Cyber-Sicherheit für Systeme und Komponenten der Brandschutz- und Sicherheitstechnik

Anforderungen

VdS 3836 : 2019-12 (01)

Herausgeber und Verlag: VdS Schadenverhütung GmbH

Amsterdamer Str. 172-174
D-50735 Köln
Telefon: (0221) 77 66 0; Fax: (0221) 77 66 341

VdS-Richtlinien für Cyber-Security

Cyber-Sicherheit für Systeme und Komponenten der Brandschutz- und Sicherheitstechnik

Anforderungen

Das vorliegende Dokument ist nur verbindlich, sofern dessen Verwendung im Einzelfall vereinbart wird; ansonsten ist die Berücksichtigung dieses Dokuments unverbindlich. Die Vereinbarung zur Verwendung dieses Dokuments ist rein fakultativ. Dritte können im Einzelfall auch andere Anforderungen nach eigenem Ermessen akzeptieren, die diesem Dokument nicht entsprechen.

Inhalt

1 Allgemeines

1.1 Geltungsbereich

Die Ausstattung vieler Systeme und Komponenten (im Weiteren Komponenten genannt) mit Netzwerkfunktionalität (z. B. IoT-Produkte) schreitet voran. Aufgrund der zunehmenden Vernetzung softwarebasierter Komponenten und dem damit verbundenen zunehmenden Datenaustausch untereinander steigt auch das potentielle Schadensrisiko bei Ausfall solcher Komponenten. Daher muss die Cyber-Sicherheit dieser Komponenten gewährleistet sein. Zum Nachweis eines angemessenen Cyber-Sicherheitsniveaus bietet VdS Schadenverhütung GmbH mit diesen Richtlinien eine geeignete Möglichkeit zur Anerkennung der Cyber-Sicherheit für Komponenten der Brandschutz- und Sicherheitstechnik.

Diese Richtlinien gelten für Komponenten, die in

- Überfall- und Einbruchmeldeanlagen
- Brandmelde- und Sprachalarmanlagen
- Wächterkontroll- und Sicherungsanlagen
- Feuerlöschanlagen
- Zutrittskontrollanlagen
- Videosicherheitsanlagen und -managementsystemen
- anderen Gefahrenmelde- und -alarmierungsanlagen

zum Einsatz kommen.

Im weiteren Verlauf des Anerkennungsprozesses wird die Komponente hinsichtlich der Umsetzung der Anforderungen zur Cyber-Sicherheit betrachtet.

Anforderungen an dedizierte Netze sind nicht Bestandteil dieser Richtlinien. Dennoch wird darauf hingewiesen, dass der Betrieb von Komponenten der vorgenannten Anlagen und Systeme, innerhalb eines dedizierten Netzes, das Schutzniveau signifikant erhöhen kann.

Die Prüfung, Anerkennung und Zertifizierung nach diesen Richtlinien erfolgt nach den Vorgaben der VdS 2344. Es gelten die AGB VdS 3177 in der zum Zeitpunkt des Vertragsschlusses gültigen Fassung.

1.2 Gültigkeit

Diese Richtlinien sind gültig ab 01.01.2020.

1.3 Anwendungshinweise

Eine Anerkennung nach diesen Richtlinien kann nur in Kombination mit einer produktspezifischen Anerkennung gemäß den geltenden Richtlinien erteilt werden. Die vorliegenden Richtlinien können nur dann Anwendung finden, wenn dies in den zugrundeliegenden Anforderungen (Richtlinien für Produkte, Systeme oder Anlagen, Planung und Einbau etc.) nicht ausgeschlossen ist.

Zudem muss bei Anerkennung einer Komponente nach diesen Richtlinien gewährleistet sein, dass die ursprünglich anerkannten Produkteigenschaften nicht negativ beeinflusst werden (dies gilt sowohl für die Komponente als auch für die zugrundliegende sicherheitstechnische Anlage). Kann die Rückwirkungsfreiheit vom Hersteller nicht nachgewiesen

werden, so muss im Rahmen der Anerkennung nach diesen Richtlinien ebenfalls die entsprechende produktspezifische Anerkennung erneut durchlaufen werden. Der Umfang der Nachprüfung wird durch die Zertifizierungsstelle festgelegt.

Stehen einzelne Anforderungen dieser Richtlinien im Widerspruch zu Anforderungen der zugrundeliegenden produktspezifischen Richtlinien oder sind Anforderungen aufgrund des vorgesehenen Einsatzzwecks der Komponente nicht sinnvoll oder anwendbar, sind diese im Wege der Risikoanalyse gemäß Abschnitt 5.7 zu dokumentieren bzw. zu behandeln.

1.4 Abgleich mit anderen Regelwerken

Über die hier aufgeführten Normen, Richtlinien und Dokumente hinaus, sind die Richtlinien VdS 3836 mit weiteren Regelwerken abgeglichen. Der Abgleich beinhaltet nicht die Übernahme von Inhalten dieser Regelwerke, sondern vielmehr den Ausschluss, dass die Richtlinien VdS 3836 inhaltlich in Widerspruch zu diesen Regelwerken stehen. Ein Abgleich erfolgte unter anderem mit folgenden Regelwerken:

- IEC 62443, Normenreihe Industrial communication networks – Network and system security
- Positionspapier des Gesamtverbandes der Deutschen Versicherungswirtschaft (GDV) zu den Anforderungen an Smart Home Installationen sowie Geräten des „Internet der Dinge“
- ETSI TS 103 645 Technical Specification, Cyber; Cyber Security for Consumer Internet of Things

2 Normative Verweise

Diese Richtlinien enthalten datierte und undatierte Verweise auf andere Regelwerke. Die Verweise erfolgen in den entsprechenden Abschnitten, die Titel werden im Folgenden aufgeführt. Änderungen oder Ergänzungen datierter Regelwerke gelten nur, wenn sie durch Änderung dieser Richtlinien bekannt gegeben werden. Von undatierten Regelwerken gilt die jeweils zuletzt veröffentlichte Fassung.

Algorithms, key size and parameters report – 2014

BSI C5 Anforderungskatalog Cloud Computing (C5)

BSI TR-02102-2 Kryptographische Verfahren: Verwendung von Transport Layer Security (TLS)

ETSI TS 103 645 Cyber Security for Consumer Internet of Things

EU-DSGVO 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

ISO/IEC 29147 Information technology – Security techniques – Vulnerability disclosure

IT-Sicherheitsgesetz Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme

Kriterienkatalog für Cloud Services (Herausgeber: Bundesministerium für Wirtschaft und Energie)

NIST Special Publication 800-57 Part 1 Revision 4 Recommendation for Key Management, Part 1: General

VdS 2203 VdS Richtlinien für Brandschutz und Sicherungstechnik, Software, Anforderungen und Prüfmethoden

VdS 3177 Allgemeine Geschäftsbedingungen, AGB der VdS Schadenverhütung GmbH für Dienstleistungen des Bereichs Produkte und Unternehmen

3 Begriffe, Definitionen und Abkürzungen

3.1 Begriffe und Definitionen

Benutzer: Person, Komponente, Organisationseinheit oder automatisierter Prozess, der auf ein System zugreift

Dedizierter Kommunikationsweg: Kommunikationsweg, der für die Datenübertragung (hier in Form elektronischer Signale) einer einzigen Anwendung exklusiv zur Verfügung steht

Duty Cycle: Der Duty Cycle (zu Deutsch etwa Tastverhältnis oder Auslastungsgrad) ist ein Kennwert von Pulsen, das durch das zeitliche Verhältnis von Pulsdauer zu Pulsperiode definiert ist. In den vorliegenden Richtlinien wird der Begriff in Zusammenhang mit der geregelten Begrenzung der Sendezeit von Funkkomponenten verwendet. Das Ziel der Sendezeitbegrenzung ist es, die Funktion jeder Komponente im entsprechenden Frequenzbereich zu gewährleisten.

Fremdprodukte/Fremddienste: Komponenten oder Dienste, welche nicht speziell für das anzuerkennende Produkt hergestellt oder angeboten wurden, welche aufgrund der technischen Eigenschaften aber als zusätzliche Funktionseinheit eingesetzt bzw. betrieben werden können

Hinweis: Öffentliche Teile des Übertragungsweges, herkömmliche Computer z. B. für Wartungsarbeiten oder cloudbasierte Datenverarbeitungsdienste können beispielsweise als Fremdkomponente oder Fremddienste eingesetzt werden.

Headless API: (Programmier-)Schnittstelle (von englisch application programming interface), die eine Reihe von Funktionen und Verfahren zur Verfügung stellt, mit denen Anwendungen erstellt werden können, die auf die Funktionen oder Daten eines Betriebssystems, einer Anwendung oder eines anderen Dienstes zugreifen können. Die Eigenheit einer headless API ist, dass der Zugriff auf die definierten Funktionen und Verfahren der eigentlichen API durch eine Drittanwendung ausgeführt werden können.

Komponente: materielle Einheit zur Bereitstellung einer oder mehrerer Funktionen mit Netzwerkanbindung

Netzübergang: Schnittstelle zwischen zwei unterschiedlichen Netzwerken

Hinweis: Dabei können sich die Netzwerke z. B. durch die physikalischen Übertragungsmedien, durch die verwendeten Protokolle, durch eine unterschiedliche administrative Hoheit oder unterschiedliche Sicherheitsniveaus voneinander unterscheiden.

Pairing: Verfahren zur gegenseitigen Authentisierung zweier Kommunikationspartner und der Vereinbarung eines gemeinsamen Verbindungsschlüssels zur Sicherung der nachfolgenden Kommunikation

(Sicherheits-)kritische Daten: Daten,

- die nach Kenntniserlangung durch eine Person oder ein System, die Person oder das System auf den Sicherheitszustand der Komponente oder des Systems schließen lässt.
- die nach Kenntniserlangung durch eine Person oder ein System, eine potentielle Einflussnahme auf den Sicherheitszustand der Komponente oder des Systems zur Folge haben können.
- die durch Verordnungen oder Gesetze als (sicherheits-)kritisch definiert sind.
- *Hinweis 1: Im Rahmen dieser Richtlinien wird die vorgenannte Definition analog für (sicherheits-)kritische Ereignisse, Funktionen und Dienste verwendet.*
- *Hinweis 2: Kritische Daten, die durch Verordnungen oder Gesetze als solche definiert sind, können z. B. besondere Kategorien personenbezogener Daten im Sinne des Art. 9 EU-DSGVO sein.*

Sicherheitszustand: Durch Akzeptanz oder durch Umsetzung von Maßnahmen gegen bestimmte Risiken definierter Zustand (bzw. definiertes Schutzniveau)

Hinweis: Der angestrebte Sicherheitszustand einer Komponente wird mit einzuhaltenden, messbaren Größen vorgegeben und kann bspw. durch organisatorische oder technische Maßnahmen erreicht werden.

System: Zusammenstellung von Komponenten, die frei kombinierbar oder in festgelegten Konfigurationen zum Bau von Anlagen eingesetzt werden können und diesbezüglich auf ein funktionsgemäßes Zusammenwirken abgestimmt sind

Telemetriedaten: Messwerte eines am Messort befindlichen Messfühlers (Sensor), aus denen z. B. Rückschlüsse auf den Betriebszustand des Messwertaufnehmers respektive des Telemetriesenders gezogen werden können

3.2 Abkürzungen

In den vorliegenden Richtlinien werden die folgenden Abkürzungen verwendet:

BSI	Bundesamt für Sicherheit in der Informationstechnik
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoS	Denial of Service
ETSI	European Telecommunications Standards Institute
EU-DSGVO	Datenschutzgrundverordnung
FTP	File Transfer Protocol
IoT	Internet of Things
JTAG	Joint Test Action Group
NIST	National Institute of Standards and Technology
NSL	Notruf- und Service-Leitstelle
SMTP	Simple Mail Transfer Protocol
TS	Technical Specification

4 Klassifizierung

Die Anforderungen an Komponenten und Systemen in diesen Richtlinien sind in drei unterschiedliche Klassen (im Sinne von Sicherheitsleveln) strukturiert. Je nach Einsatzzweck der Komponenten müssen die Anforderungen der entsprechenden Klasse erfüllt sein. Sind Anforderungen aufgrund der technischen Komponentenausführung, des jeweiligen Einsatzzwecks, aufgrund rechtlicher oder anderweitiger Regelungen oder ähnlichem nicht anwendbar, muss der Hersteller dies im Rahmen der Risikoanalyse gemäß Abschnitt 5.7 dokumentieren bzw. behandeln. Die Prüfung der gesamten Dokumentation durch VdS (siehe Abschnitt 5.6.1) ist Bestandteil des Anerkennungsprozesses.

Der Hersteller muss mit der Beauftragung eines Anerkennungsverfahrens nach diesen Richtlinien der Zertifizierungsstelle schlüssig darlegen, welche Klassifizierung er für die anzuerkennende Komponente anstrebt. Ausschlaggebend für eine Klassifizierung sind u. a. der übliche Anwendungsfall und dessen Schutzziel sowie die bei dem Anwendungsfall zu erwartende Gefährdung der Komponente.

Die nachfolgende Tabelle gibt eine Übersicht über die klassenspezifisch gültigen Anforderungen des Abschnittes 5:

Anforderungen	**Klasse A**	**Klasse B**	**Klasse C**
Allgemeine Anforderungen			
Gewährleistung von Offline-Funktionalität („Notbetrieb“) gemäß Abschnitt 5.1.1	op	m	m
Herstellung eines sicheren Zustandes (Security by Default) gemäß Abschnitt 5.1.2	m	m	m
Anpassung der Konfiguration gemäß Abschnitt 5.1.3	op	m	m
Handhabung von Fehlfunktionen und Störungen gemäß Abschnitt 5.1.4	op	m	m
Vorbestimmter Zustand von Schnittstellen gemäß Abschnitt 5.1.5	op	m	m
Funktionalität für sichere Außerbetriebnahme der Komponente gemäß Abschnitt 5.1.6	op	m	m
Manipulationssicherheit gemäß Abschnitt 5.1.7	m	m	m
Minimierung von Auswirkungen eines Denial-of-Service-Vorfalls gemäß Abschnitt 5.1.8	op	m	m
Notstromversorgung gemäß Abschnitt 5.1.9	op	m	m
Anforderungen an Benutzer-/Zugriffsmanagement			
Zugriffsschutz durch Authentisierung gemäß Abschnitt 5.2.1	op	m	m
Verzicht auf fest codierte Zugangsparameter gemäß Abschnitt 5.2.2	op	m	m
Individualisierte Benutzerkonten gemäß Abschnitt 5.2.3	op	m	m
Minimale Zugriffsrechte von Benutzerkonten gemäß Abschnitt 5.2.4	m	m	m
Zusätzlicher Zugriffsschutz bei (sicherheits-)kritischen Daten gemäß Abschnitt 5.2.5	op	op	m
Beendigung der Kommunikationssitzung bei Inaktivität gemäß Abschnitt 5.2.6	op	m	m
Anforderungen an die Vertraulichkeit und Integrität			
Verschlüsselung von Daten bei der Übertragung (Transportverschlüsselung) gemäß Abschnitt 5.3.1	m	m	m
Integrität von Daten bei der Übertragung gemäß Abschnitt 5.3.2	m	m	m
Gewährleistung der Integrität der Software gemäß Abschnitt 5.3.3	op	op	m
Plausibilität von Benutzereingaben/-aktionen gemäß Abschnitt 5.3.4	op	m	m
Sicherung von System-/Konfigurationsdaten gemäß Abschnitt 5.3.5	op	m	m
Sicherung von Nutzdaten gemäß Abschnitt 5.3.6	op	m	m
Protokollierung/Ereigniserfassung			
Überwachung/Protokollierung von Ereignissen (Audit Log) gemäß Abschnitt 5.4.1	m	m	m
Benachrichtigung bei sicherheitsrelevanten Ereignissen gemäß Abschnitt 5.4.2	op	m	m
Weitergehende Behandlung von protokollierten Ereignissen gemäß Abschnitt 5.4.3	op	m	m
Erfassung von Telemetriedaten gemäß Abschnitt 5.4.4	op	op	m
Zeitstempel und Zeitsynchronisation gemäß Abschnitt 5.4.5	m	m	m
Anforderungen an den Datenfluss			
Pairing mit weiteren Systemen/Komponenten gemäß Abschnitt 5.5.1	m	m	m
Fremdprodukte/-dienste gemäß Abschnitt 5.5.2	op	m	m
„Call Home“-Funktion gemäß Abschnitt 5.5.3	m	m	m
Verwaltung von Schnittstellen gemäß Abschnitt 5.5.4	op	m	m
Konfiguration von Remote-Zugängen gemäß Abschnitt 5.5.5	m	m	m
Begleitende Maßnahmen			
Vollständige Dokumentation der Komponente gemäß Abschnitt 5.6.1	m	m	m
Umfassende Bereitstellung Support gemäß Abschnitt 5.6.2	m	m	m
Automatische Update-Prüfung gemäß Abschnitt 5.6.3	op	m	m

m – mandatory/verpflichtend; op – optional/wahlweise

Tabelle 4-1: Klassifizierungen

Im Vergleich zu den Anforderungen der Normenreihe IEC 62443 ergibt sich folgende Korrelation:

- Klasse A orientiert sich an Security Level 1
- Klasse B orientiert sich an Security Level 2
- Klasse C orientiert sich an Security Level 3

5 Anforderungen

5.1 Allgemeine Anforderungen

5.1.1 Gewährleistung von Offline-Funktionalität („Notbetrieb“)

Die Komponente muss, sofern technisch möglich, auch bei abgeschalteten Netzwerk-Diensten (wie z. B. Cloud-Diensten) oder bei Eintritt von externen Störungen oder Fehlfunktionen (z. B. Netzwerkausfall) ein möglichst hohes Maß der Grundfunktionalität weiterhin zur Verfügung stellen.

Der Hersteller muss in der Bedienungsanleitung gemäß Abschnitt 5.6.1 den Umfang der Offline-Funktionalität beschreiben.

Hinweis: Entsprechende oder vergleichbare Anforderungen weiterer VdS-Richtlinien (z. B. Produkt-Richtlinien) bleiben hiervon unberührt.

5.1.2 Herstellung eines sicheren Zustandes (Security by Default)

Jede Komponente und deren Hard- sowie Software muss bei Inbetriebnahme und im Regelbetrieb einen sicheren Zustand annehmen. Es müssen z. B. alle (Netzwerk-)Zugriffsrechte, Freigaben, Zugänge, Fernzugänge, Dienste, Anwendungen, Schnittstellen und Ports, auf ein für die Funktion der Komponente notwendiges Mindestmaß reduziert sein. Werden Funktionen und Dienste nicht verwendet sind diese ganz abzuschalten.

Jede Aktivierung von weitergehenden Funktionen und Diensten sind nach den Vorgaben von Abschnitt 5.1.3 durchzuführen.

In der Bedienungsanleitung muss der Umfang der sicheren Konfiguration beschrieben sein.

5.1.3 Anpassung der Konfiguration

Nur autorisierte Benutzer dürfen die Möglichkeit haben, die Konfiguration anpassen zu können. Stellt die Aktivierung oder Deaktivierung einer Funktion, eines Dienstes oder einer Schnittstelle eine potentielle Gefahrenquelle für die Cyber-Sicherheit dar, ist der Benutzer über potentielle, negative Auswirkungen zu unterrichten (z. B. mittels Meldungsfenster o. ä.). Wird für die Konfiguration eine übergeordnete zentrale Steuerinstanz verwendet (z. B. headless API), so muss die Benachrichtigung des Benutzers dort erfolgen.

Der Hersteller muss in der Bedienungsanleitung darauf hinweisen, dass unnötige Funktionen, Ports, Protokolle und/oder Dienste nach Möglichkeit abgeschaltet werden sollten.

Die Anpassung der Konfiguration ist gemäß Abschnitt 5.4.1 zu protokollieren.

Hinweis: Eine potentielle Gefahrenquelle im obigen Sinne kann z. B. die Aktivierung von Fernzugriffsmöglichkeiten oder der Öffnung zusätzlicher Ports sein.

5.1.4 Handhabung von Fehlfunktionen und Störungen

Fehlfunktionen oder Störungen des Systems/der Komponente dürfen nicht die Cyber-Sicherheit der Komponente oder ggf. weiterer angeschlossener Komponenten und Netzwerke beeinträchtigen. Treten Fehlfunktionen und Störungen auf, muss die Komponente in einen sicheren Zustand versetzt werden. Dabei darf die Komponente nicht automatisch in ihren Ursprungszustand versetzt werden (z. B. Rücksetzung auf Default-Passwörter).

Sofern technisch möglich, sollten bei Eintritt von externen Störungen oder Fehlfunktionen (z. B. Strom- oder Netzwerkausfall) Kompensationsmaßnahmen getroffen werden, damit möglichst viele Funktionen der Komponente weiterhin betriebsbereit bleiben.

Bei Beseitigung der ursächlichen Fehlfunktion oder Störung muss sich die Komponente - sofern technisch möglich - automatisch wieder in den Regelbetrieb versetzen. Ist die Komponente Teil eines größeren Systemverbunds muss bei Wiederaufnahme des Regelbetriebs gesichert sein, dass durch die Wiedereinschaltung aller betroffener Komponenten nicht die Sicherheit und Leistung des gesamten Netzwerkverbunds beeinträchtigt wird (z. B. durch gleichzeitige Ausführung eines gemeinsamen Dienstes).

Fehlfunktionen oder Störungen müssen gemäß Abschnitt 5.4.1 protokolliert werden.

5.1.5 Vorbestimmter Zustand von Schnittstellen

Komponenten, deren Schnittstellen Einfluss auf weitere Abläufe, Aktionen oder den Zustand anderer Komponenten haben, müssen die Möglichkeit bieten, die Ausgangswerte im Falle von Fehlfunktionen und Störungen auf einen vorab definierten Zustand zu setzen. Der Hersteller muss in der Dokumentation die Konfigurationsmöglichkeiten und Zustände beschreiben.

5.1.6 Funktionalität für sichere Außerbetriebnahme der Komponente

Für eine sichere Außerbetriebnahme der Komponente sind Funktionen vorzusehen, durch welche ein autorisierter Benutzer alle gespeicherten Informationen oder installierten Dienste auf der Komponente und ggf. weiterer angeschlossener Komponenten (wie z. B. Sensoren) unwiderruflich löschen kann.

Hinweis: Unter zu löschende Informationen fallen je nach Einsatzzweck und Gerätetyp beispielsweise Konfigurationseinstellungen, Passwörter, Zertifikate, Daten aus Zwischenspeichern oder temporären Dateien, abgelegte Sicherungskopien, Auslagerungsdateien oder gespeicherte Video- oder Tonaufzeichnungen.

Werden Informationen auch durch weitere Dienste verarbeitet, wie z. B. Cloud-Dienste, müssen die Informationen auch auf diesen gelöscht werden. Wenn die Löschung der Daten in weiteren Diensten nicht durch Funktionen auf der Komponente gewährleistet werden kann und hierzu zusätzliche Aktionen autorisierter Benutzer notwendig sind (z. B. im Benutzer/Administrator-Portal eines Cloud-Dienstes o. ä.), muss dies in der Bedienungsanleitung transparent und für den Benutzer verständlich erläutert sein.

In der Bedienungsanleitung muss klar und transparent beschrieben sein, welche Daten durch die Löschfunktionen gelöscht werden und welche Daten ggf. nicht gelöscht werden können (z. B. bei Sicherungskopien bei Cloud-Anwendungen) und wie die Löschfunktion zu bedienen ist.

5.1.7 Manipulationssicherheit

Die Komponente muss (mechanische) Manipulationen oder unautorisierte Zugriffsversuche (z. B. über die Übertragungswege oder durch unautorisierte Benutzer) erkennen und

wirksam verhindern, dass ein Zugriff auf (sicherheits-)kritische Daten erlangt werden kann. Der Versuch einer Manipulation oder eines unautorisierten Zugriffs muss nach den Vorgaben des Abschnitts 5.4.2 zu einer Benachrichtigung führen.

Jeder Manipulationsversuch oder sonstiger unautorisierte Zugriff muss gemäß Abschnitt 5.4.1 protokolliert werden.

5.1.8 Minimierung von Auswirkungen eines Denial-of-Service-Vorfalls

Sollte die Komponente aufgrund eines Denial-of-Service-Vorfalls (DoS) in einen reduzierten Betriebszustand übergehen, muss die Komponente dennoch wichtige Funktionen aufrechterhalten. In der Bedienungsanleitung muss der Umfang des Funktionsumfangs beschrieben sein. Zudem muss der Hersteller im Projektierungshandbuch/Hardening Guide beschreiben, welche weiteren möglichen Sicherungsmaßnahmen innerhalb der IT-Infrastruktur für den entsprechenden Anwendungsfall der Komponente getroffen werden können, um einen DoS-Vorfall auf die Komponente zu vermeiden bzw. dessen Auswirkungen abzumildern.

Nach Beendigung des DoS-Vorfalls muss die Komponente selbstständig wieder in den regulären Betriebszustand wechseln.

Die Überlastung bzw. Nichtverfügbarkeit von Schnittstellen und Diensten muss gemäß Abschnitt 5.4.1 protokolliert werden.

5.1.9 Notstromversorgung

Die Komponente muss im Falle eines Ausfalls der Energieversorgung auf eine Notstromversorgung umschalten können, ohne die zu diesem Zeitpunkt durchgeführten Datenübertragungen oder -verarbeitungen zu unterbrechen. Ebenso muss ein Wechsel in den Normalbetrieb ohne Unterbrechung erfolgen.

Der Hersteller muss in seiner Bedienungsanleitung angeben für welchen Mindestzeitraum (ab Aktivierung des Notstrombetriebs) die Funktionalität der Komponente im vorgesehenen Regelbetrieb garantiert wird.

Beim Wechsel in den Notstrombetrieb bzw. zurück in den Normalbetrieb muss eine Benachrichtigung gemäß Abschnitt 5.4.2 erfolgen.

Der Wechsel in den Notstrombetrieb bzw. zurück in den Normalbetrieb muss gemäß Abschnitt 5.4.1 protokolliert werden.

5.2 Anforderungen an Benutzer-/Zugriffsmanagement

5.2.1 Zugriffsschutz durch Authentisierung

Vor der Benutzung einer Anwendung, eines Dienstes oder eines Zugangs einer Komponente muss sich jeder Benutzer authentisieren. Hierfür sind ausschließlich starke Authentisierungsmerkmale zu verwenden, die dem Stand der Technik entsprechend konfiguriert werden können.

Das Authentisierungsprotokoll muss eine dem Einsatzzweck der Komponente entsprechende ausreichende Sicherheit bieten.

Hinweis: Eine ausreichende Sicherheit muss der Zertifizierungsstelle gegenüber mittels Risikoeinschätzung belegt werden.

Insbesondere muss das Authentisierungsprotokoll folgende Anforderungen mindestens erfüllen:

- eine angemessene Sicherheit des Authentisierungsmerkmals
- ausschließlich angemessen verschlüsselte Übertragung der Authentisierungsmerkmale im Netzwerk
- Schutz gegen Replay- und Man-in-the-Middle-Attacken (z. B. durch Verwendung eines Authentisierungsprotokolls mit Instanzauthentisierung)
- konfigurierbarer Schutz gegen Ausprobieren von Authentisierungsinformationen (z. B. mittels Eingabeverzögerung, Begrenzung von Falscheingaben oder mittels Begrenzung der Anmeldeversuche pro IP-Adresse)
- bei Eingabe von Authentisierungsinformationen dürfen erfolglose Anmeldeversuche keinen Rückschluss auf die Ursache der Zurückweisung zulassen (z. B. durch Meldungen, Fehlercodes oder Antwortzeiten)
- keine Klartextdarstellung von Authentisierungsmerkmalen in Eingabemasken o. ä. (z. B. Zeichenverschleierung bei Passworteingabe)
- zugriffsgesicherte Speicherung von Authentisierungsmerkmalen (z. B. mittels dedizierter Passwort-Hashing-Funktionen)
- der Benutzer muss jederzeit die Möglichkeit haben, das Authentisierungsmerkmal ändern oder sperren zu können (z. B. Sperrung nach Kompromittierungsverdacht)
- bei Rücksetzen der Komponente (z. B. auf Werkseinstellungen) müssen eingestellte Authentisierungsmerkmale (wie z. B. Passwörter) zurückgesetzt werden

5.2.2 Verzicht auf fest codierte Zugangsparameter

Bei der Benutzung von Zugängen oder Schnittstellen dürfen keine fest codierten Zugangsparameter verwendet werden.

5.2.3 Individualisierte Benutzerkonten

Jeder Benutzer darf eine Komponente softwareseitig ausschließlich über ein individualisiertes Benutzerkonto bedienen. Die Rechtevergabe eines Benutzerkontos sollte anhand von zugewiesenen Rollen erfolgen.

Hinweis: Sind abweichende Benutzerkontenstrukturen unumgänglich, sind diese im Wege der Risikoanalyse (gemäß Abschnitt 5.7) zu behandeln.

Werden voreingestellte Authentisierungsmerkmale verwendet, dürfen diese ausschließlich zum Zwecke einer Initialisierung einmalig verwendet werden und müssen nach Benutzung umgehend vom Benutzer personalisiert werden.

Jede An-/Abmeldung eines Benutzers muss gemäß Abschnitt 5.4.1 protokolliert werden.

5.2.4 Minimale Zugriffsrechte von Benutzerkonten

Bei der Erstinbetriebnahme oder dem Rücksetzen einer Komponente dürfen Benutzerkonten ausschließlich die Zugriffsrechte haben, die für die Inbetriebnahme unbedingt notwendig sind.

Nicht notwendige Benutzerkonten sind standardmäßig zu deaktivieren.

Hinweis: Bei der Inbetriebnahme sollte z. B. nur ein Konto nutzbar sein. Bei einer Rücksetzung müssen alle ggf. weiteren schon eingerichteten Benutzerkonten vorübergehend deaktiviert werden. Nach der erfolgten Inbetriebnahme können die Standardkonten dann wieder aktiviert werden.

5.2.5 Zusätzlicher Zugriffsschutz bei (sicherheits-)kritischen Daten

Der Zugriff auf (sicherheits-)kritische Daten muss durch eine Multifaktor-Authentisierung (mindestens zwei Faktoren) abgesichert sein. Dabei sind Mechanismen zu benutzen, die dem Stand der Technik entsprechen.

Der Zugriff auf (sicherheits-)kritische Daten muss gemäß Abschnitt 5.4.1 protokolliert werden.

5.2.6 Beendigung der Kommunikationssitzung bei Inaktivität

Alle Anwendungen, Dienste oder Zugänge, für deren Nutzung eine Benutzerauthentisierung notwendig ist, müssen nach erfolgreicher Authentifizierung eines Benutzers eine eindeutige Sitzungskennung nach anerkanntem Stand der Technik erzeugen. Ungültige Sitzungskennungen müssen zurückgewiesen werden.

Dem Benutzer muss die Möglichkeit zur manuellen Sitzungsbeendigung zur Verfügung stehen. Sitzungen müssen nach einer einstellbaren Inaktivität (maximal eine Stunde) eines angemeldeten Benutzers zudem automatisch beendet werden.

Möchte der Benutzer nach der Sitzungsbeendigung (gleichgültig ob nach automatischer oder manueller Beendigung) anschließend wieder auf die Anwendung, den Dienst oder Zugang zugreifen, muss er sich erneut authentisieren.

Die automatische Beendigung muss gemäß Abschnitt 5.4.1 protokolliert werden.

5.3 Anforderungen an die Vertraulichkeit und Integrität

5.3.1 Verschlüsselung von Daten bei der Übertragung (Transportverschlüsselung)

Eine Komponente und ggf. weitere angeschlossene Komponenten oder Systeme, muss alle Informationen mit Verschlüsselungsverfahren und sicheren Netzwerkprotokollen übertragen, die dem Stand der Technik entsprechen.

Hinweis: Der aktuelle Stand der Technik ist den Empfehlungen einschlägiger Publikationen von Regulierungsbehörden zu entnehmen, wie z. B. dem Bundesamts für Sicherheit in der Informationstechnik - BSI (BSI TR-02102), dem National Institute of Standards and Technology – NIST (NIST Special Publication 800-57 Part 1 Revision 4) oder der European Union Agency for Network and Information Security – ENISA (Algorithms, key size and parameters report – 2014).

5.3.2 Integrität von Daten bei der Übertragung

Bei der Übertragung von Daten müssen die eingesetzten Übertragungsprotokolle eine Veränderung von Daten erkennen. Hierzu sind dem Stand der Technik entsprechende Verfahren zur Integritätsprüfung einzusetzen.

Hinweis: Der aktuelle Stand der Technik ist den Empfehlungen von einschlägigen Publikationen von Regulierungsbehörden zu entnehmen, wie z. B. dem Bundesamts für Sicherheit in der Informationstechnik – BSI (BSI TR-02102), dem National Institute of Standards and Technology – NIST (NIST Special Publication 800-57 Part 1 Revision 4) oder der European Union Agency for Network and Information Security – ENISA (Algorithms, key size and parameters report – 2014).

5.3.3 Gewährleistung der Integrität der Software

Bei Inbetriebnahme oder Rücksetzen der Komponente müssen vor Verwendung die Integrität der Software, Firmware und Konfigurationsdaten überprüft werden, die für die Boot- und Laufzeitprozesse der Komponente erforderlich sind.

Hinweis: Eine Überprüfung kann z. B. mittels Prüfsummen oder Signaturen erfolgen.

Alle unautorisierten Änderungen an der Software müssen im Regelbetrieb verhindert werden. Weiterhin muss jede autorisierte Änderung an der Software im Regelbetrieb erkannt und protokolliert werden.

5.3.4 Plausibilität von Benutzereingaben/-aktionen

Sämtliche Benutzereingaben oder -aktionen (inkl. Übertragungen über application programming interfaces (APIs)) sind auf Plausibilität zu prüfen. Erst nach erfolgreicher Datenvalidierung dürfen die Eingaben, Aktionen oder Übertragungen wirksame Änderungen an der Komponente oder den verarbeiteten Daten vornehmen.

Hinweis: Die Plausibilitätsprüfung prüft z. B. ob die Eingabe des Benutzers einen bestimmten Datentyp beinhaltet, eine entsprechende Syntax hat oder Teilmenge einer vorgegebenen Wertemenge ist.

5.3.5 Sicherung von System-/Konfigurationsdaten

Die Komponente muss eine Funktion zur Verfügung stellen, mit welcher sich die System-/Konfigurationsdaten extern sichern und bei Bedarf wieder zurückspielen lassen. Der Sicherungsvorgang darf den normalen Betrieb der Komponente nicht beeinträchtigen.

Hinweis: Das Speichermedium sollte nicht ständig mit der Komponente verbunden sein.

Die Sicherungskopie sollte verschlüsselt abgelegt sein. Das Verschlüsselungsverfahren muss dem aktuellen Stand der Technik entsprechen. Wird auf eine Verschlüsselung verzichtet, muss der Benutzer über die Risiken informiert werden.

Hinweis: Der aktuelle Stand der Technik ist den Empfehlungen von einschlägigen Publikationen von Regulierungsbehörden zu entnehmen, wie z. B. dem Bundesamts für Sicherheit in der Informationstechnik - BSI (BSI TR-02102), dem National Institute of Standards and Technology – NIST (NIST Special Publication 800-57 Part 1 Revision 4) oder der European Union Agency for Network and Information Security – ENISA (Algorithms, key size and parameters report – 2014).

In der Bedienungsanleitung muss darauf hingewiesen werden, dass bei Verschlüsselung der gesicherten Daten, der Schlüssel zur Entschlüsselung sicher gegen unbefugte Kenntniserlangung, Verlust oder unbeabsichtigter Veränderung geschützt werden muss.

5.3.6 Sicherung von Nutzdaten

Die Komponente muss eine Funktion zur Verfügung stellen, mit welcher sich die Nutzdaten extern sichern und bei Bedarf wieder zurückspielen lassen. Der Sicherungsvorgang darf den normalen Betrieb der Komponente nicht beeinträchtigen.

Hinweis: Das Speichermedium sollte nicht ständig mit der Komponente verbunden sein.

Die Sicherungskopie sollte verschlüsselt abgelegt sein. Das Verschlüsselungsverfahren muss dem aktuellen Stand der Technik entsprechen. Wird auf eine Verschlüsselung verzichtet, muss der Benutzer über die Risiken informiert werden.

Hinweis: Der aktuelle Stand der Technik ist den Empfehlungen von einschlägigen Publikationen von Regulierungsbehörden zu entnehmen, wie z. B. dem Bundesamts für Sicherheit in der Informationstechnik – BSI (BSI TR-02102), dem National Institute of Standards and Technology – NIST (NIST Special Publication 800-57 Part 1 Revision 4) oder der European Union Agency for Network and Information Security – ENISA (Algorithms, key size and parameters report – 2014).

5.4 Protokollierung/Ereigniserfassung

5.4.1 Überwachung/Protokollierung von Ereignissen (Audit Log)

Alle Ereignisse, die im Rahmen dieser Richtlinien zu protokollieren sind, müssen mit den nachfolgenden Informationen in einem persistenten Speicher abgelegt werden. Die zu protokollierenden Ereignisse sind den entsprechenden Hinweisen in den Abschnitten dieser Richtlinien zu entnehmen. Darüber hinaus müssen grundsätzlich alle Ereignisse protokolliert werden, die in Zusammenhang stehen mit Zugangskontrollen, fehlerhaften Anfragen, relevanten Vorfällen im Betriebssystem, relevanten Vorfällen bei der Sicherung und Wiederherstellung von Daten, Konfigurationsänderungen, Kommunikationsanfragen und Verbindungsabbrüchen.

- Ereignis*
- Auslösender Benutzer (Person, Komponente, Organisationseinheit oder automatisierter Prozess)
- Datum und Uhrzeit (rückführbar auf die Zeit der entsprechenden Zeitzone, in der die Komponente betrieben wird - siehe hierzu auch Abschnitt 5.4.5)
- Kategorie
- Art
- Kennung
- Ergebnis

* *Bei der Speicherung eines Ereignisses ist dieses nicht bloß durch Ereigniscodes o. ä., sondern im Klartext (menschenverständlich) zu erfassen. Zudem müssen bei der Protokollierung von Benutzeraktionen die einzelnen Schritte der Benutzeraktion, wie z. B. der Bedienung einzelner Steuerelemente oder die Eingabe von Zwischenwerten, soweit möglich, erfasst werden und nicht nur das Ergebnis der Benutzeraktion. Werden Steuerelemente verwendet, die die Einzelerfassung der Bedienung nicht unterstützen, sind diese in der technischen Dokumentation aufzuführen.*

Die Ereignisspeicherung muss innerhalb der Komponente erfolgen. Wird für die Konfiguration und den Betrieb eine übergeordnete zentrale Steuerinstanz verwendet, so muss die Ereignisspeicherung dort erfolgen.

Bei der Übertragung von Ereignissen an eine übergeordnete Steuerinstanz muss durch entsprechende Maßnahmen gewährleistet werden, dass durch die Erzeugung und Übertragung von einer Vielzahl an Ereignissen (z. B. durch Fehler/Störung eines Bauteils, böswilliger/fehlerhafter Kommunikationsanfragen (DoS-Angriff) oder funkintensiver Konfigurationsvorgänge) auch weiterhin die Verfügbarkeit aller an der Kommunikation beteiligter Komponenten (hierzu zählt z. B. die zugesicherte Betriebsdauer bei batteriebetriebenen Komponenten oder die Sende-/Empfangsfähigkeit) gewährleistet bleibt.

Hinweis: Entsprechende Gegenmaßnahmen können z. B. Wechsel von Frequenzbändern bei funkbasierter Kommunikation, zeitversetztes Übertragen von Ereignissen bei begrenzter Sendezeit (z. B. durch Duty Cycle) oder die zyklische Ereignisabfrage durch die zentrale Steuerinstanz sein.

Für die Aufzeichnung der Ereignisse muss die Komponente oder die zentrale Steuerinstanz ausreichend Speicherkapazität gemäß allgemein anerkannten Empfehlungen, anderweitigen Richtlinien, Vorschriften oder Geschäftsanforderungen bereitstellen. Der Betreiber muss die Möglichkeit haben, die entsprechende Speicherkapazität respektive die Speicherdauer für Aufzeichnungen von Ereignissen flexibel an den tatsächlichen Bedarf anpassen zu können. Falls die zugeteilte Speicherkapazität einen einstellbaren Anteil der gesamten Speicherkapazität für die Ereignisspeicherung erreicht, muss die Komponente oder die zentrale Steuerinstanz eine entsprechende Warnung eines (oder mehrerer) Benutzer ausgeben.

Das Erreichen oder Überschreiten der maximalen Ereignisspeicherkapazität darf nicht den Ausfall der Komponente zur Folge haben. Bei Verwendung einer zentralen Steuerungsinstanz gelten die vorgenannten Anforderungen für jede angeschlossene Komponente. Zudem muss durch jede Komponente gesichert sein, dass bei Übertragung eines Ereignisses an die zentrale Steuerinstanz die Speicherung des Ereignisses nicht durch Störung der Übertragungswege, Ausfall der Steuerinstanz o. ä. verloren geht.

Hinweis: Die Sicherung der Ereignisübertragung an eine zentrale Steuerinstanz kann z. B. durch einen geeigneten lokalen Pufferspeicher in der Komponente umgesetzt werden.

Der Zugriff auf den Ereignisspeicher darf ausschließlich zugriffsgeschützt erfolgen und ist nur autorisierten Personen möglich.

Es darf nicht möglich sein, erfasste Ereignisse zu editieren oder zu löschen. Zwei Ausnahmen von dem Löschverbot stellen die sichere Außerbetriebnahme der Komponente nach Abschnitt 5.1.6 und der Überschreiberlaubnis von nicht besonders sicherheitsrelevanten Ereignissen gemäß Abschnitt 5.4.3 dar. In diesem Fall muss der Ereignisspeicher unwiderruflich gelöscht werden.

Eine Änderung der Systemzeit darf keinen Einfluss auf bereits protokollierte Ereigniseinträge haben.

5.4.2 Benachrichtigung bei sicherheitsrelevanten Ereignissen

Einem autorisierten Benutzer muss es möglich sein, sich bei Auftreten eines sicherheitsrelevanten Ereignisses automatisch benachrichtigen zu lassen.

Hinweis: Eine Benachrichtigung kann z. B. mittels E-Mail oder einer Meldung an eine NSL o. ä. erfolgen.

Erfolgt eine Benachrichtigung ungesichert über nicht dedizierte Leitungswege, dürfen aus der Benachrichtigung für Dritte keine (sicherheits-)kritischen Daten hervorgehen.

Sicherheitsrelevante Ereignisse sowie die ausgelöste Benachrichtigung eines Benutzers sind gemäß Abschnitt 5.4.1 zu protokollieren.

5.4.3 Weitergehende Behandlung von protokollierten Ereignissen

Es muss möglich sein, die protokollierten Ereignisse in einem standardisierten Format exportieren zu können, um diese mit standardisierten Analysewerkzeugen zu bearbeiten.

Der Betreiber muss die Möglichkeit haben, sicherheitsrelevante Ereignisse anhand der unterschiedlichen Parameter in Abschnitt 5.4.1 als solche kennzeichnen zu können. Bei Erreichen der maximalen Speicherkapazität dürfen diese sicherheitsrelevanten Ereigniseinträge nicht überschrieben werden. Für den Fall, dass bei ausgelasteter Speicherkapazität noch weitere sicherheitsrelevante Ereignisse auftreten, muss dem Betreiber vorab die Möglichkeit zur Verfügung stehen, für diese Fälle eine Regelung definieren zu können.

Hinweis: Eine Regelung könnte sein, dass die entsprechende Funktion, die das sicherheitsrelevante Ereignis auslöst, dem Bediener nicht mehr zur Verfügung steht.

Alle Ereignisse, die nicht als sicherheitsrelevant gekennzeichnet wurden, dürfen bei ausgelasteter Speicherkapazität nach dem FIFO-Prinzip (First In – First Out) überschrieben werden.

5.4.4 Erfassung von Telemetriedaten

Stellt die Komponente (sicherheits-)kritische Funktionen oder Dienste bereit oder ist sie Teil eines (sicherheits-)kritischen Systemverbundes, muss die Komponente über Schnittstellen verfügen, über welche autorisierte Benutzer oder Systeme Telemetriedaten der Komponente erhalten können. Anhand der Telemetriedaten muss es möglich sein, den aktuellen Zustand der Komponente zu ermitteln.

Es darf nicht möglich sein, dass aus den Telemetriedaten Rückschlüsse auf das Verhalten von Benutzern gezogen werden kann.

In der Bedienungsanleitung muss klar und transparent beschrieben sein, welche Telemetriedaten zu welchem Zweck erfasst werden, sowie Art und Umfang der entsprechenden Schnittstellen.

5.4.5 Zeitstempel und Zeitsynchronisation

Die Komponente muss die Möglichkeit bieten, eindeutige Zeitstempel generieren zu können (z. B. für die Protokollierung von Ereignissen).

Wird eine Komponente nicht ausschließlich im Stand-Alone Modus betrieben (die Komponente tauscht mit weiteren Systemen/Komponenten Daten aus), muss diese die Möglichkeit bieten, die interne Systemzeit mit einer Zeitquelle zu synchronisieren.

Hinweis: Eine Zeitquelle kann z. B. eine übergeordnete Steuerinstanz oder ein öffentlicher Zeitserver sein.

Es darf nur autorisierten Benutzern möglich sein, den Zeitsynchronisationsmechanismus auszulösen.

Die Änderungen der Systemzeit bzw. das Auslösen des Zeitsynchronisationsmechanismus muss gemäß Abschnitt 5.4.1 protokolliert werden.

5.5 Anforderungen an den Datenfluss

5.5.1 Pairing mit weiteren Systemen/Komponenten

Tauscht eine Komponente mit weiteren Systemen/Komponenten Daten über nicht dedizierte Kommunikationswege aus (z. B. mit einem übergeordneten Management-System oder angeschlossenen Sensoren), müssen sich die Geräte gegenseitig authentisieren. Die Authentisierung muss durch kryptografische Methoden abgesichert sein, die dem Stand der Technik entsprechen.

Hinweis: Mobile Geräte (wie z. B. Smartphones) können unerwünschten Netzverkehr erzeugen, Schadprogramme einschleusen und Informationen offenlegen. Daher sollten für deren Einsatz besondere Maßnahmen getroffen werden.

Die Authentisierung zweier Komponenten ist gemäß Abschnitt 5.4.1 zu protokollieren.

Der Datenaustausch zwischen Komponente und weiteren Systemen/Komponenten darf ausschließlich gemäß Abschnitt 5.3.1 gesichert erfolgen.

5.5.2 Fremdprodukte/-dienste

Sind für den vorgesehenen Betrieb der Komponente Fremdprodukte oder -dienste notwendig, muss der Hersteller in der Bedienungsanleitung darüber informieren:

- durch wen das Fremdprodukt oder der Fremddienst zur Verfügung gestellt wird
- welche Informationen übermittelt und verarbeitet werden
- wo diese Informationen verarbeitet und gespeichert werden
- zu welchem Zweck die Informationen übermittelt werden
- in welchem Umfang die Komponente nach Abschaltung der Fremdkomponente oder des Fremddienstes noch seine vorgesehene Funktion erfüllt.

Verwendete Fremdprodukte/-dienste dürfen nicht das Niveau der Cyber-Sicherheit der Komponente verringern und müssen eine Rückwirkungsfreiheit auf die Komponente garantieren.

Es dürfen ausschließlich Fremdprodukte/-dienste eingebunden werden, die eine anerkannte Zertifizierung in Bezug auf die Informationssicherheit vorweisen können.

Hinweis: Eine anerkannte Zertifizierung von Produkten kann z. B. nach Common Criteria oder nach Technischen Richtlinien des BSI erfolgen. Die Zertifizierung/Testierung von (Cloud-)Diensten kann z. B. nach dem Anforderungskatalog Cloud Computing (C5) des BSI oder des Trusted Cloud Labels des Kompetenznetzwerks Trusted Cloud e.V. erfolgen.

5.5.3 „Call Home“-Funktion

Besitzt eine Komponente eine Call Home-Funktionalität, die Informationen ohne Wissen des Betreibers direkt an den Hersteller übermittelt (z. B. Informationen über aufgetretene Fehler, Systemstatusänderungen, Versionsabgleich, Diagnoseinformationen o. ä.), ist diese im Auslieferungszustand und bei Rücksetzen automatisch zu deaktivieren. Die Call Home-Funktion darf ausschließlich nur nach einer bestätigten Abfrage an einen autorisierten Benutzer (z. B. Administrator oder Errichter) aktiviert werden. Zudem muss der Benutzer in der Bedienungsanleitung einsehen können, welche Informationen an den Hersteller übermittelt werden.

Die Aktivierung/Deaktivierung der Call Home Funktion muss gemäß Abschnitt 5.4.1 protokolliert werden.

Nach einem Software-Update darf sich die Call Home-Funktion nicht selbstständig aktivieren.

5.5.4 Verwaltung von Schnittstellen

Alle Schnittstellen einer Komponente müssen durch autorisierte Benutzer flexibel konfiguriert werden können. Zumindest die Aktivierung bzw. Deaktivierung von Schnittstellen muss möglich sein.

Soll die Komponente weitere Komponenten verwalten oder ansteuern, muss die Konfiguration der Schnittstelle mindestens die Autorisierung, Überwachung und Einschränkung der Verwendung gemäß dem Stand der Technik unterstützen.

Nur die für den Regelbetrieb erforderlichen Schnittstellen dürfen aktiviert sein.

Anwenderschnittstellen sind durch sichere Authentisierungsmechanismen zu schützen.

Stellt die Komponente ggf. werkseitige Diagnose- oder Testschnittstellen (z. B. JTAG-Schnittstellen) zur Verfügung, sind diese wirksam gegen unautorisierte Benutzung zu schützen. Entsprechende Schnittstellen sind in der technischen Dokumentation aufzuführen.

Die Verwaltung von Schnittstellen ist gemäß Abschnitt 5.4.1 zu protokollieren.

5.5.5 Konfiguration von Remote-Zugängen

Kann eine Komponente direkt über das Netz oder durch netzbasierte Verwaltungstools verwaltet werden, müssen diese Zugänge und die übertragenen Daten durch Sicherungsmaßnahmen gemäß dem Stand der Technik abgesichert werden.

Hinweis: Geeignete Maßnahmen sind hier bspw. Bedienung nur durch autorisierte Benutzer, ausschließlich gesicherte Datenübertragung (basierend auf kryptografischen Mechanismen), Integritätsprüfung der empfangenen Daten, Protokollierung aller Aktionen etc.

Remote-Zugänge müssen nach Inbetriebnahme oder Rücksetzen der Komponente automatisch deaktiviert sein und dürfen erst nach Aktivierung eines autorisierten Benutzers zur Verfügung stehen.

Wird ein Remote-Zugang aktiviert/deaktiviert muss dies gemäß Abschnitt 5.4.1 protokolliert werden.

5.6 Begleitende Maßnahmen

5.6.1 Vollständige Dokumentation der Komponente

Der Hersteller muss eine vollständige und ausführliche Dokumentation der Komponente vorlegen.

Alle Teile der Dokumentation müssen

- mit einem Gültigkeitsvermerk (bei gedruckten Dokumenten z. B. Stempel mit Datum und Unterschrift) bei VdS eingereicht werden
- in deutscher und ggf. bei Vertrieb im nicht deutschsprachigen Raum in englischer Sprache ausgeführt sein.

Die Einreichung der Dokumente auf elektronischem Weg wird bevorzugt.

Die Dokumentation besteht aus folgenden Teilen (falls zutreffend):

- Bedienungsanleitung
  - z. B. Produkt- und Funktionsbeschreibung, Beschreibung hinsichtlich des sicheren und bestimmungsgemäßen Umgangs mit dem Produkt, Bedienung und Betrieb, Konfiguration, Wartung und Reparatur, Pflege, Störungsbeseitigung, Informationen zum Transport, Lagerung, Lieferumfang bei der Übergabe, Entsorgung
- Projektierungshandbuch/Hardening Guide
  - erforderliche bzw. empfohlene Voraussetzungen und Maßnahmen je nach Risikoklassifizierung in Bezug auf die IT-Infrastruktur und Komponentenkonfiguration zur Gewährleistung eines sicheren Betriebs (sog. Hardening Guide); hierzu gehören bspw. empfohlene Firmware-/Software-Versionsstände, Einstellungen zur Benutzerauthentisierung und Rechteverwaltung, Verschlüsselungs- und Signierungsmöglichkeiten, Benennung oder Umgang von offenen Schnittstellen der Komponente, erforderliche Netzwerkprotokolle und -ports, Einstellungen zum Monitoring, empfohlene Einstellungen von Diensten (z. B. FTP, SMTP, DNS, DHCP), empfohlene Schutzmaßnahmen vor böswilligem Code

- Installationsanleitung
  - z. B. Montage/Installation/Aufstellen/Inbetriebnahme
- Technische Dokumentation
  - z. B. Allgemeine technische Daten, Schnittstellen, Schaltpläne, Blockschaltbilder/Funktionsbeschreibungen, Prozessbeschreibung zur transparenten und bewährten Verwaltung von Schwachstellen (Incident Management)
- Dokumentation der Software:
  - Dokumentation gemäß VdS 2203
  - ggf. darüber hinaus Struktur der Software, Programmcodelisting, Versionierungsschema, begleitende Softwaredokumentation, Programmablaufplan/Prozessbeschreibung, Auflistung der verwendeten Kommunikationsprotokolle

Die Dokumentation muss in einer übersichtlichen und in einer leicht verständlichen Art und Weise vorgehalten werden. Zudem muss der Hersteller diese immer auf dem aktuellsten Stand halten und eine Versionierung vorsehen.

5.6.2 Umfassende Bereitstellung Support

Der Hersteller ist verpflichtet, die Komponente (einschließlich aller verwendeten Teilkomponenten und für den Betrieb notwendiger Software Dritter) über einen Mindestzeitraum zu beobachten, erkannte Sicherheitslücken unverzüglich zu schließen und entsprechende Maßnahmen über Updates und Patches bereitzustellen.

Hinweis: Eine unverzügliche und abschließende Behandlung von Sicherheitslücken kann je nach Problem und Fehlerbehebung sowie weiteren Faktoren variieren. Eine besonders kritische Sicherheitslücke sollte umgehend vom Hersteller behandelt werden und z. B. in Form einer umgehenden Softwareaktualisierung („Hotfix“) zeitnah geschlossen werden. Weniger kritische Sicherheitslücken können z. B. mit der Auslieferung turnusmäßiger Updates geschlossen werden.

Der Hersteller muss den Support nach Abkündigung des Produktes noch weitere 60 Monate gewährleisten. Sind verschiedene Evolutionsstufen des Produktes verfügbar, so erstreckt sich der Mindestsupportzeitraum auf 60 Monate ab dem Tag der Einstellung der jeweiligen Produktversion. In der Bedienungsanleitung muss für den Betreiber klar und transparent angegeben sein, bis wann der Hersteller mindestens den Support verbindlich bereitstellt („End-of-Life“-Datum).

Hinweis: Die Behandlung der Ursache eines Sicherheitsproblems muss ggf. mit Hinblick auf Auswirkungen für weitere Komponenten (z. B. bei gemeinsamer Codebasis o. ä.) erfolgen und sollte dokumentiert werden.

Zudem muss er einen Informationsdienst zur Verfügung stellen, welcher interessierten Personenkreisen (z. B. Distributoren, Resellern, Errichtern, Betreibern, Sicherheitsforschern etc.) die Möglichkeit gibt, sich über entdeckte Sicherheitslücken und Schwachstellen sowie bestehender Handlungsempfehlungen aktiv (z. B. per Push-Benachrichtigung) informieren zu lassen. Ist dies dem Hersteller nicht möglich, so muss er zumindest entdeckte Sicherheitslücken und Schwachstellen an die nationalen Behörden (für Deutschland: BSI) melden.

Hinweis: Eine Push-Benachrichtigung könnte bspw. durch Mailinglisten, Messenger-Dienste, RSS-Feeds oder Anzeigen durch die Komponente selbst bzw. durch eine entsprechende Verwaltungssoftware erfolgen. Weitergehende Hinweise zur koordinierten Offenlegung von Schwachstellen können der ISO/IEC 29147 entnommen werden.

Weiterhin muss eine Möglichkeit bestehen, dem Hersteller erkannte Sicherheitslücken zu melden. Die Kontaktaufnahme sollte mindestens über Telefon, E-Mail oder Webformular möglich sein. Die Kontaktmöglichkeiten sind in der Bedienungsanleitung zu beschreiben.

5.6.3 Automatische Update-Prüfung

Die Komponente muss bei Verbindung zum öffentlichen Netzwerk automatisch die Verfügbarkeit von Updates prüfen.

Hinweis: Die Verfügbarkeitsprüfung beinhaltet nicht die Installation des Updates.

Alternativ kann dies auch durch andere Mechanismen, wie z. B. über ein zentrales Softwareverteilungssystem o. ä. geschehen. Sollte keine direkte Verbindung zum öffentlichen Netzwerk bestehen, liegt es im Verantwortungsbereich des Betreibers bzw. Errichters selbstständig auf Updateverfügbarkeit zu prüfen und zu installieren.

Hinweis: Keine direkte Verbindung zum öffentlichen Netzwerk liegt vor, wenn sich mindestens ein Netzübergang zwischen Komponente und öffentlichem Netzwerk befindet oder weil die Komponente als Stand-Alone Lösung betrieben wird.

Sofern nicht anderweitig abweichend geregelt (Produktrichtlinien, Planung- und Einbau-Richtlinien usw.), muss der Benutzer in den Einstellungen der Komponente die Wahl haben, wie Softwareupdates auf der Komponente oder zugehöriger Teilkomponenten (wie z. B. Sensoren) installiert werden. Zur Wahl muss die automatische und manuelle Installationsweise stehen.

Hinweis: Vor der Installation von Updates sind die zugrundeliegenden produktspezifischen Richtlinien und Normen der sicherheitstechnischen Anlagen (gemäß Abschnitt 1.1) auf ggf. existierende Vorgaben in Bezug auf Softwareinstallationen zu prüfen (z. B. kann bei Updateinstallation eine vollständige Funktionsprüfung der Komponente notwendig werden).

Entscheidet sich ein Benutzer für die automatische Ausführung des Autoupdate-Dienstes, so müssen Updates automatisch und umgehend nach Bekanntwerden installiert werden. Bei der Installation von Updates dürfen keine Einstellungen, Systemzustände o. ä. zurückgesetzt (verändert) werden, die eine Verringerung der Cyber-Sicherheit zur Folge haben können.

Wird die manuelle Installationsart gewählt, kann der Benutzer sich über die Verfügbarkeit eines Updates benachrichtigen lassen (z. B. per E-Mail), den Installationszeitpunkt aber selbst bestimmen. Eine manuelle Update-Installation muss für den Betreiber einfach durchzuführen sein.

Hinweis: Sollte die Komponente nicht selbst über die Möglichkeit der Benachrichtigung bei Vorliegen eines Updates verfügen, kann diese auch durch eine übergeordnete Steuerinstanz (z. B. ein zentrales Softwareverteilungssystem) vorgenommen werden.

Alle Updates und Patches müssen direkt über den Hersteller der Komponente, oder von einem von ihm beauftragten Partner bereitgestellt werden und über einen sicheren Kanal übermittelt werden.

Jedes Update muss vor der Installation auf Authentizität und Integrität geprüft werden. Die zu verwendenden Mechanismen müssen dem Stand der Technik entsprechen (z. B. Prüfsummen, digitale Signatur). Komponenten mit (sicherheits-)kritischen Funktionen müssen während eines Aktualisierungsvorgangs die Funktionsweise des Gerätes aufrechterhalten und dürfen nicht vollständig abgeschaltet werden.

5.7 Risikoanalyse und Abweichung

Werden eine oder mehrere der in diesen Richtlinien genannten Anforderungen vom Hersteller nicht umgesetzt (z. B. weil technisch nicht umsetzbar o. ä.), muss der Hersteller eine Risikoanalyse betreiben und deren Ergebnisse dokumentieren.

Das Ergebnis der Risikoanalyse bzgl. nichtanwendbarer Anforderungen wird im Zertifikat aufgeführt.

Sollen andere, als die beschriebenen Maßnahmen eine oder mehrere Anforderungen ersetzen, so muss der Hersteller diese Maßnahmen detailliert beschreiben und die Wirksamkeit und Gleichwertigkeit mittels einer Risikoanalyse nachweisen.

Die Prüfung der Risikoanalyse im Hinblick auf Begründung, Plausibilität und Nachvollziehbarkeit ist Teil des Anerkennungsprozess.