Cyber Security für kleine und mittlere Unternehmen (KMU)

Leitfaden zur Interpretation und Umsetzung der VdS 3473 für Industrielle Automatisierungssysteme

VdS 3473-1

VdS 3473-1: 2017-04

VdS-Richtlinien für die Informationssicherheit

Cyber Security für kleine und mittlere Unternehmen (KMU)

Leitfaden zur Interpretation und Umsetzung der VdS 3473 für Industrielle Automatisierungssysteme

Inhalt

Disclaimer:

Es kann keine Verantwortung für Schäden übernommen werden, die durch das Vertrauen auf Inhalte dieses Dokuments oder anderen Gebrauch entstehen.

Der vorliegende Leitfaden ist unverbindlich. Dritte können im Einzelfall auch andere Sicherheitsvorkehrungen zu nach eigenem Ermessen festgelegten Konditionen akzeptieren, die diesen technischen Spezifikationen nicht entsprechen.

Anwendungshinweis:

Die nachfolgenden Kommentare (Erläuterungen, Ergänzungen) beziehen sich auf die Formulierungen des Ursprungsdokuments, den VdS-Richtlinien 3473 „Cyber-Security für kleine und mittlere Unternehmen (KMU), Anforderungen“ in den jeweils genannten Absätzen. Kursiv gehaltene Kommentare beziehen sich auf die kursiv gehaltenen Passagen in den jeweiligen Abschnitten des Ursprungsdokuments. Kommentare existieren nicht für alle Absätze des Ursprungsdokuments.

Herausgeber und Verlag: VdS Schadenverhütung GmbH

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

1 Allgemeines

1.1 Motivation

Die Richtlinien VdS 3473 sind generisch formuliert. Damit soll eine Anwendung auf verschiedene Anwendungsfelder ermöglicht werden. Mit dem hier vorliegenden Leitfaden zur VdS 3473 werden die Anforderungen der Richtlinien um Anwendungshinweise für die Produktion mit Industriellen Automatisierungssystemen (IACS) ergänzt. Als Ergänzung zu diesen Richtlinien wird zusätzlich auch auf die Normenreihen IEC_62443 und VDI 2182 verwiesen. Kritische Infrastrukturen, wie sie im IT-Sicherheitsgesetz (ITSichG2015) behandelt werden, fallen nicht unter diese Richtlinien.

1.2 Geltungsbereich

Diese Richtlinien legen Mindestanforderungen an die Informationssicherheit für Industrielle Automatisierungssysteme fest und können für kleine und mittlere Unternehmen (KMU) angewendet werden.

1.3 Anwendungshinweise

In den Richtlinien VdS 3473 wird der Begriff „Informationssicherheit“ verwendet. Die Kommentare im Leitfaden richten sich insbesondere auf die Aspekte der Informationssicherheit in Produktionsanlagen. Für die Anwendung des Leitfadens ist es erforderlich, dass auch Fachwissen in Bezug auf die Anforderungen im Produktionsbereich vorliegt. Es ist zu beachten, dass im Produktionsbereich die Priorisierung der Schutzziele von denen der IT im restlichen Teil des Unternehmens abweichen kann.

1.4 Gültigkeit

Dieser Leitfaden gilt ab dem 24.04.2017.

2 Normative Verweise

Für den Einsatz im Produktionsbereich sind die folgenden Regelwerke zusätzlich relevant:

- IEC 62443 Normenreihe IEC 62443 Industrial communication networks: Network and system security.
- ITSichG2015: Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), 2015.
- VDI 2182 VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik (GMA) Normenreihe VDI/VDE 2182: Informationssicherheit in der industriellen Automatisierung.
- BSI-Standard CS-123: Empfehlungen für Fortbildungs- und Qualifizierungsmaßnahmen im ICS-Umfeld.

3 Glossar

Die mit einem * gekennzeichneten Begriffe werden für die Anwendung in der Automatisierungstechnik zusätzlich definiert.

Administrativer Zugang: Administrative Zugänge existieren auch für Automatisierungskomponenten.

Administrator: Im Produktionsbereich ist unter IT-System auch das Automatisierungssystem zu verstehen.

Aktive Netzwerkkomponente: Aktive Netzwerkkomponenten werden auch im Produktionsbereich eingesetzt. Hier werden sie in der Regel in industrietauglicher Ausführung verwendet (z. B. Hutschienen-Montage, Versorgung mit 24-V-Gleichspannung, lüfterloser Betrieb).

*** Automatisierungssystem:** Dient dazu, die in einem technischen System ablaufenden Prozesse selbsttätig zu führen. Ein Automatisierungssystem setzt sich u. a. aus den folgenden Automatisierungskomponenten zusammen: Steuerungen (SPS, Controller), Ein-/Ausgabe-Systeme, Sensoren und Aktoren, Server, Bedien- und Beobachtungsstationen, Engineering-Station(en) und das Automatisierungsnetzwerk.

*** Automatisierungskomponente**: Teil eines Automatisierungssystems. Automatisierungskomponenten

können z. B. speicherprogrammierbare Steuerungen (SPS), Controller, Sensoren und Aktoren, Server, Bedien- und Beobachtungsstationen, Engineering-Station(en) und das Automatisierungsnetzwerk sein.

*** Automatisierungsnetzwerk:** Netzwerk zur Datenkommunikation über das die Komponenten eines Automatisierungssystems untereinander kommunizieren. Teile des Automatisierungsnetzwerkes (Kommunikation im Feldbereich) unterliegen Echtzeitanforderungen.

*** Demilitarisierte Zone (DMZ):** Bezeichnet einen abgeschotteten Bereich, der für das Ein- und Ausschleusen von Daten verwendet werden kann.

*** Engineering Station /Engineering Workstation:** System zur Konfiguration, Inbetriebnahme und Überwachung eines Automatisierungssystems.

*** Funktionale Sicherheit:** Bezeichnet den Teil der Sicherheit eines Systems, der von der korrekten Funktion des sicherheitsbezogenen Systems und anderer risikomindernder Maßnahmen abhängt. Nicht zur funktionalen Sicherheit gehören u. a. elektrische Sicherheit, Brandschutz oder Strahlenschutz.

Informationssicherheit: In einer Produktionsumgebung ist die Verfügbarkeit der Produktionsanlage von besonderer Bedeutung.

Informationssicherheitsbeauftragter (ISB): Der ISB ist der Prozessverantwortliche des Informationssicherheitsprozesses. Diese Zuständigkeit umfasst auch den Informations-sicherheitsprozess in der Produktion.

Informationstechnik (IT): Diese Definition umfasst auch die Komponenten im Produktionsbereich.

IT-Infrastruktur: Umfasst auch die Einrichtungen im Produktionsbereich.

IT-Ressource: Umfasst auch die Betriebsmittel im Produktionsbereich.

IT-Verantwortlicher: Für die IT-Ressourcen im Produktionsbereich (Automatisierungssysteme) sind entsprechende IT-Verantwortliche zu benennen.

IT-System: Umfasst auch die Anlagen im Produktionsbereich. Hierunter fallen z. B. Engineering-Station(en), Operator-Konsolen, speicherprogrammierbare Steuerungen, IO-Systeme, etc.

Kritisches IT-System: Automatisierungssysteme können zu den kritischen IT-Systemen gehören, sofern Sie die Bedingungen gem. Abschnitt 9.3. erfüllen.

Kritische Verbindung: Verbindungen im Produktionsbereich können kritische Verbindungen sein, sofern Sie die Bedingungen gemäß Abschnitt 9.3 erfüllen.

Mitarbeiter: Der Begriff umfasst alle internen und externen Mitarbeiter. Externe Mitarbeiter können in einem direkten (z. B. Berater, Freiberufler) oder in einem indirekten Vertragsverhältnis (z. B. Mitarbeiter von Auftragnehmern oder Unterauftragnehmern) zum Unternehmen stehen.

Mobiles IT-System: Ob es sich bei einem IT-System um ein mobiles IT-System handelt, wird durch seinen Einsatzzweck bestimmt, nicht durch seine Bauart. So gilt z. B. ein Notebook, das stationär als Workstation betrieben wird, nicht als mobiles IT-System. Die Beschreibung betrifft auch Automatisierungskomponenten, deren Einsatzzweck durch Mobilität und die Anwendung im Produktionsbereich gekennzeichnet ist. Typische mobile Automatisierungskomponenten sind z. B. Notebooks, Smartphones, Tablets oder Digitalkameras, die im Produktionsbereich eingesetzt werden.

*** Mehr-Faktor-Authentifizierung:** Nachweis der Identität mit Hilfe von mehreren unabhängigen Merkmalen.

*** Operator-Station / Operator Konsole / Konsole / Leitstation:** Unter diesen Begriffen ist der Teil eines Automatisierungssystems zu verstehen, mit dem der technische Prozess bedient und beobachtet werden kann. Darüber hinaus stellt die Operator-Station auch Diagnosefunktionen für die Überwachung des Automatisierungssystems zur Verfügung.

Personal: Hierunter fallen in der Automatisierungstechnik auch die so genannten Systemintegratoren (System Integrators).

*** Produktionsanlage:** Anlage im Unternehmen, auf dem die Güter produziert / verarbeitet werden. Die Produktionsanlage umfasst neben den physischen Anlagenteilen (z. B. Pressen, Transportanlagen, Werkzugmaschinen, etc.) auch das Automatisierungssystem und die zum Automatisierungssystem gehörigen IT-Ressourcen (Netzwerkkomponenten, Server, Router, Software).

*** Produktionsbereich:** Teil eines Unternehmens, welcher direkt mit der Produktion der Güter beschäftigt ist. Hinweis: In diesem Dokument wird aus Vereinfachungsgründen teilweise die verkürzte Fassung „in der Produktion“ verwendet.

*** Produktionsverantwortlicher:** Leiter der Produktion, bzw. das für die Produktion zuständige Management.

*** Schichtzugang (Gruppen-Account):** Zugang zu einem IT-System oder Automatisierungssystem, bei dem sich mehrere Personen einer Schicht einen Zugang (Account) teilen. Ein Schichtzugang findet im Allgemeinen Anwendung in einem räumlich eingegrenzten Umfeld, z. B. in Leitwarten.

4 Organisation der Informationssicherheit

4.1 Verantwortlichkeiten

4.1.1 Zuweisung und Dokumentation

4.1.1.2 Hierbei sind auch die Ressourcen im Produktionsbereich zu berücksichtigen

4.1.4 Delegieren von Aufgaben

Diese Festlegung ermöglicht eine Delegation von Aufgaben im Produktionsbereich an Personen, die in diesem Gebiet über besondere Erfahrungen verfügen.

4.3 Informationssicherheitsbeauftragter (ISB)

Der ISB trägt die Verantwortung für das gesamte Unternehmen, um eine unternehmensweite Implementierung der Informationssicherheit zu gewährleisten. Dies schließt den Produktionsbereich ein. Das Delegieren von Aufgaben gemäß Abschnitt 4.1.4 ist zulässig.

4.3.1 Dieser Informationssicherheitsprozess ist als übergreifender Prozess das gesamte Unternehmen. Dies schließt den Produktionsbereich ein. Insbesondere die Schnittstelle zwischen dem Produktionsbereich und dem restlichen Unternehmen ist hierbei von besonderer Bedeutung.

4.3.8 Die Automatisierungssysteme im Produktionsbereich (Produktionsanlagen) fallen unter diesen Punkt.

4.4 Informationssicherheitsteam (IST)

In produzierenden Unternehmen gibt es i.d.R. die Rolle des Produktionsverantwortlichen. Der Produktionsverantwortliche oder eine von ihm benannte Person MUSS Mitglied des IST sein. Eine Delegation dieser Aufgabe ist möglich. In jedem Fall MUSS der Produktionsbereich im IST repräsentiert sein.

4.5 IT-Verantwortliche

In Unternehmen existieren häufig mehrere IT-Infrastrukturen (IT im Bürobereich, Netzwerktechnik, Telefonanlage, Automatisierungssystem, Gebäudeleittechnik), die von unterschiedlichen Abteilungen betreut werden. Die VdS 3473 kann aufgrund ihres generischen Ansatzes auf die gesamte IT-Infrastruktur angewandt werden. Um ihre Umsetzung in den einzelnen IT-Infrastrukturen fachlich fundiert zu gewährleisten, fordert die VdS 3473 vom Unternehmen, einen oder mehrere IT-Verantwortliche zu benennen.

4.10 Lieferanten und sonstige Auftragnehmer

Im Produktionsbereich fällt das Personal von Systemintegratoren und sonstiges Inbetriebnahme- und Service-Personal in die beschriebene Kategorie der Lieferanten und sonstigen Auftragnehmer. Es ist davon auszugehen, dass dieses Personal grundsätzlich auf die Einhaltung der Maßnahmen und Regelungen zu verpflichten ist. Diese Leitlinie ist so auszuführen, dass der gesamte Bereich des Unternehmens abgedeckt ist. Dies schließt den Produktionsbereich ein.

5 Leitlinie zur Informationssicherheit (IS-Leitlinie)

Diese Leitlinie ist so auszuführen, dass der gesamte Bereich des Unternehmens abgedeckt ist. Dies schließt den Produktionsbereich ein.

6 Richtlinien zur Informationssicherheit (IS-Richtlinien)

6.3 Regelungen für Nutzer

Das Bedienpersonal von Automatisierungssystemen (Operator) fällt in die Kategorie Nutzer. Das Bedienen und Beobachten sowie das Engineering von Automatisierungssystemen fällt in die Kategorie der IT-Nutzung.

6.3.2 (a) Eine private Nutzung der IT im Produktionsbereich ist grundsätzlich nicht erlaubt.

6.3.2 (b) Eine private Nutzung der IT im Produktionsbereich ist grundsätzlich nicht erlaubt.

6.3.3 (a) Dies betrifft auch die Komponenten des Automatisierungssystems (Automatisierungskomponenten).

6.3.3 (c) Dies betrifft auch Schutzeinrichtungen für den Personenschutz, z. B. Sensoren und Zuhaltungen an Schutzzäunen (Systeme mit funktionaler Sicherheit).

6.3.5 *Die VdS 3473 erlaubt Ausnahmen von den obigen Regelungen. Ausnahmen können im Unternehmensalltag z. B. für bestimmte Benutzer, Benutzergruppen, Geräte oder Gerätegruppen sinnvoll und notwendig sein. Das kann z. B. für die Schichtzugänge im Produktionsbereich gelten.*

6.4 Regelungen für Lieferanten und sonstige Auftragnehmer

Im Produktionsbereich fällt das Personal von Systemintegratoren und sonstiges Inbetriebnahme- und Service-Personal in die Kategorie der Lieferanten und sonstigen Auftragnehmer. Es ist davon auszugehen, dass dieses Personal grundsätzlich auf die Einhaltung der Maßnahmen und Regelungen zu verpflichten ist.

6.4.3 (a) Dies betrifft auch Schutzeinrichtungen für den Personenschutz, z. B. Sensoren und Zuhaltungen an Schutzzäunen (Systeme mit funktionaler Sicherheit).

6.4.4 (a) Der Zugriff auf eine Produktionsanlage bzw. ein Automatisierungssystem ist in der Regel als ein Zugriff auf nichtöffentliche IT anzusehen.

6.4.4 (b) Der Anschluss von Diagnose-, Konfigurations- oder Inbetriebnahme-PCs eines Systemintegrators an ein Automatisierungssystem kann als ein solcher Zugriff angesehen werden

6.4.5 (a) Die Integration von IT-Systemen kann große Auswirkungen auf die Produktion haben (z.B. Störungen verursachen). Die Freigabe durch einen Administrator soll sicherstellen, dass die entsprechenden Basisschutzmaßnahmen (siehe Abschnitt 10.3) umgesetzt werden. Es kann im Produktionsbereich auch eine Festlegung erfolgen, dass die Integration eines IT-Systems nicht zulässig ist.

6.4.6 (b) Es kann im Produktionsbereich auch eine Festlegung erfolgen, dass der Einsatz von mobilen Datenträgern nicht zulässig ist. In diesem Fall sind ggf. alternative Möglichkeiten, z .B. das Einschleusen von Daten über eine Datenschleuse oder eine demilitarisierten Zone (DMZ) vorzusehen.

6.4.7 (*a) Die VdS 3473 erlaubt Ausnahmen von den obigen Regelungen. Ausnahmen können im Unternehmensalltag z. B. für bestimmte Benutzer, Benutzergruppen, Geräte oder Gerätegruppen sinnvoll und notwendig sein. Das kann z. B. für so genannte Schichtzugänge im Produktionsbereich gelten.*

7 Personal

7.3 Beendigung oder Wechsel der Anstellung

7.3.2 Schichtzugänge, zu denen der Mitarbeiter Zugriff hatte, sind ebenfalls anzupassen.

8 Wissen

8.1 Aktualität des Wissens

8.1.1 Die Hersteller von Automatisierungssystemen liefern teilweise Informationen über bekannt gewordene Schwachstellen ihrer Produkte. Diese sind auf der Webseite des Herstellers einsehbar. Teilweise wird auch ein E-Mail-Service angeboten. Es wird empfohlen, diese Informationen zu nutzen. Darüber hinaus stellen auch staatliche Stellen (z. B. das Bundesamt für Sicherheit in der

Informationstechnik, BSI https://www.bsi.bund.de oder das ICS-CERT https://ics-cert.us-cert.gov/) Informationen in Bezug auf bekannte Schwachstellen von Automatisierungskomponenten zur Verfügung.

8.2 Sensibilisierung, Aus- und Weiterbildung

8.2.1 Einen Anhalt über die erforderlichen Inhalte gibt z. B. der BSI-Standard CS-123 (Empfehlungen für Fortbildungs- und Qualifizierungsmaßnahmen im ICS-Umfeld).

9 Identifizieren kritischer IT-Ressourcen

Die Komponenten eines Automatisierungssystems (Automatisierungskomponenten) und das Automatisierungsnetzwerk können zu den kritischen Ressourcen eines Unternehmens gehören.

9.1 Prozesse

Produktionsprozesse können zu zentralen Geschäftsprozessen oder zu Prozessen mit hohem Schadenspotential gehören.

9.3 IT-Systeme, mobile Datenträger und Verbindungen

Die Komponenten eines Automatisierungssystems (Automatisierungskomponenten) können kritische IT-Systeme sein.

9.4 Individualsoftware

Hierbei kann es sich auch um Individualsoftware für den Einsatz im Produktionsbereich handeln.

10 IT-Systeme

10.1 Inventarisierung

Die Komponenten eines Automatisierungssystems (Automatisierungskomponenten) sind als IT-Systeme anzusehen und MÜSSEN inventarisiert werden.

10.1.2 Bei stationären IT-Systemen ist dies in der Regel der Standort, bei mobilen IT-Systemen der Besitzer.

10.2 Lebenszyklus

10.2.1 Inbetriebnahme und Änderung

Automatisierungskomponenten sind wie IT-Systeme zu behandeln.

10.2.1.4 Diese Maßnahme erfordert nicht zwingend, dass für jedes IT-System individuelle Authentifizierungsmerkmale vergeben werden. Wichtig ist die Entfernung der voreingestellten Standard-Authentifizierungsmerkmale.

10.2.2 Ausmusterung und Weiterverwendung

Automatisierungskomponenten sind wie IT-Systeme zu behandeln.

10.3 Basisschutz

Automatisierungskomponenten sind wie IT-Systeme zu behandeln. Wenn einzelne Maßnahmen des Basisschutzes für Automatisierungssysteme nicht umzusetzen sind, kann dies durch eine Risikoanalyse und Behandlung kompensiert werden.

10.3.1 Updates

Diese Maßnahme ist eine Maßnahme des Basisschutzes. Sofern sie nicht umgesetzt werden kann, ist dem entstehenden Risiko mit einer Risikoanalyse und Behandlung zu begegnen. Siehe Abschnitt 10.3.

10.3.3 Protokollierung

Automatisierungskomponenten sind wie IT-Systeme zu behandeln.

In der Regel verfügen Automatisierungssysteme über eine eigene Uhrzeitführung, die den Echtzeitanforderungen des Systems genügt. Damit Protokolldaten ggf. übergreifend (im gesamten

Unternehmen) ausgewertet werden können, müssen die Uhrzeiten synchronisiert sein. Im Automatisierungssystem wird dies z. B. über eine externe Zeitbasis umzusetzen sein.

10.3.5 Schadsoftware

Automatisierungskomponenten sind wie IT-Systeme zu behandeln.

Diese Maßnahme ist eine Maßnahme des Basisschutzes. Sofern sie nicht umgesetzt werden kann, ist dem entstehenden Risiko mit einer Risikoanalyse und Behandlung zu begegnen. Siehe Abschnitt 10.3.

10.3.6 Starten von fremden Medien

Automatisierungskomponenten sind wie IT-Systeme zu behandeln.

Ein BIOS-Passwort ist für Automatisierungskomponenten in der Regel nicht realisierbar.

10.3.7 Authentifizierung

Automatisierungskomponenten sind wie IT-Systeme zu behandeln. Wenn ein geeignetes Anmeldeverfahren nicht umgesetzt werden kann, weil eine entsprechende Funktionalität nicht vorhanden ist, MUSS dem dadurch entstehenden Risiko durch eine Risikoanalyse und -behandlung (siehe Anhang A 2) begegnet werden. Dies betrifft z. B. die Anmeldung an Engineering- oder Operator-Stationen aber auch die Anmeldung an Web-Interfaces von Automatisierungskomponenten.

10.3.7.1 Diese Forderung wird u. U. nicht von allen Automatisierungskomponenten unterstützt (Web-Interfaces).

10.3.7.2 Diese Forderung wird u. U. nicht von allen Automatisierungskomponenten unterstützt (Web-Interfaces).

10.3.7.3 Diese Maßnahme ist eine Maßnahme des Basisschutzes. Sofern sie nicht umgesetzt werden kann, ist dem entstehenden Risiko mit einer Risikoanalyse und Behandlung zu begegnen. Siehe Abschnitt 10.3.

10.3.7.4 Diese Forderung wird u. U. nicht von allen Automatisierungskomponenten unterstützt (Web-Interfaces).

10.3.8 Zugriffsbeschränkungen

Diese Forderung wird u. U. nicht von allen Automatisierungskomponenten unterstützt (Web-Interfaces).

10.4 Zusätzliche Maßnahmen für mobile IT-Systeme

Mobile Automatisierungskomponenten sind wie mobile IT-Systeme zu behandeln.

10.5 Zusätzliche Maßnahmen für kritische IT-Systeme

Kritische Automatisierungskomponenten sind wie kritische IT-Systeme zu behandeln.

10.5.1 Risikoanalyse und -behandlung

Automatisierungssysteme können zu den kritischen IT-Systemen gehören.

10.5.3 Robustheit

Bei kritischen IT-Systemen fordert die VdS 3473 eine Trennung von Produktivsystemen und Entwicklungs- bzw. Testsystemen.

Jeder aktivierte Dienst, der einen Netzwerkzugriff auf das IT-System ermöglicht, stellt ein Risiko dar, da durch diesen ein Kompromittieren des IT-System möglich sein kann. Ungenutzte Netzwerkdienste müssen unzugänglich gemacht werden.

10.5.4 Externe Schnittstellen und Laufwerke

Dies ist eine zusätzliche Maßnahme für kritische IT-Systeme. Sofern sie nicht umgesetzt werden kann, ist dem entstehenden Risiko mit einer Risikoanalyse und Behandlung zu begegnen. Siehe Abschnitt 10.5.

10.5.5 Änderungsmanagement

Automatisierungssysteme können zu den kritischen IT-Systemen gehören. Änderungen sind z.B. Konfigurationsänderungen, Installieren von neuer Software, Einspielen von Updates, etc. Die VdS 3473 definiert nicht, wie Tests und Freigaben erfolgen müssen, sondern fordert lediglich eine vom Produktivsystem getrennte Testumgebung.

- Obgleich Änderungen an kritischen IT-Systemen vor ihrer Umsetzung in einer Testumgebung geprüft und freigegeben werden müssen, können sie noch immer zu Störungen oder zu Ausfällen der Produktivsysteme führen. Deshalb fordert die VdS 3473 einen Mechanismus, der in diesem Fall die Rückkehr zum ursprünglichen Zustand (und damit zum Regelbetrieb) innerhalb der MTA sicherstellt.
- Der geforderte Mechanismus sollte mit den geforderten Maßnahmen abgestimmt sein.

10.5.6 Dokumentation

Automatisierungssysteme können zu den kritischen IT-Systemen gehören.

10.5.8 Überwachung

Diese Funktion wird für Automatisierungssysteme in der Regel über die Operator-Station oder die Engineering-Station zur Verfügung gestellt.

Optionale Anforderung. Durch eine Überwachung der Ressourcen (z.B. Datenspeicher) können sich anbahnende Probleme und Störungen schon im Vorfeld erkannt und beseitigt werden.

10.5.9 Ersatzsysteme und -verfahren

Automatisierungssysteme sind z. T. in hochverfügbaren Ausführungen verfügbar (1 aus 2 Redundanz). In vielen Fällen wird bei kritischen IT-Systemen im Automatisierungsbereich eine hochverfügbare, redundante Ausführung zum Einsatz kommen.

10.5.10 Kritische Individualsoftware

Dies gilt auch für kritische Individualsoftware, die für den Einsatz im Produktionsbereich vorgesehen ist.

11 Netzwerke und Verbindungen

11.1 Dokumentation

Die folgenden Festlegungen gelten auch für Automatisierungsnetzwerke

11.1.1 Diese können z. B. Switches oder Router sein.

11.1.2 Unter Verbindungen sind physikalischen Verbindungen (wie z.B. Kabel, Funkstrecke, optische Verbindung) als auch logische Verbindungen (wie z. B. VPN-Tunnel) zu verstehen.

11.1.3 Unter einem externen Netzwerk ist ein Netzwerk zu verstehen, das nicht unter der administrativen Kontrolle des Unternehmens steht. Hierunter sind z. B. die Netze von Providern, Dienstleistern, Partnern und das Internet zu verstehen.

11.3 Netzübergänge

11.3.2 Die Umsetzung dieser Maßnahme setzt voraus, dass die angestrebten Verkehrsbeschränkungen definiert sind. Die Verkehrsbeschränkungen werden durch Abschnitt 11.4.2 und Abschnitt 11.4.3 vorgegeben: diese Maßnahmen fordern, dass nur die unbedingt benötigten Verbindungen erlaubt sein dürfen (Whitelist). Ob die Verkehrsbeschränkungen wirksam umgesetzt wurden, kann anhand der Durchsicht der Konfiguration oder anhand eines Port-Scans geprüft werden.

11.4 Basisschutz

11.4.2 **Segmentierung**

In jedem Fall ist eine Segmentierung des Netzwerkes so vorzusehen, dass der Produktionsbereich von den restlichen Teilen des Unternehmens separiert wird. Ggf. ist eine weitere Segmentierung innerhalb des Produktionsbereichs sinnvoll.

11.4.4 **Netzwerkkopplung**

In der Praxis fordert diese Maßnahme eine verschlüsselte Verbindung und die Authentifizierung der Teilnehmer (wie z.B. ein VPN) oder die Definition des zwischengeschalteten Netzes als vertrauenswürdig (wie z.B. das MPLS-Netzwerk des Providers).

13 Umgebung

Diese Festlegung betrifft auch Automatisierungskomponenten und das Automatisierungsnetzwerk.

13.1 Server, aktive Netzwerkkomponenten und Netzwerkverteilstellen

Dies betrifft auch Server und aktive Netzwerkkomponenten, die im Produktionsbereich eingesetzt werden.

15 Zugänge und Zugriffsrechte

Dies betrifft auch die Zugänge zu Automatisierungskomponenten

15.1 Verwaltung

Dies betrifft auch die Zugänge zu Automatisierungskomponenten.

15.1.1 Dies betrifft auch die Zugänge zu Automatisierungskomponenten.

15.1.2 Dies betrifft auch die Zugänge zu Automatisierungskomponenten.

15.1.3 Dies betrifft auch die Zugänge zu Automatisierungskomponenten.

15.1.4 Dies betrifft auch die Zugänge zu Automatisierungskomponenten.

15.1.5 Dies betrifft auch die Zugänge zu Automatisierungskomponenten.

15.1.6 Dies betrifft auch die Zugänge zu Automatisierungskomponenten.

15.2 Zusätzliche Maßnahmen für kritische IT-Systeme und Daten

Dies betrifft ggf. auch die Zugänge zu Automatisierungskomponenten.

Dies betrifft auch die Zugänge zu Automatisierungskomponenten.

16 Datensicherung und Archivierung

Die Automatisierungssysteme sind in die Datensicherung einzubeziehen.

16.2 Archivierung

Dies betrifft auch die Archivdaten von Automatisierungssystemen.

16.3 Verfahren

Dies betrifft auch die Archivdaten von Automatisierungssystemen.

16.3.1 Dies betrifft auch die Archivdaten von Automatisierungssystemen.

16.3.2 Dies betrifft auch die Archivdaten von Automatisierungssystemen.

Dies betrifft auch die Archivdaten von Automatisierungssystemen.

16.4 Weiterentwicklung

Dies betrifft auch die Archivdaten von Automatisierungssystemen.

16.5 Basisschutz

16.5.1 **Speicherorte**

Dies betrifft auch die Archivdaten von Automatisierungssystemen.

16.5.2 **Server**

Dies betrifft auch die Server des Automatisierungssystems.

16.5.5 **Tests**

16.5.5.1 Automatisierungssysteme sind in diesen Prozess einzubinden.

16.6 Zusätzliche Maßnahmen für kritische IT-Systeme

Automatisierungssysteme können kritische IT-Systeme sein.

16.6.2 Verfahren

16.6.2.1 Automatisierungssysteme können kritische IT-Systeme sein.

16.6.3 Tests

Automatisierungssysteme können kritische IT-Systeme sein.

17 Störungen und Ausfälle

17.3 Zusätzliche Maßnahmen für kritische IT-Systeme

17.3.1 Wiederanlaufpläne

Automatisierungssysteme können kritische IT-Systeme sein.

17.3.2 Abhängigkeiten

17.3.2.1 Automatisierungssysteme können kritische IT-Systeme sein.

18 Sicherheitsvorfälle

18.1 IS-Richtlinie

Diese Bestimmungen schließen Sicherheitsvorfälle im Produktionsbereich ein.

18.2 Erkennen

Diese Überwachungsmaßnahmen sind insbesondere auch für den Produktionsbereich sinnvoll.