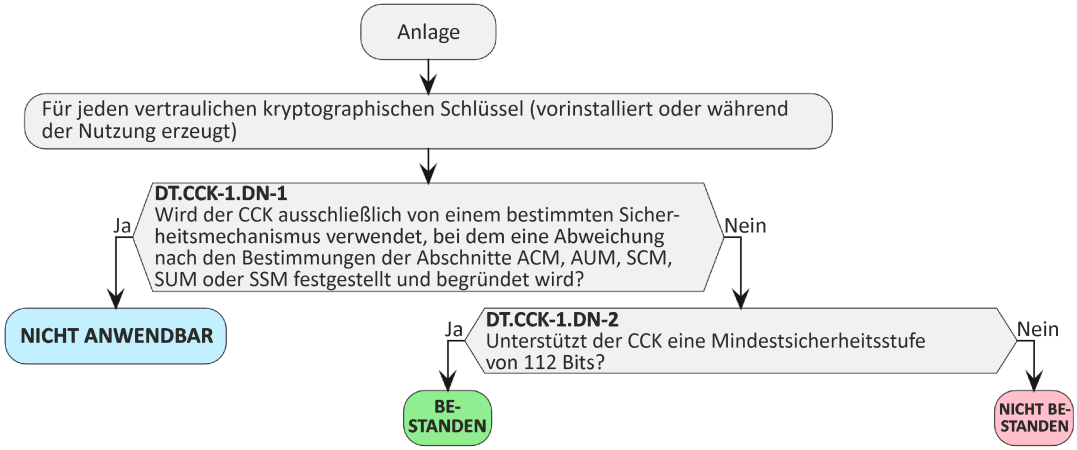



**Bild 33 — Entscheidungsbaum für Anforderung CCK-1**

Für jeden in [E.Info.CCK-1.CCK] dokumentierten vertraulichen kryptographischen Schlüssel ist zu prüfen, ob der Pfad durch den in [E.Info.DT.CCK-1] dokumentierten Entscheidungsbaum mit „NICHT ANWENDBAR“ oder „BESTANDEN“ endet.

Für jeden in [E.Info.DT.CCK-1] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.CCK-1] dokumentierte Begründung zu untersuchen.

##### 6.9.1.4.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— mindestens ein Pfad durch den in [E.Info.DT.CCK-1] dokumentierten Entscheidungsbaum mit „BESTANDEN“ endet; und

— kein Pfad durch den in [E.Info.DT.CCK-1] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; und

— die in [E.Just.DT.CCK-1] angegebenen Informationen korrekte Begründungen für alle Pfade durch den in [E.Info.DT.CCK-1] dokumentierten Entscheidungsbaum sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— ein Pfad durch den in [E.Info.DT.CCK-1] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; oder

— eine in [E.Just.DT.CCK-1] angegebene Begründung für einen Pfad durch den in [E.Info.DT.CCK-1] dokumentierten Entscheidungsbaum nicht korrekt ist oder fehlt.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

#### 6.9.1.4.5 Beurteilung der funktionalen Vollständigkeit

##### 6.9.1.4.5.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob die Dokumentation der CCKs vollständig ist.

##### 6.9.1.4.5.2 Voraussetzungen

Die Anlage befindet sich im Betriebszustand.

##### 6.9.1.4.5.3 Beurteilungseinheiten

Es ist funktional zu beurteilen, ob CCKs vorinstalliert sind oder vom Gerät erzeugt werden, die nicht in [E.Info.CCK-1.CCK] dokumentiert sind.

##### 6.9.1.4.5.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn alle gefundenen CCKs in [E.Info.CCK-1.CCK] dokumentiert sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn ein gefundener CCK nicht in [E.Info.CCK-1.CCK] dokumentiert ist.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

#### 6.9.1.4.6 Beurteilung der funktionalen Suffizienz

##### 6.9.1.4.6.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob die in [E.Info.CCK-1.CCK] dokumentierten vertraulichen kryptographischen Schlüssel wie dokumentiert implementiert sind.

ANMERKUNG Die Beurteilung der Bitlänge ist nur eine notwendige Bedingung und stellt keine vollständige Beurteilung der funktionalen Suffizienz der Sicherheitsstufe dar.

##### 6.9.1.4.6.2 Voraussetzungen

Die Anlage befindet sich im Betriebszustand.

##### 6.9.1.4.6.3 Beurteilungseinheiten

Für jeden in [E.Info.CCK-1.CCK] dokumentierten vertraulichen kryptographischen Schlüssel ist funktional zu beurteilen, ob die in [E.Info.CCK-1.CCK] dokumentierte Länge des CCK in Übereinstimmung mit [E.Info.CCK-1.CCK.SecurityStrength] implementiert ist.

##### 6.9.1.4.6.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn kein Nachweis vorliegt, dass die in [E.Info.CCK-1.CCK] dokumentierte Länge eines CCK von seiner Dokumentation abweicht.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn ein Nachweis vorliegt, dass die in [E.Info.CCK-1.CCK] dokumentierte Länge eines CCK von der Dokumentation abweicht.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

### 6.9.2 [CCK-2] Mechanismen zur Erzeugung des CCK

#### 6.9.2.1 Anforderung

Die Erzeugung vertraulicher kryptographischer Schlüssel muss bewährten kryptographischen Verfahrensweisen entsprechen, mit Ausnahme der folgenden:

— die Erzeugung der CCKs für einem bestimmten Sicherheitsmechanismus, bei dem eine Abweichung nach den Vorgaben der Abschnitte ACM, AUM, SCM, SUM oder SSM festgestellt und begründet wird.

ANMERKUNG Vertraulicher kryptographischer Schlüssel ist ein definierter Begriff. Andere Sicherheitsinformationen, deren Offenlegung nicht dazu verwendet werden kann, den Schutz der Daten des Benutzers oder Teilnehmers zu kompromittieren, wie Sicherheitsinformationen, die ausschließlich dem Schutz des geistigen Eigentums dienen, fallen nicht unter die Definition des vertraulichen kryptographischen Schlüssels.

#### 6.9.2.2 Begründung

CCKs, die vom Gerät erzeugt und zum Schutz von Sicherheitswerten oder Datenschutzwerten verwendet werden, müssen angemessen generiert werden, um erfolgreiche Angriffe auf der Grundlage von CCKs mit unzureichender Sicherheitsstufe zu verhindern. Ein angemessener CCK-Erzeugungsmechanismus stellt sicher, dass die CCKs über die notwendigen Eigenschaften verfügen, die für die Risiken und die Betriebsbedingungen der Anlage angemessen sind.

#### 6.9.2.3 Leitlinie

Die Sicherheitsstufe eines CCK wird weitgehend durch die Zufallszahlenquelle (die Hauptquelle der Entropie) und den Zufallszahlengenerator sowie den Algorithmus zur Schlüsselgenerierung/-ableitung bestimmt, die sie erzeugen.

Risiken im Zusammenhang mit einer schlechten Wahl der Zufallsquelle, der Zufallszahlengeneratoren und der Schlüsselableitung können dazu führen, dass CCKs Angriffen ausgesetzt sind wie

— das Erraten eines CCKs; oder

— einem Brute-Force-Angriff auf einen CCK; oder

— die Rekonstruktion eines CCKs auf Grundlage von zugänglichen Informationen.

Es ist daher entscheidend, dass der Mechanismus zur Erzeugung der CCKs keine CCKs mit unzureichender Sicherheitsstufe erzeugt. Ein robuster Mechanismus zur Erzeugung von CCKs beruht auf einem sicheren RNG, der Zufallszahlen mit ausreichender Entropie liefert. Es ist eine sehr komplexe Aufgabe, einen sicheren und robusten CCK-Generierungsmechanismus und den zugrunde liegenden RNG zu entwickeln. Es wird dringend empfohlen, zu diesem Zweck allgemein anerkannte Normen zu befolgen.

ANMERKUNG 1 Es gibt unterschiedliche anerkannte Normen für Schlüsselerzeugungsmechanismen. Anerkannte bewährte Verfahrensweisen für Zufallszahlgeneratoren sind beispielsweise NIST SP800-90A [11], NIST SP800-90B [12], NIST SP800-90C [13], BSI AIS20 [42], BSI AIS31 [19], ISO/IEC 18031 [43].

ANMERKUNG 2 Beispiele für anerkannte bewährte Verfahrensweisen für die Schlüsselableitung sind z. B. im SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms [24] beschrieben. Alternativen sind hier verfügbar: ISO/IEC 11770 [28], NIST SP 800-108r1 [14], NIST SP 800-132 [16].

#### 6.9.2.4 Beurteilungskriterien

##### 6.9.2.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung CCK-2.

##### 6.9.2.4.2 Umsetzungskategorien

Nicht anwendbar.

##### 6.9.2.4.3 Erforderliche Informationen

[E.Info.CCK-2.Generation]: Beschreibung der einzelnen Generierungsmechanismen für vertrauliche kryptographische Schlüssel, einschließlich der folgenden Einzelheiten:

— [E.Info.CCK-2.Generation.CCK]: Festlegung der vertraulichen kryptographischen Schlüssel, die der Mechanismus generiert, und Angabe, ob deren Generierung der bewährten kryptographischen Verfahrensweise entspricht; und

— (wenn der Generierungsmechanismus für CCK auf einer Zufallszahlenquelle beruht und für die Generierung vertraulicher kryptographischer Schlüssel verwendet wird, die den bewährten kryptographischen Verfahrensweisen entsprechen) [E.Info.CCK-2.Generation.RNSource]:

  — es sind die bewährten Verfahrensweisen anzugeben, gefolgt von der Zufallszahlenquelle; und

  — es ist zu erläutern, warum die Zufallszahlenquelle eine ausreichende Sicherheitsstufe bietet; und

  — es ist zu erläutern, wie die Zufallszahlenquelle konfiguriert und initialisiert wird; und

  — wenn angegeben wird, dass der CCK anerkannten Sicherheitsnormen oder Zertifizierungsprogrammen entspricht, sind Nachweise über die anerkannten Sicherheitsnormen oder Zertifizierungsprogramme vorzulegen, denen der CCK entspricht; und

— (wenn der Generierungsmechanismus für CCK auf einem Zufallszahlengenerator beruht und für die Generierung vertraulicher kryptographischer Schlüssel verwendet wird, die den bewährten kryptographischen Verfahrensweisen entsprechen) [E.Info.CCK-2.Generation.RNG]:

  — es ist anzugeben, ob es ein deterministischer oder nicht-deterministischer Zufallszahlengenerator ist; und

  — es sind die bewährten Verfahrensweisen anzugeben, gefolgt vom Zufallszahlengenerator; und

  — es ist anzugeben, warum der Zufallszahlengenerator eine ausreichende Sicherheitsstufe bietet; und

  — es ist zu erläutern, wie der Zufallszahlengenerator konfiguriert und initialisiert wird; und

  — wenn angegeben wird, dass der CCK anerkannten Sicherheitsnormen oder Zertifizierungsprogrammen entspricht, sind Nachweise über die anerkannten Sicherheitsnormen oder Zertifizierungsprogramme vorzulegen, denen der CCK entspricht; und

— (wenn der Generierungsmechanismus für CCK auf einem Mechanismus zur Ableitung/Erstellung beruht und für die Generierung vertraulicher kryptographischer Schlüssel verwendet wird, die den bewährten Verfahrensweisen für Kryptographie entsprechen) [E.Info.CCK-2.Generation.Implementation]:

  — es sind die bewährten Verfahrensweisen anzugeben, gefolgt vom Mechanismus zur Ableitung/Erstellung; und

  — es ist der dafür verwendete Algorithmus zur Schlüsselableitung/-erzeugung anzugeben; und

— (wenn der Erzeugungsmechanismus vertrauliche kryptographische Schlüssel generiert, die ausschließlich von einem bestimmten Sicherheitsmechanismus verwendet werden, bei dem eine Abweichung von der kryptographischen bewährten Verfahrensweise im Sinne der Abschnitte ACM, AUM, SCM, SUM oder SSM festgestellt und begründet wird) [E.Info.CCK-2.Generation.Deviation]:

  — Verweisung auf die entsprechende Begründung und auf die erforderlichen Informationen, auf die sich die Begründung stützt.

ANMERKUNG Die oben genannten Informationen stehen dem Hersteller möglicherweise nicht immer zur Verfügung, wenn der Erzeugungsmechanismus von einem Anbieter bereitgestellt wird, der diese Informationen aus Sicherheitsgründen nicht preisgibt, jedoch alle notwendigen Sicherheitsanweisungen zur Verwendung des Erzeugungsmechanismus bereitstellt.

[E.Info.DT.CCK-2]: Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 34 für jeden in [E.Info.CCK-2.Generation] dokumentierten Erzeugungsmechanismus für vertrauliche kryptographische Schlüssel.

[E.Just.DT.CCK-2]: Begründung für den gewählten Pfad durch den in [E.Info.DT.CCK-2] dokumentierten Entscheidungsbaum mit den folgenden Eigenschaften:

— (wenn eine Entscheidung aus [DT.CCK-2.DN-1] zu „NICHT ANWENDBAR“ führt) basiert die Begründung für die Entscheidung [DT.CCK-2.DN-1] auf [E.Info.CCK-2.Generation.Deviation]; und

— die Begründung für die Entscheidung [DT.CCK-2.DN-2] basiert auf [E.Info.CCK-2.Generation].

#### 6.9.2.4.4 Konzeptuelle Beurteilung

##### 6.9.2.4.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob alle in [E.Info.CCK-2.Generation] aufgeführten Mechanismen zur Erzeugung vertraulicher kryptographischer Schlüssel den Anforderungen von CCK-2 entsprechen.

##### 6.9.2.4.4.2 Voraussetzungen

Keine.

#### 6.9.2.4.4.3 Beurteilungseinheiten

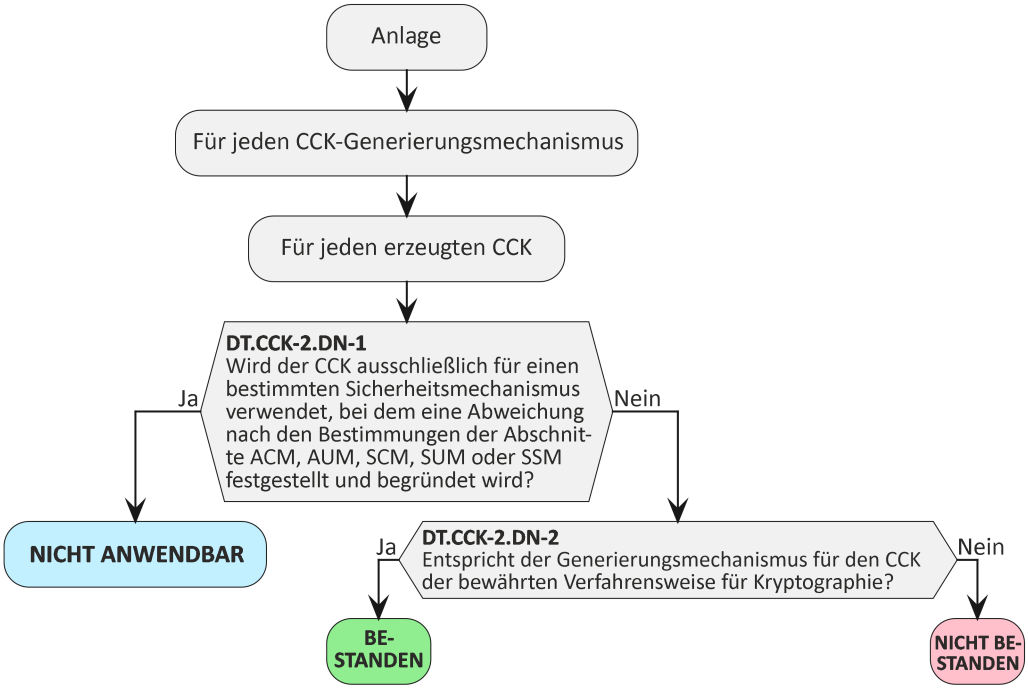



**Bild 34 — Entscheidungsbaum für Anforderung CCK-2**

Für jeden in [E.Info.CCK-2.Generation] dokumentierten Mechanismus zur Erzeugung vertraulicher kryptographischer Schlüssel auf der Anlage ist zu prüfen, ob der Pfad durch den in [E.Info.DT.CCK-2] dokumentierten Entscheidungsbaum mit „NICHT ANWENDBAR“ oder „BESTANDEN“ endet.

Für jeden in [E.Info.DT.CCK-2] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.CCK-2] dokumentierte Begründung zu untersuchen.

#### 6.9.2.4.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— mindestens ein Pfad durch den in [E.Info.DT.CCK-2] dokumentierten Entscheidungsbaum mit „BESTANDEN“ endet; und

— kein Pfad durch den in [E.Info.DT.CCK-2] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; und

— die in [E.Just.DT.CCK-2] angegebenen Informationen korrekte Begründungen für alle Pfade durch den in [E.Info.DT.CCK-2] dokumentierten Entscheidungsbaum sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— ein Pfad durch den Entscheidungsbaum mit „NICHT BESTANDEN“ endet; oder

— eine in [E.Just.DT.CCK-2] angegebene Begründung für einen Pfad durch den in [E.Info.DT.CCK-2] dokumentierten Entscheidungsbaum nicht korrekt ist oder fehlt.

Die Entscheidung NICHT ANWENDBAR wird anderweitig zugewiesen.

#### 6.9.2.4.5 Beurteilung der konzeptuellen Vollständigkeit der Dokumentation

##### 6.9.2.4.5.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist es, konzeptuell zu beurteilen, ob alle Erzeugungsmechanismen für vertrauliche kryptographische Schlüssel auf der Anlage in [E.Info.CCK-2.Generation] dokumentiert sind.

##### 6.9.2.4.5.2 Voraussetzungen

Keine.

##### 6.9.2.4.5.3 Beurteilungseinheiten

Durch eine Konsistenzprüfung mit [E.Info.CCK-1.CCK] ist zu prüfen, ob keine Nachweise für Erzeugungsmechanismen für vertrauliche kryptographische Schlüssel auf der Anlage vorliegen, die nicht in [E.Info.CCK-2.Generation] dokumentiert sind.

##### 6.9.2.4.5.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn kein Nachweis vorliegt, dass es Erzeugungsmechanismen für vertrauliche kryptographische Schlüssel gibt, die nicht in [E.Info.CCK-2.Generation] dokumentiert sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn ein Nachweis vorliegt, dass es Erzeugungsmechanismen für vertrauliche kryptographische Schlüssel gibt, die nicht in [E.Info.CCK-2.Generation] dokumentiert sind.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

#### 6.9.2.4.6 Beurteilung der funktionalen Suffizienz

Die Validierung von Mechanismen zur Erzeugung von kryptographischen Schlüsseln ist sehr komplex und wird in der Regel von einer Drittpartei mit umfangreichen kryptographischen Fachkenntnissen durchgeführt, die wahrscheinlich keine Einzelheiten über solche Schlüsselerzeugungsprozesse preisgeben wird. In Anbetracht dieser Erwägungen wird für diese Anforderung keine Beurteilung der funktionalen Suffizienz vorgenommen.

### 6.9.3 [CCK-3] Verhinderung von statischen Vorgabewerten für vorinstallierte CCKs

#### 6.9.3.1 Anforderung

Vorinstallierte vertrauliche kryptographische Schlüssel müssen faktisch eindeutig für jedes Gerät sein, mit Ausnahme von:

— CCKs, die nur für die Erstellung von anfänglichen Vertrauensbeziehungen unter Bedingungen verwendet werden, die von einer autorisierten Entität kontrolliert werden; oder

— CCKs, bei denen es sich um gemeinsame Parameter handelt, die für die vorgesehene Funktionalität der Anlage erforderlich sind.

ANMERKUNG Vertraulicher kryptographischer Schlüssel ist ein definierter Begriff. Andere Sicherheitsinformationen, deren Offenlegung nicht dazu verwendet werden kann, den Schutz der Daten des Benutzers oder Teilnehmers zu kompromittieren, wie Sicherheitsinformationen, die ausschließlich dem Schutz des geistigen Eigentums dienen, fallen nicht unter die Definition des vertraulichen kryptographischen Schlüssels.

#### 6.9.3.2 Begründung

Anlagen können Verschlüsselung und damit CCKs zum Schutz der Sicherheitswerte und Datenschutzwerte auf der Anlage einsetzen. Die CCKs werden manchmal vordefiniert, z. B. während der Herstellung. CCKs, die für

den oben genannten Zweck verwendet werden, müssen angemessen sein, um erfolgreiche Angriffe auf der Grundlage von CCKs mit unzureichender Stärke zu verhindern, besonders wenn sie vorinstalliert sind.

#### 6.9.3.3 Leitlinie

CCKs können bei der Herstellung auf der Anlage vorinstalliert werden. Vorinstallierte, für jede Geräteinstanz eindeutige CCKs, die Brute-Force-Angriffen standhalten, können das mit der spezifischen Verwendung des CCK verbundene Cyber-Sicherheitsrisiko eindämmen.

Eindeutig bedeutet, dass das Passwort nicht systematisch wiederverwendet wird oder für ein anderes Gerät des gleichen Produkttyps abgeleitet werden kann, und dass es nicht einfach von den Eigenschaften der Anlage (z. B. dem Herstellernamen, dem Modellnamen oder der Media Access Control-(MAC-)Adresse) abgeleitet werden kann. Ein gängiger Zufallsgenerator kann verwendet werden, um faktisch eindeutige kryptographische Schlüssel zu erzeugen.

In einigen Fällen werden die Schlüssel nur für den Aufbau erster Vertrauensbeziehungen unter Bedingungen verwendet, die von einer autorisierten Entität kontrolliert werden, oder der Schlüssel als gemeinsam genutzter Parameter ist für den Betrieb der Anlage unerlässlich, z. B. für Softwareaktualisierungen oder die Konfiguration der Migration für Netzwerkgeräte. In solchen Fällen können statische Schlüssel verwendet werden.

#### 6.9.3.4 Beurteilungskriterien

##### 6.9.3.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung CCK-3.

##### 6.9.3.4.2 Umsetzungskategorien

Nicht anwendbar.

##### 6.9.3.4.3 Erforderliche Informationen

[E.Info.CCK-3.CCK]: Beschreibung jedes vorinstallierten vertraulichen kryptographischen Schlüssels auf der Anlage, einschließlich:

— (wenn angegeben wird, dass die faktische Eindeutigkeit des vertraulichen kryptographischen Schlüssels nicht erforderlich ist, weil er nur zur Herstellung erster Vertrauensbeziehungen unter Bedingungen verwendet wird, die von einer autorisierten Entität kontrolliert werden) [E.Info.CCK-3.CCK.Controlled]: Beschreibung:

  — der anfänglichen Vertrauensbeziehung, die durch den vertraulichen kryptographischen Schlüssel hergestellt werden soll; und

  — der Bedingungen, die von einer autorisierten Entität kontrolliert werden; und

— (wenn angegeben wird, dass die faktische Eindeutigkeit des vertraulichen kryptographischen Schlüssels nicht erforderlich ist, weil er ein für die vorgesehene Anlagenfunktionalität geteilter Parameter ist) [E.Info.CCK-3.CCK.Shared]: Beschreibung der Anlagenfunktionalitäten, für die der vertrauliche kryptographische Schlüssel ein geteilter Parameter ist; und

— (wenn angegeben wird, dass der CCK faktisch eindeutig für jedes Gerät ist) [E.Info.CCK-3.CCK.Unique]: Beschreibung der Methoden, die dazu führen, dass der CCK faktisch eindeutig für jedes Gerät ist.

[E.Info.DT.CCK-3]: Beschreibung des gewählten Pfads durch den in Bild 35 dargestellten Entscheidungsbaum für jeden vorinstallierten in [E.Info.CCK-3.CCK] dokumentierten CCK.

[E.Just.DT.CCK-3]: Begründung für den gewählten Pfad durch den in [E.Info.DT.CCK-3] dokumentierten Entscheidungsbaum mit den folgenden Eigenschaften:

— (wenn eine Entscheidung aus [DT.CCK-3.DN-2] zu „NICHT ANWENDBAR“ führt) basiert die Begründung für die Entscheidung [DT.CCK-3.DN-2] auf [E.Info.CCK-3.CCK.Controlled]; und

— (wenn eine Entscheidung aus [DT.CCK-3.DN-3] zu „NICHT ANWENDBAR“ führt) basiert die Begründung für die Entscheidung [DT.CCK-3.DN-3] auf [E.Info.CCK-3.CCK.Shared]; und

— die Begründung für die Entscheidung [DT.CCK-3.DN-1] basiert auf [E.Info.CCK-3.CCK.Unique].

#### 6.9.3.4.4 Konzeptueller Beurteilungsfall

##### 6.9.3.4.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob die vorinstallierten vertraulichen kryptographischen Schlüssel wie nach CCK-3 erforderlich implementiert sind.

##### 6.9.3.4.4.2 Voraussetzungen

Keine.

##### 6.9.3.4.4.3 Beurteilungseinheiten

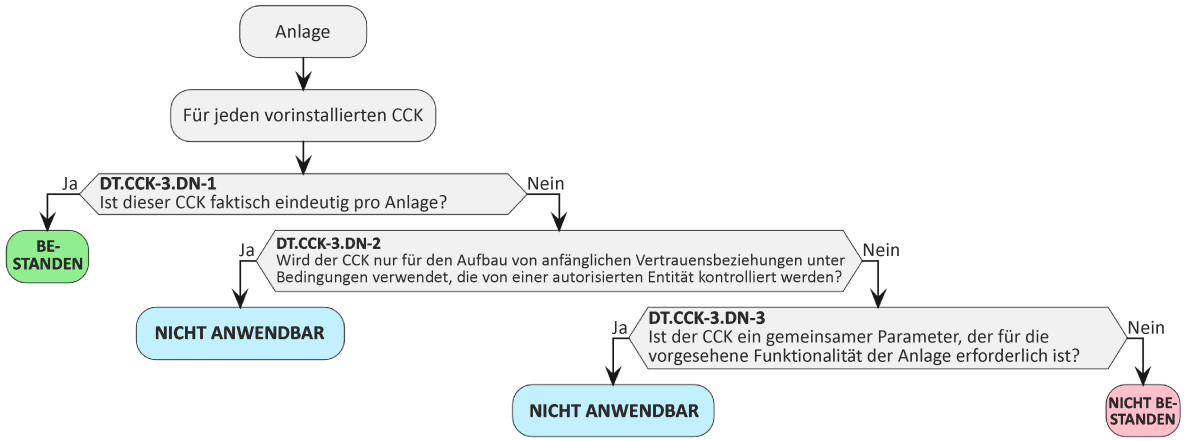



**Bild 35 — Entscheidungsbaum für Anforderung CCK-3**

Für jeden in [E.Info.CCK-3.CCK] dokumentierten vertraulichen kryptographischen Schlüssel ist zu prüfen, ob der Pfad durch den in [E.Info.DT.CCK-3] dokumentierten Entscheidungsbaum mit „NICHT ANWENDBAR“ oder „BESTANDEN“ endet.

Für jeden in [E.Info.DT.CCK-3] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.CCK-3] dokumentierte Begründung zu untersuchen.

#### 6.9.3.4.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— mindestens ein Pfad durch den in [E.Info.DT.CCK-3] dokumentierten Entscheidungsbaum mit „BESTANDEN“ endet; und

— kein Pfad durch den in [E.Info.DT.CCK-3] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; und

— die in [E.Just.DT.CCK-3] angegebenen Informationen korrekte Begründungen für alle Pfade durch den in [E.Info.DT.CCK-3] dokumentierten Entscheidungsbaum sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— ein Pfad durch den in [E.Info.DT.CCK-3] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; oder

— eine in [E.Just.DT.CCK-3] angegebene Begründung für einen Pfad durch den in [E.Info.DT.CCK-3] dokumentierten Entscheidungsbaum nicht korrekt ist oder fehlt.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

#### 6.9.3.4.5 Beurteilung der funktionalen Vollständigkeit

##### 6.9.3.4.5.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob alle vorinstallierten CCKs dokumentiert sind.

##### 6.9.3.4.5.2 Voraussetzungen

Die Anlage befindet sich in Werksvoreinstellung.

##### 6.9.3.4.5.3 Beurteilungseinheiten

Es ist funktional zu beurteilen, ob vorinstallierte CCKs auf der Anlage gespeichert sind, die nicht in [E.Info.CCK-3.CCK] dokumentiert sind.

##### 6.9.3.4.5.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn alle gefundenen vorinstallierten CCKs in [E.Info.CCK-3.CCK] dokumentiert sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn ein gefundener vorinstallierter CCK nicht in [E.Info.CCK-3.CCK] dokumentiert ist.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

#### 6.9.3.4.6 Beurteilung der funktionalen Suffizienz

##### 6.9.3.4.6.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob die vorinstallierten CCKs, von denen angenommen wird, dass sie faktisch eindeutig für jedes Gerät sind, ausreichend unabhängig voneinander sind.

##### 6.9.3.4.6.2 Voraussetzungen

Zwei Instanzen der Anlage entsprechen der Werkeinstellung.

##### 6.9.3.4.6.3 Beurteilungseinheiten

Für jeden in [E.Info.CCK-3.CCK] dokumentierten CCK, wobei [E.Info.CCK-3.CCK.Unique] angibt, dass der CCK für jedes Gerät faktisch eindeutig ist, ist funktional zu beurteilen, dass die jeweiligen CCKs der beiden Anlagen faktisch eindeutig sind, indem:

— (wenn die CCKs zugänglich sind) Vergleich der CCKs und die Bestätigung, dass sie nicht gleich sind und dass es kein offensichtliches Verfahren gibt, um den einen vom anderen abzuleiten; und

— (wenn die CCKs nicht zugänglich sind, aber zusammen mit den damit verbundenen zugänglichen öffentlichen kryptographischen Schlüsseln, z. B. als Paare von privaten/öffentlichen Schlüsseln, bereitgestellt wer-

den, die damit verbundenen öffentlichen kryptographischen Schlüssel vergleichen und bestätigen, dass sie nicht gleich sind.

ANMERKUNG Die spezifische funktionale Prüfung ist möglicherweise nicht immer für jeden CCK durchführbar, da üblicherweise nicht alle CCKs zugänglich sind oder über einen zugänglichen öffentlichen kryptographischen Schlüssel verfügen.

#### 6.9.3.4.6.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn kein Nachweis vorliegt, dass ein in [E.Info.CCK-3.CCK] dokumentierter CCK, wobei [E.Info.CCK-3.CCK.Unique] angibt, dass der CCK für jedes Gerät faktisch eindeutig ist, faktisch nicht für jedes Gerät eindeutig ist.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn ein Nachweis vorliegt, dass ein in [E.Info.CCK-3.CCK] dokumentierter CCK, wobei [E.Info.CCK-3.CCK.Unique] angibt, dass der CCK für jedes Gerät faktisch eindeutig ist, faktisch nicht eindeutig für jedes Gerät ist.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

## 6.10 [GEC] Allgemeine Gerätefähigkeiten (en: General Equipment Capabilities)

### 6.10.1 [GEC-1] Aktuelle Software und Hardware ohne öffentlich bekannte ausnutzbare Schwachstellen

#### 6.10.1.1 Anforderung

Die Anlage darf keine öffentlich bekannten ausnutzbaren Schwachstellen aufweisen, die, wenn sie ausgenutzt werden, Sicherheitswerte und Datenschutzwerte gefährden, außer bei Schwachstellen:

— die unter den spezifischen Bedingungen der Anlage nicht ausgenutzt werden können; oder

— die bis zu einem akzeptablen Restrisiko eingedämmt wurden; oder

— die auf Risikobasis akzeptiert wurden.

#### 6.10.1.2 Begründung

Anlagen können aus Hardware und Software bestehen, die von verschiedenen Lieferanten stammen, und der Hersteller hat möglicherweise unzureichende Einsicht in die Sicherheitspraktiken dieser Lieferanten.

Es ist wichtig, dass der Hersteller öffentlich bekannte ausnutzbare Schwachstellen in der auf den Anlagen eingesetzten Hardware und Software identifizieren kann, sowohl bei kommerzieller als auch bei Open-Source-Software, und dass er mit diesen Schwachstellen umgehen kann.

#### 6.10.1.3 Leitlinie

Um die Überwachung von Software-Schwachstellen zu erleichtern, erstellt der Gerätehersteller eine technische Dokumentation der Gerätesoftware, und zwar sowohl für die Open-Source-Software als auch für die kommerziellen Standardkomponenten. Gleichermaßen kann die technische Hardware-Dokumentation die Identifikation von Hardware-Schwachstellen unterstützen.

Um die öffentlich bekannten ausnutzbaren Schwachstellen der Gerätehardware und -software zu identifizieren, zieht der Hersteller eine öffentliche Schwachstellendatenbank zu Rate (z. B. NIST National Vulnerabilities Database https://nvd.nist.gov/ und bestehende National European Vulnerabilities Databases).

Zu den unterschiedlichen Faktoren, die der Hersteller bei der Beurteilung der öffentlich bekannten ausnutzbaren Schwachstellen berücksichtigt, gehören unter anderem:

— die Angriffsfläche der Anlage und die Vektoren/Pfade, über die sich der Angreifer Zugang zum Gerät verschaffen kann, um die Schwachstelle auszunutzen;

— der Nachweis, dass die Schwachstelle aktiv ausgenutzt wurde oder dass es für sie bereits dokumentierte Machbarkeitsnachweise oder Code-Ausnutzungen gibt;

— die im Gerät implementierten Sicherheitsfähigkeiten und Mechanismen, die die Ausnutzung der Schwachstelle eindämmen können;

— die „vorgesehene Anlagenfunktionalität“;

— die „für die Nutzung“ der Anlage vorgesehene Betriebsumgebung“, einschließlich Bedrohungsumfeld, Sicherheitsfähigkeiten und zusätzlicher, durch die Umgebung bereitgestellter Gegenmaßnahmen, die die Ausnutzung der Schwachstelle eindämmen oder beheben können.

#### 6.10.1.4 Beurteilungskriterien

##### 6.10.1.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung GEC-1.

##### 6.10.1.4.2 Umsetzungskategorien

Nicht anwendbar.

##### 6.10.1.4.3 Erforderliche Informationen

[E.Info.GEC-1.SecurityAsset]: Beschreibung jedes Sicherheitswerts der Anlage.

[E.Info.GEC-1.PrivacyAsset]: Beschreibung jedes Datenschutzwerts der Anlage.

[E.Info.GEC-1.SoftwareDocumentation]: Beschreibung der Gerätesoftware, einschließlich ihrer Versionen, soweit es die in [E.Info.GEC-1.SecurityAsset] dokumentierten Sicherheitswerte und in [E.Info.GEC-1.PrivacyAsset] dokumentierten Datenschutzwerte betrifft.

[E.Info.GEC-1.HardwareDocumentation]: Beschreibung der Gerätehardware, soweit es die in [E.Info.GEC-1.SecurityAsset] dokumentierten Sicherheitswerte und die in [E.Info.GEC-1.PrivacyAsset] dokumentierten Datenschutzwerte betrifft.

[E.Info.GEC-1.ListOfVulnerabilities]: Beschreibung aller öffentlich bekannten, ausnutzbaren Schwachstellen in der Hardware und Software, die die in [E.Info.GEC-1.SecurityAsset] und [E.Info.GEC-1.PrivacyAsset] dokumentierten Sicherheitswerte und Datenschutzwerte betreffen. Das Dokument enthält auch die Quelle der Informationen über die Schwachstellen. Darüber hinaus wird für jede Schwachstelle, die sich auf Datenschutzwerte und Sicherheitswerte auswirkt, eine Begründung zur Behebung, Eindämmung und Nicht-Ausnutzung der aufgeführten, öffentlich bekannten ausnutzbaren Schwachstellen der Hardware oder Software gegeben, einschließlich:

— (wenn die Schwachstelle behoben ist) [E.Info.GEC-1.ListOfVulnerabilities.Remediated]: die Maßnahmen, die zur Behebung der Schwachstelle ergriffen wurden; und

— (wenn die Schwachstelle unter den spezifischen Bedingungen der Anlage nicht ausgenutzt werden kann) [E.Info.GEC-1.ListOfVulnerabilities.SpecificCondition]: Die Beschreibung der spezifischen Bedingungen, unter denen die Schwachstelle nicht ausgenutzt werden kann; und

— (wenn die Schwachstelle eingedämmt ist) [E.Info.GEC-1.ListOfVulnerabilities.Mitgated]: Die Beschreibung der Maßnahmen zur Eindämmung; und

— (wenn die Schwachstelle anerkannt wird) [E.Info.GEC-1.ListOfVulnerabilities.Accepted]: Die Beschreibung der Anerkennung der Schwachstelle auf Risikobasis.

[E.Info.DT.GEC-1]: Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 36 für jede in [E.Info.GEC-1.SoftwareDocumentation] und [E.Info.GEC-1.HardwareDocumentation] dokumentierte Software und Hardware, bei denen öffentlich bekannte, ausnutzbare Schwachstellen bestehen.

[E.Just.DT.GEC-1]: Begründung für den gewählten Pfad durch den in [E.Info.DT.GEC-1] dokumentierten Entscheidungsbaum mit den folgenden Eigenschaften:

— die Begründung für die Entscheidung [DT.GEC-1.DN-1] basiert auf [E.Info.GEC-1.ListOfVulnerabilities]; und

— (wenn eine Entscheidung aus [DT.GEC-1.DN-2] zu „NICHT ANWENDBAR“ führt) basiert die Begründung für die Entscheidung [DT.GEC-1.DN-2] auf [E.Info.GEC-1.ListOfVulnerabilities] und [E.Info.GEC-1.ListOfVulnerabilities.Remediated]; und

— (wenn eine Entscheidung aus [DT.GEC-1.DN-3] zu „NICHT ANWENDBAR“ führt) basiert die Begründung für die Entscheidung [DT.GEC-1.DN-3] auf [E.Info.GEC-1.ListOfVulnerabilities.SpecificCondition]; und

— (wenn eine Entscheidung aus [DT.GEC-1.DN-4] zu „NICHT ANWENDBAR“ führt) basiert die Begründung für die Entscheidung [DT.GEC-1.DN-4] auf [E.Info.GEC-1.ListOfVulnerabilities.Mitgated]; und

— die Begründung für die Entscheidung [DT.GEC-1.DN-5] basiert auf [E.Info.GEC-1.ListOfVulnerabilities.Accepted].

#### 6.10.1.4.4 Konzeptuelle Beurteilung

##### 6.10.1.4.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob die in der Hardware und Software der geprüften Anlagen vorhandenen, öffentlich bekannten Hardware- und Software-Schwachstellen bei Werksvoreinstellung nicht in der Lage sind, Datenschutzwerte oder Sicherheitswerte zu beeinträchtigen, wenn sie wie nach GEC-1 erforderlich ausgenutzt werden.

##### 6.10.1.4.4.2 Voraussetzungen

Keine.

#### 6.10.1.4.4.3 Beurteilungseinheiten

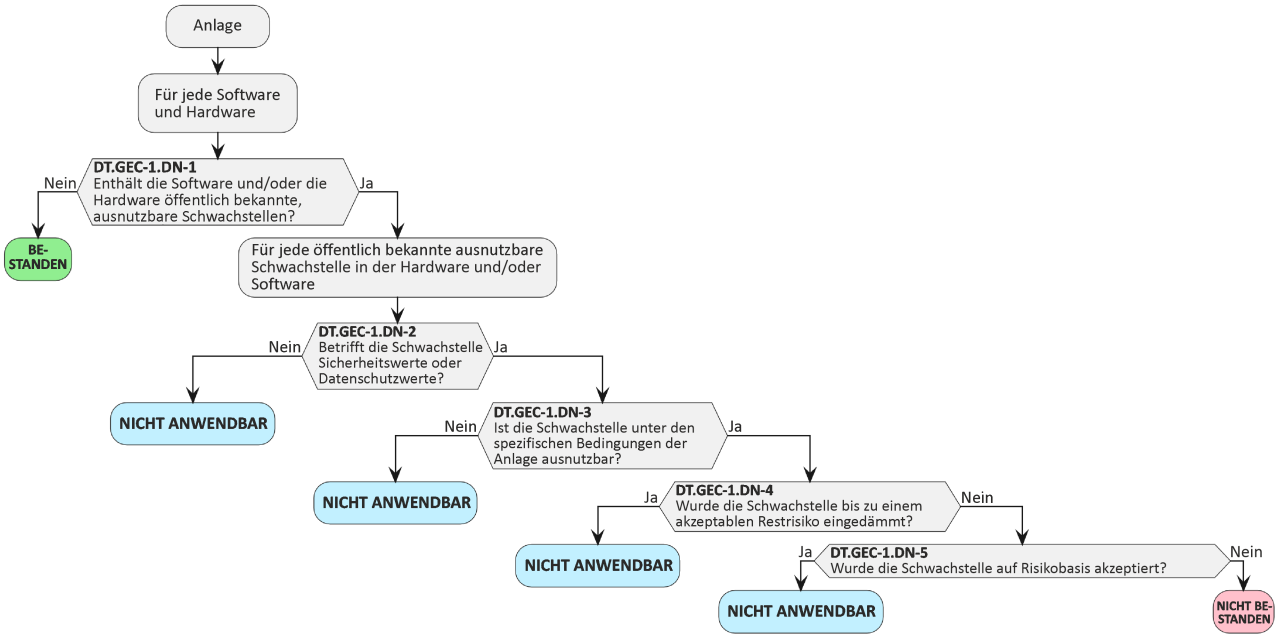



**Bild 36 — Entscheidungsbaum für Anforderung GEC-1**

Für jede in [E.Info.GEC-1.SoftwareDocumentation] dokumentierte Software und in [E.Info.GEC-1.HardwareDocumentation] dokumentierte Hardware ist zu prüfen, ob der Pfad durch den in [E.Info.DT.GEC-1] dokumentierten Entscheidungsbaum mit „NICHT ANWENDBAR“ oder „BESTANDEN“ endet.

Für jeden in [E.Info.DT.GEC-1] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.GEC-1] dokumentierte Begründung zu untersuchen.

#### 6.10.1.4.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— mindestens ein Pfad durch den in [E.Info.DT.GEC-1] dokumentierten Entscheidungsbaum mit „BESTANDEN“ endet; und

— kein Pfad durch den in [E.Info.DT.GEC-1] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; und

— die in [E.Just.DT.GEC-1] angegebenen Informationen korrekte Begründungen für alle Pfade durch den in [E.Info.DT.GEC-1] dokumentierten Entscheidungsbaum sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— ein Pfad durch den in [E.Info.DT.GEC-1] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; oder

— eine in [E.Just.DT.GEC-1] angegebene Begründung für einen Pfad durch den in [E.Info.DT.GEC-1] dokumentierten Entscheidungsbaum nicht korrekt ist oder fehlt.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

#### 6.10.1.4.5 Beurteilung der funktionalen Vollständigkeit

##### 6.10.1.4.5.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung des geprüften Geräts, um die Vollständigkeit der Dokumentation zu verifizieren, dass die im Gerät vorhandenen Schwachstellen, die Datenschutzwerte oder Sicherheitswerte betreffen, nur diejenigen sind, die in [E.Info.GEC-1.ListOfVulnerabilities] aufgeführt sind.

##### 6.10.1.4.5.2 Voraussetzungen

Die Anlage befindet sich im Betriebszustand.

Die Quelle, die für die Liste öffentlich bekannter, für die Beurteilung verwendeter ausnutzbarer Schwachstellen herangezogen wird, ist aktuell.

##### 6.10.1.4.5.3 Beurteilungseinheiten

Durch die Anwendung aktueller Bewertungsmethoden ist funktional zu beurteilen, ob es öffentlich bekannte Hardwareschwachstellen gibt, die die Sicherheitswerte und die Datenschutzwerte betreffen und die nicht in [E.Info.GEC-1.ListOfVulnerabilities] aufgeführt sind.

Durch die Anwendung aktueller Bewertungsmethoden ist funktional zu beurteilen, ob es öffentlich bekannte Softwareschwachstellen gibt, die die Sicherheitswerte und die Datenschutzwerte betreffen und die nicht in [E.Info.GEC-1.ListOfVulnerabilities] aufgeführt sind.

ANMERKUNG Es gibt verschiedene Software-Tools und Messgeräte, die automatisch nach Software- und Hardware-Schwachstellen suchen.

##### 6.10.1.4.5.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn alle gefundenen öffentlich bekannte Software- und Hardware-Schwachstellen, die die Sicherheitswerte und Datenschutzwerte betreffen, in [E.Info.GEC-1.ListOfVulnerabilities] dokumentiert sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn eine öffentlich bekannte Software- oder Hardware-Schwachstelle, die einen Sicherheitswert oder einen Datenschutzwert betrifft, nicht in [E.Info.GEC-1.ListOfVulnerabilities] dokumentiert ist.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

#### 6.10.1.4.6 Beurteilung der funktionalen Suffizienz

##### 6.10.1.4.6.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob die in den Anlagen vorhandenen Schwachstellen, die in [E.Info.GEC-1.ListOfVulnerabilities] aufgeführt sind, nicht in der Lage sind, Sicherheitswerte oder Datenschutzwerte zu beeinträchtigen, wenn sie ausgenutzt werden.

##### 6.10.1.4.6.2 Voraussetzungen

Die Anlage befindet sich im Betriebszustand.

Die Quelle, die für die Liste öffentlich bekannter, für die Beurteilung verwendeter ausnutzbarer Schwachstellen herangezogen wird, ist aktuell.

#### 6.10.1.4.6.3 Beurteilungseinheiten

Es ist funktional zu beurteilen, ob die in [E.Info.GEC-1.ListOfVulnerabilities] beschriebenen Maßnahmen implementiert sind, wobei auch die in [E.Info.GEC-1.ListOfVulnerabilities] definierten spezifischen Bedingungen für die Ausnutzbarkeit zu berücksichtigen sind, um sicherzustellen, dass die Schwachstellen nicht in der Lage sind, Sicherheitswerte und Datenschutzwerte zu beeinträchtigen, wenn sie ausgenutzt werden.

ANMERKUNG Für viele Schwachstellen gibt es Pentest-Tools, mit denen die Ausnutzbarkeit verifiziert werden kann.

#### 6.10.1.4.6.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn kein Nachweis vorliegt, dass Maßnahmen, die sicherstellen, dass Schwachstellen nicht in der Lage sind, Sicherheitswerte und Datenschutzwerte zu beeinträchtigen, wenn sie ausgenutzt werden, nicht wie in [E.Info.GEC-1.ListOfVulnerabilities] beschrieben implementiert wurden, wobei auch die in [E.Info.GEC-1.ListOfVulnerabilities] definierten spezifischen Bedingungen für die Ausnutzbarkeit berücksichtigt werden.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn ein Nachweis vorliegt, dass Maßnahmen, die sicherstellen, dass Schwachstellen nicht in der Lage sind, Sicherheitswerte und Datenschutzwerte zu beeinträchtigen, wenn sie ausgenutzt werden, nicht wie in [E.Info.GEC-1.ListOfVulnerabilities] beschrieben implementiert wurden, wobei auch die in [E.Info.GEC-1.ListOfVulnerabilities] definierten spezifischen Bedingungen für die Ausnutzbarkeit berücksichtigt werden.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

### 6.10.2 [GEC-2] Begrenzung der Offenlegung von Diensten über entsprechende Netzwerkschnittstellen

#### 6.10.2.1 Anforderung

Bei Werksvoreinstellung darf die Anlage nur Folgendes zugänglich machen:

— Netzwerkschnittstellen; und

— Dienste über Netzwerkschnittstellen

die Sicherheitswerte und Datenschutzwerte betreffen, die für die Anlage oder den grundlegenden Betrieb der Anlage erforderlich sind.

#### 6.10.2.2 Begründung

Zugängliche Dienste sind ein wichtiger Faktor zur Reduzierung des möglichen Risikos einer Kompromittierung von Anlagen, beispielsweise um das Netzwerk zu schädigen. Daher müssen die zugänglichen Dienste auf solche beschränkt werden, die für die Einrichtung der Anlage und für dessen Betrieb in der für die Nutzung vorgesehenen Betriebsumgebung erforderlich sind.

#### 6.10.2.3 Leitlinie

Die Gerätekonfiguration kann sich unterscheiden, abhängig vom Zweck der Anlage.

Allgemein muss zwischen zwei Gerätearten unterschieden werden:

— Mehrzweckgeräte, z. B. Smartphones, Laptops: Die von Mehrzweckgeräten bereitgestellten Dienste und deren Funktionalität sind nur bis zur Markteinführung der Anlage unter Kontrolle des Herstellers; und

— Anlagen mit einer kontrollierten, festgelegten Funktionalität, z. B. Sensoren, Router: Die bereitgestellten Dienste und die Anlagenfunktionalität sind in eine gerätespezifische Software eingebettet, die vom Hersteller bereitgestellt wird.

Bei Anlagen mit einer kontrollierten festen Funktionalität dürfen bei Werkeinstellung nur die Netzwerkschnittstellen oder Dienste (über Netzwerkschnittstellen) zugänglich sein, die für die Einrichtung oder Nutzung dieser Funktionalität erforderlich sind.

Ein Mehrzweckgerät hat keine spezifische Vorgabesgemäße Verwendung, sondern wird in der Regel vom Hersteller mit einer Reihe von vorinstallierten Anwendungen geliefert. Darüber hinaus bietet die Anlage bei Werkeinstellung ein betriebsfähiges System für die folgenden typischen Anwendungsfälle:

— Verwaltung/Steuerung der Hardware der Anlage,

— Nutzung der vorinstallierten Anwendungen,

— Installation weiterer Anwendungen,

— Installation von Softwareaktualisierungen.

Diese Anwendungsfälle definieren den zulässigen Anwendungsbereich für die zugänglichen Netzwerkschnittstellen und Dienste (über Netzwerkschnittstellen).

Die Beeinträchtigung von Sicherheitswerten bedeutet, dass eine Beeinträchtigung der Netzwerkschnittstelle oder des Dienstes (über Netzwerkschnittstellen) Auswirkungen auf die Sicherheit der Anlagen haben kann.

#### 6.10.2.4 Beurteilungskriterien

##### 6.10.2.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung GEC-2.

##### 6.10.2.4.2 Umsetzungskategorien

Nicht anwendbar.

##### 6.10.2.4.3 Erforderliche Informationen

[E.Info.GEC-2.NetworkInterface.Exposure]: Beschreibung jeder Netzwerkschnittstelle und jedes zugänglichen Dienstes (über Netzwerkschnittstellen) bei Werksvoreinstellung der Anlage, einschließlich der Information, ob sie für den grundlegenden Betrieb oder für die Einrichtung der Anlage erforderlich sind oder ob sie optional sind.

(wenn für die Anlage ein Einrichtungsprozess implementiert ist) [E.Info.GEC-2.Setup]: Dokumentation, wie die Anlage einzurichten ist.

[E.Info.GEC-2.SecurityAsset]: Beschreibung jedes Sicherheitswerts, der über Netzwerkschnittstellen zugänglich ist.

[E.Info.GEC-2.PrivacyAsset]: Beschreibung jedes Datenschutzwerts, der über Netzwerkschnittstellen zugänglich ist.

[E.Info.DT.GEC-2]: Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 37 für jede Netzwerkschnittstelle und jeden Dienst (über Netzwerkschnittstellen) wie in [E.Info.GEC-2.NetworkInterface.Exposure] dokumentiert.

[E.Just.DT.GEC-2]: Begründung für jeden gewählten Pfad durch den in [E.Info.DT.GEC-2] Bild 5 dokumentierten Entscheidungsbaum mit den folgenden Eigenschaften:

— (wenn eine Entscheidung aus [DT.GEC-2.DN-1] zu „NICHT ANWENDBAR“ führt) basiert die Begründung für die Entscheidung [DT.GEC-2.DN-1] auf [E.Info.GEC-2.NetworkInterface.Exposure]; und

— (wenn eine Entscheidung aus [DT.GEC-2.DN-2] zu „NICHT ANWENDBAR“ führt) basiert die Begründung für die Entscheidung [DT.GEC-2.DN-2] auf [E.Info.GEC-2.SecurityAsset] und [E.Info.GEC-2.PrivacyAsset]; und

— die Begründung für die Entscheidung [DT.GEC-2.DN-3] basiert auf [E.Info.GEC-2.NetworkInterface.Exposure].

#### 6.10.2.4.4 Konzeptuelle Beurteilung

##### 6.10.2.4.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob bei Werksvoreinstellung der Anlage die Offenlegung von Netzwerkschnittstellen und Diensten (über Netzwerkschnittstellen), die Sicherheitswerte oder Datenschutzwerte bei Werksvoreinstellung betreffen, die in [E.Info.GEC-2.NetworkInterface.Exposure] dokumentiert sind, auf diejenigen beschränkt ist, die für die Einrichtung der Anlage oder für den grundlegenden Betrieb der Anlage wie nach GEC-2 erforderlich sind.

##### 6.10.2.4.4.2 Voraussetzungen

Keine.

##### 6.10.2.4.4.3 Beurteilungseinheiten

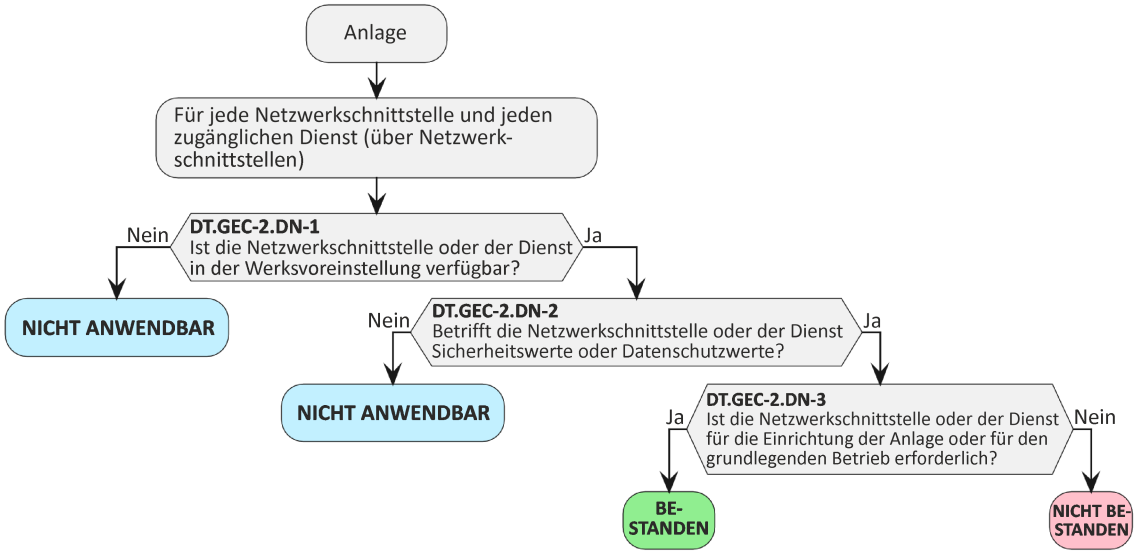



**Bild 37 — Entscheidungsbaum für Anforderung GEC-2**

Für jede in [E.Info.GEC-2.NetworkInterface.Exposure] dokumentierte Netzwerkschnittstelle und jeden offengelegten Dienst ist zu prüfen, ob der Pfad durch den in [E.Info.DT.GEC-2] dokumentierten Entscheidungsbaum mit „NICHT ANWENDBAR“ oder „BESTANDEN“ endet.

Für jeden in [E.Info.DT.GEC-2] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.GEC-2] dokumentierte Begründung zu untersuchen.

##### 6.10.2.4.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— mindestens ein Pfad durch den in [E.Info.DT.GEC-2] dokumentierten Entscheidungsbaum mit „BESTANDEN“ endet; und

— kein Pfad durch den in [E.Info.DT.GEC-2] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; und

— die in [E.Just.DT.GEC-2] angegebenen Informationen korrekte Begründungen für alle Pfade durch den in [E.Info.DT.GEC-2] dokumentierten Entscheidungsbaum sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— ein Pfad durch den in [E.Info.DT.GEC-2] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; oder

— eine in [E.Just.DT.GEC-2] angegebene Begründung für einen Pfad durch den in [E.Info.DT.GEC-2] dokumentierten Entscheidungsbaum nicht korrekt ist oder fehlt.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

#### 6.10.2.4.5 Beurteilung der funktionalen Vollständigkeit

##### 6.10.2.4.5.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob bei Werksvoreinstellung nur Netzwerkschnittstellen oder zugängliche für die Einrichtung oder den grundlegenden Betrieb des Gerätes erforderliche Dienste (über Netzwerkschnittstellen) offengelegt sind.

##### 6.10.2.4.5.2 Voraussetzungen

Die Anlage ist in Werksvoreinstellung, und es hat, falls verfügbar, bisher keine Einrichtung oder sonstige Konfiguration stattgefunden.

Physische Netzwerkverbindungen zur Prüfung der Offenlegung von Diensten über Netzwerkschnittstellen sind eingerichtet.

##### 6.10.2.4.5.3 Beurteilungseinheiten

Es ist funktional zu beurteilen, ob bei Werksvoreinstellung weitere Netzwerkschnittstellen oder (über Netzwerkschnittstellen) zugängliche Dienste vorhanden sind, die nicht in [E.Info.GEC-2.NetworkInterface.Exposure] aufgeführt sind, oder die nicht für die Einrichtung nach [E.Info.GEC-2.Setup] oder für den grundlegenden Betrieb der Anlage erforderlich sind.

ANMERKUNG Es gibt verschiedene Software-Tools und Messgeräte, die automatisch nach offengelegten Netzwerkschnittstellen oder Diensten suchen, die über eine Netzwerkschnittstelle zugänglich sind.

##### 6.10.2.4.5.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird zugewiesen, wenn bei Werksvoreinstellung jede erkannte Netzwerkschnittstelle oder jeder (über Netzwerkschnittstellen) erkannte Dienst offengelegt sind, in [E.Info.GEC-2.NetworkInterface.Exposure] aufgeführt und für die Einrichtung nach [E.Info.GEC-2.Setup] oder für den grundlegenden Betrieb der Anlage erforderlich sind.

Die Entscheidung NICHT BESTANDEN wird zugewiesen, wenn bei Werksvoreinstellung eine zugängliche Netzwerkschnittstelle oder ein (über Netzwerkschnittstellen) zugänglicher Dienste erkannt werden, die nicht in [E.Info.GEC-2.NetworkInterface.Exposure] aufgeführt sind, oder die nicht für die Einrichtung nach [E.Info.GEC-2.Setup] oder für den grundlegenden Betrieb der Anlage erforderlich sind.

Die Entscheidung NICHT ANWENDBAR wird anderweitig zugewiesen.

#### 6.10.2.4.6 Beurteilung der funktionalen Suffizienz

Nicht anwendbar.

### 6.10.3 [GEC-3] Konfiguration von optionalen Diensten und zugehörigen offengelegten Netzwerkschnittstellen

#### 6.10.3.1 Anforderung

Bei optionalen Netzwerkschnittstellen oder über Netzwerkwerkschnittstellen zugänglichen optionalen Diensten, von denen Sicherheitswerte oder Datenschutzwerte betroffen sind und die Teil der Werksvoreinstellung sind, muss es für einen autorisierten Benutzer möglich sein, die Netzwerkschnittstelle oder den Dienst zu aktivieren und zu deaktivieren.

#### 6.10.3.2 Begründung

Dies reduziert die Angriffsfläche in Bezug auf Netzwerkschnittstellen und darüber zugängliche Dienste.

#### 6.10.3.3 Leitlinie

Die Anlage verfügt für einen autorisierten Benutzer über die Funktionalität zur Konfiguration (Aktivierung/Deaktivierung) der offengelegten optionalen Dienste und der zugehörigen Netzwerkschnittstellen, die Teil der Werksvoreinstellung sind.

Die Konfiguration netzwerkbezogener Dienste sollte entsprechend Zugangssteuerungsmechanismus (ACM) und Authentisierungsmechanismus (AUM) geschützt sein.

#### 6.10.3.4 Beurteilungskriterien

#### 6.10.3.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung GEC-3.

#### 6.10.3.4.2 Umsetzungskategorien

Nicht anwendbar.

#### 6.10.3.4.3 Erforderliche Informationen

[E.Info.GEC-3.NetworkInterface.Exposure]: Beschreibung jeder Netzwerkschnittstelle und jedes zugänglichen Dienstes (über Netzwerkschnittstellen) bei Werksvoreinstellung der Anlage, einschließlich der Information, ob es für einen autorisierten Benutzer möglich ist, die Netzwerkschnittstelle oder den Dienst zu aktivieren oder zu deaktivieren.

[E.Info.GEC-3.SecurityAsset]: Beschreibung jedes Sicherheitswerts, der über Netzwerkschnittstellen zugänglich ist.

[E.Info.GEC-3.PrivacyAsset]: Beschreibung jedes Datenschutzwerts, der über Netzwerkschnittstellen zugänglich ist.

[E.Info.DT.GEC-3]: Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 38 für jede in [E.Info.GEC-3.NetworkInterface.Exposure] dokumentierte Netzwerkschnittstelle und jeden (über Netzwerkschnittstellen) zugänglichen optionalen Dienst.

[E.Just.DT.GEC-3]: Begründung für jeden gewählten Pfad durch den in [E.Info.DT.GEC-3] dokumentierten Entscheidungsbaum mit den folgenden Eigenschaften:

— (wenn eine Entscheidung aus [DT.GEC-3.DN-1] zu „NICHT ANWENDBAR“ führt) basiert die Begründung für die Entscheidung [DT.GEC-3.DN-1] auf [E.Info.GEC-3.SecurityAsset] und [E.Info.GEC-3.NetworkAsset]; und

— die Begründung für die Entscheidung [DT.GEC-3.DN-2] basiert auf [E.Info.GEC-3.NetworkInterface.Exposure].

#### 6.10.3.4.4 Konzeptuelle Beurteilung

##### 6.10.3.4.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob jede optionale Netzwerkschnittstelle und jeder (über Netzwerkschnittstellen) zugängliche Dienste, der Teil der Werksvoreinstellung der Anlage ist, konfigurierbar ist, mindestens mit der Option, den Dienst wie nach GEC-3 erforderlich zu aktivieren und zu deaktivieren.

##### 6.10.3.4.4.2 Beurteilungseinheiten

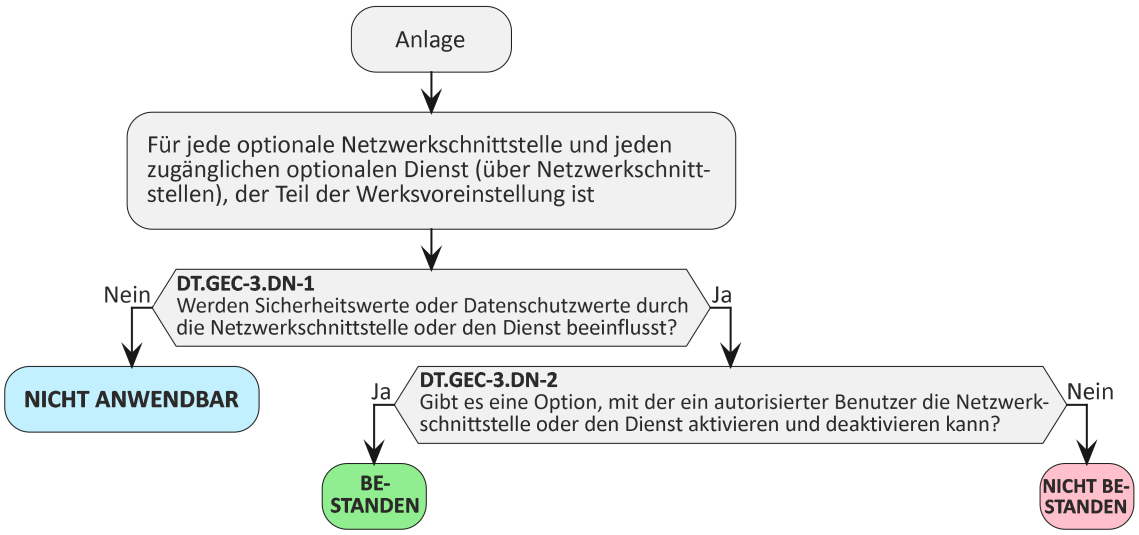



**Bild 38 — Entscheidungsbaum für Anforderung GEC-3**

Für jede optionale in [E.Info.GEC-3.NetworkInterface.Exposure] dokumentierte Netzwerkschnittstelle und jeden(über Netzwerkschnittstellen) offengelegten Dienst, der Teil der Werksvoreinstellung ist, ist zu prüfen, ob der Pfad durch den in [E.Info.DT.GEC-3] dokumentierten Entscheidungsbaum mit „NICHT ANWENDBAR“ oder „BESTANDEN“ endet.

Für jeden in [E.Info.DT.GEC-3] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.GEC-3] dokumentierte Begründung zu untersuchen.

##### 6.10.3.4.4.3 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— mindestens ein Pfad durch den in [E.Info.DT.GEC-3] dokumentierten Entscheidungsbaum mit „BESTANDEN“ endet; und

— kein Pfad durch den in [E.Info.DT.GEC-3] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; und

— die in [E.Just.DT.GEC-3] angegebenen Informationen korrekte Begründungen für alle Pfade durch den in [E.Info.DT.GEC-3] dokumentierten Entscheidungsbaum sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— ein Pfad durch den in [E.Info.DT.GEC-3] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN" endet; oder

— eine in [E.Just.DT.GEC-3] angegebene Begründung für einen Pfad durch den in [E.Info.DT.GEC-3] dokumentierten Entscheidungsbaum nicht korrekt ist oder fehlt.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

#### 6.10.3.4.5 Beurteilung der funktionalen Vollständigkeit

##### 6.10.3.4.5.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob alle optionalen Netzwerkschnittstellen und (über Netzwerkschnittstellen) offengelegten optionalen Dienste, die Teil der Werksvoreinstellung sind, mindestens mit der Option konfigurierbar sind, den Dienst zu aktivieren und zu deaktivieren. Hierfür muss die Vollständigkeit der Dokumentation untersucht werden.

##### 6.10.3.4.5.2 Voraussetzungen

Die Anlage ist im Betriebszustand und die Einrichtung, falls verfügbar, ist abgeschlossen.

Die notwendigen Berechtigungen sind für die Konfiguration der Einstellungen der optionalen Netzwerkschnittstellen oder optionalen (über Netzwerkschnittstellen zugänglichen) Dienste verfügbar.

##### 6.10.3.4.5.3 Beurteilungseinheiten

Es ist funktional zu beurteilen, ob optionale Netzwerkschnittstellen oder (über Netzwerkschnittstellen) offengelegte optionale Dienste vorhanden sind, die nicht in [E.Info.GEC-3.NetworkInterface.Exposure] aufgeführt sind.

##### 6.10.3.4.5.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn keine optionale Netzwerkschnittstellen oder (über Netzwerkschnittstellen) zugängliche optionale Dienste vorliegen, die nicht in [E.Info.GEC-3.NetworkInterface.Exposure] aufgeführt sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn optionale Netzwerkschnittstellen oder optionale (über Netzwerkschnittstellen) offengelegte Dienste vorhanden sind, die nicht in [E.Info.GEC-3.NetworkInterface.Exposure] aufgeführt sind.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

#### 6.10.3.4.6 Beurteilung der funktionalen Suffizienz

##### 6.10.3.4.6.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob alle optionalen Netzwerkschnittstellen und (über Netzwerkschnittstellen) offengelegte optionale Dienste, die Teil der Werksvoreinstellung sind, mindestens mit der Option konfigurierbar sind, den Dienst zu aktivieren und zu deaktivieren.

##### 6.10.3.4.6.2 Voraussetzungen

Die Anlage ist im Betriebszustand und die Einrichtung, falls verfügbar, ist abgeschlossen.

Die notwendigen Berechtigungen sind für die Konfiguration der Einstellungen der optionalen Netzwerkschnittstellen oder (über Netzwerkschnittstellen) optionalen Dienste verfügbar.

#### 6.10.3.4.6.3 Beurteilungseinheiten

Für jede optionale Netzwerkschnittstelle und jeden (über Netzwerkschnittstellen) zugänglichen optionalen Dienst, der Teil der Werksvoreinstellung ist:

— Es ist funktional zu beurteilen, ob die optionalen Netzwerkschnittstellen und (über Netzwerkschnittstellen) offengelegten optionalen Dienste vorhanden sind, die Teil der Werksvoreinstellung und in [E.Info.GEC-3.NetworkInterface.Exposure] dokumentiert sind, konfigurierbar sind; und

— es ist funktional zu beurteilen, ob es möglich ist, mindestens den Status der optionalen Netzwerkschnittstellen und der (über Netzwerkschnittstellen) offengelegten optionalen Dienste auf aktiviert und deaktiviert zu ändern; und

— es ist funktional zu beurteilen, ob die Konfiguration der Einstellungen der optionalen Netzwerkschnittstellen und der (über Netzwerkschnittstellen) offengelegten optionalen Dienste, die Teil der Werksvoreinstellung und in [E.Info.GEC-3.NetworkInterface.Exposure] aufgeführt sind, nur durch autorisierte Benutzer möglich ist.

#### 6.10.3.4.6.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn ein Nachweis vorliegt, dass alle optionalen Netzwerkschnittstellen oder (über Netzwerkschnittstellen) offengelegten optionalen Dienste mindestens mit der Option konfigurierbar sind, die Netzwerkschnittstelle oder den Dienst zu aktivieren und zu deaktivieren, oder dass die Änderung des Status der optionalen Netzwerkschnittstellen oder (über Netzwerkschnittstellen) offengelegten optionalen Dienste auf aktiviert oder deaktiviert nur durch einen autorisierten Benutzer möglich ist, wie in [E.Info.GEC-3.NetworkInterface.Exposure] beschrieben.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn kein Nachweis vorliegt, dass alle optionalen Netzwerkschnittstellen oder (über Netzwerkschnittstelle) offengelegten optionalen Dienste mindestens mit der Option konfigurierbar sind, die Netzwerkschnittstelle oder den Dienst zu aktivieren und zu deaktivieren, oder dass die Änderung des Status der optionalen Netzwerkschnittstelle oder der (über eine Netzwerkschnittstelle) offengelegten optionalen Dienste auf aktiviert oder deaktiviert nur durch einen autorisierten Benutzer möglich ist, wie in [E.Info.GEC-3.NetworkInterface.Exposure] beschrieben.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

### 6.10.4 [GEC-4] Dokumentation von zugänglichen Netzwerkschnittstellen und über Netzwerkschnittstellen zugänglichen Diensten

#### 6.10.4.1 Anforderung

Die Benutzerdokumentation der Anlage muss eine Beschreibung enthalten von

— allen zugänglichen Netzwerkschnittstellen; und

— allen über Netzwerkschnittstellen zugänglichen Diensten,

die als Teil der Werksvoreinstellung bereitgestellt werden.

#### 6.10.4.2 Begründung

Die Anlage selbst und das umgebende Netzwerk müssen ordnungsgemäß konfiguriert sein, um die Funktionalität der Anlage sicherzustellen und die Netzwerksicherheit zu unterstützen. Daher ist es wichtig, Benutzerinformationen zu den zugänglichen Netzwerkschnittstellen und (über Netzwerkschnittstellen) zugänglichen Diensten sowie die für die Nutzung vorgesehene Betriebsumgebung bereitzustellen.

#### 6.10.4.3 Leitlinie

Alle Netzwerkschnittstellen und (über Netzwerkschnittstellen) zugänglichen Dienste bei Werksvoreinstellung müssen in der Dokumentation aufgeführt sein. Für jeden Dienst könnte auch sein Zweck angegeben werden. Ziel ist es, dem Benutzer Transparenz über die Konnektivität der Anlagen zu verschaffen. Darüber hinaus dient die Dokumentation der Beurteilung, ob durch die Inbetriebnahme der Anlagen potentielle Angriffsflächen für die vorgesehene Nutzungsumgebung des Benutzers entstehen.

#### 6.10.4.4 Beurteilungskriterien

##### 6.10.4.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung GEC-4.

##### 6.10.4.4.2 Umsetzungskategorien

Nicht anwendbar.

##### 6.10.4.4.3 Erforderliche Informationen

[E.Info.GEC-4.UserDoc.NetworkInterface.Exposure]: Benutzerdokumentation jeder zugänglichen Netzwerkschnittstelle und jedes der in Werksvoreinstellung der Anlage (über Netzwerkschnittstellen) zugänglichen Dienstes.

[E.Info.GEC-4.NetworkInterface.Exposure]: Beschreibung jeder zugänglichen Netzwerkschnittstelle und des in Werksvoreinstellung der Anlage (über Netzwerkschnittstellen) zugänglichen Dienstes.

[E.Info.DT.GEC-4]: Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 39 für jede zugängliche Netzwerkschnittstelle und jeden (über Netzwerkschnittstellen) zugänglichen Dienst wie in [E.Info.GEC-4.NetworkInterface.Exposure] dokumentiert.

[E.Just.DT.GEC-4]: Begründung für jeden gewählten Pfad durch den in [E.Info.DT.GEC-4] dokumentierten Entscheidungsbaum mit den folgenden Eigenschaften:

— (wenn eine Entscheidung aus [DT.GEC-4.DN-1] zu „NICHT ANWENDBAR“ führt) basiert die Begründung für die Entscheidung [DT.GEC-4.DN-1] auf [E.Info.GEC-4.NetworkInterface.Exposure]; und

— die Begründung für die Entscheidung [DT.GEC-4.DN-2] basiert auf [E.Info.GEC-4.UserDoc.NetworkInterface.Exposure].

##### 6.10.4.4.4 Konzeptuelle Beurteilung

###### 6.10.4.4.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob alle Netzwerkschnittstellen und Dienste, die über Netzwerkschnittstellen zugänglich sind und die als Teil der Werksvoreinstellung bereitgestellt werden, in der Benutzerdokumentation, wie nach GEC-4 erforderlich, beschrieben sind.

###### 6.10.4.4.4.2 Voraussetzungen

Keine.

#### 6.10.4.4.4.3 Beurteilungseinheiten

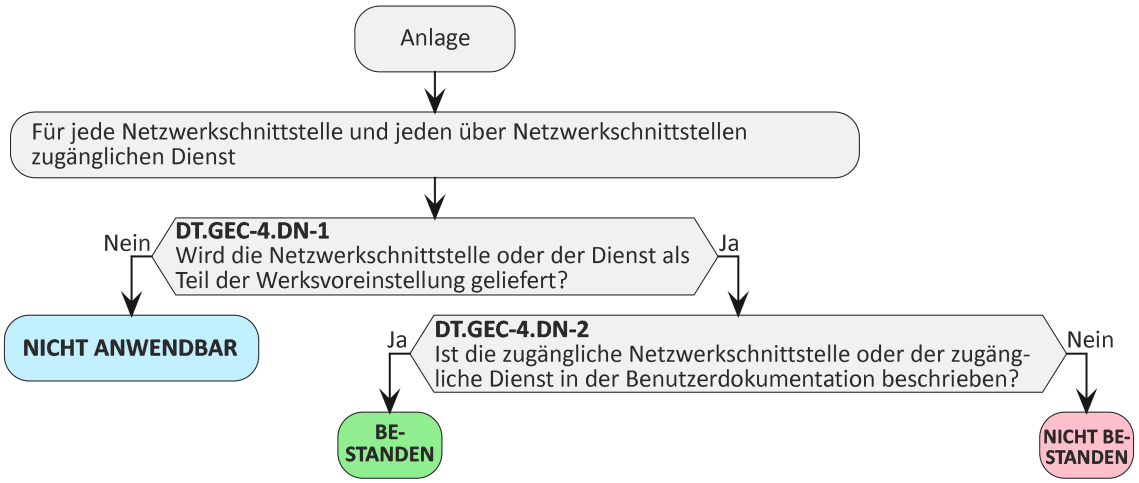



**Bild 39 — Entscheidungsbaum für Anforderung GEC-4**

Für jede Netzwerkschnittstelle und jeden offengelegten Dienst (über Netzwerkschnittstellen) in [E.Info.GEC-4.NetworkInterface.Exposure] ist zu prüfen, ob der Pfad durch den in [E.Info.DT.GEC-4] dokumentierten Entscheidungsbaum mit „NICHT ANWENDBAR“ oder „BESTANDEN“ endet.

Für jeden in [E.Info.DT.GEC-4] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.GEC-4] dokumentierte Begründung zu untersuchen.

#### 6.10.4.4.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— mindestens ein Pfad durch den in [E.Info.DT.GEC-4] dokumentierten Entscheidungsbaum mit „BESTANDEN“ endet; und

— kein Pfad durch den in [E.Info.DT.GEC-4] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; und

— die in [E.Just.DT.GEC-4] angegebenen Informationen korrekte Begründungen für alle Pfade durch den in [E.Info.DT.GEC-4] dokumentierten Entscheidungsbaum sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— ein Pfad durch den in [E.Info.DT.GEC-4] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; oder

— eine in [E.Just.DT.GEC-4] angegebene Begründung für einen Pfad durch den in [E.Info.DT.GEC-4] dokumentierten Entscheidungsbaum nicht korrekt ist oder fehlt.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

#### 6.10.4.4.5 Beurteilung der funktionalen Vollständigkeit

##### 6.10.4.4.5.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob die Benutzerdokumentation jede Netzwerkschnittstelle und jeden (über Netzwerkschnittstellen) offengelegten Dienst beschreibt, die als Teil der Werksvoreinstellung bereitgestellt werden.

##### 6.10.4.4.5.2 Voraussetzungen

Die Anlage befindet sich in Werksvoreinstellung.

Netzwerkverbindungen zur Prüfung der Offenlegung von Netzwerkschnittstellen und Diensten (über Netzwerkschnittstellen) sind eingerichtet.

##### 6.10.4.4.5.3 Beurteilungseinheit

Es ist zu beurteilen, ob die Dokumentation von Netzwerkschnittstellen und (über Netzwerkschnittstellen) zugänglichen Diensten vollständig ist:

— es ist funktional zu beurteilen, ob weitere Netzwerkschnittstellen, die in der Werksvoreinstellung offengelegt sind, vorhanden sind, die nicht in [E.Info.GEC-4.UserDoc.NetworkInterface.Exposure] dokumentiert sind; und

— es ist funktional zu beurteilen, ob es weitere (über Netzwerkschnittstellen) offengelegte Dienste gibt, die nicht in [E.Info.GEC-4.UserDoc.NetworkInterface.Exposure] dokumentiert sind.

ANMERKUNG Offengelegte Netzwerkschnittstellen und Dienste können mit Netzwerk-Scanning-Tools und Dienst-Scanning-Tools gefunden werden.

##### 6.10.4.4.5.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn alle gefundenen Netzwerkschnittstellen oder (über Netzwerkschnittstellen) zugängliche Dienste in der Werksvoreinstellung vorliegen, die in [E.Info.GEC-4.NetworkInterface.Exposure] dokumentiert sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn eine Netzwerkschnittstelle oder ein (über Netzwerkschnittstellen) offengelegter Dienst in Werksvoreinstellung gefunden wird, der nicht in [E.Info.GEC-4.NetworkInterface.Exposure] dokumentiert ist.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

#### 6.10.4.4.6 Beurteilung der funktionalen Suffizienz

Keine.

### 6.10.5 [GEC-5] Keine unnötigen externen Schnittstellen

#### 6.10.5.1 Anforderung

Die Anlage darf nur dann physische externe Schnittstellen aufweisen, wenn diese für die vorgesehene Funktionalität notwendig sind.

#### 6.10.5.2 Begründung

Physische externe Kommunikationsschnittstellen müssen so gering wie möglich gehalten werden, um die mögliche Angriffsfläche zu minimieren.

#### 6.10.5.3 Leitlinie

Falls eine unnötige physische externe Schnittstelle physisch durch die für die Nutzung vorgesehene Betriebsumgebung geschützt wird, gilt diese externe Schnittstelle als nicht vom Gerät offengelegt. Deaktivierte oder blockierte externe Schnittstellen gelten ebenfalls als nicht vom Gerät offengelegt.

Physische externe Geräteschnittstellen können externe Schnittstellen einschließen, die Vorgabesgemäß für die interne Systemkommunikation sowie Benutzungsschnittstellen und Maschinenschnittstellen verwendet werden.

Die vorgesehene Funktionalität könnte mehrere Anwendungsfälle abdecken, und die offengelegten physischen externen Schnittstellen müssen einem Zweck in mindestens einem der Anwendungsfälle dienen.

#### 6.10.5.4 Beurteilungskriterien

##### 6.10.5.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung GEC-5.

##### 6.10.5.4.2 Umsetzungskategorien

Nicht anwendbar.

##### 6.10.5.4.3 Erforderliche Informationen

[E.Info.GEC-5.PhysicalExternalInterface]: Beschreibung jeder physischen externen Schnittstelle, einschließlich:

— [E.Info.GEC-5.PhysicalExternalInterface.Purpose]: des Zwecks der Schnittstelle; und

— [E.Info.SCM-1.PhysicalExternalInterface.Type]: Beschreibung des Schnittstellentyps (z. B. USB-C).

[E.Info.GEC-5.IntFunc]: Beschreibung der vorgesehenen Funktionalität der Anlage.

[E.Info.DT.GEC-5]: Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 40 für jede in [E.Info.GEC-5.PhysicalExternalInterface] dokumentierte physische externe Schnittstelle.

[E.Just.DT.GEC-5]: Begründung für den gewählten Pfad durch den in [E.Info.DT.GEC-5] dokumentierten Entscheidungsbaum mit der folgenden Eigenschaft:

— die Begründung für die Entscheidung [DT.GEC-5.DN-1] basiert auf [E.Info.GEC-5.PhysicalExternalInterface].

##### 6.10.5.4.4 Konzeptuelle Beurteilung

###### 6.10.5.4.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob jede Offenlegung physischer externer Schnittstellen auf solche beschränkt ist, die für die vorgesehene Funktionalität wie nach GEC-5 erforderlich notwendig sind.

###### 6.10.5.4.4.2 Voraussetzungen

Keine.

#### 6.10.5.4.4.3 Beurteilungseinheiten

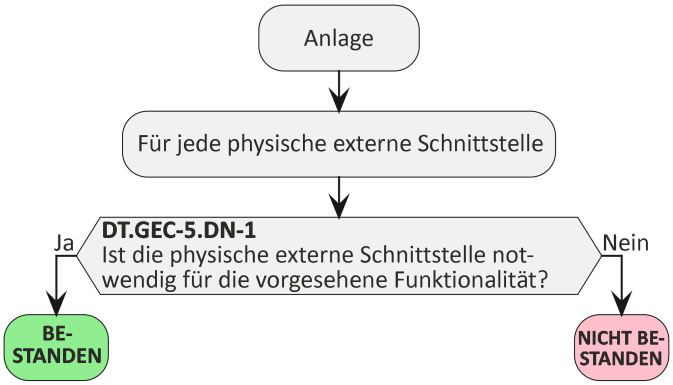



**Bild 40 — Entscheidungsbaum für Anforderung GEC-5**

Für jede in [E.Info.GEC-5.PhysicalExternalInterface] dokumentierte physische externe Schnittstelle ist zu prüfen, ob der Pfad durch den in [E.Info.DT.GEC-5] dokumentierten Entscheidungsbaum mit „BESTANDEN“ endet.

Für jeden in [E.Info.DT.GEC-5] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.GEC-5] dokumentierte Begründung zu untersuchen.

#### 6.10.5.4.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— alle Pfade durch den in [E.Info.DT.GEC-5] dokumentierten Entscheidungsbaum mit „BESTANDEN“ enden; und

— die in [E.Just.DT.GEC-5] angegebenen Informationen korrekte Begründungen für alle Pfade durch den in [E.Info.DT.GEC-5] dokumentierten Entscheidungsbaum sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— ein Pfad durch den in [E.Info.DT.GEC-5] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; oder

— eine in [E.Just.DT.GEC-5] angegebene Begründung für einen Pfad durch den in [E.Info.DT.GEC-5] dokumentierten Entscheidungsbaum nicht korrekt ist oder fehlt.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

### 6.10.5.4.5 Beurteilung der funktionalen Vollständigkeit

#### 6.10.5.4.5.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob nur physische externe Schnittstellen offengelegt werden, die für die vorgesehene Funktionalität, wie in [E.Info.GEC-5.PhysicalExternalInterface] dokumentiert, erforderlich sind.

#### 6.10.5.4.5.2 Voraussetzungen

Die Anlage ist betriebsbereit.

#### 6.10.5.4.5.3 Beurteilungseinheiten

Versuch der Aufdeckung der gesamten, durch die Anlage offengelegten physischen externen Schnittstellen, auch wenn die entsprechende Funktion nicht aktiviert oder in [E.Info.GEC-5.PhysicalExternalInterface] dokumentiert ist:

— Untersuchung der Anlagendokumentation wie Gestaltungsdokumentation, Dokumentation von Anwendungsfällen und Benutzerhandbuch; und

— Untersuchung der Anlage, welche physischen externen Schnittstellen an der Anlage vorhanden sind, wie Mikrofone, Bildschirme, Tasten oder Steckplätze für Erweiterungskarten.

Für jede aufgedeckte physische externe Schnittstelle ist bei der Untersuchung der Dokumentation und auch bei der Untersuchung der Anlagen die Dokumentation in [E.Info.GEC-5.PhysicalExternalInterface] zu beurteilen.

#### 6.10.5.4.5.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn alle gefundenen physischen externen Schnittstellen in [E.Info.GEC-5.PhysicalExternalInterface] dokumentiert sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn eine physische externe Schnittstelle gefunden wird, die nicht in [E.Info.GEC-5.PhysicalExternalInterface] dokumentiert ist.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

#### 6.10.5.4.6 Beurteilung der funktionalen Suffizienz

Nicht anwendbar.

### 6.10.6 [GEC-6] Eingabevalidierung

#### 6.10.6.1 Anforderung

Die Anlage muss über externe Schnittstellen empfangene Eingaben validieren, wenn diese Eingaben potentielle Auswirkungen auf Sicherheitswerte und/oder Datenschutzwerte haben.

#### 6.10.6.2 Begründung

Die Anlage muss alle Eingaben validieren, die potentielle Auswirkungen auf Sicherheitswerte oder Datenschutzwerte haben, um potentiellen Missbrauch, Korruption oder unbefugte Extraktion von Daten über Sicherheitswerte und Datenschutzwerte zu verhindern.

Die Eingabevalidierung ist notwendig, um beispielsweise die Syntax, die Länge und den Inhalt sämtlicher Eingabedaten zu validieren, die als erwartete Eingaben bereitgestellt werden und die Eigenschaften aufweisen, die für die korrekte Bearbeitung der Daten erforderlich sind.

Die unzureichende Eingabevalidierung wird als einer der häufigsten und gefährlichsten Software-Schwachpunkte angesehen, der auch zu einigen anderen Softwareschwächen beiträgt, wie beispielsweise zu Schreibvorgängen außerhalb des zulässigen Bereichs und zu einer unzureichenden Neutralisierung; dies kann zu verschiedenen Injection-Schwachstellen führen (z. B. SQL-Injection, OS-Command-Injection und Path Traversal).

Besonders Daten aus potentiell nicht vertrauenswürdigen Quellen, wie beispielsweise alle über Netzwerkschnittstellen empfangenen Eingaben, müssen einer Eingabevalidierung unterzogen werden, bei der die Eingaben sowohl bezüglich Syntax als auch bezüglich korrekter Semantik geprüft werden. Diese Prüfungen sollten so früh wie möglich bei der Verarbeitung von Eingaben durchgeführt werden, um die Verbreitung von ungültigen und möglicherweise sogar böswilligen Eingaben zu verhindern.

#### 6.10.6.3 Leitlinie

Eine unzureichende Eingabevalidierung ist eine der Hauptursachen für viele Sicherheitsschwachstellen; die Eingabe kann nur erfolgreich verarbeitet werden, wenn durch syntaktische und semantische Prüfung sowohl der Rohdaten als auch der Metadaten festgestellt wurde, dass die Eingabe gültig ist.

Bei der Syntaxvalidierung wird geprüft, dass die Eingabe die richtige Struktur aufweist, beispielsweise durch Prüfung:

— des Formats einer Datumseingabe (z. B. TT-MM-JJJJ oder MM-TT-JJJJ);

— der Verwendung eines Dezimalpunkts oder -kommas bei numerischen Eingaben;

— der Länge der Eingabe;

— der richtigen Header und Strukturen von unterschiedlichen Dateitypen (z. B. Validierung einer .ZIP-, .BMP- oder .JPEG-Dateistruktur);

— einer gültigen json-, xml- oder html-Datei.

Bei der Semantikvalidierung wird geprüft, ob die Eingabe mit den richtigen Werten erfolgt, beispielsweise:

— ob ein Wert außerhalb des erwarteten Bereichs liegt (z. B. eine Zahl, die zu klein oder zu groß ist, ein Geburtsdatum in der Zukunft);

— ob Sonderzeichen enthalten sind, die bei Texteingaben nicht zulässig sind, z. B. spezielle Escape-Zeichen, die bei SQL-Injection verwendet werden;

— ob fehlerhafte Datengrößen und Offset-Werte in einer Struktur vorhanden sind (eine fehlerhafte Größe könnte zu einem Pufferüberlauf führen, wenn Daten ohne Prüfung kopiert werden, oder ein negativer Offset könnte fehlerhafte Daten aus dem Stack kopieren);

— „Inclusive Listing“ (auch bekannt als „Allow Listing“) ist eine Methode, die nur definierte Eingaben (z. B. bestimmte Werte oder Ausdrücke) zulässt, alles andere wird als Eingabe zurückgewiesen.

Die Verwendung von Parsern und/oder regulären Ausdrücken sind Methoden zur Validierung beispielsweise von Texteingaben. Ein Entwickler könnte auch andere Verfahren wie Filterung und Codierung in Betracht ziehen, um sicherzustellen, dass eine Eingabe erfolgreich verarbeitet werden kann.

Weitere zu berücksichtigende Leitlinien:

— Common Weakness Enumeration: Improper Input Validation (CWE-20), Improper Encoding or Escaping of Output (CWE-116), Improper Neutralization of Special Elements (CWE-138) und Improper Filtering of Special Elements (CWE-790); https://cwe.mitre.org/data/index.html

— Open Web Application Security Project (OWASP) Input Validation Cheat Sheet – https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html

— IEC EN 62443-4-2 [2] CR 3.5 (Input validation) und

— ETSI EN 303 645 [6] 5.13 (Validate input data).

#### 6.10.6.4 Beurteilungskriterien

##### 6.10.6.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung GEC-6.

#### 6.10.6.4.2 Umsetzungskategorien

Nicht anwendbar.

#### 6.10.6.4.3 Erforderliche Informationen

[E.Info.GEC-6.ExternalInterface]: Beschreibung jeder externen Schnittstelle, einschließlich:

— [E.Info.GEC-6.ExternalInterface.Capabilities]: Beschreibung aller verwendeten APIs, Protokolle, Eingabedatentypen, Dateiformaten; und

— [E.Info.GEC-6.ExternalInterface.Validation]: Beschreibung, wie die Eingabe beispielsweise durch Überprüfung der syntaktischen und semantischen Korrektheit validiert wird.

[E.Info.GEC-6.SecurityAsset]: Beschreibung jedes Sicherheitswerts, der über externe Schnittstellen potentiell betroffen ist.

[E.Info.GEC-6.PrivacyAsset]: Beschreibung jedes Datenschutzwerts, der über externe Schnittstellen potentiell betroffen ist.

[E.Info.DT.GEC-6]: Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 41 für jede der in [E.Info.GEC-6.ExternalInterface] dokumentierten externen Schnittstellen.

[E.Just.DT.GEC-6]: Begründung für den gewählten Pfad durch den in [E.Info.DT.GEC-6] dokumentierten Entscheidungsbaum mit den folgenden Eigenschaften:

— (wenn eine Entscheidung aus [DT.GEC-6.DN-1] zu „NICHT ANWENDBAR“ führt) basiert die Begründung für die Entscheidung [DT.GEC-6.DN-1] auf [E.Info.GEC-6.ExternalInterface] und [E.Info.GEC-6.ExternalInterface.Capabilities]; und

— die Begründung für die Entscheidung [DT.GEC-6.DN-2] basiert auf [E.Info.GEC-6.ExternalInterface], [E.Info.GEC-6.ExternalInterface.Validation] und [E.Info.GEC-6.ExternalInterface.Capabilities].

#### 6.10.6.4.4 Konzeptuelle Beurteilung

##### 6.10.6.4.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob die Eingabevalidierungsfunktionalität der Anlage für die externen Schnittstellen angewandt wird und einen angemessenen Schutz von Sicherheitswerten und/oder Datenschutzwerten gegen häufige Angriffe unter Berücksichtigung der vorgesehenen Funktionalität der Anlage wie nach GEC-6 erforderlich bietet.

##### 6.10.6.4.4.2 Voraussetzungen

Keine.

#### 6.10.6.4.4.3 Beurteilungseinheiten

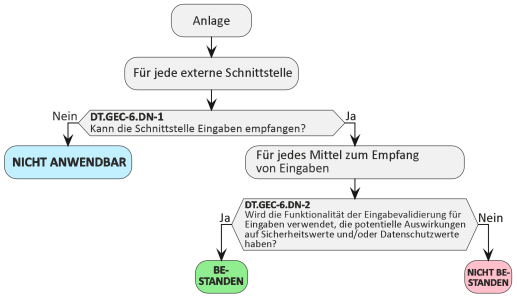



**Bild 41 — Entscheidungsbaum für Anforderung GEC-6**

Für jede in [E.Info.GEC-6.ExternalInterface] dokumentierte externe Schnittstelle ist zu prüfen, ob der Pfad durch den in [E.Doc.DT.GEC-6] dokumentierten Entscheidungsbaum mit „BESTANDEN“ oder „NICHT ANWENDBAR“ endet.

Für jeden in [E.Info.DT.GEC-6] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.GEC-6] dokumentierte Begründung zu untersuchen.

#### 6.10.6.4.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— mindestens ein Pfad durch den in [E.Info.DT.GEC-6] dokumentierten Entscheidungsbaum mit „BESTANDEN“ endet; und

— kein Pfad durch den in [E.Info.DT.GEC-6] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; und

— die in [E.Just.DT.GEC-6] angegebenen Informationen korrekte Begründungen für alle Pfade durch den in [E.Info.DT.GEC-6] dokumentierten Entscheidungsbaum sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— ein Pfad durch den in [E.Info.DT.GEC-6] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; oder

— eine in [E.Just.DT.GEC-6] angegebene Begründung für einen Pfad durch den in [E.Info.DT.GEC-6] dokumentierten Entscheidungsbaum nicht korrekt ist oder fehlt.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

### 6.10.6.4.5 Beurteilung der funktionalen Vollständigkeit

#### 6.10.6.4.5.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung der externen Schnittstellen der Anlage und der zugehörigen Eingabemechanismen hinsichtlich der Vollständigkeit der Dokumentation.

#### 6.10.6.4.5.2 Voraussetzungen

Die Anlage befindet sich im Betriebszustand, und alle externen Schnittstellen, die Teil der Vorgabengemäßen Verwendung sind, sind entweder aktiviert oder so konfiguriert, dass sie aktiviert werden können, so dass alle externen Schnittstellen geprüft werden können.

Wenn für den Zugang zu einer externen Schnittstelle eine Authentisierung erforderlich ist, wird ein Mittel bereitgestellt, um die Schnittstelle prüfen zu können.

#### 6.10.6.4.5.3 Beurteilungseinheiten

Es ist funktional zu beurteilen, ob es Eingabemethoden gibt, die nicht in [E.Info.GEC-6.ExternalInterface] dokumentiert sind durch:

— die funktionale Beurteilung des Datenverkehrs von Netzwerkschnittstellen, um Eingabemethoden aufzudecken, z. B. über Netzwerkanalysetools; die Angaben in [E.Info.GEC-6.ExternalInterface] dienen als Leitfaden; und

— die funktionale Beurteilung von Anlagen, um Eingabemethoden für externe Schnittstellen, die keine Netzwerkschnittstellen sind, durch Sichtprüfung, Benutzerhandbuch und Gestaltungsdokumentation aufzudecken; und

— nach der Beschreibung in [E.Info.GEC-6.ExternalInterface.Capabilities], um die zugehörigen Eingabemethoden auszulösen, z. B. durch Generierung der beschriebenen Nachrichten (z. B. über ein Webinterface oder generische Tools zur Nachrichtengenerierung oder Fuzzing-Tools).

#### 6.10.6.4.5.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn alle gefundenen externen Schnittstellen in [E.Info.GEC-6.ExternalInterface] dokumentiert sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn eine externe Schnittstelle gefunden wird, die nicht in [E.Info.GEC-6.ExternalInterface] dokumentiert ist.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

### 6.10.6.4.6 Beurteilung der funktionalen Suffizienz

#### 6.10.6.4.6.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung der Techniken, um die Implementation der dokumentierten Techniken zu verifizieren.

#### 6.10.6.4.6.2 Voraussetzungen

Die Anlage befindet sich im Betriebszustand, und alle externen Schnittstellen, die Teil der Vorgabesgemäßen Verwendung sind, sind entweder aktiviert oder so konfiguriert, dass sie aktiviert werden können, so dass alle externen Schnittstellen geprüft werden können.

Wenn für den Zugang zu einer externen Schnittstelle eine Authentisierung erforderlich ist, wird ein Mittel bereitgestellt, um die Schnittstelle prüfen zu können.

#### 6.10.6.4.6.3 Beurteilungseinheiten

Es ist funktional zu beurteilen, ob jede externe Schnittstelle unter Berücksichtigung ihrer Funktionalität und der vorgesehenen Funktionalität der Anlage gegenüber häufige Eingabeangriffe resilient ist durch Folgendes:

— nach der Beschreibung in [E.Info.GEC-6.ExternalInterface], um die zugehörigen Eingabemethoden zu prüfen, z. B. durch Generierung fehlerhafter oder ungültiger Nachrichten (z. B. über ein Webinterface oder generische Tools zur Nachrichtengenerierung oder Fuzzing-Tools). Versuch, die in [E.Info.GEC-6.Security-Asset] beschriebenen Sicherheitswerte und die in [E.Info.GEC-6.NetworkAsset] beschriebenen Netzwerkwerte zu verfälschen, zu extrahieren oder zu missbrauchen, indem spezifische Angriffe im Zusammenhang mit Eingabemechanismen wie SQL-Injection, Ajax-Injection, OS-Command-Injection oder Path-Traversal ausgeführt werden; und

— es wird funktional beurteilt, ob das in [E.Info.GEC-6.ExternalInterface] beschriebene Verhalten oder die Ausgabe wie dokumentiert erzeugt wird, wobei das Anlagenhandbuch oder die Gestaltungsdokumentation als Leitlinien dienen.

#### 6.10.6.4.6.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn kein Nachweis vorliegt, dass eine Prüfung zur Eingabevalidierung erfolgreich war, um einen Sicherheitswert wie in [E.Info.GEC-6.SecurityAsset] oder einen Datenschutzwert wie in [E.Info.GEC-6.PrivacyAsset] beschrieben zu verfälschen, zu extrahieren oder zu missbrauchen.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn ein Nachweis vorliegt, dass eine Prüfung zur Eingabevalidierung erfolgreich war, um einen Sicherheitswert, wie in [E.Info.GEC-6.SecurityAsset] beschrieben, oder einen Datenschutzwert, wie in [E.Info.GEC-6.PrivacyAsset] beschrieben, zu verfälschen, zu extrahieren oder zu missbrauchen.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

### 6.10.7 [GEC-7] Dokumentation externer Sensorikfähigkeiten

#### 6.10.7.1 Anforderung

Alle externen Sensorikfähigkeiten der Anlage, die im Zusammenhang mit dem Schutz der Daten von Benutzern oder Teilnehmern stehen, müssen für den Benutzer dokumentiert sein.

#### 6.10.7.2 Begründung

Externe Sensorikfähigkeiten könnten missbraucht werden, um den Benutzer der Anlage auszuspähen. Wenn sich der Benutzer der Sensorikfähigkeiten der Anlage nicht bewusst ist, kann er dieses unbeabsichtigt an Orten verwenden, an denen der Schutz der Privatsphäre gefährdet ist. Die Dokumentation der externen Sensorikfähigkeiten macht den Benutzern bewusst, was die Anlage technisch über ihre Privatsphäre offenlegen könnte. Mit diesem Bewusstsein können Benutzer ihre Nutzung der Anlage so anpassen, dass das Risiko der Kompromittierung ihrer Privatsphäre minimiert wird.

#### 6.10.7.3 Leitlinie

Der Hersteller muss für den Benutzer klar und transparent darstellen, was mit den im Gerät vorhandenen Sensoren erfasst werden kann. Auf der Grundlage dieser Informationen könnte der Benutzer z. B. die Kamera mit einem Aufkleber versehen. Darüber hinaus können Informationen über die Sensorikfähigkeiten der Anlage während des anfänglichen Konfigurationsprozesses bereitgestellt werden.

Ein Beispiel für eine externe Sensorikfähigkeit ist ein Mikrofon oder eine Kamera.

#### 6.10.7.4 Beurteilungskriterien

##### 6.10.7.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung GEC-7.

##### 6.10.7.4.2 Umsetzungskategorien

Nicht anwendbar.

##### 6.10.7.4.3 Erforderliche Informationen

(Wenn externe, nicht netzwerkbezogene Schnittstellen verfügbar sind) [E.Info.GEC-7.NonNetworkInterface]: Beschreibung jeder externen, nicht netzwerkbezogenen Schnittstelle der Anlage, die den Schutz des Benutzers oder Teilnehmers beeinträchtigen kann.

(Wenn externe, nicht netzwerkbezogene Schnittstellen den Schutz des Benutzers oder Teilnehmers beeinträchtigen können) [E.Info.GEC-7.UserDoc.NonNetworkInterface]: Benutzerdokumentation, die jede externe, nicht netzwerkbezogene Schnittstelle der Anlage beschreibt, die den Schutz des Benutzers oder Teilnehmers beeinträchtigen kann.

[E.Info.DT.GEC-7]: Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 42 für jede in [E.Info.GEC-7.NonNetworkInterface] dokumentierte externe, nicht netzwerkbezogene Schnittstelle.

[E.Just.DT.GEC-7]: Begründung für jeden gewählten Pfad durch den in [E.Info.DT.GEC-7] dokumentierten Entscheidungsbaum mit den folgenden Eigenschaften:

— (wenn eine Entscheidung aus [DT.GEC-7.DN-1] zu „NICHT ANWENDBAR“ führt) basiert die Begründung für die Entscheidung [DT.GEC-7.DN-1] auf [E.Info.GEC-7.NonNetworkInterface]; und

— die Begründung für die Entscheidung [DT.GEC-7.DN-2] basiert auf [E.Info.GEC-7.UserDoc.NonNetworkInterface].

#### 6.10.7.4.4 Konzeptuelle Beurteilung

##### 6.10.7.4.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob alle externen, nicht netzwerkbezogenen Schnittstellen, die über Datenschutzwerte betreffende Sensorikfähigkeiten verfügen und mit dem Schutz des Benutzers oder Teilnehmers in Zusammenhang stehen, in der Benutzerdokumentation wie nach GEC-7 erforderlich beschrieben sind.

##### 6.10.7.4.4.2 Voraussetzungen

Keine.

##### 6.10.7.4.4.3 Beurteilungseinheiten

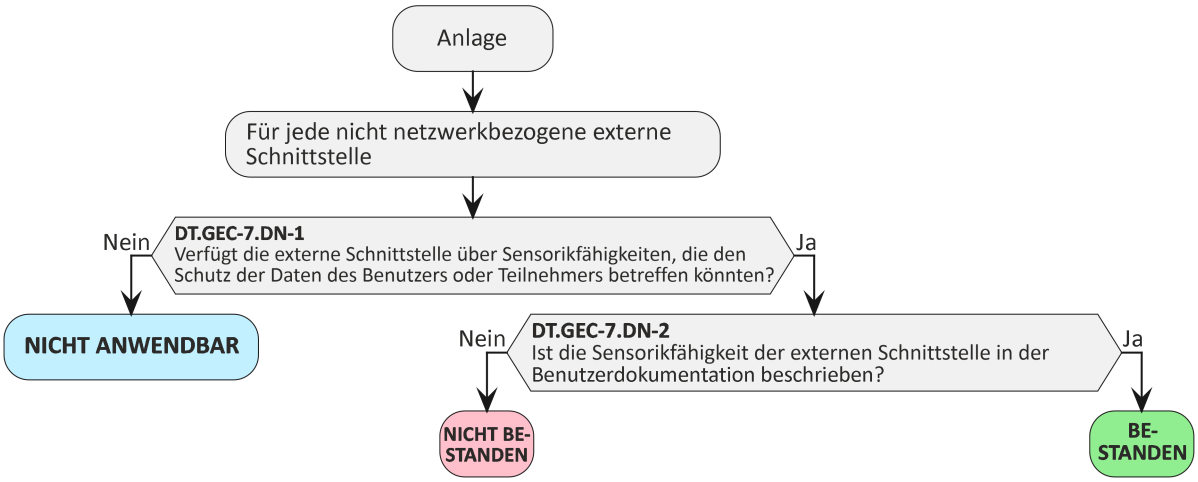



**Bild 42 — Entscheidungsbaum für Anforderung GEC-7**

Für jede in [E.Info.GEC-7.NonNetworkInterface] dokumentierte externe, nicht netzwerkbezogene Netzwerkschnittstelle ist zu prüfen, ob der Pfad durch den in [E.Info.DT.GEC-7] dokumentierten Entscheidungsbaum mit „NICHT ANWENDBAR“ oder „BESTANDEN“ endet.

Für jeden in [E.Info.DT.GEC-7] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.GEC-7] dokumentierte Begründung zu untersuchen.

#### 6.10.7.4.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— mindestens ein Pfad durch den in [E.Info.DT.GEC-7] dokumentierten Entscheidungsbaum mit „BESTANDEN“ endet; und

— kein Pfad durch den in [E.Info.DT.GEC-7] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; und

— die in [E.Just.DT.GEC-7] angegebenen Informationen korrekte Begründungen für alle Pfade durch den in [E.Info.DT.GEC-7] dokumentierten Entscheidungsbaum sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— ein Pfad durch den in [E.Info.DT.GEC-7] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; oder

— eine in [E.Just.DT.GEC-7] angegebene Begründung für einen Pfad durch den in [E.Info.DT.GEC-7] dokumentierten Entscheidungsbaum nicht korrekt ist oder fehlt.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

### 6.10.7.4.5 Beurteilung der funktionalen Vollständigkeit

#### 6.10.7.4.5.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, alle externen, nicht netzwerkbezogenen Schnittstellen, die den Schutz der Daten von Benutzern oder Teilnehmern betreffen können, in der Benutzerdokumentation beschrieben sind.

#### 6.10.7.4.5.2 Voraussetzungen

Die Anlage befindet sich im Betriebszustand.

#### 6.10.7.4.5.3 Beurteilungseinheiten

Es ist funktional zu beurteilen, ob weitere externe, nicht netzwerkbezogene Schnittstellen vorhanden sind, die den Schutz der Daten von Benutzern oder Teilnehmern betreffen können und die nicht in [E.Info.GEC-7.NonNetworkInterface] dokumentiert sind.

#### 6.10.7.4.5.4 Entscheidungszuweisung

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn alle gefundenen externen, nicht netzwerkbezogenen Schnittstellen, die den Schutz der Daten von Benutzern oder Teilnehmern betreffen können, in [E.Info.GEC-7.NonNetworkInterface] dokumentiert sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn eine gefundene externe, nicht netzwerkbezogene Schnittstelle, die den Schutz der Daten von Benutzern oder Teilnehmern betreffen kann, nicht in [E.Info.GEC-7.NonNetworkInterface] dokumentiert ist.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

### 6.10.7.4.6 Beurteilung der funktionalen Suffizienz

Keine.

## 6.11 [CRY] Kryptographie (en: Cryptography)

### 6.11.1 [CRY-1] Bewährte Verfahrensweisen für Kryptographie

#### 6.11.1.1 Anforderung

Die Anlage muss bewährte Verfahrensweisen für Kryptographie nutzen, die zum Schutz der Sicherheitswerte oder Datenschutzwerte eingesetzt werden, mit Ausnahme von:

— Kryptographie, die für einen bestimmten Sicherheitsmechanismus verwendet wird, bei dem eine Abweichung nach den Vorgabeen der Abschnitte ACM, AUM, SCM, SUM oder SSM festgestellt und begründet wird.

#### 6.11.1.2 Begründung

Kryptographie, die für den Schutz von Sicherheitswerten oder Datenschutzwerten eingesetzt wird und die nicht stark genug für den Anwendungsfall ist, weil sie beispielsweise nicht geeignet oder fehlerhaft ist, stellt für diese Werte ein Sicherheitsrisiko dar. Der Einsatz bewährter Verfahrensweisen oder sogar einer fortschrittlicheren, offensichtlich geeigneten Kryptographie schafft Vertrauen in den kryptographischen Schutz dieser Werte.

Wenn ein kryptographischer Algorithmus geknackt wird oder kryptographische Elemente kompromittiert werden, kann es erforderlich sein, die Anlage entsprechend zu aktualisieren (siehe Anforderung SUM), um den Schutz der durch Kryptographie geschützten Sicherheitswerte und Datenschutzwerte zu erhalten. Zwar gibt es keine absolute Garantie, dass dies nicht bei Kryptographieverfahren vorkommt, die als bewährte Verfahrensweisen gelten, aber es ist wahrscheinlicher, dass die Kryptographie für einen bestimmten Anwendungsfall ungeeignet ist, wenn bereits Hinweise vorliegen, dass die Kryptographie während der vorhergesehenen Lebensdauer der Anlage veralten wird.

Allerdings kann die Anlage unter Umständen nicht für die Aktualisierung der Kryptographie vorbereitet werden, beispielsweise wenn die Anlage selbst über das Internet kommunizieren kann und einen hardwarebasierten Krypto-Beschleuniger enthält. In diesen Fällen ist es wichtig, dass keine Hinweise vorliegen, dass die Kryptographie während der vorhergesehenen Lebensdauer nicht mehr zu den bewährten Verfahrensweisen zählen wird.

#### 6.11.1.3 Leitlinie

Es gibt verschiedene Sicherheitsleitlinien, die zur Identifizierung bewährter Verfahrensweisen für Kryptographie verwendet werden können; siehe entsprechende ISO/IEC-Normen, öffentliche, von SDOs und Behörden bereitgestellte Krypto-Kataloge wie beispielsweise sogis.eu, „SOGIS agreed Cryptographic Mechanisms“ [24], ETSI TS 119 312 „Electronic Signatures and Infrastructures; Cryptographic Suites“ [27] und von ENISA und nationalen Behörden bereitgestellte Leitlinien wie NIST SP800-Reihe [8] bis [18] und BSI TR-02102-1 [20].

Ein häufig für einen bestimmten Anwendungsfall eingesetztes kryptographisches Verfahren, für das kein Nachweis möglicher Angriffe mit aktuell einfach verfügbaren Techniken vorliegt, kann als bewährte Verfahrensweise gelten.

Es ist aber auch möglich, den Nachweis zu liefern, dass eine neue Kryptographie für einen bestimmten Anwendungsfall geeignet ist und daher als bewährte Verfahrensweise für Kryptographie gelten kann.

Kryptographie wird häufig für den Schutz entsprechender Sicherheitswerte und Datenschutzwerte eingesetzt, beispielsweise:

— Authentisierung (siehe AUM),

— sichere Aktualisierung (siehe SUM),

— sichere Speicherung (siehe SSM),

— sichere Kommunikation (siehe SCM),

— Erzeugung vertraulicher kryptographischer Schlüssel (siehe CCK-2).

Der kryptographische Schutz entspricht möglicherweise nicht bewährten Verfahrensweisen, wenn die Interoperabilität gefordert ist. Legacy-Mechanismen, die in großem Umfang eingesetzt werden, bieten kurzfristig eine annehmbare Sicherheit und weisen im Vergleich zu den in den oben zitierten Krypto-Katalogen (siehe z. B. sogis.eu) ausgewiesenen Mechanismen bewährter Verfahrensweisen einige Einschränkungen in Bezug auf die Sicherheit auf. Die Krypto-Kataloge werden in regelmäßigen Abständen (z. B. jährlich) aktualisiert, um aktuelle Listen der Legacy-Mechanismen und deren Gültigkeitsdauer zu erhalten, die durch eine Auslauffrist festgelegt ist.

Wenn überprüfte oder bewertete Implementationen öffentlich verfügbar sind, die der bewährten Verfahrensweise entsprechen, dürfen diese bevorzugt eingesetzt werden, um Netzwerk- und Sicherheitsfunktionen bereitzustellen, insbesondere im Bereich der Kryptographie.

Um während der vorhergesehenen Lebensdauer der Anlage bewährte Verfahrensweisen für Kryptographie zu nutzen, sollte zusätzlich das Konzept der Krypto-Agilität in Betracht gezogen werden, das es ermöglicht, die Kryptographie auf der Anlage in Übereinstimmung mit SUM zu aktualisieren, um auf neue Angriffe und neue technologische Entwicklungen zu reagieren.

Elemente, die bei der Vorbereitung der Kryptographie für die Aktualisierung zu beachten sind, sind unter anderem:

— kryptographische Verfahren, Protokolle, Algorithmen, Konstruktoren und Primzahlen,

— die Art der verwendeten sensiblen Sicherheitsparameter, und

— spezifische SSPs, wie beispielsweise Vertrauensgrundlagen.

Bei Anlagen, deren kryptographische Algorithmen oder Elemente nicht aktualisiert werden können, beispielsweise weil die Implementation oder das Teil eine hardwarebasierte Vertrauensgrundlage verwenden, ist es wichtig, dass die vorhergesehene Lebensdauer der Anlage nicht länger ist als die empfohlene Lebensdauer für die Nutzung der vom Gerät verwendeten kryptographischen Algorithmen und Elemente.

#### 6.11.1.4 Beurteilungskriterien

##### 6.11.1.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung CRY-1.

##### 6.11.1.4.2 Umsetzungskategorien

Nicht anwendbar.

##### 6.11.1.4.3 Erforderliche Informationen

[E.Info.CRY-1.Assets]: Liste aller Sicherheitswerte und Datenschutzwerte auf dem kryptographisch geschützten Gerät, einschließlich für jede für den kryptographischen Schutz verwendete Kryptographie:

— [E.Info.CRY-1.Assets.Cryptography]: Beschreibung der zum kryptographischen Schutz genutzten Kryptographie, einschließlich:

  — Beschreibung der einzelnen kryptographischen Schutzziele; und

  — Nachweis, dass die Kryptographie den bewährten Verfahrensweisen für die kryptographischen Schutzziele entspricht

oder;

— (wenn eine Abweichung nach den Vorgabeen der Abschnitte ACM, AUM, SCM, SUM oder SSM festgestellt und begründet wird) [E.Info.CRY-1.Assets.Deviation]: Verweisung auf die entsprechende Begründung und auf die erforderlichen Informationen, auf die sich die Begründung stützt.

ANMERKUNG 1 Die Dokumentation eines kryptographischen Schutzzieles schließt die von der Kryptographie bereitgestellten Sicherheitszielsetzungen ein.

ANMERKUNG 2 Kryptographie, die für den kryptographischen Schutz eingesetzt wird, kann unter anderem kryptographische Verfahren, Algorithmen, Konstruktoren und Primzahlen nutzen.

ANMERKUNG 3 Der Nachweis, dass die Kryptographie die bewährte Verfahrensweise für die kryptographischen Schutzziele darstellt, kann auf der Grundlage von Referenzkatalogen, z. B. SOGIS Agreed Cryptographic Mechanisms (https://www.sogis.eu) [24], oder anderen Nachweisen, z. B. durch Kryptoanalyse, erbracht werden.

[E.Info.DT.CRY-1]: Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 43 für jeden in [E.Info.CRY-1.Assets] beschriebenen Sicherheitswert und Datenschutzwert.

[E.Just.DT.CRY-1]: Begründung für jeden gewählten Pfad durch den in [E.Info.DT.CRY-1] dokumentierten Entscheidungsbaum mit den folgenden Eigenschaften:

— (wenn eine Entscheidung aus [DT.CRY-1.DN-1] zu „NICHT ANWENDBAR“ führt) basiert die Begründung für die Entscheidung [DT.CRY-1.DN-1] auf [E.Info.CRY-1.Assets.Deviation]; und

— die Begründung für die Entscheidung [DT.CRY-1.DN-2] basiert auf [E.Info.CRY-1.Assets.Cryptography].

#### 6.11.1.4.4 Konzeptuelle Beurteilung

##### 6.11.1.4.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob die zum Schutz von Sicherheitswerten oder Datenschutzwerten implementierte Kryptographie als bewährte Verfahrensweise wie nach CRY-1 erforderlich gilt.

##### 6.11.1.4.4.2 Voraussetzungen

Keine.

#### 6.11.1.4.4.3 Beurteilungseinheiten

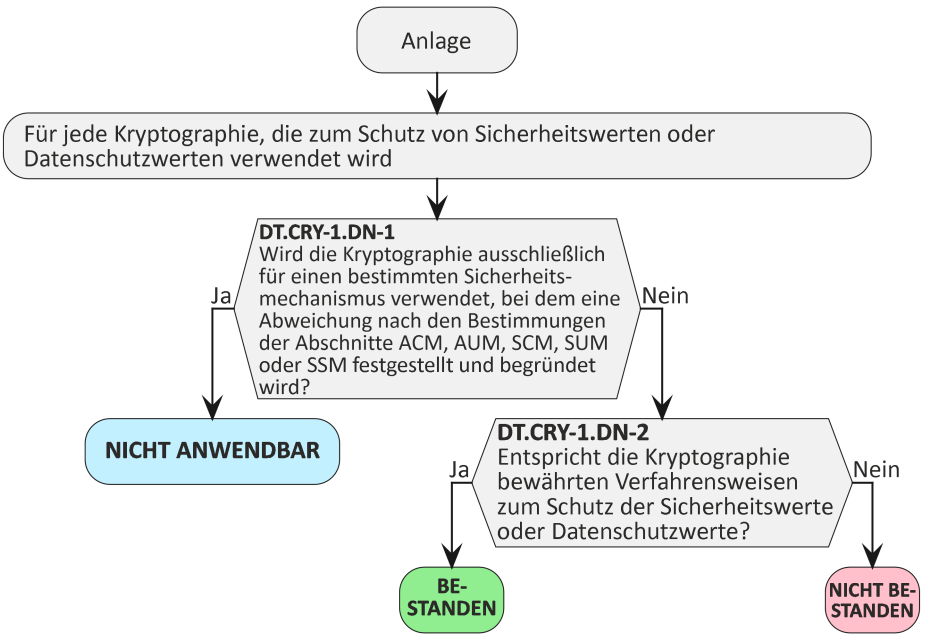



**Bild 43 — Entscheidungsbaum für Anforderung CRY-1**

Für jeden in [E.Info.CRY-1.Assets] dokumentierten Sicherheitswert und Datenschutzwert ist zu prüfen, ob der Pfad durch den in [E.Info.DT.CRY-1] dokumentierten Entscheidungsbaum mit „NICHT ANWENDBAR“ oder „BESTANDEN“ endet.

Für jeden in [E.Info.DT.CRY-1] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.CRY-1-1] dokumentierte Begründung zu untersuchen.

#### 6.11.1.4.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— mindestens ein Pfad durch den in [E.Info.DT.CRY-1] dokumentierten Entscheidungsbaum mit „BESTANDEN“ endet; und

— kein Pfad durch den in [E.Info.DT.CRY-1] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ endet; und

— die in [E.Just.DT.CRY-1] angegebenen Informationen korrekte Begründungen für alle Pfade durch den in [E.Info.DT.CRY-1] dokumentierten Entscheidungsbaum sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— alle Pfade durch den in [E.Info.DT.CRY-1] dokumentierten Entscheidungsbaum mit „NICHT BESTANDEN“ enden; oder

— eine in [E.Just.DT.CRY-1] angegebene Begründung für einen Pfad durch den in [E.Info.DT.CRY-1] dokumentierten Entscheidungsbaum nicht korrekt ist oder fehlt.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

#### 6.11.1.4.5 Beurteilung der funktionalen Vollständigkeit

##### 6.11.1.4.5.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob die Dokumentation in [E.Info.CRY-1.Assets.Cryptography] vollständig ist.

##### 6.11.1.4.5.2 Voraussetzungen

Die Anlage befindet sich im Betriebszustand.

##### 6.11.1.4.5.3 Beurteilungseinheiten

Es ist zu prüfen, ob ein Nachweis für den Einsatz von Kryptographie auf den Geräten zum Schutz der Sicherheitswerte oder Sicherheitswerte vorhanden ist, der nicht in [E.Info.CRY-1.Assets.Cryptography] dokumentiert ist.

ANMERKUNG Kryptographie, die durch Softwareaktualisierungen eingeführt wird, um Schwachstellen zu beseitigen oder die Sicherheitsstufe zu erhöhen, ist nicht als Abweichung von der Dokumentation zu betrachten.

##### 6.11.1.4.5.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn kein Nachweis für die auf der Anlage verwendete Kryptographie gefunden wird, die nicht in [E.Info.CRY-1.Assets.Cryptography] dokumentiert ist.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn ein Nachweis für die auf der Anlage verwendete Kryptographie gefunden wird, die nicht in [E.Info.CRY-1.Assets.Cryptography] dokumentiert ist.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

#### 6.11.1.4.6 Beurteilung der funktionalen Suffizienz

##### 6.11.1.4.6.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob die Kryptographie-Dokumentation in [E.Info.CRY-1.Assets.Cryptography] wie dokumentiert implementiert ist.

##### 6.11.1.4.6.2 Voraussetzungen

Die Anlage befindet sich im Betriebszustand.

##### 6.11.1.4.6.3 Beurteilungseinheiten

Für jeden in [E.Info.CRY-1.Assets.Cryptography] dokumentierten kryptographischen Schutz ist zu prüfen, ob es einen Nachweis dafür gibt, dass die Implementation von der Dokumentation abweicht.

ANMERKUNG Unterschiede infolge von Softwareaktualisierungen, um Schwachstellen zu beseitigen oder die Sicherheitsstufe zu erhöhen, ist nicht als Abweichung von der Dokumentation zu betrachten.

##### 6.11.1.4.6.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn kein Nachweis für die Abweichung der Kryptographie von ihrer Dokumentation in [E.Info.CRY-1.Assets.Cryptography] gefunden wird.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn ein Nachweis für die Abweichung der Kryptographie von der Dokumentation in [E.Info.CRY-1.Assets.Cryptography] gefunden wird.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

# Anhang A
(informativ)

# Begründung

## A.1 Allgemeines

Dieser Anhang enthält eine Begründung für die Begriffe und Konzepte in Zusammenhang mit diesem Dokument.

## A.2 Begründung

### A.2.1 Normenfamilie

Dieses Dokument gehört zu einem Satz von drei Normen, die die in Artikel 3.3.d, Artikel 3.3e und Artikel 3.3.f der Verordnung 2014/53/EU [36] festgelegten und von der Delegierten Verordnung (EU) 2022/30 [37] der Kommission aktivierten grundlegenden Anforderungen behandeln. Ein erster Schritt, um mit der Durchsetzung von Cybersicherheits-Anforderungen für die europäische Markteinführung von Funkanlagen zu beginnen, war die Nutzung der Funkanlagen-Richtlinie, denn die mangelhafte Sicherheit insbesondere bei Endverbraucher-IoT-Anlagen war und ist ein zunehmendes gesellschaftliches Problem.

Zwar liegt der Schwerpunkt der drei Normen auf unterschiedlichen grundlegenden Anforderungen (Netzwerkschäden, personenbezogene Daten und Privatsphäre sowie Schutz vor (finanziellem) Betrug), aber sie umfassen sowohl eindeutige als auch sich überlappende Anforderungen, für die eine wachsende Anzahl stärkerer Sicherheitskontrollen implementiert werden muss, um das Netzwerk, die Privatsphäre und die finanziellen Werte in einem Umfeld zunehmender Bedrohungen zu schützen.

Ob für eine bestimmte Funkanlage eine oder mehrere Normen gelten, ist eine Erwägung, die der Wirtschaftsteilnehmer anstellt, indem er eine produktbezogene Risikobeurteilung [38] zur Notwendigkeit der Erfüllung grundlegender Anforderungen der Funkanlagen-Richtlinie durchführt, und zwar mit dem Ziel, Bedrohungen zu ermitteln und Risiken zu beurteilen. Der „Blue Guide“ [35] und der „RED Guide“ [36] der Europäischen Kommission enthalten weitere Leitlinien zu diesem Thema.

### A.2.2 Sicherheit durch Gestaltung (en: Security by Design)

Ein effektives Sicherheitsmanagement erfordert etablierte Prozesse der Sicherheit durch Gestaltung, die in diesem Dokument, das häufige Sicherheitsanforderungen für Anlagen festlegt, nicht abgedeckt wird. Beispiele für Security-by-Design-Prozessnormen, die bei der Erfüllung von Sicherheitsanforderungen unterstützen können, sind unter anderem:

— IEC 62443-4-1 [1]: Security for industrial automation and control systems — Part 4-1: Secure product development lifecycle requirements

— NIST 800-160 [17]: Systems Security Engineering; Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems

— NIST 800-218 [18]: Secure Software Development Framework (SSDF)

— Microsoft Security Development Lifecycle (SDL)

— SAFECode Fundamental Practices for Secure Software Development

— GSMA FS.16 NESAS Development and Lifecycle Security Requirements

### A.2.3 Bedrohungsmodellierung und Sicherheitsrisikobeurteilung

STRIDE ist ein Beispiel für ein Klassifikationsschema, das für die Systemaufgliederung nützlich ist, um erkannte Bedrohungen nach den vom Angreifer verwendeten Arten von Angriffen zu charakterisieren. Das Akronym STRIDE setzt sich aus den Anfangsbuchstaben der folgenden Bedrohungskategorien zusammen:

**Tabelle A.1 — STRIDE**

| Bedrohung | Gewünschte Eigenschaft | Beschreibung |
|---|---|---|
| Spoofing | Authentizität | unrechtmäßiger Zugang zu Werten, indem man vorgibt, eine andere Person zu sein (Anmeldedaten, Netzwerkadresse) |
| Manipulation (en: Tampering) | Integrität | Verhindern einer schädlichen Veränderung von Daten (einschließlich der Systemkonfiguration) |
| Ablehnung (en: Repudiation) | Nichtabstreitbarkeit | Fähigkeit zum Nachweis, dass eine Aktion zwischen zwei Parteien stattgefunden hat (und keine Wiederholung zulässt) |
| Informations-offenlegung | Vertraulichkeit | kein Offenlegen von Informationen an nicht autorisierte Benutzer (personenbezogene Daten, Systemkonfiguration) |
| Denial-of-Service | Verfügbarkeit | Unerreichbarkeit eines Systems oder von Daten für autorisierte Benutzer durch Überlastung des Systems |
| Erweiterung der Berechtigung | Autorisierung | ein unberechtigter Benutzer erhält privilegierten Zugang und könnte das gesamte System gefährden |

Jede Sicherheitseigenschaft verfügt über primäre Abhilfemaßnahmen, um den Schwachstellen zu begegnen, die durch einen Risikomanagementprozess ermittelt werden könnten. Tabelle A.2 enthält eine Liste von Eindämmungsmaßnahmen, die in diesem Dokument als Sicherheitsanforderungen bereitgestellt werden und in die folgenden Kategorien eingeteilt sind, die von ISO/IEC TR 27103 [44] und dem NIST Cybersecurity Framework [45] definiert werden:

— Identifizieren: Prozess zur Erkennung der Attribute, die das Objekt identifizieren.

— Schützen: Die Fähigkeit, die Auswirkungen eines potentiellen Cybersicherheitsereignisses zu begrenzen oder abzuwehren.

  — Verhindern: Maßnahmen, die ein Cybersicherheitsereignis vermeiden oder ausschließen.

  — Grenzwert: Maßnahmen zur Verringerung der Auswirkungen eines Cybersicherheitsereignisses.

— Erkennen: Sicherheitsmaßnahmen zur Erkennung eines Cybersicherheitsvorfalls.

— Reagieren: Angemessene Aktivitäten, die bei einem erkannten Cybersecurity-Ereignis durchzuführen sind.

— Wiederherstellen: Angemessene Aktivitäten zur Aufrechterhaltung von Plänen für die Resilienz und zur Wiederherstellung von Fähigkeiten oder Diensten, die durch ein Cyber-Sicherheitsereignis beeinträchtigt wurden.

In Tabelle A.2 wird die Zuordnung der Bedrohungen für jede STRIDE-Kategorie zu den durch die einzelnen Sicherheitsanforderungen erreichten Eindämmungsmaßnahmen dargestellt. Die Eindämmungstechniken können beurteilt und implementiert werden, um sicherzustellen, dass sie den identifizierten Bedrohungen auf der Grundlage des Anwendungsfalls und der vorgesehenen Funktion der Funkanlage gerecht werden.

**Tabelle A.2 — Sicherheitsanforderungen, Fähigkeiten, Eindämmungstechniken und Gestaltungsgrundsätze**

| Eindämmungskategorie | | Sicherheitsanforderung/Fähigkeit/Eindämmungs-technik/Gestaltungsgrundsatz | S | T | R | I | D | E |
|---|---|---|---|---|---|---|---|---|
| Identifizieren | | Authentisierungsmechanismus (AUM) | X | X | | | X | |
| | | Vertrauliche kryptographische Schlüssel (CCK) | X | X | X | | | |
| Schützen | Verhindern | Zugangssteuerungsmechanismus (ACM) | | X | | X | X | X |
| | | Sicherer Speichermechanismus (SSM) | X | X | | X | | X |
| | | Sicherer Kommunikationsmechanismus (SCM) | X | X | X | X | | X |
| | | Löschungsmechanismus (DLM) | | | | X | | |
| | | Verschlüsselung (CRY) | | X | | X | | |
| | | Modernste Software und Hardware (GEC-1) | X | X | X | X | X | X |
| | | Konfiguration optionaler Dienste (GEC-3) | | | | X | X | X |
| | | Benutzerdokumentation (GEC-4 und GEC-7) | | | | X | | |
| | Begrenzen | Begrenzung der Offenlegung (GEC-2 und GEC-5) | | | | X | | X |
| | | Eingabevalidierung (GEC-6) | | X | | X | | |
| Erkennen | | Protokollierungsmechanismus (LGM) | | | X | | | |
| | | Benutzer-Benachrichtigungsmechanismus (UNM) | | X | | X | | X |
| Reagieren | | — | | | | | | |
| Wiederherstellen | | Sicherer Aktualisierungsmechanismus (SUM) | X | X | X | X | X | X |

Die ermittelten Bedrohungen werden vom Hersteller als eine der Eingaben für die Sicherheitsrisikobeurteilung verwendet, um die Auswirkungen und die Angemessenheit der gewählten Eindämmungsmaßnahmen zu bestimmen.

### A.2.4 Beurteilung der funktionalen Suffizienz

Bei der Beurteilung der funktionalen Suffizienz, bei der die Angemessenheit der Implementation untersucht und geprüft wird, werden unterschiedliche, anforderungsabhängige Ansätze verwendet, um eine wirksame Beurteilung zu erleichtern.

Bei einem Ansatz legen die Beurteilungseinheiten durchzuführende Aktionen fest, um Abweichungen zwischen der Dokumentation innerhalb der erforderlichen Informationen und der tatsächlichen Implementation des zu prüfenden Geräts zu ermitteln.

ANMERKUNG Die konzeptionelle Beurteilung umfasst bereits die Beurteilung der Dokumentation, die die geforderten Informationen in Bezug auf die Anforderung enthält.

Bei einem anderen Ansatz legen die Beurteilungseinheiten durchzuführende Aktionen fest, um die Umsetzung einer Anforderung durch die Anlage direkt zu beurteilen und mögliche Abweichungen, z. B. aus der Sicht eines Angreifers, zu ermitteln.

### A.2.5 Umsetzungskategorien

Im Allgemeinen sind die Anforderungen und Beurteilungskriterien so formuliert, dass unterschiedliche technische Umsetzungen abgedeckt werden können. Bestimmte Beurteilungseinheiten für die funktionale Suffizienz bieten jedoch zusätzlich zu den generischen Beurteilungseinheiten auch umsetzungsspezifische Beurteilungs-

einheiten, die für häufige technische Lösungen geeignet sind und als „Umsetzungskategorien“ bezeichnet werden.

### A.2.6 Werte

Um sicherzustellen, dass Anforderungen über die drei horizontalen Normen hinweg – die alle einen spezifischen Anwendungsbereich behandeln – angeglichen werden können, wurden Werte als Hauptziele eingeführt, auf die die Anforderungen anzuwenden sind: Die verschiedenen Arten von Werten sind in Tabelle A.3 zusammengefasst:

**Tabelle A.3 — Werte und grundlegende Anforderungen**

| Grundlegende Anforderungen | 3.3.d | 3.3.e | 3.3.f |
|---|---|---|---|
| Sicherheitswert | √ | √ | √ |
| Netzwerkwert | √ | | |
| Datenschutzwert | | √ | |
| Finanzieller Wert | | | √ |

Beim Schutz von Werten geht es nicht nur um den Schutz der spezifischen gespeicherten und kommunizierten oder anderweitig durch die Anlage verarbeiteten Daten, sondern auch um den Schutz der vom Gerät genutzten Funktionen und der Konfiguration dieser Funktionen.

Diese Korrelation spiegelt sich in den nachstehenden Definitionen für die Werte wider.

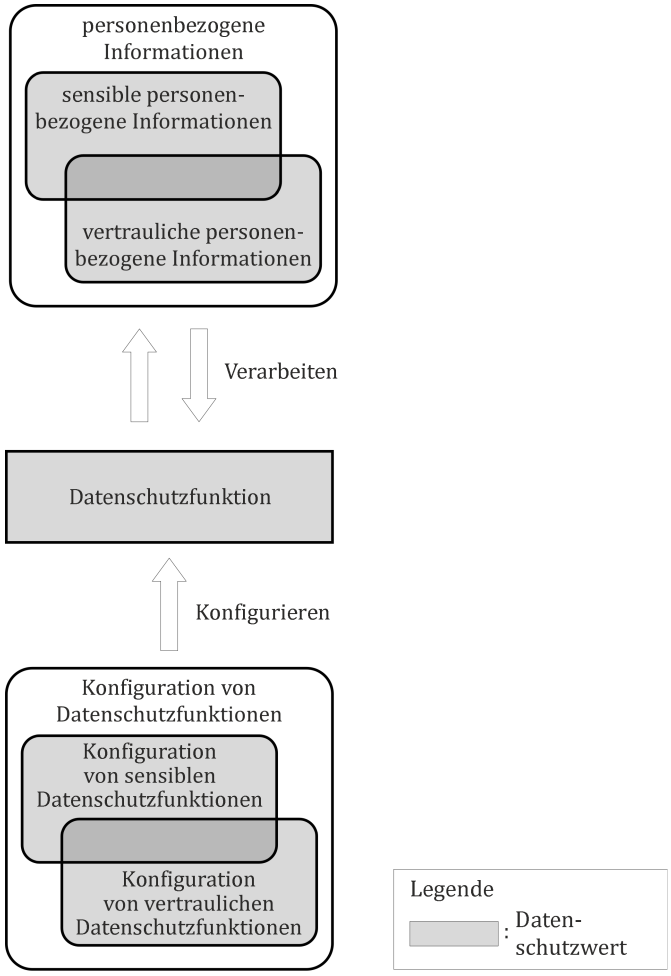



**Bild A.1 — Datenschutzwert der Anlage**

Beispiele für Datenschutzfunktionen sind:

— eine Implementation zur Aufzeichnung des GPS-Tracks des Benutzers,

— eine E-Mailing-Funktion, die den Namen und die E-Mail-Adresse des Benutzers speichert.

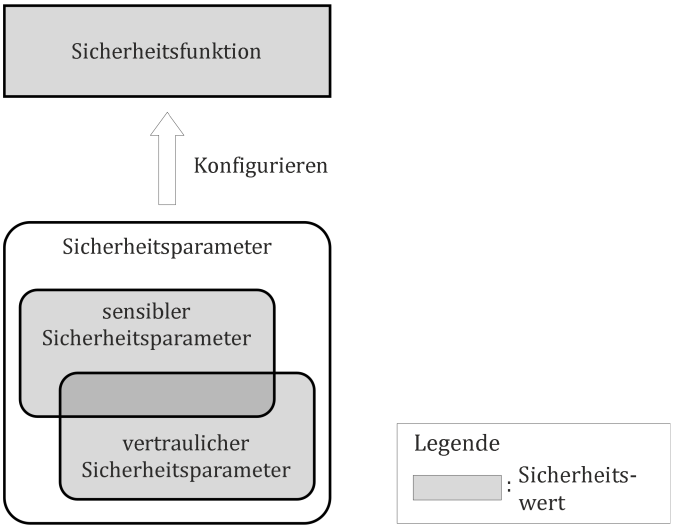



**Bild A.2 — Sicherheitswert der Anlage**

Ein Sicherheitsparameter ist eine in Sicherheitsfunktionen zum Schutz von Werten verwendete Information:

— Per Definition handelt es sich bei einem vertraulichen Sicherheitsparameter (CSP) um eine geheime sicherheitsrelevante Information, deren Offenlegung die Sicherheit eines Werts kompromittieren kann. Übliche Beispiele sind PINs und Passwörter, symmetrische kryptographische Schlüssel oder private asymmetrische kryptographische Schlüssel.

— Ein sensibler Sicherheitsparameter (SSP) ist eine sicherheitsbezogene Information, deren Manipulation die Sicherheit eines Werts kompromittieren kann. Übliche Beispiele sind symmetrische und asymmetrische kryptographische Schlüssel oder Zugangsrechte.

— Ein öffentlicher Sicherheitsparameter (PSP) ist ein sensibler Sicherheitsparameter, der nicht vertraulich ist. Übliche Beispiele sind öffentliche asymmetrische Schlüssel.

— Ein Sicherheitsparameter kann sowohl sensibel als auch vertraulich sein, und nach den oben angeführten Beispielen fällt ein privater symmetrischer kryptographischer Schlüssel üblicherweise in diese Kategorie.

Sicherheitsfunktionen werden zum Schutz von Datenschutzwerten oder anderen Sicherheitswerten verwendet. Die Implementation eines Zugangssteuerungsmechanismus ist zum Beispiel eine Sicherheitsfunktion.

In einigen Fällen schützen die Sicherheitsfunktionen sogar ihre eigenen Sicherheitsparameter, z. B. kann eine Zugangssteuerung vorhanden sein, bevor der Zugriff auf sensible oder vertrauliche Sicherheitsparameter der Zugangssteuerung gewährt wird.

Das vorliegende Dokument legt nicht die Granularität der Dokumentation in Bezug auf Sicherheitswerte und Datenschutzwerte fest. Eine geeignete Granularität im Hinblick auf den Dokumentationsaufwand kann gemeinsame Zugriffspfade zu und Zugangssteuerungsmechanismen von (Gruppen von) bestimmten Werten berücksichtigen. So können beispielsweise sensible Sicherheitsparameter, die nur über eine bestimmte API zugänglich sind, die einen bestimmten Zugangssteuerungsmechanismus verwendet, in Gruppen zusammengefasst werden.

### A.2.7 Mechanismen

In diesem Dokument wird das Konzept von Mechanismen verwendet, um spezifische Sicherheitsanforderungen zu behandeln und die Anwendbarkeit und Angemessenheit der Anforderungen für verschiedene Geräteimplementationen und Anwendungsbereiche zu ermöglichen. Da dieses Dokument eine horizontale Norm ist, muss es einen weiten Bereich von Produkten und Anwendungsfällen abdecken.

Ob und wie allgemeine Sicherheitsziele zu erreichen sind, hängt von der vorgesehenen Anlagenfunktionalität und der für die Nutzung vorgesehenen Betriebsumgebung ab. Diese beeinflussen, welche Implementationen von Sicherheitsmaßnahmen tatsächlich bei einem bestimmten Gerät erforderlich sind und wie stark die Kontrollen sein müssen. Eine spezifische Sicherheitsmaßnahme kann für ein Produkt angemessen sein, kann aber für andere Produkte oder das gleiche Produkt beim Einsatz in einer anderen Umgebung zu schwach oder zu stark sein.

Dieses Dokument enthält spezifische Einschränkungen und Bewertungsfragen; diese sollen als Anleitung dienen und um eine vollständige Abhängigkeit von der Sorgfalt des Herstellers zu vermeiden, soweit es die notwendigen Sicherheitsmaßnahmen bei der vorgesehenen Anlagenfunktionalität in der für die Nutzung vorgesehenen Betriebsumgebung betrifft.

Um Benutzer dieses Dokuments dabei anzuleiten, wann ein bestimmter Mechanismus anzuwenden ist, behandelt die erste Anforderung die Anwendbarkeit des Mechanismus. Diese Anforderungen dürfen eine Komponente enthalten, die mit „außer“ beginnt; sie gibt mögliche Bedingungen an, bei denen der Mechanismus nicht erforderlich ist. Wenn festgelegt wurde, dass der Mechanismus nicht anwendbar ist, dann sind alle weiteren Anforderungen in diesem spezifischen Abschnitt nicht länger verpflichtend.

Falls ein Mechanismus erforderlich ist, wird die Suffizienz bestimmt, indem die Angemessenheit der Anforderung und die Beurteilungskriterien bewertet werden. Alle unterstützenden Anforderungen in diesem Abschnitt sind dann ebenfalls anwendbar.

Diese Entscheidung wird für jede angegebene Einheit getroffen; beispielsweise wird bei der Prüfung der Anwendbarkeit einer Anforderung auf externe Schnittstellen die Entscheidung, ob die Anforderung und alle weiteren Anforderungen erfüllt werden müssen, unabhängig für jede externe Schnittstelle getroffen.

### A.2.8 Beurteilungskriterien

Die Sicherheitsmechanismen, die Funktionalität oder andere für die Anlage geltenden Verpflichtungen wurden in möglichst präzisen und objektiven Begriffen beschrieben, ohne den technologieagnostischen Grundton dieses Dokuments in Frage zu stellen. Die Art und Weise, wie der Hersteller die einzelnen Anforderungen erfüllt, wird durch die Bereitstellung der Daten für die Konformitätsprüfung der Anlage dokumentiert.

#### A.2.8.1 Entscheidungsbäume

Ob ein Mechanismus oder eine Anforderung anwendbar und/oder angemessen ist, hängt von der vorgabengemäßen Verwendung und der für die Nutzung vorgesehenen Betriebsumgebung ab. Dieses Dokument verwendet Entscheidungsbäume, um die Entscheidungsfindung und Beurteilung zu unterstützen und klare Anweisungen vorzugeben. Ein Beispiel ist im Folgenden dargestellt.

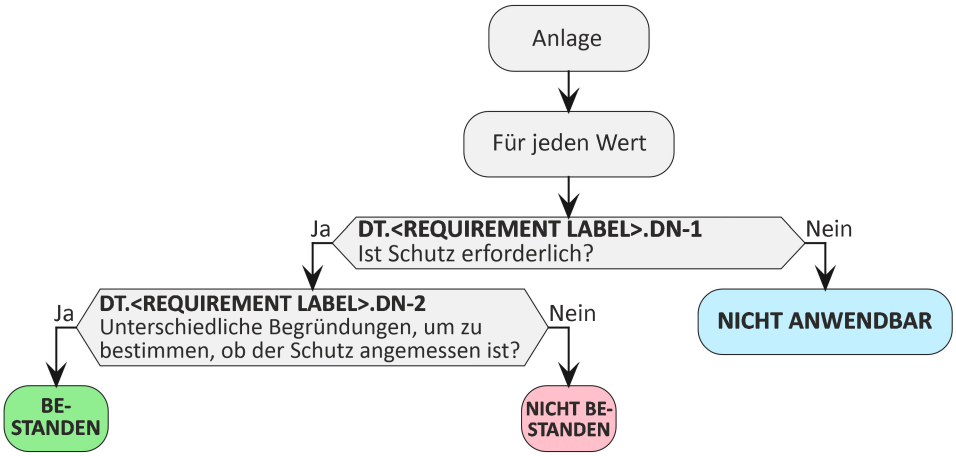



**Bild A.3 — Beispiel für einen Entscheidungsbaum**

Am Anfang der meisten Entscheidungsbäume steht die Anlage, gefolgt von einem Element, über das iteriert wird (z. B. die oben erwähnten Werte). Für jedes dieser Elemente werden Fragen zu den Geräteeigenschaften oder den entsprechenden Umgebungsfaktoren beantwortet. Jeder Entscheidungsbaum hat mindestens jeweils einen Pfad, der in BESTANDEN und NICHT BESTANDEN endet, und er kann optional einen oder mehrere Pfade haben, der/die in NICHT ANWENDBAR enden. Für jeden gewählten Pfad muss die Begründung dokumentiert werden.

### A.2.8.2 Technische Dokumentation

Die Beurteilungen sind von den Informationen abhängig, die als Teil der technischen Dokumentation vom Hersteller bereitzustellen sind, sowie von den Ergebnissen der angewandten Prüfmethodik, die für die jeweilige Umsetzungskategorie vorgeschrieben ist, sofern vorhanden. Die spezifischen Informationselemente, die für die Beurteilung in der technischen Dokumentation des Herstellers enthalten sein müssen, werden als [E.Info.xxxxx] bezeichnet, wobei xxxxx für den spezifischen geforderten Informationssatz steht; beispielsweise enthält [E.Info.ACM-1.ACM] die Identifizierung einiger der Informationen über die Zugangssteuerungsmechanismen, die für die Beurteilungen zur Anforderung ACM-1 bereitzustellen sind, oder [E.Info.AUM-1-1.ACM.NetworkInterface] für die Beschreibung der Netzwerkschnittstellen zur Beurteilung der Anforderung AUM-1-1.

Zu den erwarteten allgemeinen Informationen gehören:

— Informationen zur vorgesehenen Anlagenfunktionalität

— technische Informationen über die Anlage

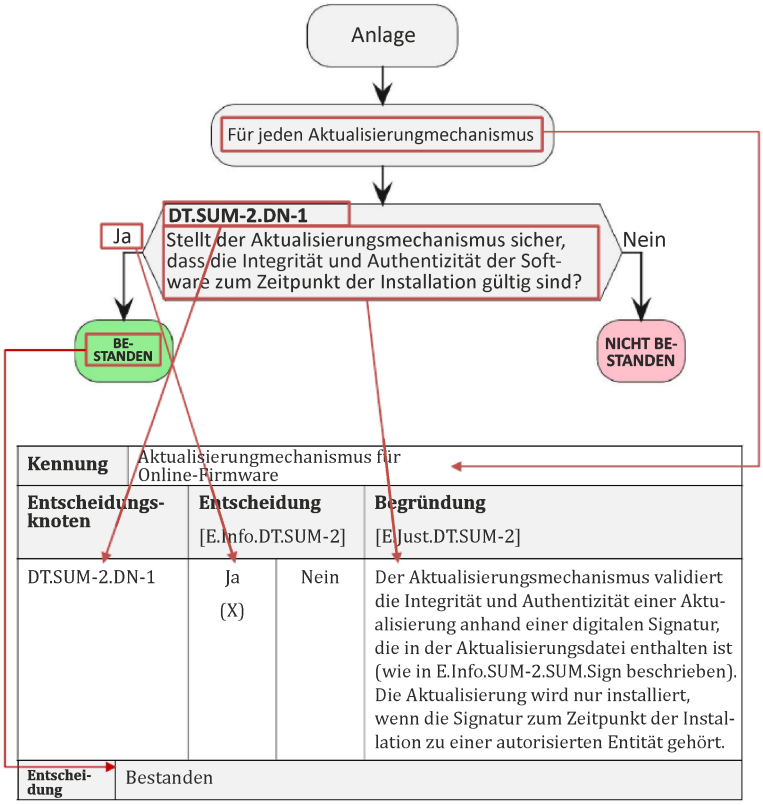
— unter Berücksichtigung des spezifischen Anwendungsfalls zur bewährten Verfahrensweise erklärt

— spezifische Einzelheiten, wie beispielsweise eine Liste externer Schnittstellen

— Sicherheitsrisikobeurteilung

Die Beurteilung einer Anforderung könnte die gleichen oder ähnliche Informationen wie andere Anforderungen erfordern (z. B. Schnittstelleninformationen). In diesem Fall könnte eine Verweisung innerhalb der Dokumentation verwendet werden.

Pfade durch den Entscheidungsbaum, die als Eingänge für die Beurteilung dienen, werden mit [E.Info.DT.xxxxxx] bezeichnet, und die Begründung wird mit [E.Just.DT.xxxxxx] bezeichnet. Je nach gewählter Umsetzungskategorie und Pfad durch den Entscheidungsbaum sind möglicherweise nicht alle angegebenen Informationselemente erforderlich. Die folgende Tabelle ist nur ein Beispiel, wie dies bei einer konzeptuellen Beurteilung umgesetzt werden könnte.




| **Kennung** | Aktualisierungmechanismus für Online-Firmware | | |
|---|---|---|---|
| **Entscheidungs-knoten** | **Entscheidung** [E.Info.DT.SUM-2] | | **Begründung** [E.Just.DT.SUM-2] |
| DT.SUM-2.DN-1 | Ja (X) | Nein | Der Aktualisierungsmechanismus validiert die Integrität und Authentizität einer Aktualisierung anhand einer digitalen Signatur, die in der Aktualisierungsdatei enthalten ist (wie in E.Info.SUM-2.SUM.Sign beschrieben). Die Aktualisierung wird nur installiert, wenn die Signatur zum Zeitpunkt der Installation zu einer autorisierten Entität gehört. |
| **Entscheidung** | Bestanden | | |

**Bild A.4 — Beispiel: Nachweis durch Entscheidungsbaum**

### A.2.8.3 Sicherheitsprüfung

Die Angemessenheit der meisten Sicherheitsprüfungen ist nicht quantitativ messbar, da es keine zu einem Thermometer oder einem Frequenzmessgerät äquivalenten Geräte gibt, um die Stellung der Ausrüstung in Bezug auf Sicherheit zu messen, und keine stringente Definition, wann „gut“ gut genug ist.

Das Ergebnis ist daher vom Wissen des Beurteilers und seiner Wahrnehmung der Bedrohungslandschaft abhängig sowie davon, was für eine spezifische Ausrüstung in einer spezifischen Umgebung angemessen ist; dies trägt zusätzlich zu der Schwierigkeit bei, verifizierbare, objektive und reproduzierbare Prüfkriterien zu definieren, weil selbst zwei Beurteiler geringfügig abweichende Ansichten und/oder Meinungen haben können.

Tools für Sicherheitsprüfungen weisen oft anhand von Negativprüfungen nach, dass bestimmte Schwachstellen nicht vorhanden sind; weil aber Sicherheitstools ständig aktualisiert werden, können aufgrund aktualisierter Informationen oder bei der Ausführung über längere Zeiträume neue Probleme erkannt werden – so führt auch dies nicht zu reproduzierbaren Prüfungsergebnissen.

Daher verbessert der in diesem Dokument gewählte Ansatz zwar das Ergebnis der Beurteilung, aber er kann das Problem nicht lösen. Die meisten Beurteilungen beruhen darauf, dass ausreichende Informationen zur Verfügung stehen.

### A.2.9 Schnittstellen

Schnittstellen sind ein wesentliches Konzept zur Beschreibung der Kommunikationsbeziehungen zwischen Entitäten. Die Definitionen für die Schnittstellen sind hierarchisch aufgebaut:

**Tabelle A.4 — Schnittstellen**

| Definition | | | Anmerkung |
|---|---|---|---|
| Schnittstelle | | | abstrakte Basisdefinition |
| | externe Schnittstelle | | auf die Anlage abgestimmte Definition |
| | | Benutzungsschnittstelle | spezifische Schnittstellentypen, die auf die Anlage abgestimmt sind |
| | | Maschinenschnittstelle | |
| | | Netzwerkschnittstelle | |

Die hierarchische Struktur kann durch die folgenden Beziehungen beschrieben werden:

— Eine „externe Schnittstelle“ ist eine „Schnittstelle“.

— Eine „Benutzungsschnittstelle“, eine „Maschinenschnittstelle“ und eine „Netzwerkschnittstelle“ sind alle „externe Schnittstellen“.

In diesem Dokument werden nur bestimmte Schnittstellentypen definiert, die in den Anwendungsbereich dieses Dokuments fallen.

Für die Kommunikation zwischen der Anlage und einer Entität wird ein mehrschichtiges Kommunikationsmodell verwendet. Je nach Anwendungsfall können je nach Kommunikationsschicht verschiedene Typen von Schnittstellen verwendet werden.

Ein Webdienst auf der Anlage könnte beispielsweise eine Webseite für ein Gerät bereitstellen, um mit dem Benutzer der Anlage zu interagieren. Während es sich aus Sicht der Anwendung um eine Benutzungsschnittstelle handelt, wird die Webseite mit Hilfe einer Netzwerkschnittstelle über das Netzwerk übertragen.

Die folgenden Beispiele erläutern den Ansatz.

#### A.2.9.1 Beispiel: Laptop mit einer eingebauten Tastatur

In diesem Beispiel ist die Tastatur ein integraler Bestandteil der Anlage. Die Anlage kommuniziert mit dem Benutzer über die Benutzungsschnittstelle.

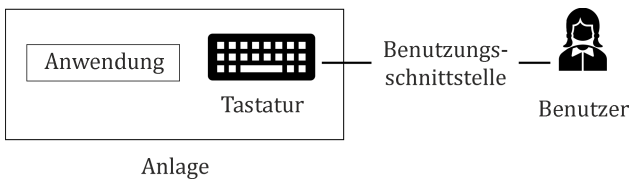



**Bild A.5 — Beispiel: Laptop mit einer eingebauten Tastatur**

#### A.2.9.2 Beispiel: Gerät mit einer USB-Tastatur

In diesem Beispiel ist die Tastatur nicht Teil der Anlage, sondern über USB verbunden. Aus der Sicht der Anlage ist die Tastatur ein externes Gerät, mit dem es über eine Maschinenschnittstelle kommuniziert. Aus der Sicht der Anwendung erfolgt die Kommunikation mit dem Benutzer jedoch über eine Benutzungsschnittstelle.

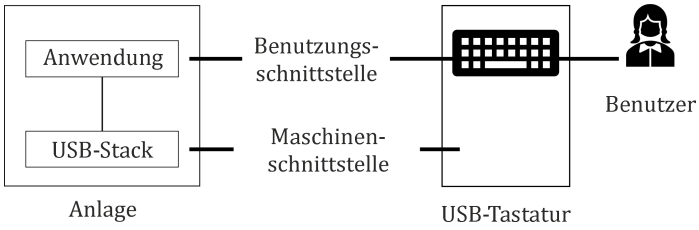



**Bild A.6 — Beispiel: Gerät mit einer USB-Tastatur**

### A.2.9.3 Beispiel: Benutzungsschnittstelle über ein Netzwerk

Ein Benutzer verwendet ein Gerät, um über das Netz mit dem System zu kommunizieren, indem er eine Tastatur benutzt. Für dieses Beispiel ist es unerheblich, ob die Tastatur in das Gerät eingebaut ist oder ob sie auf andere Weise mit der Anlage verbunden ist.

Die Anlage verwendet den Netzwerkstack, um mit der Anlage des Benutzers zu kommunizieren, d. h. auf dieser Schicht erfolgt die Kommunikation über eine Netzwerkschnittstelle. Aus der Sicht der Anwendung wird eine Benutzungsschnittstelle zwischen der Anwendung der Anlage und dem Benutzer verwendet.

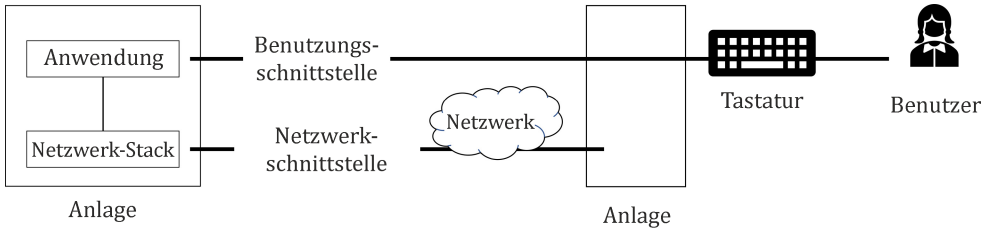



**Bild A.7 — Beispiel: Benutzungsschnittstelle über dem Netzwerk**

### A.2.9.4 Beispiel: USB-Drucker

Ein Drucker ist über USB mit der Anlage verbunden. Das Beispiel entspricht der USB-Tastatur mit dem einzigen Unterschied, dass aus Sicht der Anwendung die Kommunikation über eine Maschinenschnittstelle erfolgt.

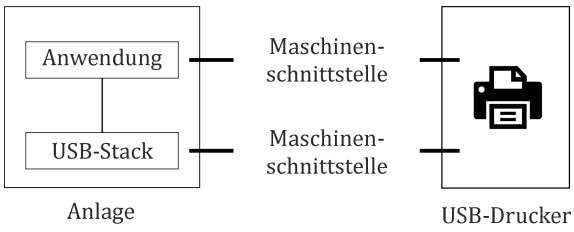



**Bild A.8 — Beispiel: USB-Drucker**

### A.2.9.5 Beispiel: Netzwerkdrucker

In diesem Beispiel kommuniziert die Anlage mit einem über das Netzwerk erreichbaren Drucker. Wie beim Beispiel der Benutzungsschnittstelle über das Netzwerk spielt es keine Rolle, wie der Drucker mit dem Netzwerk verbunden ist. Auf der Anwendungsschicht erfolgt die Kommunikation über eine Maschinenschnittstelle, während aus Sicht der Netzwerkschicht eine Netzwerkschnittstelle für die Kommunikation verwendet wird.

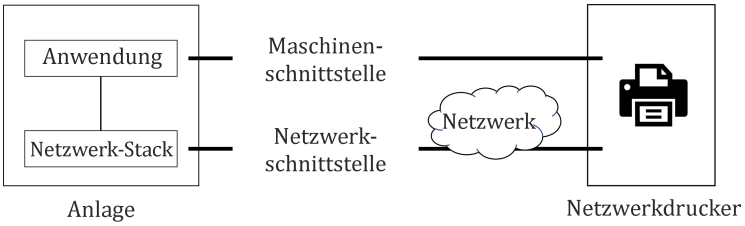



**Bild A.9 — Beispiel: Netzwerkdrucker**

# Anhang B
(informativ)

# Abbildung mit EN IEC 62443-4-2:2019

## B.1 Allgemeines

Die Absicht dieses informativen Anhangs ist es, eine Abbildung zwischen den Anforderungen in diesem Dokument und den in EN IEC 62443-4-2:2019 [2] spezifizierten Komponentenanforderungen (CR) zu erstellen zur Unterstützung von Herstellern, die bereits EN IEC 62443-4-2:2019 [2] anwenden.

Die erforderliche Sicherheitsstufe und die geltenden Anforderungen werden als Ergebnis der vom Hersteller durchgeführten Risikobeurteilung ermittelt.

Die Anforderungen an den Lebenszyklus der sicheren Produktentwicklung sind in EN IEC 62443-4-1:2018 festgelegt und werden in diesem Anhang nicht behandelt.

Erfüllung der Anforderungen EN IEC 62443-4-2:2019 (z. B. dokumentiert durch ein Zertifikat) stellen für sich genommen noch keine Konformität mit den Anforderungen dieses Dokuments dar.

## B.2 Abbildung

| Anf.ID | EN IEC 62443-4-2:2019 Anf.ID |
|---|---|
| ACM-1 | FR1: CR 1.1 – CR 1.14<br>CR 2.1<br>CR 2.2<br>CR 2.3 |
| ACM-2 | FR1: CR 1.1 – CR 1.14<br>CR 2.1<br>CR 2.2<br>CR 2.3 |
| ACM-3 | Spielzeuge und Kinderbetreuungsgeräte sind nicht in den Anwendungsbereich von EN IEC 62443-4-2:2019 einbezogen |
| ACM-4 | Spielzeuge und Kinderbetreuungsgeräte sind nicht in den Anwendungsbereich von EN IEC 62443-4-2:2019 einbezogen |
| ACM-5 | Spielzeuge und Kinderbetreuungsgeräte sind nicht in den Anwendungsbereich von EN IEC 62443-4-2:2019 einbezogen |
| ACM-6 | Spielzeuge und Kinderbetreuungsgeräte sind nicht in den Anwendungsbereich von EN IEC 62443-4-2:2019 einbezogen |
| AUM-1 | FR1: CR 1.1 – CR 1.14 |
| AUM-2 | FR1: CR 1.1 – CR 1.14 |
| AUM-3 | CR 1.5<br>CR 1.10 |
| AUM-4 | CR 1.5 |
| AUM-5 | CR 1.7 |

| Anf.ID | EN IEC 62443-4-2:2019 Anf.ID |
|---|---|
| AUM-6 | CR 1.7<br>CR 1.11 |
| SUM-1 | CR 3.10 |
| SUM-2 | CR 3.10 |
| SUM-3 | CR 3.10 |
| SSM-1 | CR 3.1<br>CR 4.1 |
| SSM-2 | CR 3.1 |
| SSM-3 | CR 4.1 |
| SCM-1 | CR 3.1<br>CR 3.8<br>CR 4.1 |
| SCM-2 | CR 3.1<br>CR 3.8<br>CR 4.1 |
| SCM-3 | CR 4.1 |
| SCM-4 | CR 3.1<br>CR 3.8 |
| LGM-1 | CR 2.8<br>CR 2.9 |
| LGM-2 | CR 2.8<br>CR 2.9<br>CR 2.10 |
| LGM-3 | CR 2.9<br>CR 2.10 |
| LGM-4 | CR 2.11 |
| DLM-1 | CR 4.2 |
| UNM-1 | nicht abgedeckt durch eine Komponentenanforderung (CR) in EN IEC 62443-4-2:2019 |
| UNM-2 | nicht abgedeckt durch eine Komponentenanforderung (CR) in EN IEC 62443-4-2:2019 |
| CCK-1 | CR 4.3<br>CR 1.9<br>CR 1.14 |
| CCK-2 | CR 4.3 |
| CCK-3 | CR 4.3 |
| GEC-1 | nicht abgedeckt durch eine Komponentenanforderung (CR) in EN IEC 62443-4-2:2019 |

| Anf.ID | EN IEC 62443-4-2:2019 Anf.ID |
|---|---|
| GEC-2 | CR 7.6<br>CR 7.7<br>CR 5.2 |
| GEC-3 | CR 2.1<br>CR 7.6<br>CR 5.2 |
| GEC-4 | CR 7.6 |
| GEC-5 | CR 7.7 |
| GEC-6 | CR 3.5 |
| GEC-7 | CR 7.6 |
| CRY-1 | CR 4.3 |

# Anhang C
(informativ)

# Abbildung mit ETSI EN 303 645 (Cyber Security for Consumer Internet of Things: Baseline Requirements)

## C.1 Allgemeines

Dieser Anhang enthält eine Abbildung, die veranschaulicht, welche Vorgaben der ETSI EN 303 645 [6] V2.1.1 verwendet werden können, um den Nachweis der Konformität von Funkanlagen mit den Anforderungen des vorliegenden Dokuments zu unterstützen.

## C.2 Abbildung

| Anf.ID | ETSI EN 303 645 Vorgabe: Begründung |
|---|---|
| ACM-1 | Vorgabe 5.5-4.<br>Die Vorgabe betrifft die Gerätefunktionalität, die Sicherheitswerte und Datenschutzwerte umfasst.<br>Vorgabe 5.5-5.<br>Der Schwerpunkt der Vorgabe liegt auf der Sicherheitskonfiguration, die ebenfalls zu den Sicherheitswerten gehört. |
| ACM-2 | Vorgabe 5.5-5.<br>Zu den Sicherheitswerten gehört auch die Sicherheitskonfiguration, die durch die Vorgabe abgedeckt ist.<br>Vorgabe 5.6-7.<br>Das „Least-Privilege-Prinzip“, wie im Abschnitt „Leitlinien“ beschrieben, ist sichergestellt. |
| ACM-3 | Nicht abgedeckt in EN 303 645 [6] |
| ACM-4 | Nicht abgedeckt in EN 303 645 [6] |
| ACM-5 | Vorgabe 5.5-5.<br>Zu den sicherheitsrelevanten Konfigurationsänderungen gehört auch die Konfiguration von Zugangssteuerungsmechanismen. |
| ACM-6 | Vorgabe 5.5-5.<br>Zu den sicherheitsrelevanten Konfigurationsänderungen gehört auch die Konfiguration von Zugangssteuerungsmechanismen. |
| AUM-1 | Vorgabe 5.5-4.<br>Die Vorgabe betrifft nur einen Anfangszustand.<br>Vorgabe 5.5-5.<br>Zu den Sicherheitswerten gehört auch die Sicherheitskonfiguration, die durch die Vorgabe abgedeckt ist. |
| AUM-2 und CRY-1 | Vorgabe 5.1-3.<br>Es kann davon ausgegangen werden, dass die Authentifizierung gegenüber der Anlage auch den Schutz von Netzwerkwerten und Sicherheitswerten umfasst, indem bewährte Kryptographie, einschließlich Authentisierungsmechanismen (die auch PKI-basierte Authentisierung umfassen können), verlangt wird. |

| Anf.ID | ETSI EN 303 645 Vorgabe: Begründung |
|---|---|
| AUM-3 | Nicht abgedeckt in EN 303 645 [6] |
| AUM-4 | Vorgabe 5.1-4.<br>Die Vorgabe umfasst eine Änderung der Authentisierungsmechanismen, zu denen auch Authentifikator-Tokens gehören. |
| AUM-5 | Vorgabe 5.1-1.<br>Die Eindeutigkeit von Passwörtern für verschiedene Geräte wird erzwungen.<br>Vorgabe 5.1-2.<br>Vorgabepasswörter sollten von einem CSPRNG generiert werden und daher nicht durch automatisierte Angriffe angreifbar sein.<br>Vorgabe 5.1-3.<br>Die Vorgabe deckt die Anforderung bezüglich der „bewährten Verfahrensweise in Bezug auf die Stärke“ ab, da sie die Verwendung der bewährten Verfahrensweisen für Kryptographie verlangt. |
| AUM-6 | Vorgabe 5.1-5.<br>Sowohl die Vorgabe als auch die Anforderung verlangen den Schutz/die Eindämmung von Brute-Force-Angriffen (einschließlich Angriffen auf die Massenauthentisierung) |
| SUM-1 | Vorgabe 5.3-1.<br>Die Vorgabe verlangt sichere Aktualisierungen für jede Komponente.<br>Vorgabe 5.3-2.<br>Sichere Aktualisierungen sind erforderlich, wenn es keine anderen Gründe gibt, sie nicht durchzuführen (z. B. Geräte mit begrenztem Platzverbrauch)<br>Vorgabe 5.3-15.<br>Die Leitlinien enthalten eine Ersatzstrategie für Geräte. |
| SUM-2 | Vorgabe 5.3-9.<br>Die Vorgabe garantiert die Authentizität und Integrität der Aktualisierungen.<br>Vorgabe 5.3-10.<br>Die Vorgabe garantiert die Authentizität und Integrität der Aktualisierungen, besonders über ein Netzwerk. |
| SUM-3 | Vorgabe 5.3-3.<br>Die Leitlinien umfassen die einfache Aktualisierbarkeit aus der Sicht eines Benutzers.<br>Vorgabe 5.3-4.<br>Die Vorgabe umfasst automatische Aktualisierungen ohne menschliche Interaktion.<br>Vorgabe 5.3-5.<br>Die Leitlinien sehen vor, dass nach dem Start und in regelmäßigen Abständen nach Aktualisierungen gesucht wird.<br>Vorgabe 5.3-6.<br>Vor allem die Punkte „Abfrage der Zustimmung des Benutzers zur Aktivierung von automatischen Aktualisierungen“ und „Überprüfung auf Aktualisierungen nach dem Start und in regelmäßigen Abständen“ werden in die Leitlinien aufgenommen. |

| Anf.ID | ETSI EN 303 645 Vorgabe: Begründung |
|---|---|
| SSM-1 | Vorgabe 5.4-1.<br>Für Sicherheitswerte (zu denen auch Sicherheitsparameter gehören) werden sichere Speichermechanismen verlangt.<br>Vorgabe 5.6-3.<br>Die Vorgabe bezieht sich nur auf den physischen Schutz, aber „Hardware und physischer Schutz“ sind im Abschnitt „Leitlinien“ enthalten. |
| SSM-2 | Vorgabe 5.4-1.<br>Die Vorgabe schützt auch die Sicherheitswerte (zu denen auch die Sicherheitsparameter gehören).<br>Vorgabe 5.4-2.<br>Die Vorgabe zielt darauf ab, Schutz gegen den Verlust der Integrität, z. B. durch Manipulation, zu bieten. In der Begründung der prEN ist der Schutz vor Manipulationen enthalten, aber die Vorgabe konzentriert sich nur auf Fälle fest einprogrammierter Identität. |
| SSM-3 | Vorgabe 5.4-1.<br>Für Sicherheitswerte (zu denen auch Sicherheitsparameter gehören) werden sichere Speichermechanismen verlangt. |
| SCM-1 | Vorgabe 5.5-6.<br>Kritische Sicherheitsparameter sind durch die Vorgabe geschützt, aber Datenschutzwerte sind nicht unbedingt abgedeckt.<br>Vorgabe 5.5-7.<br>Der Schwerpunkt der Vorgabe liegt auf der Vertraulichkeit der Sicherheitsparameter bei der Übertragung.<br>Vorgabe 5.8-1.<br>Der Schwerpunkt der Vorgabe liegt auf der Vertraulichkeit der personenbezogenen Daten bei der Übertragung.<br>Vorgabe 5.8-2.<br>Der Schwerpunkt der Vorgabe liegt auf der Vertraulichkeit der sensiblen personenbezogenen Daten bei der Übertragung. |
| SCM-2 | Nicht abgedeckt in EN 303 645 [6] |
| SCM-3 | Vorgabe 5.5-6.<br>Die Vorgabe verlangt eine Verschlüsselung der übermittelten kritischen Sicherheitsparameter.<br>Vorgabe 5.5-7.<br>Die Vorgabe verlangt eine Verschlüsselung der übermittelten kritischen Sicherheitsparameter.<br>Vorgabe 5.8-1.<br>Die Vorgabe verlangt eine Verschlüsselung der übermittelten personenbezogenen Daten.<br>Vorgabe 5.8-2.<br>Die Vorgabe verlangt eine Verschlüsselung der übermittelten personenbezogenen Daten. |
| SCM-4 | Vorgabe 5.5-1.<br>Zu den bewährten Verfahrensweisen der Kryptographie gehört die Resilienz gegen Replay-Angriffe (siehe Abschnitt „Begriffe“). |
| LGM-1 | Nicht abgedeckt in EN 303 645 [6] |
| LGM-2 | Nicht abgedeckt in EN 303 645 [6] |

| Anf.ID | ETSI EN 303 645 Vorgabe: Begründung |
|---|---|
| LGM-3 | Nicht abgedeckt in EN 303 645 [6] |
| LGM-4 | Nicht abgedeckt in EN 303 645 [6] |
| DLM-1 | Vorgabe 5.9-1.<br>Der Abschnitt „Leitlinien“ legt fest: Der Löschungsmechanismus der Anlage ist resilient gegenüber Unterbrechungen, wozu auch Ausfälle gehören können.<br>Vorgabe 5.11-1.<br>Die Vorgabe verlangt einen Löschungsmechanismus. |
| UNM-1 | Vorgabe 6-1.<br>Die Anforderung bezieht sich nur auf Änderungen, die Vorgabe gilt für Datenschutzbenachrichtigungen im Allgemeinen. |
| UNM-2 | Vorgabe 6-1.<br>Die Anforderung bezieht sich nur auf Änderungen, die Vorgabe gilt für Datenschutzbenachrichtigungen im Allgemeinen. |
| CCK-1 | Nicht abgedeckt in EN 303 645 [6] |
| CCK-2 | Vorgabe 5.1-3.<br>Die Methoden zum Schutz des Zugriffs auf Sicherheitswerte müssen die bewährten Verfahrensweisen der Kryptographie verwenden. |
| CCK-3 | Vorgabe 5.1-1.<br>Der Abschnitt „Leitlinien“ enthält „Sicherheitszugangsdaten“, zu denen auch Passwörter gehören.<br>Vorgabe 5.4-4.<br>Die Vorgabe deckt auch eindeutige Sicherheitsparameter ab. |
| GEC-1 | Diese Anforderung wird auf der Ebene der Produktanforderungen nicht erfüllt. Einem Hersteller, der die Prozessvorgaben 5.2-1, 5.2-2 und 5.2-3 einhält, wird es jedoch erleichtert, die Anforderung GEC-1 zu erfüllen. |
| GEC-2 | Vorgabe 5.6-1.<br>Unnötige Schnittstellen können als unbenutzt betrachtet werden. Daher haben beide die gleichen Anforderungen.<br>Vorgabe 5.6-5.<br>Nur Dienste für den Betrieb und die Einrichtung der Anlage sind für beide erlaubt. |
| GEC-3 | Nicht abgedeckt in EN 303 645 [6] |
| GEC-4 | Nicht abgedeckt in EN 303 645 [6] |
| GEC-5 | Vorgabe 5.6-1.<br>Eine nicht vorgesehene Anlagenfunktionalität kann als unbenutzt betrachtet werden.<br>Vorgabe 5.6-3.<br>Nur physische Schnittstellen sind durch die EN abgedeckt. |
| GEC-6 | Vorgabe 5.13-1.<br>Sowohl die Vorgabe als auch die Anforderung erfordern eine Eingabevalidierung. |

| Anf.ID | ETSI EN 303 645 Vorgabe: Begründung |
|---|---|
| GEC-7 | Vorgabe 5.8-3.<br>Sensorikfähigkeiten werden dokumentiert. |
| CRY-1 | Vorgabe 5.1-3.<br>Die Vorgabe betrifft die Authentisierungsmechanismen, die einen Teil der Anforderung darstellen.<br>Vorgabe 5.3-7.<br>Die Vorgabe betrifft sichere Aktualisierungen, die Teil der Anforderung sind.<br>Vorgabe 5.5-1.<br>Die Vorgabe betrifft die sichere Kommunikation, die Teil der Anforderung ist.<br>Vorgabe 5.5-2.<br>Überprüfte oder bewertete Kryptographie wird im Abschnitt „Leitlinien“ bevorzugt.<br>Vorgabe 5.5-3.<br>Die Vorgabe betrifft die Krypto-Agilität, die im Abschnitt „Leitlinien“ behandelt wird.<br>Vorgabe 5.8-1.<br>Die Vorgabe betrifft übertragene personenbezogene Daten, die Teil der Anforderung ist.<br>Vorgabe 5.8-2.<br>Die Vorgabe betrifft übertragene sensible personenbezogene Daten, die Teil der Anforderung ist. |

# Anhang D
(informativ)

# Abbildung mit Sicherheitsbewertungsstandard für IoT-Plattformen (SESIP, en: Security Evaluation for Secure IoT Platforms)

## D.1 Allgemeines

Dieser Anhang enthält eine Abbildung, die veranschaulicht, wie die Ergebnisse einer SESIP-Bewertung (EN 17927:2023) von verbundenen Plattformen, auf denen Funkanlagen basieren, als Nachweis zur Erfüllung der Anforderungen dieses Dokuments an Funkanlagen verwendet werden können.

## D.2 Abbildung

| Anf.ID | EN 17927:2023 SESIP-Unterstützung – Nachweis der Umsetzung und Bewertung auf der Ebene der Geräteelemente/Teilkomponenten |
|---|---|
| ACM-1 bis ACM-6 | Kryptographischer Betrieb, kryptographische Schlüsselgenerierung, kryptographischer Schlüsselspeicher und/oder kryptographische Zufallszahlengenerierung: Diese SESIP-Sicherheitsansprüche beurteilen die Implementation sicherer kryptographischer Dienste, die von den Anlagen zur Umsetzung eines Zugangssteuerungsmechanismus verwendet werden können.<br>Authentisierte Zugangssteuerung: Dieser SESIP-Sicherheitsanspruch beurteilt die Implementation eines sicheren, auf Authentisierung basierenden Zugangssteuerungsmechanismus, der direkt von den Anlagen zum Zwecke der Zugangssteuerung verwendet werden kann. |
| AUM-1 bis AUM-6 | Kryptographischer Betrieb, kryptographische Schlüsselgenerierung, kryptographischer Schlüsselspeicher und/oder kryptographische Zufallszahlengenerierung: Diese SESIP-Sicherheitsaussagen beurteilen die Implementation sicherer kryptographischer Dienste, die von den Geräten zur Umsetzung eines Authentisierungsmechanismus verwendet werden können.<br>Authentisierte Zugangssteuerung: Dieser SESIP-Sicherheitsanspruch beurteilt die Implementation eines sicheren, auf Authentisierung basierenden Zugangssteuerungsmechanismus, der direkt von den Anlagen zum Zwecke der Authentisierung verwendet werden kann.<br>Eine explizite Präzisierung der Anforderung kann die Validierung des Authentifikators, die Möglichkeit, den Authentifikator zu ändern, die Verhinderung von statischen und Vorgabewerten erfordern. Der Schutz gegen Brute-Force- und andere kryptographische Angriffe ist Teil der SESIP-Schwachstellenanalyse (AVA_VAN.SESIP). |
| SUM-1 bis SUM-3 | Sichere Aktualisierung der Plattform, sichere Aktualisierung der Anwendung: Diese SESIP-Sicherheitsansprüche beurteilen die Implementation eines sicheren Aktualisierungs-mechanismus für den veränderlichen Teil des zu bewertenden Geräteelements, einschließlich der Integritäts- und Authentizitätsprüfung des zu installierenden/ladenden Bildes.<br>ALC_FLR: Mit dieser SESIP-Evaluierungsaufgabe wird beurteilt, ob für das zu evaluierende Geräteelement ein Verfahren zur Behebung von Mängeln vorhanden ist, das die Überwachung, Meldung und Korrektur von Sicherheitsproblemen ermöglicht, die in der Praxis festgestellt werden könnten und die den Einsatz des sicheren Aktualisierungsmechanismus zur Eindämmung des Sicherheitsproblems auslösen würden. |

| Anf.ID | EN 17927:2023 SESIP-Unterstützung – Nachweis der Umsetzung und Bewertung auf der Ebene der Geräteelemente/Teilkomponenten |
|---|---|
| SSM-1 bis SSM-4 | Sichere vertrauenswürdige Speicherung, sichere vertrauliche Speicherung, sichere verschlüsselte Speicherung und/oder sichere Datenserialisierung: Diese SESIP-Sicherheitsansprüche beurteilen die Implementation von sicheren Speichermechanismen, einschließlich Authentizitäts-, Integritäts- und/oder Vertraulichkeitsschutz, je nachdem, welcher Schutz für die gespeicherten Werte erforderlich ist.<br>Kryptographischer KeyStore (Schlüsselspeicher): Dieser SESIP-Sicherheitsanspruch beurteilt, ob das zu bewertende Element einen sicheren Speicherdienst für kryptographisches Material implementiert, der von der Funkanlage zur Speicherung vertraulicher kryptographischer Schlüssel verwendet werden kann. |
| SCM-1 bis SCM-4 | Sichere Kommunikationsunterstützung und sichere Kommunikationsdurchsetzung: Diese SESIP-Sicherheitsansprüche beurteilen die Implementation eines sicheren Kommunikationsmechanismus, einschließlich Authentizität, Integrität, Vertraulichkeit und/oder Replay-Schutz, je nachdem, welcher Schutz für die damit verbundenen Transitwerte erforderlich ist. |
| LGM-1 bis LGM-4 | Erstellung und Speicherung von Auditprotokollen: Mit diesem SESIP-Sicherheitsanspruch wird die Implementation der Erstellung von Auditprotokollen und der sicheren Speicherung durch das zu bewertende Geräteelement beurteilt, das dann in den endgültigen Geräteprotokollierungsmechanismus integriert werden kann.<br>Die explizite Präzisierung kann die Bearbeitung einer Mindestanzahl von Ereignissen und zeitbezogenen Informationen erfordern. |
| DLM-1 | Zurücksetzen der Plattform auf die Werkseinstellungen, Außerbetriebnahme der Plattform und/oder Rückgabe: Diese SESIP-Sicherheitsansprüche beurteilen, dass die Benutzerdaten vor einer Änderung des Lebenszyklus, die eine Rückstellung oder einen Wechsel der Zuständigkeit beinhalten könnte, sicher gelöscht werden.<br>Löschen der Restinformationen: Dieser SESIP-Sicherheitsanspruch beurteilt die Implementation eines sicheren Löschmechanismus für Benutzerdaten, die von einem Geräteelement bearbeitet werden, das bei Bedarf von den oberen Schichten der Anlage ausgelöst werden kann.<br>Sichere Deinstallation von Anwendungen: Dieser SESIP-Sicherheitsanspruch beurteilt die Implementation einer sicheren Deinstallation von Anwendungen, so dass alle Anwendungsdaten zerstört werden. |
| UNM-1 bis UNM-2 | Nicht anwendbar |
| CCK-1 bis CCK-3 | Kryptographische Schlüsselgenerierung: Dieser SESIP-Sicherheitsanspruch beurteilt die Implementation der kryptographischen Schlüsselgenerierung, die von der Funkanlage verwendet werden kann, um CCK-2 zu erfüllen.<br>Alle SESIP-Sicherheitsdienste, die kryptographische Schlüssel beinhalten (kryptographische Dienste, sichere Initialisierung, sichere Aktualisierung, sichere Kommunikation, sichere Speicherung usw.), werden beurteilt, um zu überprüfen, ob diese Schlüssel sicher gehandhabt werden und den bewährten Verfahrensweisen der Kryptographie entsprechen.<br>Eine explizite Präzisierung eines solchen Anspruchs auf Sicherheitsdienste kann verlangen, dass keine statischen Vorgabewerte für vertrauliche kryptographische Schlüssel verwendet werden. |

| Anf.ID | EN 17927:2023 SESIP-Unterstützung – Nachweis der Umsetzung und Bewertung auf der Ebene der Geräteelemente/Teilkomponenten |
|---|---|
| GEC-1 bis GEC-7 | AVA_VAN.SESIP: Diese SESIP-Sicherheitsevaluierungsaufgabe erfordert eine Schwachstellenanalyse der angegebenen Sicherheitsdienstimplementation, bei der:<br>— überprüft wird, ob die zu bewertende Implementation keine öffentlich bekannten, ausnutzbaren Schwachstellen enthält und ob für jeden Lebenszykluszustand nur die benötigten Schnittstellen offengelegt werden.<br>— geprüft wird, ob die notwendige Eingabevalidierung durchgeführt wird.<br>Sichere Entwicklung: Mit diesem SESIP-Sicherheitsanspruch wird beurteilt, ob das zu bewertende Element nach sicheren Entwicklungsregeln entwickelt wurde, wozu auch die Verifizierung der offengelegten Angriffsflächen gehören könnte. Es ist zu beachten, dass die Funkanlagenrichtlinie nur produktspezifische Anforderungen und keine Prozessanforderungen abdeckt, so dass diese Aufgabe eine ergänzende Maßnahme ist.<br>AGD_OPE/PRE: Diese SESIP-Sicherheitsevaluierungsaufgaben erfordern die Dokumentation der Sicherheitsdienste, denen die Benutzer ausgesetzt sind. |
| CRY-1 | Alle Bewertungen von SESIP-Sicherheitsdienstansprüchen, die kryptographische Schlüssel umfassen (kryptographische Dienste, sichere Initialisierung, sichere Aktualisierung, sichere Kommunikation, sichere Speicherung usw.), verifizieren, dass diese Schlüssel sicher gehandhabt werden und den bewährten Verfahrensweisen der Kryptographie entsprechen. |

# Anhang ZA
(informativ)

# Zusammenhang zwischen dieser Europäischen Norm und der Delegierten Verordnung (EU) 2022/30 zur Ergänzung der Verordnung 2014/53/EU des Europäischen Parlaments und des Rates im Hinblick auf die Anwendung der grundlegenden Anforderungen, wie in Artikel 3(3), Punkt (d), Punkt (e) und Punkt (f) dieser abzudeckenden Verordnung in Bezug genommen

Diese Europäische Norm wurde im Rahmen eines von der Europäischen Kommission erteilten Normungsauftrages [C(2022) 5637] und seiner Änderung [C(2023) 5624 final] erarbeitet, um ein freiwilliges Mittel zur Erfüllung der grundlegenden Anforderungen der Verordnung 2014/53/EU [Amtsblatt L 153] des Europäischen Parlaments und des Rates zur Anwendung der in Artikel 3(3) in Bezug genommenen grundlegenden Anforderungen bereitzustellen.

Im Falle von Unterschieden zwischen in dieser Europäischen Norm definierten Begriffen und in der genannten Verordnung definierten Begriffen ist die Verordnung maßgebend.

Sobald diese Norm im Amtsblatt der Europäischen Union im Sinne dieser Delegierten Verordnung (EU) 2022/30 in Bezug genommen worden ist, berechtigt die Übereinstimmung mit den in Tabelle ZA.1 aufgeführten normativen Abschnitten dieser Norm innerhalb der Grenzen des Anwendungsbereiches dieser Norm zur Vermutung der Konformität mit den entsprechenden grundlegenden Anforderungen der Richtlinie 2014/53/EU und der zugehörigen EFTA-Vorschriften.

**Tabelle ZA.1 — Zusammenhang zwischen dieser Europäischen Norm und der Richtlinie 2014/53/EU [Amtsblatt L 153]**

| Grundlegende Anforderungen der Richtlinie 2014/53/EU | Abschnitt(e)/Unterabschnitt(e) dieser EN | Erläuterungen/Anmerkungen |
|---|---|---|
| 3.3.(e) | 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9, 6.10.1, 6.10.2, 6.10.3, 6.10.5, 6.10.6, 6.11 | |

**WARNHINWEIS 1 —** Die Konformitätsvermutung bleibt nur bestehen, solange die Fundstelle dieser Europäischen Norm in der im Amtsblatt der Europäischen Union veröffentlichten Liste erhalten bleibt. Anwender dieser Norm sollten regelmäßig die im Amtsblatt der Europäischen Union zuletzt veröffentlichte Liste einsehen.

**WARNHINWEIS 2 —** Für Produkte, die in den Anwendungsbereich dieser Norm fallen, können weitere Rechtsvorschriften der EU anwendbar sein.

# Literaturhinweise

[1] EN IEC 62443-4-1, *IT-Sicherheit für industrielle Automatisierungssysteme — Teil 4-1: Anforderungen an den Lebenszyklus für eine sichere Produktentwicklung*

[2] EN IEC 62443-4-2, *IT-Sicherheit für industrielle Automatisierungssysteme — Teil 4-2: Technische Sicherheitsanforderungen an Komponenten industrieller Automatisierungssysteme (IACS)*

[3] EN ISO/IEC 27002:2022, *Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre — Informationssicherheitsmaßnahmen*

[4] EN ISO/IEC 24760 (alle Teile), *IT-Sicherheit und Datenschutz — Rahmenwerk für Identitätsmanagement*

[5] ISO/IEC 27555:2021, *Information security, cybersecurity and privacy protection — Guidelines on personally identifiable information deletion*

[6] ETSI EN 303 645, *Cyber Security for Consumer Internet of Things — Baseline Requirements*

[7] ETSI TS 103 701, *Cyber Security for Consumer Internet of Things — Conformance Assessment of Baseline Requirements*

[8] NIST SP 800-57, *Recommendation for Key Management, Part 1 Rev.5*

[9] NIST SP 800-63 (alle Teile), *Digital Identity Guidelines*

[10] NIST SP 800-63B, *Digital Identity Guidelines — Authentication and Lifecycle Management*

[11] NIST SP 800-90A Rev.1, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*

[12] NIST SP 800-90B, *Recommendation for the Entropy Sources Used for Random Bit Generation*

[13] NIST SP 800-90C, *Recommendation for Random Bit Generator (RBG) Constructions*

[14] NIST SP 800-108r1, *Recommendation for Key Derivation Using Pseudorandom Functions*

[15] NIST SP 800-131A Rev.2, *Transitioning the Use of Cryptographic Algorithms and Key Lengths*

[16] NIST SP 800-132, *Recommendation for Password-Based Key Derivation: Part 1: Storage Applications*

[17] NIST SP 800-160, *Engineering Trustworthy Secure Systems*

[18] NIST SP 800-218, *Secure Software Development Framework (SSDF) — Recommendations for Mitigating the Risk of Software Vulnerabilities*

[19] BSI AIS 31, *A Proposal for Functionality Classes for Random Number Generators*

[20] BSI TR-02102 (alle Teile), *Kryptographische Verfahren: Empfehlungen und Schlüssellängen*, Version, 2023-1

[21] FIPS 140-2, *Security Requirements for Cryptographic Modules*

[22] FIPS 140-3, *Security Requirements for Cryptographic Modules*

[23] Guideline “State of the Art” Technical and organisational measures – TeleTrusT, ENISA

[24] SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms

[25] ANSSI PA-79, guide de sélectiond'algorithmes cryptographiques

[26] EPC342-08, European Payments Council publication

[27] ETSI TS 119 312, *Electronic Signatures and Infrastructures; Cryptographic Suites*

[28] ISO/IEC 11770:2010 (alle Teile), *Information technology, Security techniques, Key management*

[29] ISO/IEC 33001:2015, *Information technology, Process assessment, Concepts and terminology*

[30] EN IEC 62443-1-1:2019, *Industrielle Kommunikationsnetze — Netzwerk- und Systemsicherheit — Teil 1-1: Terminologie, Begriffe und Modelle*

[31] Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)

[32] NIST SP 800-172, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

[33] IEC Electropedia, https://www.electropedia.org/

[34] ISO/IEC Guide 51:2014, *Safety aspects, Guidelines for their inclusion in standards*

[35] ENISA Glossary, https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/glossary

[36] Richtlinie 2014/53/EU des Europäischen Parlaments und des Rates vom 16. April 2014 über die Harmonisierung der Rechtsvorschriften der Mitgliedstaaten über die Bereitstellung von Funkanlagen auf dem Markt und zur Aufhebung der Richtlinie 1999/5/EG

[37] Delegierte Verordnung (EU) 2022/30 der Kommission vom 29. Oktober 2021 zur Ergänzung der Richtlinie 2014/53/EU des Europäischen Parlaments und des Rates im Hinblick auf die Anwendung der grundlegenden Anforderungen, wie in Artikel 3(3), Punkt (d), Punkt (e) und Punkt (f) der Richtlinie in Bezug genommen

[38] Leitfaden der Kommission für die Umsetzung der Produktvorschriften der EU 2022 („Blue Guide")

[39] Artikel 2 Absatz 1 der Richtlinie 2009/48/EG „Produkte, die – ausschließlich oder nicht ausschließlich – dazu bestimmt oder gestaltet sind, von Kindern unter 14 Jahren zum Spielen verwendet zu werden", die nicht in Anhang I der Richtlinie 2009/48/EG aufgeführt sind

[40] Artikel 4 Absatz 1 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)

[41] Artikel 2 Buchstabe b der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation)

[42] BSI AIS 20, *Functionality classes and evaluation methodology for deterministic random number generators*

[43] ISO/IEC 18031, *Information technology, Security techniques, Random bit generation*

[44] ISO/IEC TR 27103:2018, *Information technology, Security techniques, Cybersecurity and ISO and IEC Standards*

[45] The NIST Cybersecurity Framework (CSF) 2.0