Verordnung

Nr.…/2024 (… …) des Präsidenten der Aufsichtsbehörde für Regulierungsfragen (SZTFH)

über ein nationales Cybersicherheits-Zertifizierungssystem für IoT-Geräte

Auf der Grundlage der nach Abschnitt 28 Absatz 3 Buchstabe *(c)* des Gesetzes XXIII von 2023 über die Cybersicherheitszertifizierung und Cybersicherheitsaufsicht erteilten Ermächtigung und im Rahmen meiner Aufgaben im Sinne von Abschnitt 13 Buchstaben *(n)* und *(q)* des Gesetzes XXXII von 2021 über die Aufsichtsbehörde für Regulierungsfragen ordne ich Folgendes an:

Abschnitt 1

(1) Für die Zwecke dieser Verordnung bedeutet ein IoT-Gerät ein IKT-Produkt gemäß dem Gesetz XXIII von 2023 über die Cybersicherheitszertifizierung und Cybersicherheitsaufsicht (im Folgenden: Cyberzertifizierungsgesetz), das durch Signalwandlung mit der Umwelt interagiert. Die Form der Interaktion kann sein
(a) Erkennung, durch die das IoT-Gerät Daten über die Umgebung sammelt oder
(b) ein Eingriff, der Veränderungen in der Umwelt auslöst.

(2) Die Interaktion mit der in Absatz 1 genannten Umwelt kann erfolgen durch:
(a) eine Schnittstelle zur Anwendungsprogrammierung (im Folgenden: API), die es anderen Computergeräten ermöglicht, über die vom IoT-Gerät bereitgestellte Anwendung mit einem IoT-Gerät zu kommunizieren,
(b) eine Benutzeroberfläche, die eine direkte Kommunikation zwischen dem IoT-Gerät und dem Benutzer ermöglicht, oder
(c) eine Netzwerkverbindung, die die Kommunikation des IoT-Geräts mit einem elektronischen Kommunikationsnetz zum Zwecke der Kommunikation von oder zu einem IoT-Gerät gewährleistet oder den Zugriff auf die Netzwerkbenutzerschnittstelle gewährleistet.

(3) Für die Zwecke der Anwendung von Absatz 2 Buchstabe *(c)*, die Fähigkeit der Schnittstelle, eine Netzwerkverbindung herzustellen, umfasst sowohl die Hardware- als auch die Softwareumgebung, die sie betreibt und bedient.

Abschnitt 2

(1) Diese Verordnung gilt mit Ausnahme der Absätze 2 und 3 für die Selbstbewertung der IoT-Geräte und Konformitätsbewertung (im Folgenden zusammenfassend als: Bewertung).

(2) Die Verordnung erstreckt sich nicht auf die Bewertung von IoT-Werkzeugen, für die ein nationales Cybersicherheits-Zertifizierungssystem durch den Präsidenten der Aufsichtsbehörde für Regulierungsfragen (SZTFH) in einer gesonderten Verordnung eingeführt wurde.

(3) Das nationale Cybersicherheits-Zertifizierungssystem für IoT-Geräte (im Folgenden: das Zertifizierungssystem) soll sicherstellen, dass Entscheidungen von Bürgern, Unternehmen und öffentlichen Stellen bei der Beschaffung von IoT-Produkten unterstützt werden und dass die Vermögenswerte auf der Grundlage der im Zertifizierungssystem festgelegten Zuverlässigkeitsniveaus vergleichbar sind.

Abschnitt 3

(1) Das Zertifizierungssystem enthält Anforderungen an die Zuverlässigkeitsniveaus „grundlegend“, „signifikant“ und „hoch“ im Sinne von Abschnitt 8 Absatz 1 Cyberzertifizierungsgesetz.

(2) Auf der Grundlage des Zertifizierungssystems kann die Selbstbewertung der Konformität auf der Ebene der „grundlegenden“ Zuverlässigkeitsniveaus durchgeführt werden.

(3) Konformitätsbewertungen durch Konformitätsbewertungseinrichtungen können höchstens auf dem Zuverlässigkeitsniveau durchgeführt werden, das von der Aufsichtsbehörde für Regulierungsfragen als nationale Zertifizierungsstelle für Cybersicherheit gemäß Abschnitt 4 Absatz 1 Buchstabe (a) des Cyberzertifizierungsgesetzes registriert wurde (im Folgenden: Zertifizierungsbehörde), und zwar auf Antrag des Herstellers nach dem Cyberzertifizierungsgesetz (im Folgenden: Hersteller).

Abschnitt 4

(1) Ein Hersteller kann ein nationales Selbstbewertungsverfahren für die Konformität einleiten, oder eine Konformitätsbewertungsstelle kann die Konformitätsbewertungstätigkeiten aufnehmen, wenn die in Anlage 1 genannten und vom Hersteller angefertigten Unterlagen vorliegen. Eine Stichprobe der in Anlage 1 genannten Dokumente wird auf der Webseite der Zertifizierungsbehörde veröffentlicht.

(2) Die nationale Konformitätserklärung oder das nationale Cybersicherheitszertifikat (zusammen: nationales Zertifikat) darf nur für das gegebene Zuverlässigkeitsniveau ausgestellt werden, wenn das zu bewertende IoT-Gerät die Anforderungen in Anlage 2 für dieses Zuverlässigkeitsniveau erfüllt.

(3) Die Einhaltung der Vorschriften gemäß Absatz 2 kann durch Vorlage des Bewertungsberichts nachgewiesen werden, der auf der Grundlage einer nach der Bewertungsmethodik in Anlage 4 (im Folgenden: Bewertungsbericht) oder durch Durchführung eines Anfälligkeitstests für die in Anlage 3 genannten Anforderungen.

(4) Zertifikate, die auf der Grundlage einer internationalen, europäischen oder nationalen Norm ausgestellt wurden, werden anstelle der erforderlichen Informationen gemäß Absatz 3 nicht zum Nachweis der Einhaltung gemäß Absatz 2 akzeptiert.

(5) Ein Hersteller kann eine Konformitätserklärung gemäß Anlage 5 ausstellen, und eine Konformitätsbewertungsstelle kann ein nationales Cybersicherheitszertifikat gemäß Anlage 6 ausstellen, wenn der Bewertungsbericht zusammen positive Ergebnisse mit einem „Bestanden“ liefert.

(6) Der Hersteller oder die Konformitätsbewertungsstelle übermittelt der Zertifizierungsbehörde das nationale Zertifikat, die in Anlage 1 genannten Unterlagen und den Bewertungsbericht zur Registrierung mittels eines von der Zertifizierungsbehörde zu diesem Zweck erstellten elektronischen Formulars.

(7) Die Verwaltungsfrist für die Registrierung gemäß Absatz 6 beträgt 45 Tage.

Abschnitt 5

(1) Die Gültigkeitsdauer des nationalen Zertifikats (im Folgenden: Gültigkeitsdauer) beträgt maximal 365 Tage ab Ausstellungsdatum.

(2) Der Hersteller bringt das in Anlage 7 genannte Etikett als Konformitätskennzeichnung an einem IoT-Gerät an, bei dem bis zum Ende der Gültigkeitsdauer ein nationales Zertifikat erstellt wurde, und das Etikett muss den Inhalt aufweisen, der in der Entscheidung der Zertifizierungsbehörde angegeben ist.

(3) Während der Gültigkeitsdauer führt der Hersteller kontinuierlich und fortlaufend Folgenabschätzungen für jede Änderung durch, die sich auf ein IoT-Gerät auswirkt, wobei Folgendes angegeben wird:

(a) das Änderungsdatum,
(b) der Änderungsgrund;
(c) ob sich die Änderung auf die vor der Änderung hergestellten IoT-Geräte auswirkt,
(d) eine detaillierte Beschreibung der Elemente der Änderung,
(e) welche Risiken von der Veränderung betroffen sind und
(f) ob die Änderung eine Schwachstelle beseitigt oder eine neue Sicherheitskontrolle einführt.

(4) Für die Zwecke des Absatzes 3 gilt jede Änderung, die sich auf den Sicherheitsstatus des IoT-Geräts auswirkt, einschließlich der Entstehung neuer Bedrohungen und Schwachstellen, als Änderung.

(5) Der Hersteller aktualisiert das in Anlage 1 genannte Umsetzungsdokument kontinuierlich und fortlaufend während der Gültigkeitsdauer.

Abschnitt 6

(1) Der Hersteller kann mit Ausnahme von Absatz 5 einen Antrag auf Aufrechterhaltung der Gültigkeit der nationalen Konformitätserklärung im Register der Zertifizierungsbehörde stellen (im Folgenden: ein Antrag auf Aufrechterhaltung), der der Zertifizierungsbehörde mittels eines von der Zertifizierungsbehörde zu diesem Zweck erstellten elektronischen Formulars spätestens 60 Tage vor Ablauf der Gültigkeitsdauer, spätestens jedoch 30 Tage vor Ablauf der Gültigkeitsdauer übermittelt wird.

(2) Dem Antrag auf Aufrechterhaltung sind die Sicherheitsfolgenabschätzung gemäß Abschnitt 5 Absatz 3, das Umsetzungsdokument (siehe Anlage 1) in seiner aktualisierten Fassung gemäß Abschnitt 5 Absatz 3 beizufügen und die neue beantragte Gültigkeitsdauer, die 365 Tage nicht überschreiten darf, soll im Antrag genannt werden.

(3) Während des Aufrechterhaltungsverfahrens beträgt die Verwaltungsfrist der Zertifizierungsbehörde 30 Tage.

(4) Die Zertifizierungsbehörde kann eine von der im Antrag auf Aufrechterhaltung angegebenen Gültigkeitsdauer abweichende Gültigkeitsdauer festlegen, die jedoch mindestens 120 Tage ab dem Ende der ursprünglichen Gültigkeitsdauer berechnet werden sollte, wenn nicht festgestellt werden kann, dass das betreffende IoT-Gerät bei den zu prüfenden Änderungen des IoT-Geräts kontinuierlich den Anforderungen des Zertifizierungssystems entspricht und die Erreichung der Sicherheitsziele ab dem Tag der Ausstellung der nationalen Konformitätserklärung gewährleistet. Beträgt die im Antrag auf Aufrechterhaltung angegebene neue Gültigkeitsdauer weniger als 120 Tage, so legt die Zertifizierungsbehörde die neue Gültigkeitsdauer gemäß dem Antrag fest.

(5) In dem in Absatz 4 genannten Fall darf der Hersteller keinen anderen (weiteren) Antrag auf Aufrechterhaltung für die Konformitätserklärung stellen, der für das betreffende IoT-Gerät ausgestellt wurde.

(6) In dem in Absatz 4 genannten Fall oder wenn die Gültigkeitsdauer der für das IoT-Gerät ausgestellten Konformitätserklärung abgelaufen ist, kann der Hersteller bei der Zertifizierungsbehörde beantragen, die nationale Konformitätserklärung für das IoT-Gerät mit einem von der Zertifizierungsbehörde zu diesem Zweck erstellten elektronischen Formular zu verlängern.

(7) Dem Antrag nach Absatz 6 ist die neue Konformitätserklärung beizufügen, die gemäß Abschnitt 4 Absatz 5 auf der Grundlage der Prüfung gemäß Abschnitt 4 Absätze 1 bis 4, der in Anlage 1 genannten Unterlagen und des Bewertungsberichts ausgestellt wurde.

(8) Die in Absatz 6 genannte Frist für das Verlängerungsverfahren beträgt 45 Tage.

(9) Die Absätze 1 bis 4 gelten für die Aufrechterhaltung der Gültigkeit einer neuen Konformitätserklärung, die von der Zertifizierungsbehörde auf der Grundlage eines Antrags nach Absatz 6 registriert wurde.

Abschnitt 7

(1) Zur Verlängerung der Gültigkeitsdauer des Zertifikats für ein bestimmtes IoT-Gerät, das auf der Grundlage eines von einer Konformitätsbewertungsstelle ausgestellten nationalen Cybersicherheitszertifikats registriert wurde, stellt der Hersteller der Konformitätsbewertungsstelle innerhalb von 60 Tagen vor Ablauf der Gültigkeitsdauer Folgendes zur Verfügung: die Sicherheitsfolgenabschätzung nach Abschnitt 5 Absatz 3 und das Umsetzungsdokument (siehe Anlage 1) in seiner aktualisierten Fassung gemäß Abschnitt 5 Absatz 5.

(2) Auf der Grundlage der Prüfung der in Absatz 1 genannten Dokumente, sofern das IoT-Gerät auch bei den Änderungen des zu prüfenden IoT-Geräts kontinuierlich die Anforderungen des Zertifizierungssystems erfüllt und die Erreichung der Sicherheitsziele ab der Ausstellung des nationalen Cybersicherheitszertifikats gewährleistet, verlängert es das auslaufende Zertifikat spätestens 8 Tage vor Ablauf der Gültigkeitsdauer, wobei die neue Gültigkeitsdauer 365 Tage nach Ablauf der ursprünglichen Gültigkeitsdauer nicht überschreitet.

(3) Kann auf der Grundlage der in Absatz 1 genannten Dokumente nicht festgestellt werden, dass das geprüfte IoT-Gerät ab dem Tag der Ausstellung des nationalen Cybersicherheitszertifikats kontinuierlich die Anforderungen des Zertifizierungssystems erfüllt und die Erreichung der Sicherheitsziele sicherstellt, so kann die Konformitätsbewertungsstelle das abgelaufene Zertifikat unter der Bedingung verlängern, dass die neue Gültigkeitsdauer 90 Kalendertage ab dem Ende der ursprünglichen Gültigkeitsdauer nicht überschreitet.

(4) In dem in Absatz 3 genannten Fall darf die Gültigkeitsdauer des nationalen Cybersicherheitszertifikats, das für ein bestimmtes IoT-Gerät ausgestellt wurde, nach Ablauf der in Absatz 3 genannten neuen Gültigkeitsdauer nicht verlängert werden. Stattdessen kann seine Erneuerung eingeleitet werden.

(5) Der Hersteller kann die Erneuerung des nationalen Cybersicherheitszertifikats des IoT-Geräts bei der Konformitätsbewertungsstelle in dem in Absatz 3 genannten Fall oder nach Ablauf der Gültigkeitsdauer des nationalen Cybersicherheitszertifikats einleiten.

(6) Im Rahmen der Erneuerung legt die Konformitätsbewertungsstelle mittels eines von der Zertifizierungsbehörde zu diesem Zweck erstellten elektronischen Formulars Folgendes zur Registrierung vor: das neue nationale Cybersicherheitszertifikat, das gemäß Abschnitt 4 Absatz 5 auf der Grundlage der Prüfung nach Abschnitt 4 Absätze 1 bis 4 ausgestellt wurde, sowie die in Anlage 1 genannten Unterlagen und den Bewertungsbericht.

Abschnitt 8

Die Gültigkeitsdauer des nationalen Zertifikats bleibt unberührt, wenn während der Gültigkeitsdauer für das IoT-Gerät ein neues nationales Cybersicherheits-Zertifizierungssystem nach Abschnitt 2 Absatz 2 eingeführt wird, aber danach die Gültigkeitsdauer des nationalen Zertifikats für das IoT-Gerät nicht verlängert, ein Wartungsantrag nicht gestellt und das nationale Zertifikat nicht verlängert werden darf.

Abschnitt 9

Diese Verordnung tritt am dritten Tag nach ihrer Veröffentlichung in Kraft.

Abschnitt 10

Der Verpflichtung zur Notifizierung des vorliegenden Verordnungsentwurfs gemäß Artikel 5 bis 7 der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft wurde nachgekommen.

Dokumentationsanforderungen

1. Identifikationsdokument des IoT-Geräts

1.1. Das Dokument mit Informationen zur Identifizierung des IoT-Geräts, das einer Konformitäts-Selbstbewertung oder Konformitätsbewertung unterliegt (im Folgenden: VE), die möglichst detaillierte Informationen zum Prüfungsgegenstand enthält, insbesondere in Bezug auf Versionsnummern und Konfigurationsmöglichkeiten.

1.2. Mindestinhalt des Identifizierungsdokuments:

a) Name des zu untersuchenden Produkts
b) Markenbezeichnung
c) Handelsbezeichnung
d) Modell-ID
e) Hardwarekonfiguration (einschließlich Freigabenummer und Seriennummer)
f) Laufumgebung oder Betriebssystem
g) Firmware-Version im Werkszustand
h) Details zum Hersteller:
   (ha) Name
   (hb) Kurzbezeichnung
   (hc) eingetragene Anschrift
   (hd) Telefonnummer
   (he) E-Mail-Adresse
   (hf) Kontaktdaten: Name, Staatsangehörigkeit, Telefonnummer, E-Mail-Adresse
i) Geplante jährliche Anzahl der produzierten Artikel in Bezug auf VE
j) Angabe der Handelsmärkte, auf denen das untersuchte Produkt voraussichtlich im folgenden Jahr verkauft werden soll:
   (ia) nur Ungarn
   (ib) EU-Mitgliedstaaten (falls nicht in der EU insgesamt, Liste der Mitgliedstaaten) oder
   (ic) sonstige
k) Angabe des Zuverlässigkeitsniveaus, mit dem der Test durchgeführt wird: grundlegend/signifikant/hoch

2. Umsetzungsdokument

2.1. Das Umsetzungsdokument (im Folgenden: MD) enthält detaillierte Informationen, die für die Bewertung der Anforderungen in Anlage 2 relevant sind, die bei der Umsetzung des gemäß Nummer 1 ermittelten IoT-Instruments verwendet werden.

2.2. Mindestinhalt des MD

2.2.1. MD 1-UserInfo: Benutzerinformationen

Das MD listet die Dokumentation, Veröffentlichungen und Informationen, die den Benutzern zur Verfügung gestellt werden. Dazu gehören sowohl die Website des Herstellers als auch die entsprechende URL, das Benutzerhandbuch oder die integrierte Hilfe. Die Liste enthält Informationen über die Funktionsweise der folgenden unabhängigen Funktionen und Mechanismen:

	A	**B**
1.	Dokumentation der Änderungsmechanismen	Dokumentation der Mechanismen zur Änderung der Authentifizierungswerte für den Benutzer, einschließlich aller Informationen, die für den Zugriff auf die Dokumentation erforderlich sind.
2.	Dokumentation der Sensoren	Für den Benutzer bestimmte Dokumentation mit Informationen im Zusammenhang mit externen Erfassungsfunktionen, einschließlich aller für den Zugriff auf die Dokumentation erforderlichen Informationen.
3.	Dokumentation der sicheren Einstellung	Die Methodik der Benutzerdokumentation für die sichere Konfiguration von VE, einschließlich aller Informationen, die für den Zugriff auf die Dokumentation erforderlich sind.
4.	Dokumentation der Einrichtungsprüfung	Eine Beschreibung, wie die Methode zur Überprüfung der sicheren Konfiguration von VE für den Benutzer dokumentiert wird, einschließlich aller Informationen, die für den Zugriff auf die Dokumentation erforderlich sind.
5.	Dokumentation personenbezogener Daten	Die Art und Weise, auf die die Informationen über die Verarbeitung personenbezogener Daten für den Benutzer dokumentiert werden, einschließlich aller Informationen, die für den Zugriff auf die Dokumentation erforderlich sind.
6.	Dokumentation von Telemetriedaten	Die Art und Weise, auf die die Informationen über die Erfassung von Telemetriedaten für den Benutzer dokumentiert werden, einschließlich aller Informationen, die für den Zugriff auf die Dokumentation erforderlich sind.
7.	Dokumentation der Löschung	Eine für den Nutzer bestimmte Beschreibung, wie personenbezogene Daten gelöscht werden, einschließlich aller Informationen, die für den Zugriff auf die

		Dokumentation erforderlich sind.
8.	Modellbezeichnung	Eine Angabe des VE-Modells und eine kurze Beschreibung, wie die VE-Modellbezeichnung vom Benutzer erkannt werden kann. Hier soll es angegeben erden, ob die Versionsnummer von VE und dessen Softwarekomponenten mittels einer Netzwerkabfrage abgerufen werden kann und wie es gemacht wird. Wenn Open-Source-Software verwendet wird, sollten hier die Kernel- und Anwendungsversionen des Open-Source-Betriebssystems und ihre Zeit der langfristigen Unterstützung (LTS) angegeben werden.
9.	Unterstützungszeitraum	Der Zeitraum, in dem das Produkt oder die Dienstleistung vom Hersteller gewartet wird, z. B. in Form von Updates, einschließlich Kernel- und Anwendungsversionen der Open-Source-Betriebssysteme.
10.	Veröffentlichung des Unterstützungszeitraums	Die Art und Weise, auf die der Unterstützungszeitraum für den Benutzer veröffentlicht und dokumentiert wird, einschließlich aller Informationen über den Zugriff auf die Veröffentlichung.
11.	Offenlegung der Schwachstellen	Die Art und Weise, wie Schwachstellen offengelegt werden, einschließlich aller Informationen über den Zugang zur Offenlegung.
12.	Veröffentlichung von nicht aufrüstbaren Komponenten	Eine Beschreibung der Gründe für das Fehlen von Software-Updates, einschließlich aller Informationen, die für den Zugriff auf die Veröffentlichung erforderlich sind.

2.3.2. MD 2-SecDev: Sichere Entwicklungsprozesse

Das MD listet alle sicheren Entwicklungsprozesse auf, die der Hersteller durchgeführt oder für VE umgesetzt hat. Das MD enthält die folgenden Einträge

	A	**B**
1.	ID	Eindeutige Kennung für jeden Prozess, beginnend mit SecDev-1.
2.	Beschreibung	Eine kurze Beschreibung des sicheren Entwicklungsprozesses. Wird eine bestehende Norm verwendet, ist ein Verweis auf die entsprechende Norm anzugeben. Es sollte eine Beschreibung der angewandten Programmiertechniken enthalten sein, um nachzuweisen, dass sie geeignet sind, Manipulationen, Fehler und Leckageangriffe zu mildern.

2.3.3. MD 3-VulnTypes: Relevante Schwachstellen

Das MD listet jede Art von Schwachstellen auf, die für VE relevant ist. Das MD muss folgende Einträge enthalten:

	A	B
1.	ID	Eindeutige Kennung für jede Schwachstelle, beginnend mit VulnTypes-1.
2.	Beschreibung	Eine kurze Beschreibung der für VE relevanten Schwachstelle.
3.	Maßnahme	Wenn Schwachstelle festgestellt wird, eine Beschreibung der Art und Weise, auf die Maßnahmen in Bezug auf diese Art von Schwachstelle ergriffen werden, einschließlich aller an der Maßnahme beteiligten Organisationen und ihrer Verantwortlichkeiten.
4.	Zeitrahmen	Ein spezieller Zeitrahmen, in dem im Falle einer Schwachstelle spezifische Handlungsschritte geplant werden. Beispiel: 5 Tage für die erste Antwort und 90 Tage, bis die Korrektur veröffentlicht wird.

2.3.4. MD 4-Conf: Stellungnahmen, Erklärungen

Das MD listet die Erklärungen für die verschiedenen Prozesse auf. Das MD enthält die folgenden unabhängigen Einträge, für die klare JA- oder NEIN-Antworten angegeben werden sollten.

	A	B
1.	Bestätigung von Schwachstellenhandlungen	Bestätigung, dass für jede in MD 3-VulnTypes beschriebene „Handlung“ die erforderliche Infrastruktur zur Verfügung steht und dass die Betreiber informiert wurden, um den angestrebten „Zeitrahmen“ zu erreichen.
2.	Bestätigung der Schwachstellenüberwachung	Bestätigung, dass die erforderliche Infrastruktur vorhanden ist, um jede in MD 5-VulnMon beschriebene Schwachstelle zu überwachen, zu identifizieren und zu korrigieren, und dass die Betreiber informiert wurden.
3.	Bestätigung der Aktualisierungsverfahren	Bestätigung, dass für jedes in MD 6-UpdProc beschriebenen Aktualisierungsverfahren die notwendige Infrastruktur zur Verfügung steht und dass die Betreiber informiert wurden, um den angestrebten „Zeitrahmen“ zu erreichen.
4.	Bestätigung des sicheren Managements	Bestätigung, dass die in MD 15-SecMgmt beschriebenen Verfahren des sicheren Managements etabliert wurden.
5.	Bestätigung der sicheren Entwicklung	Bestätigung, dass die in MD 2-SecDev beschriebenen sicheren Entwicklungsverfahren etabliert wurden.

2.3.5. MD 5-VulnMon: Schwachstellenüberwachung

Das MD listet alle Verfahren zur Überprüfung, Identifizierung und Korrektur von Schwachstellen mit den folgenden Einträgen auf.

	A	B
1.	ID	Eindeutige Kennung für jedes Verfahren, beginnend mit VulnMon-1.
2.	Beschreibung	Eine Beschreibung, wie Sicherheitslücken in Produkten und Dienstleistungen nachverfolgt, identifiziert und behoben werden können.

2.3.6. MD 6-UpdProc: Aktualisierungsverfahren

Das MD listet die Verfahren des Herstellers für die Ausgabe von Sicherheitsupdates mit den folgenden Daten auf:

	A	B
1.	ID	Eindeutige Kennung für jedes Verfahren, beginnend mit UpdProc-1.
2.	Beschreibung	Eine kurze Beschreibung des Verfahrens für die Ausgabe von Sicherheitsupdates, einschließlich aller Organisationen und Verantwortlichkeiten.
3.	Zeitrahmen	Der geplante Zeitrahmen für den Abschluss des Verfahrens.

2.3.7. MD 7-Intf: Schnittstellen

Das MD listet alle netzwerkbezogenen, physikalischen und logischen Schnittstellen von VE mit den folgenden Parametern auf:

	A	B
1.	ID	Eindeutige Kennung für jede Schnittstelle, beginnend mit Intf-1.
2.	Beschreibung	Beschreibung der Schnittstelle, einschließlich ihres Zwecks. Bei physikalischen Schnittstellen ist auch zu beschreiben, ob die Schnittstelle immer notwendig ist, oder nur in bestimmten Fällen, wie in der Beschreibung angegeben (z. B. Verwendung mit Unterbrechungen) oder ob sie nie erforderlich ist.
3.	Typ	Angabe, ob die Schnittstelle netzwerkbezogen, physikalisch (einschließlich drahtloser Schnittstellen), logisch oder vom mehrfachen Typ ist.
4.	Status	Angabe, dass die Schnittstelle im initialisierten Zustand aktiviert oder deaktiviert ist. Bei autorisierten Schnittstellen ist eine Erklärung erforderlich.
5.	Statusänderung	Eine Liste der Schnittstellenzustände, die angibt, wie und mit welcher Rolle die Statusänderungen durch den Benutzer ausgelöst werden können, unter Berufung auf die Rolle gemäß MD 9-Role.
6.	Struktur der Beziehung	Beschreibung, wie die Schnittstelle die Verbindung aufbaut, welche Validierungs- und Authentifizierungsmechanismen sie verwendet, unter Bezugnahme auf den Authentifizierungsmechanismus nach MD-10-Auth.
7.	Veröffentlichte Informationen	Wenn die Schnittstelle eine Netzwerkschnittstelle ist: eine Beschreibung der im initialisierten Zustand ohne Authentifizierung offengelegten Informationen und die Gründe für ihre Offenlegung sowie eine Angabe, ob die Offenlegung für Informationssicherheitszwecke relevant ist.
8.	Debugging-Schnittstelle	Wenn die Schnittstelle eine physikalische Schnittstelle ist: ob die Schnittstelle als Debugging-Schnittstelle verwendet werden kann.

9.	Schutz	Wenn die Schnittstelle eine physikalische Schnittstelle ist: Beschreibung der Schutzmethoden, die erforderlich sind, um die Exposition der Schnittstelle zu begrenzen. Im Falle von Debugging-Schnittstellen ist es erforderlich, den Softwaremechanismus zu beschreiben, der zur Deaktivierung der Schnittstelle verwendet wird.

2.3.8. MD 8-DevID: Gerätekennungen

Alle VE-Kennungen, die zur Identifizierung des Produkts verwendet werden, sind in das MD aufzunehmen.

	A	**B**
1.	ID	Eine eindeutige Kennung für jede Gerätekennung, beginnend mit DevID-1.
2.	Typ der Kennung	Informationen über die Form der Kennung (Etikett, physikalische oder logische Kennung) und ihre Einzigartigkeit.
3.	Zugänglichkeit der Kennung	Mit welcher Rolle und wie kann die ID vom Benutzer in jedem Zustand des Geräts (originalverpackt, Werkseinstellung und Einrichtung) identifiziert werden. Sofern über die Identifikationsschnittstelle verfügbar, ist auf die Schnittstelle MD 7-Intf zu verweisen.
4.	Kennungsquelle	„Vorinstalliert“ oder „Kann vom Benutzer hinzugefügt werden“.
5.	Generierungsmechanismus für Kennungen	Eine kurze Beschreibung des Algorithmus, der zur Generierung der Kennung verwendet wird, wobei die Maßnahmen beschrieben werden, um auf risikoverhältnismäßige Weise sicherzustellen, dass die Kennungen das Risiko automatischer Angriffe verringern, die auf offensichtlichen Regelmäßigkeiten, bestimmten Zeichenfolgen, öffentlich zugänglichen Informationen oder unzureichender Komplexität aufbauen.
6.	Ausführung von Vorgängen	Eine Beschreibung der Vorgänge, die in Kenntnis der Kennung durchgeführt werden können, und die Art und Weise, auf die sie ausgeführt werden, unter Bezugnahme auf die Schnittstellen nach MD 7-Intf, die am Vorgang beteiligt sind.
7.	Sicherheitsziele	Eine Beschreibung der erreichten Sicherheitsziele und der Bedrohungen, auf die der Mechanismus ausgerichtet sein sollte.
8.	Brute-Force-Schutz	Wenn die Kennung direkt von einer Netzwerkschnittstelle aus zugegriffen werden kann, ist das eine Beschreibung der Methode, die entwickelt wurde, um zu verhindern, dass der Angreifer die Identifizierungsdaten durch einen Brute-Force-Angriff über die Netzwerkschnittstellen erhält.

9.	Schutz vor Timing-Angriffen	Wenn der Identifikator direkt über eine Netzwerkschnittstelle verfügbar ist, ist das eine Beschreibung der Methode, die entwickelt wurde, um zu verhindern, dass der Angreifer durch Ausnutzen von Timings eine unbefugte Autorisierung erhält.

2.3.9. MD 9-Role: Rollen

Das MD soll die Rollen enthalten, die von VE im Werkszustand behandelt werden, einschließlich Akteure, die keiner Identifizierung unterliegen und sogar der Maschine-zu-Maschine-Verbindungen.

	A	**B**
1.	ID	Eindeutige Kennung für jede Rolle, beginnend mit Role-1.
2.	Beschreibung	Eine kurze Beschreibung der Rolle.
3.	Zweck	Der allgemeine Zweck der Benutzer in der Rolle.
4.	Vorgänge	Eine Liste von Aktionen, die von den Benutzern in der Rolle ausgeführt werden können.

2.3.10. MD 10-AuthMech: Authentifizierungsmechanismen.

Alle VE-Authentifizierungsmechanismen sind in das MD aufzunehmen. Das MD muss folgende Einträge enthalten:

	A	**B**
1.	ID	Eindeutige Kennung für jeden Authentifizierungsmechanismus, beginnend mit AuthMech-1.
2.	Beschreibung	Eine kurze Beschreibung des Authentifizierungsmechanismus und des zugehörigen Autorisierungsverfahrens. Angeben, ob der Mechanismus für die Benutzerauthentifizierung oder die Maschine-zu-Maschine-Authentifizierung verwendet wird und ob auf ihn direkt über eine Netzwerkschnittstelle zugegriffen werden kann. Im Falle einer Umsetzung durch Dritte sollte erläutert werden, wie das Design der Lieferkette den Verlust von VE-spezifischen Anmeldeinformationen verhindert.
3.	Authentifizierungsfaktor	Typ des Attributs, das für die Authentifizierung verwendet wird. Bei Passwörtern ist auch anzugeben, ob das Passwort vom Benutzer im initialisierten Zustand gesetzt und verwendet wird.
4.	Passwortgenerierungsmechanismus	Wenn es sich bei dem Authentifizierungsfaktor um ein Passwort handelt, das vom Benutzer nicht

		festgelegt wurde, ist das eine Beschreibung des Mechanismus zur Generierung des Passworts, wobei darauf hingewiesen wird, dass keine detaillierte Beschreibung erforderlich ist. In der Beschreibung ist anzugeben, ob das Passwort für jedes Gerät eindeutig ist und ob es vorinstalliert ist, sie soll die Maßnahmen beschreiben, mit denen sichergestellt wird, dass Passwörter für jedes Gerät in einem anderen Zustand als Werksvoreinstellung eindeutig sind und dass das Risiko automatischer Angriffe verringert wird, die auf offensichtlichen Regelmäßigkeiten, gemeinsamen Zeichenketten, öffentlich zugänglichen Informationen oder unangemessener Komplexität aufbauen, wenn solche Passwörter als vorinstallierte und einmalige Passwörter pro Gerät verwendet werden.
5.	Sicherheitsgarantien	Eine Beschreibung der erreichten Sicherheitsziele und der Bedrohungen, auf die der Mechanismus ausgerichtet sein sollte.
6.	Kryptografische Details	Eine Beschreibung der kryptographischen Methoden (Protokolle, Operationen, Primitiven, Modi und Schlüsselgrößen), die zur Bereitstellung des Authentifizierungsmechanismus und zur Erleichterung der beschriebenen „Sicherheitsgarantien“ unter Berücksichtigung des Schlüsselmanagements verwendet werden.
7.	Brute-Force-Schutz	Wenn der Authentifizierungsmechanismus direkt über eine Netzwerkschnittstelle verfügbar ist, ist das eine Beschreibung der Methode, die entwickelt wurde, um zu verhindern, dass der Angreifer die Authentifizierungsdetails durch einen Brute-Force-Angriff über die Netzwerkschnittstellen erhält.
8.	Schutz vor Timing-Angriffen	Wenn der Authentifizierungsmechanismus direkt über eine Netzwerkschnittstelle verfügbar ist, ist das eine Beschreibung der Methode, mit der verhindert werden soll, dass der Angreifer durch das Ausnutzen von Timings eine unbefugte Autorisierung erhält.
9.	Individualisierung	Einstellungsoptionen, die mit dem Authentifizierungsmechanismus verknüpft sind.
10.	Anwendung	Die Rollen von Schnittstellen und Benutzern, die den Authentifizierungsmechanismus verwenden, mit Bezug auf Schnittstellen nach MD 7-Intf und Rollen nach MD 9-Role.
11.	Handhabung.	Beschreibung des Prozesses der Änderung der Authentifizierungskennung.

2.3.11. MD 11-Account: Kontomanagement

Das MD enthält Lösungen im Zusammenhang mit der Verwaltung von Benutzerkonten.

	A	B
1.	ID	Einmalige Kennung für jede Aktion und Lösung, beginnend mit Account-1.
2.	Vorgang	Name des Vorgangs.
3.	Beschreibung	Eine detaillierte Beschreibung des Mechanismus des ausgeführten Vorgangs.
4.	Konfiguration	Eine Beschreibung, welche Daten im Kontoverwaltungsvorgang für Benutzer mit welcher Art von Rollen nach MD 9-Role konfiguriert werden können.

2.3.12. MD 12-SoftComp: Softwarekomponenten

Das MD listet alle Softwarekomponenten von VE auf. Der angewandte Detaillierungsgrad für die Aufteilung der untersuchten Software in Softwarekomponenten soll erkennen, welche Komponenten aktualisiert werden können und welche im Falle eines Anfälligkeitstests nicht möglich sind. Das MD enthält die folgenden Einträge.

	A	B
1.	ID	Eindeutige Kennung für jede Softwarekomponente, beginnend mit SoftComp-1.
2.	Beschreibung	Eine kurze Beschreibung der Software-Komponente. Bitte gesondert angeben, ob das Update der Softwarekomponente sensible Daten enthält.
3.	Aktualisierungsmechanismus	Verweis auf die Aktualisierungsmechanismen nach MD 13-UpdMech, die zum Aktualisieren der Softwarekomponente verwendet werden. Eine leere Liste von Aktualisierungsmechanismen zeigt den Ausfall von Aktualisierungen von Softwarekomponenten an, und das Fehlen solcher Updates muss begründet werden.
4.	Kryptografische Verwendung	Gibt an, ob die Softwarekomponente kryptographische Algorithmen oder Primitiven (ja/nein) verwendet und wenn ja, ob der Hersteller die Nebenwirkungen der Aktualisierung dieser Algorithmen und Primitiven berücksichtigt hat (ja/nein).

2.3.13. MD 13-UpdMech: Aktualisierungsmechanismen

Das MD listet alle Aktualisierungsmechanismen von VE auf, für die folgende Einträge enthalten sind.

	A	B

1.	ID	Eindeutige Kennung für jeden Aktualisierungsmechanismus, beginnend mit UpdMech-1.
2.	Beschreibung	Eine kurze Beschreibung des Aktualisierungsmechanismus, einschließlich seiner Hauptmerkmale. Darüber hinaus muss angegeben werden, ob die Bereitstellung des Updates netzwerkbasiert ist.
3.	Sicherheitsgarantien	Eine Beschreibung der erreichten Sicherheitsziele und der mit dem Mechanismus zu bewältigenden Bedrohungen. Außerdem ist aus Gründen der Authentizität und Integrität anzugeben, ob die Sicherheitsgarantie von der VE selbst erbracht wird.
4.	Kryptografische Details	Eine Beschreibung der kryptographischen Methoden (Protokolle, Operationen, Primitiven, Modi und Schlüsselgrößen), die verwendet werden, um die Sicherheit des Aktualisierungsmechanismus des Schlüsselmanagements zu gewährleisten und die beschriebenen „Sicherheitsgarantien“ zu erleichtern. Methode zur Installation öffentlicher Schlüssel zur Verifizierung.
5.	Initiierung und Interaktion	Eine kurze Beschreibung, wie das Update gestartet wird, und eine kurze Beschreibung der Benutzerinteraktion, die für die Initiierung und Anwendung des Updates erforderlich ist, wobei anzugeben ist, ob es sich um einen automatischen Aktualisierungsmechanismus handelt.
6.	Konfiguration	Eine kurze Beschreibung, wie der Benutzer die Automatisierung und Benachrichtigung von Software-Updates konfigurieren kann und aus welchen Optionen (z. B. Autorisierung, Sperrung, Verschiebung) der Benutzer wählen kann. Hier sollte auch die Standardkonfiguration angegeben werden.
7.	Update-Prüfung	Eine kurze Beschreibung des Abfragemechanismus und der Zeit für die Verfügbarkeit von Sicherheitsupdates und ob die Verfügbarkeit des Sicherheitsupdates durch die VE selbst überprüft wird.
8.	Benutzerbenachrichtigung	Eine kurze Beschreibung, wie der Benutzer über das verfügbare Update und die durch den Aktualisierungsmechanismus verursachten Störungen informiert wird, z. B. die begrenzte Verfügbarkeit bestimmter Funktionen, die Angabe der in der Benachrichtigung enthaltenen Informationen und ob die Benachrichtigung durch die VE selbst umgesetzt wird.
9.	Versionsverwaltung	Eine kurze Beschreibung, wie die VE die Update-Version vor der Installation überprüft und validiert.

2.2.14. MD 14-SecParam: Sicherheitsparameter

Das MD listet alle sensiblen (öffentlichen und kritischen) Sicherheitsparameter auf, die während der normalen Nutzung dauerhaft auf VE gespeichert werden, mit folgenden Parametern:

	A	B
1.	ID	Eindeutige Kennung für jeden Parameter, beginnend mit SecParam-1.
2.	Beschreibung	Eine kurze Beschreibung des Sicherheitsparameters einschließlich seines Zwecks, und die Angabe, dass es sich bei dem Sicherheitsparameter um eine fest codierte eindeutige Gerätekennung handelt, die in dem Gerät für Sicherheitszwecke verwendet wird und im Quellcode der Software des Geräts hart-kodiert ist.
3.	Speicherort	Ort und Verfahren zur Speicherung des Sicherheitsparameters.
4.	Typ	Angabe, ob der Sicherheitsparameter öffentlich oder kritisch ist.
5.	Sicherheitsgarantien	Eine Beschreibung der erreichten grundlegenden Sicherheitsziele und der Gefahren, vor denen der Sicherheitsparameter während der Langzeitspeicherung geschützt ist.
6.	Schutzsystem	Eine Beschreibung der Maßnahmen, die ergriffen wurden, um die Sicherheitsgarantien zu erreichen, einschließlich der Berechtigungen und Rollen, über die der Zugriff auf den Parameter möglich ist, sowie die mit jeder Rolle verbundenen Rechte.
7.	Zuteilungsmechanismus	Wenn der „Typ“ angibt, dass der Parameter kritisch ist: eine Beschreibung des Mechanismus, durch den der Parameter einen Wert erhält.
8.	Kommunikationsmechanismen	Ein Verweis auf die Kommunikationsmechanismen, die in MD 16-ComMech verwendet werden, um die Parameter zu kommunizieren und anzugeben, ob die Kommunikation über von der Ferne zugängliche Schnittstellen erfolgt.
9.	Erstellungsmechanismus	Wenn der „Typ“ angibt, dass der Parameter kritisch ist oder zur Überprüfung der Integrität und Authentizität von Software-Updates oder zum Schutz der Kommunikation mit verwandten Diensten verwendet wird: eine Beschreibung des Mechanismus, der verwendet wird, um Werte für den Parameter zu erstellen, und zusätzlich ein Hinweis darauf, dass der Parameter verwendet wird, um die Integrität und Authentizität von Software-Updates zu überprüfen oder die Kommunikation mit verwandten Diensten zu schützen.

2.2.15. MD 15-SecMgmt: Sichere Managementprozesse

Der MD listet jeden sicheren Managementprozess für kritische Sicherheitsparameter auf, die der Hersteller während des VE-Lebenszyklus implementiert hat:

	A	B
1.	ID	Eindeutige Kennung für jeden Prozess, beginnend mit SecMgmt-1.
2.	Beschreibung	Eine kurze Beschreibung des sicheren Managementprozesses für den gesamten Lebenszyklus kritischer Sicherheitsparameter unter Bezugnahme auf die entsprechende Norm, wenn eine bestehende Norm angewendet wird. Der Lebenszyklus kritischer Sicherheitsparameter berücksichtigt in der Regel Generierung, Bereitstellung, Speicherung, Aktualisierung, Extraktion, Archivierung, Vernichtung, Ablaufverfahren und Parameteranfälligkeit. Während der Generierung sind auch die Methode zur Erzeugung der verwendeten Zufallszahlen und die Messung ihrer Entropie zu beschreiben. Wenn es eine Dateiintegritätsprüfung gibt, sollte auch beschrieben werden, wie sie umgesetzt wird.

2.2.16. MD 16-ComMech: Kommunikationsmechanismen

Das MD listet alle VE-Kommunikationsmechanismen mit den folgenden detaillierten Informationen auf:

	A	B
1.	ID	Eindeutige Kennung für jeden Mechanismus, beginnend mit ComMech-1.
2.	Beschreibung	Eine kurze Beschreibung des Kommunikationsmechanismus einschließlich seines Zwecks und eine Beschreibung des verwendeten Protokolls. Für standardisierte Protokolle ist ein Verweis mit einer Versionsnummer ausreichend. Außerdem sollte angegeben werden, ob der Mechanismus aus der Ferne verfügbar ist.
3.	Sicherheitsgarantien	Eine Beschreibung der erreichten Sicherheitsziele und der mit dem Mechanismus zu bewältigenden Bedrohungen.
4.	Kryptografische Details	Eine Beschreibung der kryptographischen Methoden, die zur Bereitstellung des Kommunikationsmechanismus (Protokolle, Operationen, Primitiven, Modi und Schlüsselgrößen) unter Berücksichtigung des Schlüsselmanagements verwendet werden, um die Ziele der beschriebenen „Sicherheitsgarantien“ zu erreichen.
5.	Abwehrmaßnahmen	Eine Beschreibung der Maßnahmen, um sicherzustellen, dass die Beziehung geordnet aufgebaut wird, einschließlich des erwarteten, operativen und stabilen Zustands, der zum Erreichen einer stabilen Beziehung führt.

2.2.17. MD 17-NetSecImpl: Netzwerk- und Sicherheitsumsetzungen

Das MD listet alle Umsetzungen der Netzwerk- und Sicherheitsfunktionen der VE auf.

	A	B
1.	ID	Eindeutige Kennung für jedes Element, beginnend mit NetSecImpl-1.
2.	Beschreibung	Eine kurze Beschreibung der Umsetzung des Netzwerks oder der Sicherheitsfunktion, einschließlich seines Zwecks und Umfangs.
3.	Überprüfungs-/ Bewertungsmethode	Eine Beschreibung der Methodik, die zur Überprüfung oder Bewertung der Umsetzung verwendet wird, einschließlich Grundprinzipien (z. B. Audit, Begutachtung, automatische Codeanalyse) und eine Beschreibung des Umfangs der von der Methodik abgedeckten Umsetzung.
4.	Bericht	Das Ergebnis der Überprüfung oder Bewertung oder ein Verweis auf das Zertifikat oder den Bewertungsbericht, aus dem hervorgeht, dass die Umsetzung als erfolgreich bewertet wurde.

2.2.18. MD 18-SoftServ: Softwaredienstleistungen

Das MD listet alle VE-Softwaredienstleistungen wie folgt auf:

	A	B
1.	ID	Eindeutige Kennung für jede Dienstleistung, beginnend mit SoftServ-1.
2.	Beschreibung	Eine kurze Beschreibung der Dienstleistung einschließlich ihres Zwecks, aus dem hervorgeht, ob die Dienstleistung und über welche Netzwerkschnittstelle nach MD 7-Intf verfügbar ist und ob dies auch im initialisierten Zustand der Fall ist.
3.	Status	Ein Hinweis darauf, dass der Dienst im initialisierten Zustand aktiviert oder deaktiviert ist.
4.	Begründung	Wenn die Dienstleistung autorisiert ist, ist das eine Erklärung, warum der Dienst für die ordnungsgemäße Nutzung oder den Betrieb von VE erforderlich ist.
5.	Konfiguration	Wenn die Dienstleistung über eine Netzwerkschnittstelle verfügbar ist: Informationen darüber, ob die Dienstleistung eine sicherheitsrelevante Änderung der Konfiguration ermöglicht und gegebenenfalls eine kurze Beschreibung der möglichen Konfiguration. Im Falle einer Softwarekomponente eines Drittanbieters eine Anweisung, dass die Dienstleistung standardmäßig deaktiviert ist.
6.	Authentifizierungsmechanismus	Wenn die Dienstleistung über eine Netzwerkschnittstelle verfügbar ist: Verweis in MD 10-AuthMech auf Authentifizierungsmechanismen, die vor der Nutzung der Dienstleistung für die Authentifizierung verwendet werden.
7.	SW von Drittanbietern	Angabe, ob die Softwarekomponente von einem Drittanbieter stammt. Wenn ja, eine Beschreibung des Trennverfahrens.

2.2.19. MD 19-CodeMin: Code-Minimierung

Das MD listet die Methoden auf, die verwendet werden, um die Codes zu minimieren:

	A	B
1.	ID	Eindeutige Kennung für jede Methode, beginnend mit CodeMin-1.
2.	Beschreibung	Eine kurze Beschreibung der Methode zur Minimierung des Codes auf die erforderliche Funktionalität.

2.2.20. MD 20-PrivlCtrl: Berechtigungskontrolle

Das MD listet alle Berechtigungskontrollmechanismen wie folgt auf:

	A	B
1.	ID	Eindeutige Kennung für jeden Mechanismus, beginnend mit PrivlCtrl-1.
2.	Beschreibung	Eine kurze Beschreibung des Mechanismus zur Überprüfung der Rechte und Berechtigungen für die Rollen und die Software über VE.
3.	Matrix	Die vom jeweiligen Berechtigungskontrollmechanismus verwaltete Autorisierungsmatrix.
4.	Authentifizierung	Verweis auf den Authentifizierungsmechanismus, der durch den jeweiligen Berechtigungskontrollmechanismus angefordert wird.

2.2.21. MD 21-AccCtrl: Zugangsschutz

Das MD listet die Speicherzugriffsschutzmechanismen auf Hardware-Ebene wie folgt auf.

	A	B
1.	ID	Eindeutige Kennung für jeden Mechanismus, beginnend mit AccCtrl-1.
2.	Beschreibung	Eine kurze Beschreibung des Zugangskontrollmechanismus auf Hardware-Ebene, einschließlich der Art, wie die VE das Betriebssystem unterstützt.

2.2.22. MD 22-SecBoot: Sichere System-Boot-Mechanismen

Das MD listet alle sicheren Boot-Mechanismen von VE wie folgt auf:

	A	B
1.	ID	Eindeutige Kennung für jeden Mechanismus, beginnend mit SecBoot-1.
2.	Beschreibung	Eine kurze Beschreibung des Mechanismus, der für den sicheren Startprozess von VE (einschließlich Sicherheitsannahmen) und die Identifizierung des geschützten Teils der Software verwendet wird.

		Besondere Aufmerksamkeit sollte allen Steuerungsoptionen und API-Aufrufen gewidmet werden, die sich auf den Betrieb des Mechanismus auswirken. Wenn VE ein Backup der geschützten Software verwendet, ist seine Verwendung auch in der Beschreibung enthalten.
3.	Sicherheitsgarantien	Eine Beschreibung der umgesetzten Sicherheitsziele des Mechanismus. Die Mechanismen implementieren die Authentizität und Integrität der Kernel der Betriebssysteme.
4.	Erkennungsmechanismen	Eine Beschreibung des Mechanismus zur Erkennung der unbefugten Änderung der VE-Software.
5.	Benutzerbenachrichtigung	Eine kurze Beschreibung, wie der Benutzer über jede unbefugte Änderung der Software informiert wird, als ergänzende Informationen, die angeben, welche Informationen in der Benachrichtigung enthalten sind.
6.	Benachrichtigungsfunktionen	Eine kurze Beschreibung der Netzwerkfunktionen, die für die Benutzerbenachrichtigung erforderlich sind.

2.2.23. MD 23-Store: Speicherung und Wiederherstellung

Die MD listet die Art und Weise, auf die die von VE verarbeiteten Daten gespeichert werden und wie die Daten wiederhergestellt werden können, wie folgt auf:

	A	**B**
1.	ID	Eindeutige Kennung für jede Speichermethode, beginnend mit Store-1.
2.	Speicherprodukt	Methode und Ort, wie und wo die von VE verarbeiteten Daten gespeichert werden.
3.	Redundanz	Im Falle eines Ausfalls im Speichermechanismus ist das sein Ersatzmechanismus.
4.	Die Methode der Datenwiederherstellung	Die Art und Weise, wie historische Daten im Falle eines Ausfalls von primärem Speicher oder VE wiederhergestellt werden.
5.	Verschlüsselung	Der am Speicherprodukt verwendete Verschlüsselungsalgorithmus, der angibt, ob die Verschlüsselung im Werks-Standardzustand aktiviert ist und wie und mit welcher Rolle der verschlüsselte Speicher vom Benutzer konfiguriert werden kann.

2.2.24. MD 24-DataSec: Datenschutz

Das MD listet alle von VE verarbeiteten Daten, mit Ausnahme der Telemetriedaten, wie folgt auf:

	A	**B**
1.	ID	Eindeutige Kennung für jeden Datensatz, beginnend mit DataSec-1.
2.	Beschreibung	Eine kurze Beschreibung der Datenkategorie, die durch die

		VE verarbeitet wird. Personenbezogene Daten sind Informationen über jede identifizierte oder identifizierbare natürliche Person.
3.	Verarbeitungstätigkeiten	Eine Beschreibung der Verarbeitung der Daten, die alle betroffenen Parteien beschreibt und die Zwecke, für die die Daten verarbeitet werden.
4.	Kommunikationsmechanismen:	Verweis auf die Kommunikationsmechanismen nach MD 16-ComMech, die zur Übermittlung der Daten verwendet werden, und eine Angabe, ob es sich bei dem Kommunikationspartner um einen zugehörigen Dienst handelt (ja/nein). Eine leere Liste von Kommunikationsmechanismen zeigt an, dass die Daten nicht übertragen werden.
5.	Empfindlichkeit	Ein Hinweis darauf, ob es sich bei den Daten um empfindliche Daten handelt. Empfindliche Daten sind alle Daten, deren Offenlegung der betroffenen Person wahrscheinlich schaden wird. Was als empfindliche Daten gilt, kann je nach Produkt und Nutzung variieren, aber Beispiele sind das Zahlungsinformationen, Inhalt von Kommunikationsdaten und zeitgestempelte Standortdaten.
6.	Einholung der Zustimmung	Wenn personenbezogene Daten auf der Grundlage der Einwilligung der betroffenen Person verarbeitet werden: eine Beschreibung, wie die Zustimmung eingeholt wird.
7.	Widerruf der Zustimmung	Wenn personenbezogene Daten auf der Grundlage der Einwilligung der betroffenen Person verarbeitet werden: eine Beschreibung, wie die betroffene Person ihre Zustimmung zur Verarbeitung der personenbezogenen Daten widerrufen kann.
8.	Kryptografischer Schutz	Der kryptografische Algorithmus, der zum Schutz personenbezogener Daten verwendet wird, unter Bezugnahme auf MD 12-SoftComp.
9.	Speicherprodukt	Speicherprodukt(e) zum Speichern von Daten, nach MD 23-Store.

2.2.25. MD 25-ExtSens: Externe Sensoren

Das MD listet alle externen Erfassungsfähigkeiten von VE wie folgt auf:

	A	**B**
1.	ID	Eindeutige Kennung für jeden Sensor, beginnend mit ExtSens-1.
2.	Beschreibung	Eine kurze Beschreibung der Erkennungsfähigkeit.

2.2.26. MD 26-ResMech: Abwehrmechanismen

Das MD listet alle Abwehrmechanismen für die Trennung des Netzwerks der VE oder Stromausfall wie folgt auf:

	A	B
1.	ID	Eindeutige Kennung für jeden Mechanismus, beginnend mit ResMech-1.
2.	Beschreibung	Eine Beschreibung des Abwehrmechanismus, der zur Widerstandsfähigkeit von VE gegenüber Netz- und Stromausfällen beiträgt.
3.	Typ	Der Abwehrmechanismus wird verwendet, um Störungen in der Netzwerkverbindung oder einen Stromausfall zu bewältigen oder beides zu handhaben.
4.	Sicherheitsgarantien	Eine Beschreibung der erreichten Sicherheitsziele und der Bedrohungen, auf die der Mechanismus ausgerichtet sein sollte.

2.2.27. MD 27-TelData: Telemetriedaten

Das MD listet alle von VE gesammelten Telemetriedaten wie folgt auf:

	A	B
1.	ID	Eindeutige Kennung für jeden Datensatz, beginnend mit TelData-1.
2.	Beschreibung	Eine kurze Beschreibung der Telemetriedaten, die VE gesammelt und dem Hersteller zur Verfügung gestellt hat.
3.	Zweck	Eine kurze Beschreibung der Zwecke, für die die Daten erhoben werden.
4.	Sicherheitsprüfung	Wenn die Daten für Sicherheitsprüfungen verwendet werden, ist das eine Beschreibung, wie und von wem (Gerät oder zugehörige Dienstleistung) Telemetriedaten auf Sicherheitsstörungen untersucht werden.
5.	Datenverbindungen	Referenz in MD 24-Datasec auf Daten, die in Telemetriedaten verarbeitet werden.

2.2.28. MD 28-DelFunc: Löschfunktionen

Das MD listet alle Löschfunktionen für Benutzerdaten wie folgt auf:

	A	B
1.	ID	Eindeutige Kennung für jede Löschfunktion, beginnend mit DelFunc-1.
2.	Beschreibung	Eine kurze Beschreibung der Funktion, mit der die Benutzerdaten gelöscht werden. Wenn der „Zieltyp“ anzeigt, dass er an eine verbundene Dienstleistung gerichtet ist, ist auch die von der Funktion abgedeckte Dienstleistung anzugeben.
3.	Zieltyp	Angabe, ob die Funktion für Benutzerdaten auf dem Gerät oder für personenbezogene Daten gilt, die in verwandten Dienstleistungen

		verarbeitet werden, oder beides.
4.	Initiierung und Interaktion	Eine kurze Beschreibung der Benutzerinteraktion, die zum Starten und Anwenden der Löschfunktion benötigt wird.
5.	Bestätigung	Eine kurze Beschreibung der Art und Weise, wie der Benutzer einen Hinweis erhält, dass die betreffenden Daten nach Anwendung der Löschfunktion gelöscht wurden.

2.2.29. MD 29-UserDec: Benutzerentscheidungen

Das MD listet alle Entscheidungen, die während der Installation und Wartung getroffen werden müssen, wie folgt auf:

	A	**B**
1.	ID	Eindeutige ID für jede Entscheidung, beginnend mit UserDec-1.
2.	Beschreibung	Eine Beschreibung der Entscheidungen, die der Benutzer im Rahmen der Installations- und Wartungsprozesse zu treffen hat, einschließlich der Rolle des Benutzers im Installations- oder Wartungsprozess.
3.	Optionen	Eine Beschreibung der sicherheitsrelevanten Optionen, aus denen der Benutzer wählen kann, und eine Angabe des voreingestellten Werts.
4.	Entscheidung	Eine kurze Beschreibung der Entscheidungsfindung, in der angegeben wird, ob die Entscheidung auch vom Endnutzer getroffen werden kann.

2.2.30. MD 30-UserIntf: Benutzerschnittstellen

Das MD listet alle VE-Benutzeroberflächen, die Benutzereingaben erlauben, wie folgt auf:

	A	**B**
1.	ID	Eindeutige Kennung für jede Schnittstelle, beginnend mit UserIntf-1.
2.	Beschreibung	Eine Beschreibung des Zwecks, der Funktion und der Eingabefelder der Benutzeroberfläche, die es dem Benutzer ermöglicht, Daten einzugeben und die Erklärung, wie der Benutzer auf die Schnittstelle zugreifen kann.
3.	Konfigurationsschnittstelle	Eine Angabe, ob die Schnittstelle für die VE-Konfiguration verwendet werden kann.
4.	Kommunikationsmechanismus	Wenn die Schnittstelle für die VE-Konfiguration verwendet werden kann, dann ist das ein Verweis auf Kommunikationsmechanismen in MD 16-ComMech, der zum Schutz der Schnittstelle verwendet wird.

2.2.31. MD 31-ExtAPI: Externe APIs

Der MD listet alle VE-APIs, die Daten aus externen Quellen eingeben können, wie folgt auf:

	A	B
1.	ID	Eindeutige Kennung für jede API, beginnend mit ExtAPI-1.
2.	Beschreibung	Eine Beschreibung der VE-API, die die Eingabe aus externen Quellen ermöglicht. Externe APIs werden typischerweise für die Maschine-zu-Maschine-Kommunikation verwendet.

2.2.32. MD 32-InpVal: Validierung der Dateneingabe

Das MD listet alle Validierungsmethoden für VE-Dateneingabe wie folgt auf:

	A	B
1.	ID	Eindeutige Kennung für jede Methode, beginnend mit InpVal-1.
2.	Beschreibung	Eine Beschreibung der Methode, die zur Validierung der Daten verwendet wird, die über Benutzerschnittstellen eingegeben oder über APIs oder zwischen Netzwerken in Dienstleistungen und Geräten übermittelt werden, einschließlich der Verwaltung unerwarteter Daten. Außerdem ist anzugeben, welche der Dateneingabequellen von der Methode als Ziel gesetzt werden. Um die Dateneingabe zu validieren, kann überprüft werden, ob die Daten von zulässiger Art (Format und Struktur), zulässigem Wert, erlaubter Nummer oder Ordnung sind.

2.2.33. MD 33-Notif: Benachrichtigungen

Das MD enthält alle Arten von Benutzerbenachrichtigungen wie folgt:

	A	B
1.	ID	Eindeutige Kennung für jede Benachrichtigungsmethode, beginnend mit Notif-1.
2.	Art der Benachrichtigung	Eine Beschreibung, auf welcher Schnittstelle nach MD 7-Intf die Benachrichtigung erscheint und an welche Benutzer sie gesendet wird.
3.	Verwaltung von Benachrichtigungen	Handlungen, die der Benutzer im Zusammenhang mit der Benachrichtigung zu unternehmen hat.
4.	Inhalt	Der Inhalt der Benachrichtigungen, wenn sie konfiguriert werden können, eine Beschreibung der Rolle nach MD 9-Role, mit der der Benutzer den Dateninhalt konfigurieren kann und die Tiefe, in der dies erfolgen kann.

2.2.34. MD 34-AuditLog: Protokolldaten

Das MD listet alle VE-Protokollierungsmethoden wie folgt auf:

	A	B

1.	ID	Eindeutige ID für jedes Protokollelement, beginnend mit AuditLog-1.
2.	Beschreibung	Der Umfang der Protokollierungsaktivität, der Inhalt der Protokolle.
3.	Sicherheitsgarantien	Eine Beschreibung der erreichten grundlegenden Sicherheitsziele und der Bedrohungen, vor denen Protokolldaten bei der Langzeitspeicherung geschützt werden.
4.	Schutzsystem	Eine Beschreibung der Maßnahmen zur Erreichung der Sicherheitsgarantien, in der die Berechtigungen und Rollen beschrieben werden, über die der Zugriff auf den Parameter möglich ist, einschließlich der mit jeder Rolle verbundenen Rechte.

3. Dokument, das die Bewertung untermauert

3.1. Der Hersteller stellt ein Bewertungsdokument aus, in dem die Einhaltung der Anforderungen gemäß Anlage 2 in Bezug auf das Zuverlässigkeitsniveau für die zu prüfende VE (im Folgenden: EMD).

3.2. Das Dokument enthält eine Liste der Anforderungen gemäß Anlage 2 für das Zuverlässigkeitsniveau sowie die folgenden Informationen:

a) Klassifizierung des Herstellers: Erklärung des Herstellers über die Einhaltung dieser Anforderung. Sie kann folgende Werte haben:

(aa) „Nicht anwendbar“: dies kann verwendet werden, wenn die Anforderung in Bezug auf VE nicht anwendbar ist und die physikalische Gestaltung, die beabsichtigten Funktionen und der Einsatzbereich der VE es nicht zulassen, dass die Anforderung erfüllt werden kann.

(ab) „Anwendbar und erfüllt“: dies kann verwendet werden, wenn die Anforderung für VE anwendbar ist und die VE die Anforderung erfüllt.

b) Art der Erfüllung: Im Falle der Kennzeichnung „anwendbar und erfüllt“ ist das eine Beschreibung, welche Bestandteile im MD in Bezug auf die Anforderung betroffen sind und wie sie die Anforderung einzeln oder zusammen erfüllen.

c) Erläuterung: Bei der Kennzeichnung „nicht anwendbar“, die Begründung unter Berücksichtigung aller Umstände.

Satz an Anforderungen

1. In Bezug auf die Sicherheitsanforderungen sind die Anforderungen, die von dem in Anlage 1 Nummer 1 festgelegten Gerät für das Zuverlässigkeitsniveau erfüllt werden müssen, in den Spalten C bis E angegeben.

2. Die Anforderungen wurden nach den folgenden europäischen und nationalen Normen entwickelt:
   (a) ETSI EN 303 645 V2.1.1
   (b) NIST Special Publication 800-213A und
   (c) NIST Special Publication 800-53 Revision 5.

3. In jeder Spalte
   (a) geben die mit „-“ gekennzeichneten Zeilen die Namen der Kontrollfamilien an;
   (b) weist ein „X“ darauf hin, dass die Einhaltung der Sicherheitsanforderung in dieser Zeile auf dem in den Spalten C bis E angegebenen Zuverlässigkeitsniveau obligatorisch ist;
   bedeutet eine „0“, dass die Einhaltung der Sicherheitsanforderung in dieser Zeile auf dem in den Spalten C bis E angegebenen Zuverlässigkeitsniveau nicht vorgeschrieben ist.

	A	B	C	D	E
1.	**Kennung**	**Beschreibung**	**grundlegend**	**signifikant**	**hoch**
2.		GERÄTEIDENTIFIKATION	-	-	-
3.		Geräteidentifikation	-	-	-
4.	DEVID-1	Die Modellkennzeichnung des IoT-Geräts ist klar erkennbar, entweder auf dem Etikett auf dem Gerät oder über eine physikalische Schnittstelle.	X	X	X
5.	DEVID-2	Das IoT-Gerät verfügt über eine eindeutige logische Kennung, die über eine Schnittstelle abgerufen oder auf dem Gerät gefunden werden kann.	X	X	X
6.	DEVID-3	Es ist möglich, die eindeutige Kennung und Modellkennzeichnung eines IoT-Geräts zu definieren, das ferngesteuert werden kann.	X	X	X

7.	DEVID-4	Das IoT-Tool bietet die Möglichkeit, eine eindeutige physikalische Kennung hinzuzufügen, die von autorisierten Einheiten zugegriffen werden kann.	0	X	X
8.		Ausführung von Vorgängen			
9.	DEVOP-1	Das IoT-Tool ist in der Lage, Vorgänge auszuführen, die bei der Identifizierung oder Verwendung des Geräts auftreten können.	X	X	X
10.	DEVOP-2	Das IoT-Tool ist in der Lage, zwischen identifizierten und nicht identifizierten Benutzern zu unterscheiden.	X	X	X
11.	DEVOP-3	Nicht autorisierte Benutzer können sich der eindeutigen logischen IoT-Gerätekennung nicht bewusst werden.	0	X	X
12.	DEVOP-4	Wenn man die IoT-Gerätekennung kennt, kann die aktuelle Softwareversion überprüft werden.	0	X	X
13.	DEVOP-5	Um Netzwerkgeräte zu identifizieren und zu verwalten, kann die Gerätekennung verwendet werden, um das IoT-Gerät zu erkennen.	0	0	X
14.		Unterstützung für die Geräteidentifikation	-	-	-
15.	IDSUPP-1	Das IoT-Tool ist in der Lage, sich als voridentifizierte Einheit bei anderen Positionen zu werben.	0	X	X
16.	IDSUPP-2	Die Überprüfung der Authentizität anderer IoT-Geräte ist gewährleistet.	0	X	X
17.	IDSUPP-3	Bei Netzwerk- und Fernzugriff-Netzwerkverbindungen führt das IoT-Gerät vor dem Aufbau der identifizierten Verbindung eine kryptographische bidirektionale Identifizierung durch.	0	0	X
18.	IDSUPP-4	Das IoT-Tool unterstützt zertifikatbasierte Identifizierung und Authentifizierung.	0	0	X
19.		GERÄTEKONFIGURATION	-	-	-
20.	DEVCONF-1	Die Einstellung der Rechte für logischen Zugang, die Konfiguration des IoT-Geräts – gemäß den Anforderungen „Externe Verbindungen, Schnittstellensteuerung“ – ist nur durch privilegierte Benutzer möglich.	X	X	X
21.	DEVCONF-2	Nur autorisierte Benutzer können die IoT-Geräteidentifikationsrichtlinie und die Zugangsbeschränkungslisten gemäß den Anforderungen „Externe Verbindungen, Schnittstellensteuerung“ konfigurieren.	X	X	X
22.	DEVCONF-3	Nur autorisierte Benutzer können die logischen und physikalischen Schnittstellen des IoT-Geräts gemäß den Anforderungen „Externe Verbindungen, Schnittstellensteuerung“ konfigurieren.	X	X	X
23.	DEVCONF-4	Autorisierte Benutzer können die Softwareeinstellungen des IoT-Geräts konfigurieren.	X	X	X
24.	DEVCONF-5	Autorisierte Benutzer können das IoT-Gerät auf seinen Werksstatus zurücksetzen.	X	X	X
25.	DEVCONF-6	Autorisierte Benutzer können das IoT-Gerät in einem früheren sicheren Zustand wiederherstellen, der kein Werkszustand ist.	0	0	X

26.	DEVCONF-7	Der vorherige Konfigurationsstatus wird während oder nach der Wartung des IoT-Geräts gesichert.	0	X	X
27.		DATENSCHUTZ	-	-	-
28.		Kryptografische Unterstützung	-	-	-
29.	CRYPT-1	Das IoT-Tool bietet einen kryptografischen Algorithmus mit ausreichender Stärke und Effizienz, um die Daten zu schützen.	X	X	X
30.	CRYPT-2	Das IoT-Tool ist in der Lage, einzelne Zertifikate zu validieren.	0	X	X
31.	CRYPT-3	Die digitale Signaturverifizierung ist gewährleistet.	0	X	X
32.	CRYPT-4	Das IoT-Tool kann Hash-Algorithmen ausführen.	X	X	X
33.	CRYPT-5	Sie können auf die empfohlenen Versionen von kryptographischen Algorithmen und Primitiven aktualisiert werden.	0	X	X
34.	CRYPT-6	Der Quellcode des Geräts enthält keine fest programmierten kritischen Sicherheitsparameter.	0	X	X
35.	CRYPT-7	Die kritischen Sicherheitsparameter, die verwendet werden, um die Integrität und Authentizität von Software-Updates zu überprüfen und die Kommunikation in Gerätesoftware mit zugehörigen Diensten zu schützen, sind einzigartig für jedes Gerät und werden mit einem Mechanismus erstellt, der das Risiko automatisierter Angriffe verringert.	X	X	X
36.		Unterstützung für kryptografische Schlüssel	-	-	-
37.	CRYKEY-1	Das IoT-Gerät verwaltet kryptografische Schlüssel sicher.	X	X	X
38.	CRYKEY-2	Das IoT-Tool ist in der Lage, Schlüsselpaare zu generieren.	X	X	X
39.	CRYKEY-3	Das IoT-Gerät speichert die kryptografischen Schlüssel sicher.	X	X	X
40.	CRYKEY-4	Das IoT-Gerät nimmt Änderungen an den kryptografischen Schlüsseln sicher vor.	X	X	X
41.	CRYKEY-5	Das IoT-Tool prüft die kryptografischen Schlüssel, die von externen Systemen generiert werden.	0	X	X
42.		Sichere Speicherung	-	-	-
43.	SECSTR-1	Das IoT-Gerät speichert und übermittelt keine Passwörter, ausgenommen die Speicherung des aus dem Passwort generierten Hashwerts mit der irreversiblen kryptografischen Splitting-Funktion.	X	X	X
44.	SECSTR-2	Eine sichere Speicherung kann über das IoT-Gerät oder dessen Schnittstelle zugelassen werden.	X	X	X
45.	SECSTR-3	Im Werkszustand ist eine sichere, sichere und verschlüsselte Speicherung der Daten erlaubt.	X	X	X
46.	SECSTR-4	Schutz personenbezogener Daten wird gemäß 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) sichergestellt.	X	X	X

47.	SECSTR-5	Das IoT-Gerät, einschließlich der Cloud-Infrastruktur, die den Zugriff auf die Daten sicherstellt, speichert nur die für den Betrieb benötigte Datenmenge.	X	X	X
48.	SECSTR-6	Das IoT-Gerät kann Daten lokal verschlüsselt speichern.	X	X	X
49.	SECSTR-7	Entfernte Systemelemente im Zusammenhang mit dem IoT-Gerät (z. B. Cloud) speichern die Daten verschlüsselt.	0	X	X
50.	SECSTR-8	Empfindliche Sicherheitsparameter werden im dauerhaften Speicher gespeichert.	0	X	X
51.	SECSTR-9	System- und Benutzerdaten werden auf separaten Partitionen platziert.	0	X	X
52.	SECSTR-10	Eine sichere Datensicherung ist gewährleistet.	0	X	X
53.	SECSTR-11	Benutzerdaten, die lokal auf dem IoT-Gerät gespeichert werden, können einfach und unwiederbringlich gelöscht werden.	X	X	X
54.	SECSTR-12	Benutzerdaten, die von Remote-Systemelementen gespeichert werden, die mit dem IoT-Gerät verbunden sind, können einfach gelöscht werden.	0	X	X
55.		Sichere Datenübertragung	-	-	-
56.	SECDT-1	Der Datenfluss an den Eingangs- und Ausgangsschnittstellen des IoT-Geräts ist sicher.	X	X	X
57.	SECDT-2	Der kryptografische Algorithmus zur sicheren Datenübertragung kann konfiguriert werden.	0	X	X
58.	SECDT-3	Das IoT-Gerät verfügt über einen Schutz vor unbefugtem Zugriff und Modifikation in der Datenverbindungsumgebung.	X	X	X
59.	SECDT-4	Das IoT-Tool überprüft die Integrität der übertragenen und empfangenen Daten mithilfe einer kryptografischen Lösung.	0	X	X
60.		LOGISCHER ZUGRIFF AUF SCHNITTSTELLEN	-	-	-
61.		Unterstützung bei der Identifizierung	-	-	-
62.	AUTH-1	Das IoT-Tool unterstützt Authentifizierungsmethoden.	X	X	X
63.	AUTH-2	Das IoT-Tool ist in der Lage, eine Authentifizierungsmethode zur Herstellung von Verbindungen anzufordern, insbesondere bei Remote-Verbindungen.	X	X	X
64.	AUTH-3	Für bestimmte Benutzerpopulationen unterstützt das IoT-Tool eine Multi-Faktor-Authentifizierungsmethode.	0	X	X
65.	AUTH-4	Wenn Ihr IoT-Gerät werkseitig Standardkennwörter verwendet, sind diese für jedes Gerät einmalig.	0	X	X
66.	AUTH-5	Bei der Generierung von Standardkennwörtern verwendet das IoT-Tool einen Generierungsalgorithmus, der das Risiko automatischer Angriffe reduziert.	0	X	X
67.	AUTH-6	Das Ändern eines Berechtigungsnachweises, der dem verwendeten Authentifizierungsmechanismus entspricht, wird dem Benutzer einfach sichergestellt.	X	X	X

68.	AUTH-7	Das IoT-Tool versteckt die Daten während des Authentifizierungsprozesses.	X	X	X
69.	AUTH-8	Das IoT-Tool unterstützt eine standardisierte, einheitliche Authentifizierungsmethode. (z. B. SAML, OAuth2)	0	X	X
70.	AUTH-9	Für den Fernzugriff prüft das IoT-Gerät die Authentifizierungsdaten pro Vorgang.	0	0	X
71.	AUTH-10	Durch die Bereitstellung einer versteckten Rückmeldung der Informationen, die in der Rückmeldung der Authentifizierungsmethode enthalten sind, stellt das IoT-Gerät sicher, dass Authentifizierungskennungen nicht bekannt werden und von Unbefugten nicht wiederverwendet werden können.	X	X	X
72.		Konfiguration der Identifikation	-	-	-
73.	IDENT-1	Während des gesamten Lebenszyklus des IoT-Geräts können die Methoden, Regeln und Einschränkungen der Authentizität festgelegt und geändert werden.	0	X	X
74.	IDENT-2	Das IoT-Tool unterstützt die Kontoverwaltung auf eine automatisierte Art.	0	0	X
75.	IDENT-3	Die Anzahl der fehlgeschlagenen Identifizierungsversuche kann konfiguriert werden, danach sperrt das IoT-Gerät den Benutzer für einen festgelegten Zeitraum.	0	X	X
76.	IDENT-4	Das IoT-Tool unterstützt die Wiederherstellung eines Kontos, das aufgrund erfolgloser Identifizierungsversuche mit einer alternativen Identifikationsmethode gesperrt wurde.	0	0	X
77.	IDENT-5	Das IoT-Tool gibt Rückmeldung zum Datum der letzten erfolgreichen Authentifizierung.	0	X	X
78.	IDENT-6	Das IoT-Tool unterstützt das Abmelden von inaktiven Konten, deren Inaktivitätsdauer konfiguriert werden kann.	X	X	X
79.	IDENT-7	Das IoT-Gerät verbietet automatisch temporäre Benutzerkonten auf konfigurierbare Weise.	0	X	X
80.	IDENT-8	Das IoT-Tool protokolliert erfolglose Anmeldeversuche, die gemeldet werden können.	X	X	X
81.	IDENT-9	Das IoT-Gerät gibt die Anzahl der erfolglosen Anmeldeversuche für den Benutzer während des nächsten erfolgreichen Logins an.	0	X	X
82.	IDENT-10	Das IoT-Tool unterstützt die Authentifizierung externer Benutzer und Systeme.	X	X	X
83.	IDENT-11	Der Zugriff auf Benutzerkonten, externe Benutzer und Systeme kann widerrufen werden, in diesem Fall bricht das IoT-Gerät die bestehende Verbindung ab.	0	X	X
84.	IDENT-12	Das IoT-Tool unterstützt die Festlegung eines Ablaufdatums für Konten, wodurch sichergestellt wird, dass das Konto über das Ablaufdatum hinaus blockiert wird.	0	X	X
85.		Benutzerbenachrichtigung	-	-	-
86.	NOTIF-1	Der Status des IoT-Geräts lässt sich durch die Überprüfung der Statusanzeigen visuell leicht erkennen.	X	X	X

87.	NOTIF-2	Die auf dem IoT-Gerätedisplay angezeigten Informationen können konfiguriert werden.	0	X	X
88.	NOTIF-3	Das IoT-Tool kann Benachrichtigungen an Benutzer (auf eine konfigurierte Art) senden.	X	X	X
89.	NOTIF-4	Der gesamte Inhalt von Benachrichtigungen mit personenbezogenen Daten und dem von Sicherheitsbenachrichtigungen kann erst nach der Identifizierung offengelegt werden, und empfindliche Daten werden in der Warnmeldung nicht angezeigt.	0	X	X
90.	NOTIF-5	Der Inhalt der Nachrichten, die vom IoT-Gerät angezeigt werden, kann konfiguriert werden.	0	X	X
91.	NOTIF-6	Wenn die Warnmeldung auf dem Display des IoT-Geräts angezeigt wird, stellt das IoT-Gerät sicher, dass die Nachricht bis zu einer Benutzerinteraktion auf dem Display verbleibt.	0	X	X
92.		Unterstützung für das Zugriffsmanagement	-	-	-
93.	ACCESS-1	Das IoT-Gerät ist widerstandsfähig gegen unautorisierte Vorgänge.	X	X	X
94.	ACCESS-2	Das IoT-Gerät ist in der Lage, autorisierte Benutzer und Prozesse (z. B. Verbindung der Systeme) zu identifizieren.	X	X	X
95.	ACCESS-3	Das IoT-Gerät unterscheidet zwischen autorisierten und nicht autorisierten Benutzern.	X	X	X
96.	ACCESS-4	Bestimmte Funktionen, die vom Bediener definiert werden können, stehen ohne Identifikation zur Verfügung.	X	X	X
97.		Rollenunterstützung und -verwaltung	-	-	-
98.	ROLE-1	Das IoT-Gerät kann mehrere Arten von Benutzerkonten verwalten.	X	X	X
99.	ROLE-2	Das IoT-Tool unterscheidet mindestens die folgenden Arten von Benutzerkonten: persönliche Konten (allgemein und privilegiert), getrennt privilegierte Konten.	0	X	X
100.	ROLE-3	Das IoT-Tool unterstützt das Hinzufügen von Benutzerkonten.	0	X	X
101.	ROLE-4	Die Rollen können den Benutzerkonten zugewiesen werden.	0	X	X
102.	ROLE-5	Benutzerkonten werden mit einer einmaligen Kennung versehen.	0	X	X
103.	ROLE-6	Das IoT-Tool führt eine rollenbasierte logische Zugriffskontrolle durch.	0	X	X
104.	ROLE-7	Funktionen und Prozesse, auf die ein Administrator mit den Rollen zugreifen kann, können konfiguriert werden.	0	X	X
105.	ROLE-8	Rollen sind mit standardisierten, einheitlichen Autorisierungsmethoden kompatibel, Abgleich kann konfiguriert werden (z. B. LDAPS).	0	X	X
106.	ROLE-9	Ein Administrator kann eine neue Rolle konfigurieren.	0	0	X
107.	ROLE-10	Standardmäßig werden Rollen gemäß dem Prinzip der Mindestautorisierung entworfen.	X	X	X
108.	ROLE-11	Die Konfiguration der Zugriffsverwaltung für Auditprotokolle und Sicherheitseinstellungen wird	0	X	X

		unterstützt.			
109.	ROLE-12	Mit dem IoT-Tool kann man für jeden Benutzertyp restriktive Bedingungen festlegen (z. B. zeitliche Begrenzung, IP-Grenze).	0	0	X
110.	ROLE-13	Autorisierungen und Berechtigungen, die Rollen zugewiesen werden, werden bei Benutzerinteraktionen überprüft, die darauf abzielen, privilegierte Funktionen und Prozesse zu erreichen.	0	0	X
111.	ROLE-14	Die für die verschiedenen Benutzerkonten verwendeten Authentifizierungsmethoden können konfiguriert werden.	0	0	X
112.	ROLE-15	Bei getrennten Konten kann die Berechtigung für die gleichzeitige Anmeldung pro Konto konfiguriert werden (im Werkszustand gesperrt).	0	X	X
113.	ROLE-16	Das IoT-Gerät ist in der Lage, voreingestellte Einschränkungen bei der Verwendung des Geräts durchzusetzen.	0	X	X
114.		Externe Verbindungen, Schnittstellensteuerung	-	-	-
115.	INTCTRL-1	Das IoT-Gerät stellt die Verbindung zu externen Systemen von Drittanbietern unter Verwendung einer sicheren Methode zur Verfügung.	X	X	X
116.	INTCTRL-2	Die Verwendung von Komponenten des IoT-Geräts kann eingeschränkt werden (Ports, Funktionen, Ein- und Ausgabegeräte).	X	X	X
117.	INTCTRL-3	Physikalische oder logische Schnittstellen, die für den Betrieb des IoT-Geräts nicht erforderlich sind, können deaktiviert werden.	X	X	X
118.	INTCTRL-4	Nur die minimalen logischen und physischen Schnittstellen, die für die Installation und Inbetriebnahme erforderlich sind, sind im voreingestellten Werkszustand zulässig.	X	X	X
119.	INTCTRL-5	Im voreingestellten Werkszustand schützt das IoT-Gerät vor dem Abruf von Sicherheitsinformationen ohne Identifikation.	X	X	X
120.	INTCTRL-6	Die Hardware setzt physische Schnittstellen keinen unnötigen Risiken aus.	0	X	X
121.	INTCTRL-7	Die Nutzung der Dienstleistungen des IoT-Tools kann eingeschränkt werden.	0	X	X
122.	INTCTRL-8	Der externe Zugriff auf die Verwaltungsschnittstelle kann deaktiviert werden.	0	X	X
123.	INTCTRL-9	Der Zugriff auf die logischen Schnittstellen des IoT-Geräts kann gesteuert werden.	X	X	X
124.	INTCTRL-10	Das IoT-Gerät unterstützt eine drahtlose Verbindung, deren sicheres und autorisiertes Authentifizierungsprotokoll konfiguriert werden kann.	X	X	X
125.	INTCTRL-11	Wenn Ihr IoT-Gerät über eine Debug-Schnittstelle verfügt, ist dies durch Software unzulässig.	0	X	X
126.		SOFTWARE-UPDATE	-	-	-
127.		Update-Fähigkeiten	-	-	-

128.	UPD-1	Die Software des IoT-Geräts kann sicher aktualisiert werden, wie von der Software vorgesehen oder über eine Schnittstelle.	X	X	X
129.	UPD-2	Das Software-Update kann mit einem identifizierten, autorisierten Benutzerkonto durchgeführt werden, das von einem sicheren und konfigurierbaren Mechanismus unterstützt wird.	0	X	X
130.	UPD-3	Die aktuelle Version der Software des IoT-Geräts kann abgefragt werden.	X	X	X
131.	UPD-4	Autorisierte Konten können die Software auf eine frühere Softwareversion zurücksetzen.	0	X	X
132.	UPD-5	Software-Updates stammen aus einer zuverlässigen Quelle und die Einhaltung dieser Bedingung wird vom IoT-Gerät überprüft.	X	X	X
133.	UPD-6	Software-Updates verursachen keinen Rückgang der Cybersicherheitsbereitschaft für das IoT-Gerät, und das IoT-Tool verfügt über eine integrierte Methode, um diese Anforderung zu überprüfen.	0	X	X
134.		Verwaltung von Updates durch Anwendungsunterstützung	0	0	0
135.	UPDCTRL-1	Das IoT-Tool überprüft die Authentizität und Integrität von Updates.	X	X	X
136.	UPDCTRL-2	Sie können die automatische Aktualisierung des IoT-Geräts deaktivieren.	X	X	X
137.	UPDCTRL-3	Manuelle und automatische Aktualisierungsmethoden werden unterstützt.	X	X	X
138.	UPDCTRL-4	Die Aktualisierungsmethode kann ausgewählt werden.	X	X	X
139.	UPDCTRL-5	Die Software prüft die Verfügbarkeit eines neuen Updates in Abständen, die festgelegt werden können.	X	X	X
140.	UPDCTRL-6	Neue Softwareversionen werden vom IoT-Gerät mitgeteilt, diese Funktion kann jedoch ausgeschaltet werden.	X	X	X
141.	UPDCTRL-7	Neue Softwareversionen werden vom IoT-Gerät mitgeteilt und der zu benachrichtigende Umfang kann konfiguriert werden.	0	0	X
142.	UPDCTRL-8	Das IoT-Gerät informiert den Benutzer, wenn das Update ein Risiko für die wesentliche Funktion des IoT-Geräts darstellt.	0	X	X
143.		UNTERSTÜTZUNG DES EREIGNIS-MANAGEMENTS	-	-	-
144.		Protokollierung	-	-	-
145.	LOG-1	Das IoT-Tool ist in der Lage, Ereignisse zu protokollieren.	X	X	X
146.	LOG-2	Das IoT-Gerät unterstützt eine externe Protokollierungssystemverbindung.	0	X	X
147.	LOG-3	Der Mindestinhalt der Protokolleinträge ist wie folgt: eindeutige Kennung des IoT-Geräts, Zeitsignal, Ereignisquelle, Ereignistyp, Ereignisklassifizierung, Benutzer-ID oder Prozesskennung, Ereignisbeschreibung.	0	X	X
148.	LOG-4	Das IoT-Gerät ist in der Lage, Netzwerkkommunikation zu protokollieren.	0	X	X

149.	LOG-5	Das IoT-Gerät kann Änderungen in der Gerätekonfiguration protokollieren.	0	X	X
150.	LOG-6	Das IoT-Gerät ist in der Lage, erfolgreiche und erfolglose Zugriffsversuche zu protokollieren.	X	X	X
151.	LOG-7	Das IoT-Gerät ist in der Lage, seinen eigenen Zustand und den seiner Sensoren zu erfassen.	0	X	X
152.	LOG-8	Basierend auf der Liste der Ereignisse, die protokolliert werden können, können die zu protokollierenden Ereignisse konfiguriert werden.	0	0	X
153.	LOG-9	Der Status des IoT-Geräts kann über die Schnittstelle abgefragt werden.	0	X	X
154.	LOG-10	Man kann die maximale Aufbewahrungszeit der Ereignisse, die Anzahl der gespeicherten Protokoll-Ereignisse und die maximale Größe der Protokolldatei festlegen.	0	X	X
155.	LOG-11	Das vollständige Löschen von Protokolldateien über die Aufbewahrungskriterien auf dem IoT-Gerät hinaus ist sichergestellt.	0	X	X
156.		Zeitsignalmanagement	-	-	-
157.	TIMESTP-1	Die Zeitsignalisierung von Ereignissen, die vom IoT-Gerät protokolliert werden, muss auf mindestens Sekunden genau sein.	0	X	X
158.	TIMESTP-2	Das IoT-Gerät unterstützt ein NTP.	0	X	X
159.	TIMESTP-3	Eine zuverlässige Zeitquelle kann konfiguriert werden.	0	X	X
160.	TIMESTP-4	Das IoT-Gerät verwendet ein Standardzeitsignal, das auf UTC zurückverfolgt werden kann.	0	X	X
161.		Unterstützung des Ereignis-Managements	-	-	-
162.	INC-1	Das IoT-Gerät sendet eine Warnung vor konfigurierten Vorfällen, die als Sicherheitsvorfall gelten.	0	X	X
163.	INC-2	Das IoT-Gerät sendet eine Warnung vor konfigurierten Vorfällen, die als Sicherheitsvorfälle gelten, an die zugehörigen Informationssysteme.	0	0	X
164.	INC-3	Der Warnmodus kann konfiguriert werden.	0	0	X
165.	INC-4	Das IoT-Tool unterstützt eine alternative Protokollierungslösung im Falle eines Ausfalls des primären Protokollierungsmechanismus.	0	0	X
166.		SICHERHEIT VON ANLAGEN	-	-	-
167.		Sichere Kommunikation	-	-	-
168.	SECCOM-1	Die Herstellung und Schließung einer Verbindung mit anderen Geräten erfolgt sicher.	X	X	X
169.	SECCOM-2	Das IoT-Gerät ist in der Lage, Verkehrsmanagementregeln durchzusetzen.	0	X	X
170.	SECCOM-3	Das IoT-Gerät verwendet standardisierte Protokolle während der Kommunikation.	X	X	X
171.	SECCOM-4	Die IP-Adresse des IoT-Geräts kann eingestellt werden.	X	X	X
172.	SECCOM-5	Die Ports der IoT-Geräteschnittstellen können konfiguriert werden.	0	X	X

173.	SECCOM-6	Das IoT-Gerät hat DNS-Unterstützung.	X	X	X
174.		Sicherer Ressourceneinsatz	-	-	-
175.	RESRC-1	Das IoT-Tool ist in der Lage, Ressourcen zu teilen.	0	X	X
176.	RESRC-2	Das IoT-Gerät kann den Prozessen Speicherbereiche zuordnen.	0	X	X
177.	RESRC-3	Die verschiedenen Prozesse erreichen nicht den Speicherbereich, der einem anderen Prozess zugeordnet ist.	0	X	X
178.	RESRC-4	Der Speicherbereich ist nur über den Kernel zugänglich.	0	X	X
179.	RESRC-5	Der Speicher wird durch hardwarebasierte Zugriffskontrolle geschützt.	0	X	X
180.	RESRC-6	Kontingente können der Verwendung von Festplatten zugewiesen werden.	0	0	X
181.	RESRC-7	Bei Verlust der Netzwerkverbindung ist ein eingeschränkter Betrieb gewährleistet.	X	X	X
182.	RESRC-8	Das IoT-Gerät unterstützt komprimierte Datenspeicherung.	0	0	X
183.		Integritätsschutz	-	-	-
184.	INT-1	Das IoT-Gerät verfügt über einen Schutz vor dem Ausführen eines eindeutigen Codes aus einer unzuverlässigen Quelle.	0	X	X
185.	INT-2	Das IoT-Gerät hat die Möglichkeit, unerwünschte Hardware- und Softwareänderungen zu erkennen.	0	X	X
186.	INT-3	Das IoT-Gerät verfügt über eine Funktion der Sicherheitsprüfung der Übereinstimmung für die Basiskonfiguration.	0	X	X
187.	INT-4	Das IoT-Gerät verfügt über eine Integritätsprüfungsfunktion.	0	X	X
188.	INT-5	Das IoT-Tool überprüft seine Software mithilfe sicherer System-Boot-Mechanismen.	0	X	X
189.	INT-6	Wenn das IoT-Gerät nicht autorisierte Änderungen an der Software erkennt, warnt es den Benutzer oder Administrator des Problems und stellt keine Verbindung zu Netzwerken her, die größer sind als die für die Warnfunktion erforderlichen.	0	X	X
190.	INT-7	Das IoT-Tool ist in der Lage, Manipulationen während des Entwicklungslebenszyklus des Systems zu erkennen.	0	0	X
191.	INT-8	Die Laufumgebung wird auf schreibgeschützten Medien gespeichert.	0	X	X

Anforderungen, die von Anfälligkeitstests betroffen sind

Für die folgenden Anforderungen der Anlage 2 ist während der Bewertung ein Anfälligkeitstest durchzuführen:

	A	B
1.	**Kennung**	**Beschreibung**
2.	DEVID-3	Es ist möglich, die eindeutige Kennung und Modellkennzeichnung eines IoT-Geräts zu definieren, das ferngesteuert werden kann.
3.	DEVID-4	Das IoT-Tool sollte die Möglichkeit bieten, eine eindeutige physikalische Kennung hinzuzufügen, auf die autorisierte Stellen Zugriff haben.
4.	DEVOP-3	Nicht autorisierte Benutzer können sich der eindeutigen logischen IoT-Gerätekennung nicht bewusst werden.
5.	IDSUPP-2	Die Überprüfung der Authentizität anderer IoT-Geräte ist gewährleistet.
6.	IDSUPP-3	Bei Netzwerk- und Fernzugriff-Netzwerkverbindungen führt das IoT-Gerät vor dem Aufbau der identifizierten Verbindung eine kryptographische bidirektionale Identifizierung durch.
7.	IDSUPP-4	Das IoT-Tool unterstützt zertifikatbasierte Identifizierung und Authentifizierung.
8.	DEVCONF-1	Die Konfiguration der logischen Zugriffsrechte, die Konfiguration des IoT-Geräts, wie im Abschnitt „Logischer Zugriff auf Schnittstellen“ beschrieben, ist nur durch privilegierte Benutzer möglich.
9.	DEVCONF-2	Nur autorisierte Benutzer können die IoT-Geräteidentifikationsrichtlinie und die Listen der Zugriffsbeschränkungen konfigurieren. Wie im Abschnitt „Logischer Zugriff auf Schnittstellen“ beschrieben.
10.	DEVCONF-3	Nur autorisierte Benutzer können die logischen und physikalischen Schnittstellen des IoT-Geräts gemäß dem Abschnitt „Logischer Zugriff auf Schnittstellen“ konfigurieren.
11.	CRYPT-1	Das IoT-Tool bietet einen kryptografischen Algorithmus mit ausreichender Stärke und Effizienz, um die Daten zu schützen.

12.	CRYPT-2	Das IoT-Tool ist in der Lage, einzelne Zertifikate zu validieren.
13.	CRYPT-3	Die digitale Signaturverifizierung ist gewährleistet.
14.	CRYPT-4	Das IoT-Tool kann Hash-Algorithmen ausführen.
15.	CRYPT-6	Der Quellcode des Geräts enthält keine fest programmierten kritischen Sicherheitsparameter.
16.	CRYPT-7	Die kritischen Sicherheitsparameter, die zur Überprüfung der Integrität und Authentizität von Software-Updates und zum Schutz der Kommunikation mit verwandten Diensten in der Gerätesoftware verwendet werden, müssen für jedes Gerät einzigartig sein und mit einem Mechanismus erstellt werden, der das Risiko automatisierter Angriffe auf Anlageklassen verringert.
17.	CRYKEY-1	Das IoT-Gerät verwaltet kryptografische Schlüssel sicher.
18.	CRYKEY-2	Das IoT-Tool ist in der Lage, Schlüsselpaare zu generieren.
19.	CRYKEY-3	Das IoT-Gerät speichert die kryptografischen Schlüssel sicher.
20.	CRYKEY-4	Das IoT-Gerät nimmt Änderungen an den kryptografischen Schlüsseln sicher vor.
21.	CRYKEY-5	Das IoT-Tool prüft die kryptografischen Schlüssel, die von externen Systemen generiert werden.
22.	SECSTR-1	Das IoT-Gerät speichert und übermittelt keine Passwörter, ausgenommen die Speicherung des aus dem Passwort generierten Hashwerts mit der irreversiblen kryptografischen Splitting-Funktion.
23.	SECSTR-4	Schutz personenbezogener Daten wird gemäß 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) sichergestellt.
24.	SECDT-3	Das IoT-Gerät verfügt über einen Schutz vor unbefugtem Zugriff und Modifikation in der Datenverbindungsumgebung.
25.	SECDT-4	Das IoT-Tool überprüft die Integrität der übertragenen und empfangenen Daten mithilfe einer kryptografischen Lösung.
26.	AUTH-3	Für bestimmte Benutzerpopulationen unterstützt das IoT-Tool eine Multi-Faktor-Authentifizierungsmethode.

27.	AUTH-5	Bei der Generierung von Standardkennwörtern verwendet das IoT-Tool einen Generierungsalgorithmus, der das Risiko automatischer Angriffe reduziert.
28.	AUTH-7	Das IoT-Tool versteckt die Daten während des Authentifizierungsprozesses.
29.	AUTH-8	Das IoT-Tool unterstützt eine standardisierte, einheitliche Authentifizierungsmethode. (z. B. SAML, OAuth2)
30.	AUTH-9	Für den Fernzugriff prüft das IoT-Gerät die Authentifizierungsdaten pro Vorgang.
31.	AUTH-10	Durch die Bereitstellung einer versteckten Rückmeldung der Informationen, die in der Rückmeldung der Authentifizierungsmethode enthalten sind, stellt das IoT-Gerät sicher, dass Authentifizierungskennungen nicht bekannt werden und von Unbefugten nicht wiederverwendet werden können.
32.	IDENT-10	Das IoT-Tool unterstützt die Authentifizierung externer Benutzer und Systeme.
33.	NOTIF-4	Der gesamte Inhalt von Benachrichtigungen mit personenbezogenen Daten und dem von Sicherheitsbenachrichtigungen kann erst nach der Identifizierung offengelegt werden, und empfindliche Daten werden in der Warnmeldung nicht angezeigt.
34.	ACCESS-1	Das IoT-Gerät ist widerstandsfähig gegen unautorisierte Vorgänge.
35.	ROLE-12	Mit dem IoT-Tool kann man für jeden Benutzertyp restriktive Bedingungen festlegen (z. B. zeitliche Begrenzung, IP-Grenze).
36.	INTCTRL-2	Die Verwendung von Komponenten des IoT-Geräts kann eingeschränkt werden (Ports, Funktionen, Ein- und Ausgabegeräte).
37.	INTCTRL-3	Physikalische oder logische Schnittstellen, die für den Betrieb des IoT-Geräts nicht erforderlich sind, können deaktiviert werden.
38.	INTCTRL-4	Nur die minimalen logischen und physischen Schnittstellen, die für die Installation und Inbetriebnahme erforderlich sind, sind im voreingestellten Werkszustand zulässig.
39.	INTCTRL-5	Im voreingestellten Werkszustand schützt das IoT-Gerät vor dem Abruf von Sicherheitsinformationen ohne Identifikation.
40.	INTCTRL-8	Der externe Zugriff auf die Verwaltungsschnittstelle kann deaktiviert werden.
41.	INTCTRL-9	Der Zugriff auf die logischen Schnittstellen des IoT-Geräts kann gesteuert werden.

42.	INTCTRL-10	Das IoT-Gerät unterstützt eine drahtlose Verbindung, deren sicheres und autorisiertes Authentifizierungsprotokoll konfiguriert werden kann.
43.	INTCTRL-11	Wenn Ihr IoT-Gerät über eine Debug-Schnittstelle verfügt, ist dies durch Software unzulässig.
44.	UPD-4	Autorisierte Konten können die Software auf eine frühere Softwareversion zurücksetzen. (z. B. Downgrade-Angriff)
45.	UPD-5	Software-Updates stammen aus einer zuverlässigen Quelle und die Einhaltung dieser Bedingung wird vom IoT-Gerät überprüft.
46.	SECCOM-2	Das IoT-Gerät ist in der Lage, Verkehrsmanagementregeln durchzusetzen.
47.	RESRC-3	Die verschiedenen Prozesse erreichen nicht den Speicherbereich, der einem anderen Prozess zugeordnet ist.
48.	RESRC-4	Der Speicherbereich ist nur über den Kernel zugänglich.
49.	RESRC-5	Der Speicher wird durch hardwarebasierte Zugriffskontrolle geschützt.
50.	INT-1	Das IoT-Gerät verfügt über einen Schutz vor dem Ausführen eines eindeutigen Codes aus einer unzuverlässigen Quelle.
51.	INT-2	Das IoT-Gerät hat die Möglichkeit, unerwünschte Hardware- und Softwareänderungen zu erkennen.
52.	INT-4	Das IoT-Gerät verfügt über eine Integritätsprüfungsfunktion.
53.	INT-5	Das IoT-Tool überprüft seine Software mithilfe sicherer System-Boot-Mechanismen.
54.	INT-6	Wenn das IoT-Gerät nicht autorisierte Änderungen an der Software erkennt, warnt es den Benutzer oder Administrator des Problems und stellt keine Verbindung zu Netzwerken her, die größer sind als die für die Warnfunktion erforderlichen.

Anlage 4 der Verordnung Nr .../2024 (… …) der Aufsichtsbehörde für Regulierungsfragen (SZTFH)

Bewertungsmethodik

1. Das zu prüfende IoT-Gerät

1.1. Die zu prüfende VE ist ein spezifisches IoT-Tool, das gemäß den Bestimmungen dieses Zertifizierungssystems bewertet werden muss. Der Hersteller oder die Konformitätsbewertungsstelle, die die Bewertung durchführt, ist in der Lage, VE über die verfügbaren Schnittstellen zu kontrollieren, und ist sich auf der Grundlage der im MD bereitgestellten Informationen teilweise dessen Konstruktion (Greybox-Prüfung) bewusst. Die VE muss während der Bewertung in einem betriebsfähigen Zustand sein, und andere damit zusammenhängende Dienstleistungen müssen auch dann in Betrieb sein, auch wenn sie vom Hersteller oder von der Konformitätsbewertungsstelle nicht überprüft werden.

2. Dokument, das die Bewertung untermauert

2.1. Das in Anlage 1 genannte EMD wird vom Hersteller in Bezug auf die in VE umgesetzten und unterstützten Fähigkeiten gemäß den Bestimmungen dieses Zertifizierungssystems erstellt. Im EMD erklärt der Hersteller, dass alle Anforderungen in Anlage 2 für das geprüfte Zuverlässigkeitsniveau erfüllt sind.

3. Umsetzungsdokument

3.1. Der Hersteller erstellt ein MD gemäß Anlage 1, das weitere und detailliertere Informationen zur Durchführung der Bewertung enthält. Das MD ist eine Basis für die Bewertungsmethodik und enthält einige Projektdetails für die Konformitätsbewertungsstelle.

3.2. Der Hersteller muss beim Ausfüllen des MD vollständige, detaillierte und korrekte Angaben machen.

3.3. Bei der Vervollständigung des MD kann sich der Hersteller auch auf bestehende Unterlagen beziehen; in diesem Fall stellt er der Konformitätsbewertungsstelle die Referenzdokumentation zur Verfügung.

4. Aufgaben und Pflichten des Herstellers

4.1. Der Hersteller als die Organisation, die die Bewertung einleitet, beantragt die Prüfung einer bestimmten VE im Rahmen dieses Zertifizierungssystems. Der Hersteller ist die zentrale Anlaufstelle für die Konformitätsbewertungsstelle und ist verantwortlich für die Koordinierung mit den an der Lieferkette und dem Ökosystem der VE beteiligten Parteien, insbesondere Komponentenherstellern, Dienstleistern und Anwendungsentwicklern.

4.2. Die Bewertungen bestehender Sicherheitszertifikate oder Teile von VE durch Dritte können teilweise als Nachweis der Einhaltung verwendet werden, um die für die Bewertung erforderlichen Ressourcen und Zeit zu reduzieren. In diesem Fall muss der Hersteller im EMD angeben, dass die Konformität bereits bewertet wurde, zusammen mit einem Verweis auf geeignete Nachweise. Darüber hinaus übermittelt der Hersteller der

Konformitätsbewertungsstelle alle für die Prüfung der Nachweise erforderlichen Informationen, insbesondere die Einzelheiten der Zertifizierung und der Bewertungsberichte. Während der Bewertung überprüft die Konformitätsbewertungsstelle, ob die Nachweise die Einhaltung der Anforderung gemäß Anlage 2 nachweisen können.

5. Aufgaben und Pflichten der Konformitätsbewertungsstelle

5.1. Das von der Konformitätsbewertungsstelle beauftragte Prüflabor führt die Konformitätsbewertung der VE durch. Bei der Bewertung werden auch Verbindungen zu verwandten Dienstleistungen sowie die Entwicklungs- und Managementprozesse von VE berücksichtigt. Bei Eigen-Konformitätsbewertungen gilt für die Zwecke von Nummer 6 die Konformitätsbewertungsstelle als Hersteller.

6. Das Bewertungsverfahren

6.1. Die Phasen des Bewertungsverfahrens sind wie folgt:

6.2. Für jede der im EMD als „anwendbar und erfüllt“ bezeichneten Anforderungen erfasst eine Konformitätsbewertungsstelle die Prüffälle gemäß Nummer 7 und erstellt einen Prüfplan für VE und führt die Prüfungen durch.

6.2. Für jede der im EMD genannten Anforderungen sind mehrere Prüffälle gemäß den Nummern 6.2.1 bis 6.2.5 zu prüfen.

6.2.1. Prüffall: <*Anforderungs-ID*>*-T0 – Anwendbarkeit*

Zweck der Prüfung:
Mit diesem Prüffall soll die Anwendbarkeit einer spezifischen Anforderung gemäß Anlage 2 bewertet werden.

Prüfeinheiten:

a) Eine Konformitätsbewertungsstelle überprüft, ob der Hersteller die Anforderung als „anwendbar und erfüllt“ bezeichnet hat.
b) Wurde die Anforderung als „anwendbar und erfüllt“ eingestuft, prüft eine Konformitätsbewertungsstelle, ob der Hersteller die Leistungsmethode angegeben hat.
c) Wurde die Anforderung als „Nicht anwendbar“ eingestuft, prüft und bewertet die Konformitätsbewertungsstelle ihre Begründung.

Entscheidung:
Eine „Bestanden“-Entscheidung kann getroffen werden, wenn:

- Im Falle der Einstufung „anwendbar und erfüllt“ die „Leistungsmethode“ abgeschlossen wurde
- Bei der Einstufung „nicht anwendbar“ die Begründung begründet ist.

Ansonsten ist die Entscheidung „Nicht bestanden“.

6.2.2. Prüffall: <*Anforderungs-ID*>*-T1 – Dokumentation*

Voraussetzung:
die Anforderung in Anlage 2 ist „Anwendbar und erfüllt“ gemäß EMD, und der vorherige Testfall (<Anforderungskennung>-T0) wird als „Bestanden“ bewertet.

Zweck der Prüfung:
Mit diesem Prüffall soll festgestellt werden, dass eine spezifische Anforderung nach Anlage 2 dokumentiert ist. Der Prüffall gilt für alle Zuverlässigkeitsniveaus.

Prüfeinheiten:

> Eine Konformitätsbewertungsstelle überprüft, ob die Einhaltung der Anforderung vom Hersteller ordnungsgemäß dokumentiert wurde, und ermittelt die MD-Elemente, die zum Nachweis der Einhaltung dieser Anforderung verwendet werden können.

Entscheidung:
Eine „Bestanden"-Entscheidung kann getroffen werden, wenn das MD alle relevanten Informationen über die Anforderung enthält.
Ansonsten ist die Entscheidung „Nicht bestanden".

6.2.3. Prüffall: <*Anforderungskennung*>*-T2 – Konzeptionelle Prüfung*

Voraussetzung:
die Anforderung in Anlage 2 ist „Anwendbar und erfüllt" gemäß EMD, und der vorherige Testfall (<Anforderungskennung>-T1) wird als „Bestanden" bewertet.

Zweck der Prüfung:
Zweck dieses Prüffalls ist es, die konzeptionelle Konformität der Übereinstimmung mit der Anforderung an die Dokumentation nach Anlage 2 festzustellen. Der Prüffall gilt für alle Zuverlässigkeitsniveaus.

Prüfeinheiten:
Eine Konformitätsbewertungsstelle überprüft, ob VE auf der Grundlage der im Prüffall mit <Anforderungskennung>-T1 identifizierten Informationen die Anforderung gemäß Anlage 2 konzeptionell erfüllt.

Entscheidung:
Eine „Bestanden"-Entscheidung kann getroffen werden, wenn VE auf der Grundlage der im Prüffall mit <Anforderungskennung>-T1 identifizierten Informationen konzeptionell mit der Anforderung gemäß Anlage 2 übereinstimmt und die angewandte Sicherheitskontrolle und -umsetzung für das Zuverlässigkeitsniveau risikoproportional ist.
Ansonsten ist die Entscheidung „Nicht bestanden".

6.2.4. Prüffall: <*Anforderungskennung*>*-T3 – Umsetzungsprüfung*

Voraussetzung:
die Anforderung in Anlage 2 ist „Anwendbar und erfüllt" gemäß EMD, und der vorherige Testfall (<Anforderungskennung>-T2) wird als „Bestanden" bewertet.

Zweck der Prüfung:
Zweck dieses Prüffalls ist es, durch die Dokumentation die Einhaltung der Anforderung nach Anlage 2 festzustellen. Der Prüffall gilt für alle Zuverlässigkeitsniveaus.

Prüfeinheiten:

Eine Konformitätsbewertungsstelle überprüft, ob die Umsetzung gemäß den im Prüffall mit <Anforderungskennung>-T1 ermittelten Informationen stattgefunden hat.

Entscheidung:
Eine „Bestanden"-Entscheidung kann getroffen werden, wenn die Implementierung auf der Grundlage der im Prüffall mit <Anforderungskennung>-T1 identifizierten Informationen durchgeführt wurde.
Ansonsten ist die Entscheidung „Nicht bestanden".

6.2.5. Prüffall: *<Anforderungskennung>-T4 – Anfälligkeitstest*

Voraussetzung:
die Anforderung in Anlage 2 ist „Anwendbar und erfüllt" gemäß EMD, und der vorherige Testfall (<Anforderungskennung>-T2) wird als „Bestanden" bewertet.

Zweck der Prüfung:
Der Zweck dieses Prüffalls besteht darin, die Anforderung gemäß Anlage 3 mit einer Prüfmethode für Schwachstellen zu bewerten. Der Prüffall ist mindestens auf einem Zuverlässigkeitsniveau „signifikant" anzuwenden.

Prüfeinheiten:
Die Konformitätsbewertungsstelle prüft, ob eine bekannte Schwachstelle in Bezug auf die verwendeten Lösungen vorliegt, und überprüft die Erfüllung des Sicherheitsziels mittels eines manuellen Anfälligkeitstests.

Entscheidung:
Eine „Bestanden"-Entscheidung kann getroffen werden, wenn auf der Grundlage des Tests keine Schwachstelle festgestellt werden kann.
Ansonsten ist die Entscheidung „Nicht bestanden".

7. Ergebnis der Bewertung

Als Ergebnis der Bewertung werden die Prüffallergebnisse auf Prüffallbasis erfasst. Die Konformitätsbewertungsstelle erstellt einen Bewertungsbericht über die Durchführung der Prüffälle, der Folgendes umfasst:

- die im EMD erfassten Informationen,
- die Prüffallkennungen für jede Anforderung,
- die Art und Weise, wie Prüffälle bewertet werden,
- die Tatsachen, die der Entscheidung in Bezug auf den Prüffall zugrunde liegen,
- bei einem Prüffall für Schwachstellenprüfung, den Prüfbericht,
- die Entscheidung über den Prüffall,
- eine Gesamtbewertung der Anforderungen.

Bewertung der Anforderung:

- „Erfüllt", wenn alle Testfälle im Zusammenhang mit der Anforderung „Bestanden" sind,
- Die Bewertung führt zu einem Ergebnis „Nicht erfüllt", wenn bei einem der Prüffälle im Zusammenhang mit der Anforderung ein „Nicht bestanden" vorliegt.

Eine Konformitätserklärung oder ein nationales Cybersicherheitszertifikat kann ausgestellt werden, wenn die VE für alle im EMD festgelegten Anforderungen als „Bestanden“ bewertet wird.

Anlage 5 der Verordnung Nr .../2024 (… …) der Aufsichtsbehörde für Regulierungsfragen (SZTFH)

KONFORMITÄTSERKLÄRUNG

NATIONALE KONFORMITÄTSERKLÄRUNG FÜR CYBERSICHERHEIT

Name des Herstellers:
Anschrift des Herstellers:

Losgerät	
Name:	
Versionsnummer,	
Modellnummer:	
Zuverlässigkeitsniveau:	

Sonstige technische Spezifikationen, Normen und Verfahren:

Umfang und Umstandsbeschränkung:

Gültigkeitsdauer: **Tag**

Ich erkläre, dass das oben beschriebene Produkt den Anforderungen der Verordnung der Aufsichtsbehörde für Regulierungsfragen über das nationale Cybersicherheits-Zertifizierungssystem für IoT-Geräte entspricht.
Hiermit erkläre ich, dass nur *[Name des Herstellers]* berechtigt ist, diese Erklärung auszustellen.

Ausstellungsdatum: Hier klicken, um ein Datum einzugeben.

---
autorisierte Unterschrift des Herstellers

.....

Von SZTFH auszufüllen.

Datum der Registrierung:	
Registrierungs-ID:	

SZTFH **Aufsichtsbehörde** für Regulierungsfragen

Anlage 6 der Verordnung Nr .../2024 (… …) der Aufsichtsbehörde für Regulierungsfragen (SZTFH)

Nationales CYBERSICHERHEITS-Zertifikat

NATIONALE CYBERSICHERHEIT

ZERTIFIKAT

<Name der Konformitätsbewertungsstelle> (registrierte Anschrift), eingetragen von der Aufsichtsbehörde für Regulierungsfragen unter Registrierungsnummer <Registrierungsnummer> als **eine Konformitätsbewertungsstelle** die die Kriterien für die Ausstellung von Cybersicherheitszertifikaten auf dem <Zuverlässigkeitsniveau> gemäß der Verordnung SZTFH- über die Cybersicherheitszertifizierung von Informations- und Kommunikationstechnologien erfüllt, **bescheinigt** das folgende IoT-Gerät, das von

<Name des Herstellers>,

nämlich

<IoT-Gerätename

die Anforderungen der Verordnung der Aufsichtsbehörde für Regulierungsfragen über das nationale Cybersicherheits-Zertifizierungssystem für IoT-Geräte erfüllt, auf dem Zuverlässigkeitsniveau

<Zuverlässigkeitsniveau>

.

Dieses Zertifikat wurde auf der Grundlage des Bewertungsberichts Nummer <Nummer> ausgestellt.

Erstellt im Namen von <Kundenname> (Geschäftssitz).

Gültigkeitsdauer: Tag

Ausstellungsdatum: Hier klicken, um ein Datum einzugeben.

---------- ----------

Fachzertifizierer der Konformitätsbewertungsstelle

autorisierte Unterschrift

.....

Von SZTFH auszufüllen.

Datum der Registrierung:	
Registrierungs-ID:	

SZTFH

Aufsichtsbehörde
für Regulierungsfragen

Anlage 7 der Verordnung Nr .../2024 (… …) der Aufsichtsbehörde für Regulierungsfragen (SZTFH)

Etikett und Kennzeichnung