Sicherheitsnetzwerk München

Whitepaper

Anforderungen für die IT-/OT-Sicherheit bei Planung und Betrieb von Industrie 4.0 Anlagen

Arbeitskreis: Sichere Industrie 4.0

2019-06-26
Version 1.5

Autoren des Whitepapers:

BIHLER	**Tobias Gschwend** arbeitet bei der Otto Bihler Maschinenfabrik GmbH & Co. KG in Halblech.
FELSS The smarter way of forming.	**Markus Preisinger** arbeitet bei der Firma Felss Systems GmbH am Standort Nesselwang im Bereich Entwicklung als Teamleiter der Softwareentwicklung. Sein Schwerpunkt liegt bei dem Maschinenbauunternehmen auf Industrie 4.0 bzw. IIoT.
Fraunhofer ESK	**Christian Schelter**, M. Sc. arbeitet beim Fraunhofer-Institut für Eingebettete Systeme und Kommunikationstechnik ESK als wissenschaftlicher Mitarbeiter im Bereich Entwurf und Absicherung von Anwendungsarchitekturen.
gtmuenchen	**Dr. Gabriele Haller**, Dipl.-Phys. ist bei der gt-muenchen GmbH als Beraterin und Trainerin tätig. Sie unterstützt ihre Kunden in den Bereichen Requirements Engineering und Projektmanagement.
SOFTWARE FACTORY	**Thomas Trägler** ist Geschäftsführer & Gründer der Software Factory GmbH und leitet im Sicherheitsnetzwerk München den Arbeitskreis "Sichere Industrie 4.0", in dem dieses Whitepaper entstanden ist.
ZF see. think. act.	**Rainer Rodler** arbeitet bei der Firma ZF Friedrichshafen AG im Zentralressort Produktion und leitet das weltweit an allen ZF-Standorten tätige Production IT-Security Team.

Inhaltsverzeichnis

1. Einleitung - Security im Maschinen- und Anlagenbau

Deutschland ist seit Jahren eines der führenden Maschinenbauländer der Welt. [statista1]
Neben der bereits starken Stellung steigert die Branche ihre Umsätze stetig, zu immer neuen Rekorden. [statista3] Im Jahr 2017 betrug der Produktionswert im deutschen Maschinenbau 204 Milliarden Euro. [statista2]

Aufgrund der immer weiter voranschreitenden Technologien, besonders im IT-Umfeld, befindet sich der Maschinen- und Anlagenbau aktuell in seiner vierten industriellen Revolution. In dieser Umstrukturierung werden Maschinen und Anlagen zunehmend digitalisiert und erhalten Kommunikationsschnittstellen, um sich innerhalb und untereinander austauschen zu können. So kann beispielsweise ein Austausch von Informationen zwischen Maschinen desselben Typs zu einer automatischen Lastverteilung führen. Dies bietet den Betreibern einer Maschine/Anlage eine Vielzahl von Vorteilen bezüglich Flexibilität, Geschwindigkeit und Nachvollziehbarkeit.

Durch die zunehmende Kommunikation und Integration von Software in Maschinen und Anlagen, eröffnen sich neue, ausschließlich aus der IT bekannte, Angriffsszenarien. Diese können bewirken, dass einzelne Maschinen oder ganze Produktionsstraßen übernommen werden, ausfallen oder im schlimmsten Fall fehlerhafte Produkte produzieren. Beispiele für erfolgreiche Angriffe wie WannaCry und Co existieren bereits zuhauf. Eine Auslieferung von fehlerhaft produzierten Produkten kann hierbei in vielen Fällen den Ruin von kleinen und mittleren Unternehmen und aufgrund von Haftungen unter Umständen auch des Anlagenbauers bedeuten. Allerdings ist die Gefahr die eine ungesicherte Maschine/Anlage birgt, vielen Herstellern und Betreibern bisher nicht bekannt, da Gefahren oft erst bei eigener Betroffenheit wahrgenommen werden.

Um Angriffe und daraus resultierende Schadensersatzansprüche abzuwehren, sollte sich jeder Hersteller vor der Entwicklung neuer Maschinen/Anlagen Gedanken um deren Sicherheit machen und diese im Vorfeld mit dem Betreiber klären. Hierbei unterscheidet sich die Security einer industriellen deutlich von einer Office-Umgebung. Beispielsweise sind Laufzeiten von 20 Jahren bei Maschinen keine Seltenheit, was wiederum die Aktualisierung von Betriebssystemen und den Einsatz von Antiviren-Software deutlich erschwert. Auch ist in der Produktion die Verfügbarkeit und die fehlerfreie Produktion das höchste Schutzziel, wohingegen Vertraulichkeit und Integrität in der Office-IT deutlich überwiegen.

Das vorliegende Whitepaper soll deshalb für Maschinen- und Anlagenbauer einen Leitfaden zum Erstellen von sicheren, digitalisierten Maschinen und Anlagen bieten. Hierbei liegt der Fokus nicht auf einer ausgearbeiteten Lösung für alle Szenarien, sondern in der Nennung von Punkten, über die bei jeder Maschine/Anlage separat reflektiert und für das Unternehmen individuelle Lösungen erarbeitet werden müssen. Natürlich wird nach der Erarbeitung eines Konzepts für eine Maschine ein Großteil auf andere Maschinen übertragbar sein.

Neben diesem Whitepaper gibt es eine Vielzahl von weiteren, demselben Thema gewidmeten, Dokumenten. Allerdings richtet sich dieses Dokument gegenüber den bereits existierenden, wie beispielsweise ISA/IEC Norm 62443 oder das BSI ICS Security Kompendium, an ein breites Spektrum von Maschinen- und Anlagenbauern und nicht explizit an IT-Fachkräfte. Hierbei werden sowohl aus Sicht der Lieferanten als auch aus Sicht der Kunden wichtige Anforderungen (Requirements)

hinterfragt. Zudem soll es als Checkliste für Betreiber, Hersteller und Einkäufer dienen, um wichtige Anforderungen der Industrie 4.0 bei Maschinen und Anlagen zu überprüfen.

Das Whitepaper ist in einer fragenden Form erstellt worden, dass alle für Maschinen- und Anlagenbauer sowie Betreiber nötigen Fragestellungen formuliert und Beispiele für Lösungsmöglichkeiten gibt. Zusätzlich muss das Whitepaper nicht komplett an einem Stück gelesen werden, da sich einzelne Kapitel nicht bedingen. Wo weiterführende Informationen zu dem aktuellen Kapitelpunkt aufgeführt sind, wird entsprechend verwiesen.

Die folgende Abgrenzung der ENISA (European Union Agency for Network and Information Security) [ENISA15] soll die verschiedenen Begrifflichkeiten der Security verdeutlichen:

Communications Security	Der Schutz gegen einen Angriff auf die technische Infrastruktur eines Cyber Systems, der zu einer Veränderung seines Verhaltens führt, um Aktivitäten auszuführen, die von seinen Besitzern, Entwicklern und Benutzern nicht beabsichtigt sind.
Operations Security	Der Schutz gegen die vorsätzliche Veränderung von Verfahrensweisen oder Arbeitsabläufen, die zu Ergebnisse führen, die von seinen Besitzern, Entwicklern und Benutzern nicht beabsichtigt sind.
Information Security	Der Schutz gegen die Gefahr eines Diebstahls, einer Löschung oder einer Veränderung von gespeicherten oder übertragenen Daten in einem Cyber System.
Physical Security	Der Schutz gegen physische Bedrohung, die das korrekte Verhalten eines Cyber Systems beeinflusst oder schädigt. Beispiele hierfür sind der physische Zugriff auf Server, das Einbringen von bösartiger Hardware in das Netzwerk oder die Nötigung von Anwendern oder ihrer Familien.
Public/National Security	Der Schutz gegen eine Bedrohung, dessen Ursprung aus dem Cyber Space kommt und entweder physische oder cyber-physische Anlagen auf eine Art und Weise bedroht, der einen politischen, militärischen oder strategischen Nutzen für den Angreifer hat. Beispiele hierfür sind „Stuxnet“ oder weitreichende DoS Angriffe auf Einrichtungen oder die Kommunikation von Finanzsystemen oder andere kritische öffentliche oder industrielle Einrichtungen.

Zu Beginn geht das Whitepaper in Kapitel 2 auf Risiken ein, die bei einer Maschine/Anlage beachtet werden müssen. Hierzu wird herausgearbeitet, was wogegen geschützt werden muss, sowie eine Abgrenzung zu nicht schutzbedürftigen Komponenten gegeben. Nach der Risikoanalyse werden in Kapitel 3 technische Requirements für schutzbedürftige Komponenten und Maschinen, wie beispielsweise Netzsegmentierung, Benutzerkonten, Protokolle und Fernwartung, herausgearbeitet. Hierbei werden viele Punkte, in der oben bereits vorgestellten Frageform, angesprochen und Beispiele für mögliche Ausprägungen genannt. Das Kapitel 4 geht nach den technischen Requirements auf die organisatorischen Requirements, in derselben Form wie in Kapitel 3, ein. Nach dem Erstellen der Requirements geht das Whitepaper auf die anschließend benötigten Schulungen des Personals im Kapitel 5, sowie auf die folglich benötigte Verifikation der aufgestellten Requirements in Kapitel 6 ausführlich ein. Abschließend gibt es in Kapitel 7 ein Fazit sowie einen kurzen Ausblick.

2. Risikoanalyse

Gegenstand der Risikoanalyse ist es, festzulegen, was (welche Daten, Informationen, etc.) wogegen (gegen welche Gefahren, z. B. Diebstahl, Angriff, Manipulation) geschützt werden muss.

2.1. Was soll geschützt werden?

Welche Daten und Informationen sollen geschützt werden?

Z. B.: Produktionsdaten, Prozessdaten, Konstruktionsdaten, Baupläne, Messdaten, Algorithmen, Auswertungen, kryptografische Schlüssel, Zugangsdaten, Arbeitsergebnisse

Welche Arbeitsergebnisse sollen geschützt werden?

Z. B.: Prototypen, Entwürfe, Konstruktionsmuster, Konfigurationen

Welches Wissen soll geschützt werden?

Z. B.: eigene Patente, spezifisches Fachwissen, Rezepturen, Einstellungen, Parameter

Welche Software soll geschützt werden?

Z. B.: die eigene Software, die Steuerung der Maschine/Anlage, die SPS, das Betriebssystem

Welche Hardware soll geschützt werden?

Z. B.: der Steuerungs-PC, die SPS, eine Maschine, einzelne Komponenten einer Maschine, das Netzwerk (Switche, Router, VPNs, Gateways), das Real-Time-Netz in einer Maschine

2.2. Wogegen soll es geschützt werden?

Ein vollständiger Schutz gegen jede mögliche Bedrohung ist ausgeschlossen.
Ziel der Risikoanalyse ist vielmehr, die wichtigsten Gefahren zu erkennen und zu bewerten, wie gravierend die möglichen Auswirkungen für das eigene Unternehmen bzw. die eigene Maschine/Anlage sein können.
Eine Risikoanalyse muss spezifisch für ein Unternehmen, eine Produktionsumgebung, ein System, eine Anlage oder eine Maschine durchgeführt werden.
Während es in einem Fall vertretbar sein mag, eine gewisse Gefahr in Kauf zu nehmen, mag die gleiche Gefahr in einem anderen Fall das wirtschaftliche Überleben des gesamten Unternehmens bedrohen.

Soll das Schutzobjekt gegen unbefugten Zugriff abgesichert werden?

Z. B.: unbefugtes Login, unbefugte Datenausgabe, unbefugte Ausübung von Rollen

Soll das Schutzobjekt gegen Veränderung/Manipulation abgesichert werden?

Z. B.: Einschleusen von Schadsoftware, falsche Bauteile, Veränderung von Parametern oder Einstellungen

Soll das Schutzobjekt gegen Betriebsausfall abgesichert werden?

3. Technische Requirements zur Sicherstellung von Security

Neben organisatorischen Themen, welche in Kapitel 4 betrachtet werden, gilt es vielfältige technische Aspekte zur Sicherung von Security zu beachten. Da kein allgemeingültiges Konzept für die Sicherstellung von Security existiert, müssen sowohl Hersteller, als auch Betreiber individuelle Lösungen für sich finden. Aber erst im Konsens beider kann eine umfängliche Security-Struktur geschaffen werden.
Durch die folgenden Unterkapitel soll der Leser in die Lage versetzt werden, die für sein Umfeld notwendigen technischen Anforderungen definieren zu können. Dazu sind die einzelnen Themenbereiche in einer abfragenden Form gestaltet, die zum Nachdenken, beziehungsweise zum Erstellen eigener Anforderungen und zum Erfüllen eigener Bedürfnisse nötig sind. Angeführte Beispiele und Hinweise sollen bei der Beantwortung eine mögliche Hilfestellung geben.

3.1. Netzsegmentierung

Ein wesentlicher Aspekt zur Gewährleistung von Security im zukünftigen industriellen Umfeld ist die Segmentierung des Betreibernetzes in einzelne abgetrennte Segmente.

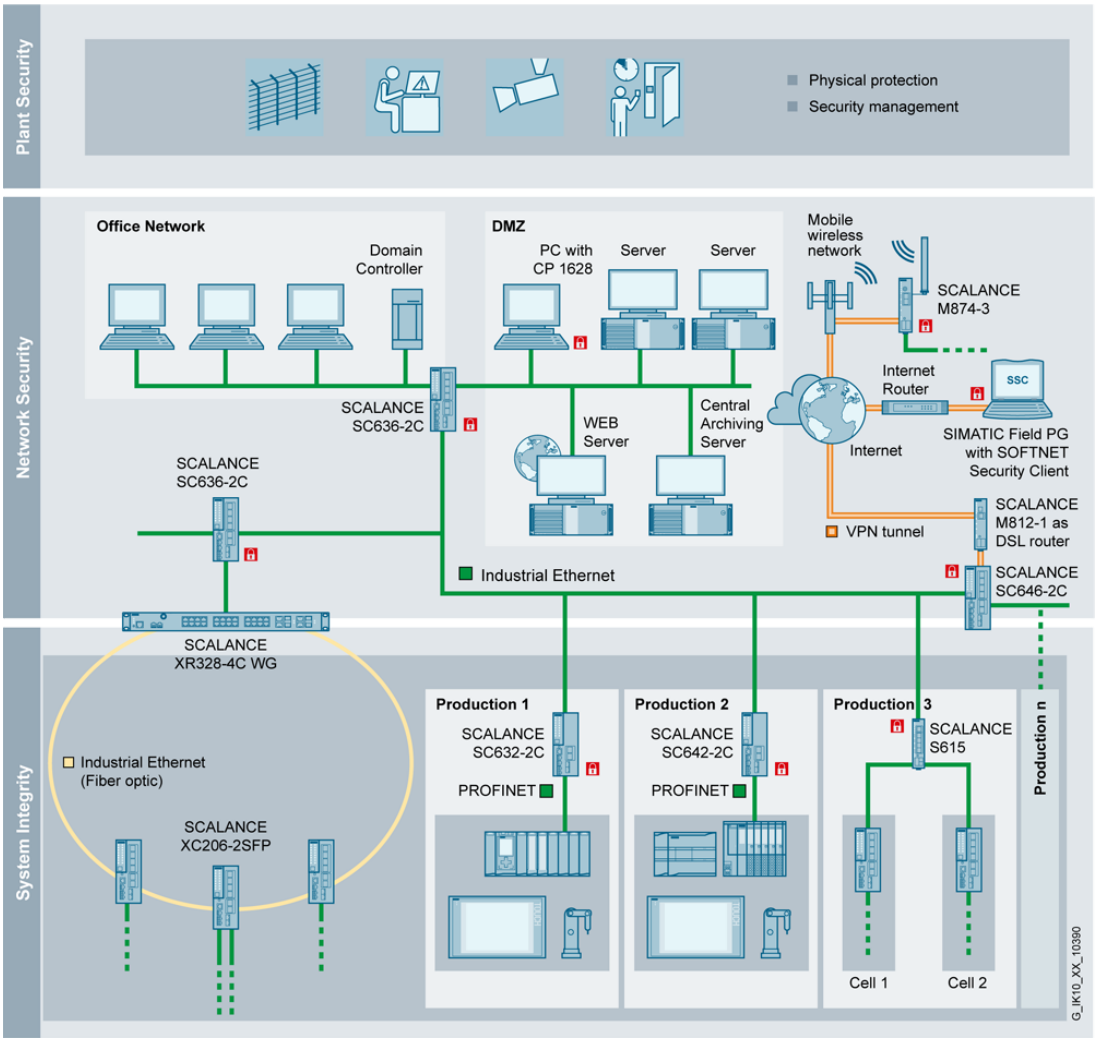

Abbildung 1: Netzwerksegmentierung nach IEC 62443; Quelle: industrial ethernet book; Aktualisierte Version von Siemens AG, DI CM IP vom 14.06.2019

Wo soll eine Netzwerksegmentierung greifen?

Zwischen Office- und Produktions-Netz (Vermeidung des Zugriffs vom Office- aufs Produktions-Netz)
Zwischen Maschine und Maschine (Vermeidung Übergriff zwischen den Maschinen)
Zwischen Maschinen- und Echtzeitnetz

Welche Gefahren sollen durch eine Netzsegmentierung vermieden werden?

Das Übergreifen von Software oder Personen auf andere schützenswürdige Komponenten.

Was soll über eine Netzsegmentierung abgesichert werden?

Übergänge zwischen einzelnen Netzen und Zonen
Schutz der Netze voreinander
Netzwerkzonen gegeneinander
Welche Kommunikation ist unerwünscht?
Welche Angriffe sollen vermieden werden?

Welche Netzwerkzonen sollen unterschieden werden?

Z. B.: DMZ, Produktions-Netz, Office-Netz, Segmentierung für jede Maschine

Wie sollen Netzwerksegmente voneinander isoliert werden?

Z. B.: Einbau von Firewalls an allen Übergängen zwischen einzelnen Netzsegmenten, Verwendung der SDN-Technologie (Vorteile: Automatisierung, Monitoring in Echtzeit, zentrale Steuerung)

Was muss regelmäßig bei der Netzsegmentierung überwacht/überprüft werden?

Z. B.: Überwachung der Zonen, Überprüfung der Services die in den Zonen laufen

Wie soll die regelmäßige Überwachung der Netzsegmentierung sichergestellt werden?

Z. B.: einzelne Audits, Überprüfung des Netzwerks bei regelmäßigen Wartungsvorgängen

Welche Services sollen in welcher Zone laufen?

Nach welchen Kriterien/Strategien soll die Aufteilung erfolgen?

Z. B.: technisch, nach Risiko

Müssen „alte“ Services isoliert werden?

3.2. Benutzerkonten, Credentials, Authentisierung und Autorisierung

Begriffserklärungen:

Die **Authentisierung** ist die Behauptung einer Identität und stellt den **Nachweis einer Person/Entität** dar, dass sie tatsächlich diejenige Person/Entität ist, die sie vorgibt zu sein. Die Credentials dienen dabei als Nachweis der Identität.
Die **Authentifizierung** ist die Verifizierung der Behauptung (s. o.) und stellt eine **Prüfung der behaupteten Authentisierung** dar.
Die Autorisierung ist die Einräumung von speziellen Rechten nach der Authentifizierung.

3.2.1. **Wie soll festgelegt werden, wer an einer Maschine/Anlage was machen darf?**

Welche Akteure (Benutzer) spielen eine Rolle?

Z. B.: Personen (des eigenen Unternehmens oder Lieferanten/Hersteller), andere Maschinen, IT-Systeme

Welche Rollen soll es geben?

Z. B.: Administratoren, Instandhalter, Einrichter, Maschinenbediener, Service-Techniker (des Maschinenlieferanten), MES-System, vorgelagerter Prozess

Welche Arten von Benutzerkonten soll es geben?

Z. B.: individuell (akteurbezogen), rollenbezogen oder eine Mischung beider

Bei individuellen Benutzerkonten kann (bei entsprechender Protokollierung) auch festgestellt werden, wer, wann und was an einer Maschine/Anlage verändert hat.

Welche Berechtigungen soll es geben bzw. werden benötigt?

Z. B.: Starten/Stoppen der Maschine, Umschalten der Betriebsart der Maschine, Zugriff auf Betriebssystem, Zugriff auf Steuerung über Programmiersystem, Leserechte auf Stückzähler und Betriebszustand (für z. B. MDE-System), Fernwartungszugang für Servicetechniker des Maschinenherstellers

Wie sollen den Akteuren entsprechende Berechtigungen zugeordnet werden?

Z. B.: Zuordnung von Rollen an einen Akteur & Zuordnung von Berechtigungen an eine Rolle, Zuordnung von Berechtigungen an einen Akteur

Wer soll welche Berechtigungen erhalten?

Z. B.: Admin:

maximale Rechte, Maschinenbediener: nur Start/Stopp, MES: Lesen des Betriebszustands,

Instandhalter:

zusätzlich zu den allgemeinen Instandhalterrechten auch Zugriff auf Betriebssystem

Grundsatz: Dem Benutzer nur die tatsächlich notwendigen Rechte zum Ausführen seiner Rolle einräumen.

3.2.2. **Wie soll die sichere Verwaltung der Benutzerkonten und der notwendigen Credentials erfolgen?**

Wer soll welche Berechtigung zur Verwaltung erhalten?

Z. B.: Nur der jeweilige Vorgesetzte, der weiß, wer welche Qualifikation besitzt.

Wo sollen die Benutzerkonten abgelegt werden?

Z. B.: Lokal auf jeder einzelnen Maschine, zentral (auf einem Server) für den gesamten Maschinenpark, zentral im Fernwartungsportal

Wie sollen die Benutzerkonten sicher gespeichert werden?

Z. B.: Verschlüsselung, Passwörter nur als Hash-Werte speichern, „sicherer“ Speicherort

Wie sollen die Credentials sicher verwaltet und verteilt werden?

Z. B.: Zentrale Verwaltung von persönlichen RFID-Chips oder Zertifikaten für die Authentisierung

Wie soll sichergestellt werden, dass die erteilten Rechte noch den aktuellen Anforderungen entsprechen bzw. ein Benutzerkonto überhaupt noch benötigt wird?

Z. B.: Wenn ein Mitarbeiter die Firma verlassen hat, die Abteilung wechselt, eine andere Rolle bekleidet: per Meldung an Verwalter

Zusätzlich regelmäßiges Überprüfen in festen Abständen durch Verwalter bzw. seine Beauftragten.

3.2.3. **Wie soll die Authentisierung erfolgen?**

Welche Arten von Credentials werden unterschieden?
Z. B.: Passwort, Hardware-Token, RFID-Chip, asymmetrischer Schlüssel, Zertifikat

Welche Authentisierungsverfahren sollen für menschliche Nutzer eingesetzt werden?
Z. B.: Benutzername und Passwort, Hardware-Token, RFID-Chip, Zertifikat

Welche Authentisierungsverfahren sollen für Softwareprozesse eingesetzt werden?
Z. B.: Public-Key mit Zertifikat

Welche Authentisierungsverfahren sollen für Komponenten eingesetzt werden?
Z. B.: Public-Key mit Zertifikat, Hardware-Token, RFID-Chip

Welche Authentisierungsverfahren sollen bevorzugt eingesetzt werden?
Z. B.: Zwei-Faktor-Authentifizierung mit Zertifikat als zweiten Faktor.

Wie soll die Sicherheit von Authentifizierungsverfahren sichergestellt werden?
Z. B.: Sicherstellung, dass Zertifikate rechtzeitig erneuert werden, Verwendung von Standardverfahren

Welche Regeln sollen bei Passwörtern eingehalten werden?
Z. B.: Mindestlänge, Zeichensatz, (Regelmäßige Pflicht zum Ändern)

Mit welchen Konzepten soll zusätzlich die Usability effizient gestaltet werden?
Z. B.: Nutzung von Verzeichnisdiensten (wie Active Directory), Single Sign-On, Single Sign-Off

3.3. Sichere Protokolle

Der Schutz von übertragenen Informationen ist eine wesentliche Anforderung der Industrie 4.0. Hierbei muss nicht nur der Inhalt durch die Sicherstellung der Vertraulichkeit, sondern auch die Integrität der Inhalte an sich sichergestellt werden.
Durch den Einsatz von sicheren Protokollen, kann im Gegensatz zum Schutz von IT-Systemen, ein nahezu hundertprozentiger Schutz der Daten mathematisch gewährleistet werden. Daher sollte dem Schutz von übertragenen Informationen viel Aufmerksamkeit gewidmet und verschlüsselte Protokolle an jeder möglichen Stelle im System eingesetzt werden.

Ab welcher Ebene muss die komplette Kommunikation gesichert sein?
Eine Sicherung jeglicher Kommunikation ist sicherlich nicht praktikabel und für die unteren Ebenen der Steuerung (Feldebene <-> Steuerungsebene) nicht zu empfehlen. Jegliche Kommunikation oberhalb der Steuerungsebene sollte, wenn möglich, über sichere Protokolle durchgeführt werden.
Hierbei gilt: Umso weniger Kontrolle über das Netzwerk und umso größer die Anzahl der Geräte im Netzwerk, durch das die Daten fließen, umso wichtiger ist der stringente Einsatz von sicheren Protokollen in diesem Netzwerk.

Wie soll die Vertraulichkeit von Informationen sichergestellt werden?
Eine Vertraulichkeit von Informationen kann durch eine eindeutige Identifikation und eine stringente Verschlüsselung der kompletten Kommunikation sichergestellt werden.
Z. B.: Zertifikate, SFTP, Netzsegmentierung, Verschlüsselung, TLS, SSH

Wie sollen Personen und Maschinen authentifiziert und autorisiert werden?

→ *Siehe hierzu Kapitel 3.2 „Benutzerkonten, Credentials, Authentisierung und Autorisierung“*

Wie soll die Integrität der Kommunikation sichergestellt werden?

Die Integrität von Informationen kann durch verschiedene (Hash)-Algorithmen sichergestellt werden. Eine Verschlüsselung der Kommunikation stellt ebenfalls die Integrität der kommunizierten Daten sicher.

Welche Verschlüsselungsalgorithmen sollen eingesetzt werden?

Beispiel: TLS >=1.2 (kein Einsatz von alten Algorithmen wie beispielsweise SSL!)

→ *Siehe hierzu Kapitel 3.9 „Kryptografie“*

Wie sollen veraltete Verschlüsselungsalgorithmen deaktiviert werden?

Beispielsweise durch einen manuellen Eingriff von Administratoren. Eine Übersicht über bereits unsichere Algorithmen gibt das BSI (siehe hierzu letzte Frage des aktuellen Kapitels).

Wie sollen neue Verschlüsselungsalgorithmen hinzugefügt werden?

Neue Algorithmen können durch Softwareupdates hinzugefügt werden. Hierbei muss im Vorfeld geregelt werden, woher diese Algorithmen stammen (eine eigene Implementierung sollte auf keinen Fall durchgeführt werden) und wer sich um die Aktualisierung kümmern muss sowie neue Algorithmen einspielen darf. Das Einspielen neuer Algorithmen, sowie das Verändern der Software muss zudem lückenlos dokumentiert werden.

→ *Siehe hierzu Kapitel 4.7 „Dokumentation“*

Wo können weiterführende Informationen zu sicheren Protokollen abgerufen werden?

Weiterführende Informationen können auf der Webseite (https://www.bsi.bund.de) des BSI eingesehen werden.

3.4. Funktechnologien

Funktechnologien gewinnen in der Industrie zunehmend an Bedeutung. Im Zuge der fortschreitenden Automatisierung und Vernetzung der Systeme kommen auch Zugriffe mit mobilen Endgeräten immer öfter zum Einsatz.

Sind eventuell auftretende Funkstörungen zu betrachten?

Die Detektion von Funkstörungen ist extrem aufwändig

Wie hoch ist das Risiko bei möglichen Angriffsszenarien?

Soll die Verbindung ausschließlich in einem separierten Bereich erfolgen?

Z. B.: Maschinen-Netz, Produktions-Netz, Office-Netz

Wie hoch sollen die Anforderungen an die Verbindung sein?

Z. B.: Echtzeit, permanente oder temporäre Anforderungen

Welche Aufgaben sollen mit der Funkverbindung ausgeführt werden?

Z. B.: Steuerung, Diagnose, Wartung, Information

Sollen unterschiedliche Funktechnologien zum Einsatz kommen?

Z. B.: WLAN, Bluetooth, RFID, NFC, Richtfunk

Welche Sicherheitsstandards sollen zum Einsatz kommen?
Z. B.: Bei WLAN: WPA, WPA2, WPA3, Radius

Sollen Technologien zur Reichweitenvergrößerung zum Einsatz kommen? Wenn ja, wird der oben geforderte Sicherheitsstandard erfüllt?
Z. B.: bei WLAN: WDS, Bridge, Repeater

Mit welchen Geräten sollen Funkverbindungen aufgebaut werden?
Von spezifizierten Handhelds bis zu privaten Smart Devices

Welche organisatorischen Maßnahmen sollen bei Devices ergriffen werden, wenn
- ein Gerät entwendet wird?
- Updates eingespielt werden müssen?
- neue Software installiert werden muss?
- Geräte ver- oder entschlüsselt werden müssen?
- Zugriff auf das Gerät benötigt wird?
- ein Gerät entsorgt wird?
- ein neues Gerät angeschafft wird?

3.5. Fernwartung

Mithilfe eines Fernwartungszugriffs auf eine Maschine/Anlage kann eine Fehlersuche und Fehlerbehebung oft kostengünstig, flexibel und innerhalb kürzester Zeit erfolgen. Bei der Möglichkeit einer Fernwartung müssen allerdings einige Punkte sowohl beim Aufbau, als auch beim Abbau einer Verbindung beachtet werden.

Wer soll zu wem eine Verbindung aufbauen?
Betreiber zum Hersteller, Hersteller zum Betreiber, Lieferant zum Hersteller, Lieferant zum Betreiber, Hersteller zum Lieferant
Der Empfänger einer Verbindung besitzt aufgrund von Freigaben stets ein erhöhtes Risiko.

Wie soll eine Fernwartungsverbindung aufgebaut werden?
Z. B.: Physisch per Schalter, Stecken von Kabeln, durch Software

Wer soll eine Fernzugriffssitzung ermöglichen?
Z. B.: Maschinenbediener, Einrichter, Abteilungsleiter,IT-Admin, IT-Datenschutzbeauftragter

Sollen besondere Schutzmaßnahmen vor dem Verbindungsaufbau berücksichtigt werden?
Z. B.: Not-Aus an der Anlage

Sollen Netzwerkverbindungen im Rahmen der Fernwartung deaktiviert werden?
Z. B.: Internetfreigabe

Welche Systeme sind im gleichen Netzwerksegment wie die Maschine erreichbar?
Z. B.: Backupserver, andere Maschinen, kritische Infrastruktur

Gibt es schutzbedürftige Verbindungen, die im Fernzugriffsfall deaktiviert werden müssen?
Z. B.: ERP-System

Welche organisatorischen und technischen Maßnahmen müssen zur Absicherung der Verbindung ergriffen werden?

Alle Betriebsabläufe sollten in stabilen Prozessen definiert und eindeutig dokumentiert sein. Geschulte Mitarbeiter stellen damit einen ordnungsgemäßen Betrieb sicher.

3.6. Sicherheit der Komponenten

„Die Kette ist nur so stark wie ihr schwächstes Glied“ – so verhält es sich auch bei der Sicherheit eines Systems. Auch wenn höchste Schutzmaßnahmen an unterschiedlichsten Stellen getroffen werden, so wird ein potenzieller Angreifer eine identifizierte Schwachstelle ausnutzen. Deshalb sollte jede einzelne ICS-Komponente auf ihre Sicherheit hin überprüft bzw. gestaltet werden.

3.6.1. **Anpassung und Prüfung von ICS Komponenten (Industrial Control Systems)**

Welche Standardeinstellungen sollen angepasst werden?

Z. B.: Default-Passwort des Administrators, Zugriffsrechte einschränken

→ *Siehe hierzu Kapitel 3.2 „Benutzerkonten, Credentials, Authentisierung und Autorisierung“*

Wie und wer dokumentiert die geänderten Einstellungen?

→ *Siehe hierzu Kapitel 4.1 „Security-Richtlinien und Prozesse“*

→ *Siehe hierzu Kapitel 4.7 „Dokumentation“*

Welche Komponente des Anlagennetzes soll zu welcher Zeit Zugriff auf das Internet haben?

Z. B.: Permanenter Zugriff für einen Daten-Logger in der Cloud, temporärer Zugriff für einen Fernwartungszugang

Wie soll die Abschottung zu anderen Komponenten in kritischen Bereichen der Maschine erfolgen?

→ *Siehe hierzu Kapitel 3.1 „Netzsegmentierung“*

→ *Siehe hierzu Kapitel 3.8 „Isolationstechniken innerhalb der Maschine/Virtualisierung“*

Wie soll die Prüfung der Security-Funktionen ausgeführt werden?

Z. B.: Verifikation, Validierung, Tests (Definition der Testfälle, Testszenarien, Testdurchführung)

→ *Siehe hierzu Kapitel 4.1 „Security Richtlinien und Prozesse“*

Wie soll die Integrität der Softwarekomponenten und Konfigurationsdaten sichergestellt werden?

Z. B.: Sichere Bootloader, Prüfung mithilfe elektronischer Signaturen

→ *Siehe hierzu Kapitel 3.9 „Kryptografie“*

→ *Siehe hierzu Kapitel 4.6 „Sicherheitsanforderungen zwischen Hersteller und Betreiber“*

→ *Siehe hierzu Kapitel 4.8 „Konfigurationsmanagement“*

3.6.2. **Verzicht auf überflüssige Komponentenfunktionen**

Jede Komponente innerhalb einer Maschine/Anlage, die eine Kommunikationsmöglichkeit bietet, kann ein potenzielles Einfallstor sein. Aus diesem Grund sind einige Überlegungen zur Absicherung von Komponenten für jede Maschine/Anlage zu treffen.

Welche Softwarekomponenten werden nicht benötigt und sollten abgeschaltet oder entfernt werden?

Z. B.: Unbenutzte Dienste mit Zugriff auf Netzwerkfunktionen, nicht benötigte Software

Welche Hardwarekomponenten werden nicht benötigt und sollten abgeschaltet oder entfernt werden?

Z. B.: Unbenutzte Schnittstellen wie USB-Ports, nur temporäre Freischaltung von Debug-Schnittstellen

3.6.3. **Komponentenhärtung**

Welche Maßnahmen sollen zur Härtung der Komponenten ergriffen werden?

Z. B.: Nur Ausführung von gehärtetem Code, Security-by-Design, Application White- und Blacklisting, Reduzierung der Systemkomplexität, Absichern der elektronischen externen Schnittstellen (besonders Debug-Schnittstellen)

3.7. "Keine Safety ohne Security"

Das im Deutschen repräsentative Wort „Sicherheit“ beinhaltet sowohl Security-, als auch Safety-Themen. Um die unterschiedliche Bedeutung klar zu machen, werden häufig die englischen Begriffe verwendet.

Im Wesentlichen beschreibt **„Security“** die Abwehr von Gefahren für ein (IT-)System. Deshalb wird dafür oft auch das Synonym „Angriffssicherheit“ verwendet.
Der Schutz des Systems (oder Teilen davon) vor Missbrauch, Diebstahl sowie absichtlich herbeigeführter Fehler stehen im Mittelpunkt.

Im Gegensatz dazu soll **„Safety“** Risiken und Gefahren abwehren, die vom System (Maschine/Anlage) selbst ausgehen.
Dabei wird von Betriebssicherheit bzw. funktionaler Sicherheit gesprochen.
Oberstes Ziel ist, dass vom System keine Gefahr für Leib und Leben (Mensch wie auch Umwelt) ausgeht und somit sichere Arbeitsbedingungen geschaffen und Unfälle vermieden werden. Eine entsprechende Safety-Lösung ist damit eine der Voraussetzungen für die CE-Kennzeichnung einer Maschine/Anlage.
Darüber hinaus darf Safety nicht mehr nur einmalig betrachtet, ausgelegt und implementiert werden, sondern ist über den gesamten Lebenszyklus der Maschine/Anlage zu sehen.
Werden in den verschiedenen Phasen die definierten Funktionen nicht bzw. nicht mehr erfüllt, entstehen Risiken, ein möglicher Verlust der CE-Kennzeichnung und damit der Verlust des Versicherungsschutzes.

3.7.1. **Wie soll die Funktionalität von Safety sichergestellt werden?**

Da in Maschinen/Anlagen immer mehr IT-Komponenten enthalten sind und eine immer stärkere Vernetzung speziell im Kontext von Industrie 4.0 stattfindet, rücken auch die beiden Sicherheitsthemen immer näher zusammen.

„**Keine Safety ohne Security**“ – diese Aussage legt die Notwendigkeit von Security dar:
Heute werden viele Safety-Funktionen in Software (auf sogenannten fehlersicheren Steuerungen) abgebildet.
Ist hierbei keine ausreichende Security vorhanden, kann die Software auf der fehlersicheren Steuerung manipuliert werden und zu Fehlfunktionen führen. Damit ist die geforderte Aufgabe der Safety nicht mehr gegeben.
Im Folge dessen ist die Umsetzung der Safety damit ebenfalls eine Softwarekomponente, für die Security-Requirements aufgestellt werden müssen. Die weiteren Kapitel in diesem Dokument geben hierzu Hilfestellungen.

Lösungsansätze für Security bei Safety-Funktionalitäten:

- Benutzermanagement für den geregelten und kontrollierten Zugriff auf die Programmierung der Sicherheitssteuerung
- Abschottung (Z.B. Sandbox, Air Gap)
- Soll eine Änderbarkeit via Fernwartung erlaubt werden?

3.8. Isolationstechniken innerhalb der Maschine/Virtualisierung

Durch Isolationstechniken innerhalb einer Maschine ist es möglich, kritische Programme oder Programme von Drittanbietern so zu isolieren, dass diese nicht auf andere Programme oder das Wirtssystem der Maschine zugreifen können.

Welche Virtualisierungstechniken sollen zum Einsatz kommen?

- Vollvirtualisierungen, die das komplette Betriebssystem virtualisieren, bieten den größten Schutz. Allerdings muss das System dafür ausgelegt sein, da jedes virtualisierte System nicht unerhebliche Hardwareressourcen benötigt. (Beispiele: VirtualBox, VMware)
- Teilvirtualisierung virtualisiert lediglich einen Teil des Betriebssystems. Hierdurch werden wesentlich weniger Ressourcen für die Virtualisierung benötigt. Viele Virtualisierungstechniken für die Teilvirtualisierung stehen allerdings nur für Linux zur Verfügung. (Beispiele: Docker)

An welchen Stellen soll Virtualisierung eingesetzt werden?

- Virtualisierung für Fernwartungszwecke beim Hersteller
  - Z. B.: Entwicklungsumgebungen, Analysetools, Monitoring, System mit direkter Verbindung (VPN) zum Betreiber
- Virtualisierung auf der Maschine beim Betreiber
  - Z. B.: Software von Drittanbietern, Kritische Konfigurationen

Welche generellen Restriktionen sollten implementiert werden?

- Restriktionen für „mobilen Code“
- Restriktionen für das Anschließen von externen Medien und Geräten

Welche Abgrenzungen sollten implementiert werden?

- Abgrenzung (besonderer Schutz) von Betriebs- und Konfigurationsdaten

3.9. Kryptografie

Die Kryptografie sichert Informationen mathematisch ab, indem nur der Besitzer des Schlüssels die Informationen (unabhängig von Ort und Zeit) entschlüsseln und verarbeiten kann.

Wie sollen eigene Kryptografische Algorithmen entwickelt werden?

- Kryptografiealgorithmen entstehen in einem langen mathematischen Prozess, und es bedarf vieler mathematischer Überprüfungen, durch unterschiedlichste Spezialisten, bis ein Algorithmus als sicher angesehen werden kann.
- Die Sicherheit eines Algorithmus darf zudem nicht von der Bekanntheit des Algorithmus (also seiner Funktionsweise) abhängen, sondern muss bei Kenntnis des Algorithmus genauso sicher sein, wie ohne deren Kenntnis.
- Aus diesen Gründen kann jedem nur ausdrücklich davon abgeraten werden, eigene Kryptografiealgorithmen zu entwickeln. Hierfür gibt es sichere und standardisierte Algorithmen, die auf nahezu allen Plattformen verfügbar und durch viele Audits überprüft worden sind.

Welche Daten/Informationen sollen verschlüsselt werden?

Welche Daten verschlüsselt abgelegt werden sollen, kann nicht pauschal beantwortet werden, da Zugriffsregelungen (siehe hierzu Kapitel 3.2 „Benutzerkonten, Credentials, Authentisierung und Autorisierung“) bereits vieles abdecken.
Eine gute Faustregel könnte lauten, alle Daten, die ein Administrator nicht einsehen darf, verschlüsselt abzulegen, da dieser von Zugriffsregelungen meist nicht eingeschränkt wird.

Wie soll der richtige Algorithmus für ein Szenario gesucht werden?

Der Einsatz von nicht standardisierten und überprüften Algorithmen sollte unter allen Umständen ausgeschlossen werden. (Das NIST überprüft und standardisiert kryptografische Algorithmen)
Umso höher die Bit-Zahl, umso stärker ist der Algorithmus (Beispiel: SHA256 ist stärker als SHA128)
Wird eine Umkehrfunktion des Algorithmus benötigt?
Asymmetrisch zur Kommunikation zwischen zwei sich nicht kennenden Partnern
Verwende beispielsweise RSA („Perfect Forward Secrecy“ beachten!)
Symmetrisch zur Speicherung und/oder Übertragung von Informationen, die mit demselben Schlüssel ver- und entschlüsselt werden
Verwende beispielsweise AES.
Wird keine Umkehrfunktion des Algorithmus benötigt (z. B. für Passwörter)?
Verwende Hash-Algorithmen wie beispielsweise SHA2 oder SHA3.

Welche organisatorischen Aspekte müssen beachtet werden?

→ *Siehe hierzu Kapitel 3.10 „Änderungsmanagement“*
→ *Siehe hierzu Kapitel 4.7 „Dokumentation“*
→ *Siehe hierzu Kapitel 4.8 „Konfigurationsmanagement“*

3.10. Änderungsmanagement

Das Änderungsmanagement umfasst alle Prozesse, die bei einer Änderung an einer Maschine durchgeführt werden müssen. Dies kann sowohl eine Hardware- oder Software-seitige Änderung als auch eine Organisatorische oder Berechtigungs-Änderung sein.

Alle organisatorischen Aspekte, die den Lebenszyklus von Maschinen und Produkten bei der Entwicklung, Betreuung und Entsorgung beschreiben, sind in Kapitel 4.8 „Konfigurationsmanagement“ beschrieben.

Wie sollen Änderungen (Hardware) an einer Maschine eingepflegt werden, damit die Security erhalten bleibt?

Hardwaremäßige Änderungen haben auf die Security meist keine Auswirkungen, außer es werden Kommunikationskomponenten verändert. Eine Absicherung der Maschine/Software muss anschließend an die veränderte Hardware angepasst werden. Alle Tests sind hierbei erneut durchzuführen.

Wie sollen Änderungen (Software) in eine Maschine eingepflegt werden, damit die Security erhalten bleibt?

Das Einbinden von neuer oder das Aktualisieren bestehender Software kann stets zu unerwartetem Verhalten an anderen Stellen führen. Daher sind nach einer Veränderung der Software stets die komplette Software sowie alle davon abhängigen Komponenten, zu testen. Für jede Maschine sollten hierbei alle durchgeführten Tests (siehe hierzu Kapitel 6 „Verifikation und Validierung von Security Requirements“) wiederholt werden.

Was muss vor einer Veränderung beachtet/analysiert werden?

Vor jeder Veränderung muss eine Risikoabschätzung aus Sicht der Security durchgeführt werden. Beispielsweise kann eine Maschine bei einem Softwareupdate ausfallen. Die Risikoabschätzung kann anschließend für jedes Szenario bestimmen, ob eine Veränderung sinnvoll ist oder nicht. Für jedes Szenario muss im Vorfeld ein Handlungsleitfaden erstellt und bereitgelegt werden.
Vor einem Einspielen neuer Software muss diese getestet und analysiert werden. Sinnvoll ist ein zweites (virtualisiertes) System, welches dem Livesystem möglichst ähnelt, zur Verfügung zu stellen und auf diesem die Software vorab ohne das Risiko eines Ausfalls zu testen.
Vor dem Aufspielen sollte eine komplette Sicherung des Systems durchgeführt und diese Sicherung versioniert abgelegt werden.
Vor jeder Veränderung muss geprüft werden, ob gegebenenfalls Zertifizierungen, wie die CE-Kennzeichnung, verloren gehen könnten. Gehen durch eine softwareseitige Änderung Zertifizierungen verloren, so muss im Vorfeld festgelegt sein, wie die Zertifizierung erneuert werden kann und welchen zeitlichen Aufwand dies bedeutet. Da ein Betreiben einer Maschine ohne CE-Zertifizierung nicht erlaubt ist, muss die Zeit zum Erneuern der Zertifizierung der Ausfallzeit hinzugerechnet werden.
Vor einer Veränderung sollte stets ein Verantwortlicher festgelegt werden, der den kompletten Änderungsprozess begleitet und alle Informationen zentral verwaltet und die Änderung organisiert.

Was muss nach einer Veränderung beachtet werden?

Nach einer Veränderung muss das komplette System erneut getestet und alle Funktionen – insbesondere Security-kritische Aspekte überprüft werden.
Alle durchgeführten Änderungen sollten in einem veränderungssicheren Dokument mit Datum, Ort, Zeit, Person und detaillierter Beschreibung der Änderung festgehalten werden.
Nach der Aktualisierung sollte eine weitere Sicherung durchgeführt und versioniert abgelegt werden, um gegebenenfalls später belegen zu können, dass Probleme nicht durch die Veränderungen hervorgerufen wurden.

4. Organisatorische Requirements zur Sicherstellung von Security

Die folgenden Kapitel geben einen Einblick in eine Vielzahl von benötigten organisatorischen Prozessen im Themenfeld von Security Requirements. Hierbei wird das in Kapitel 3 verwendete Schema der anregenden Fragen und möglichen Antworten beibehalten. Der Leser soll die aufgezeigten Fragen reflektieren und auf die eigene Unternehmens- und Securitystruktur übertragen. Schließlich soll er auf diese Weise seine individuellen Bedürfnisse für die organisatorischen Prozesse identifizieren und umsetzen.

4.1. Security-Richtlinien und Prozesse

Neben den technischen Umsetzungen der Security müssen in einem Unternehmen zusätzlich Security Richtlinien und Prozesse erarbeitet und umgesetzt werden, um den Sicherheitsanspruch des Unternehmens fortwährend gewährleisten zu können.

4.1.1. **Aufbau der Sicherheitspolitik**

Soll es ein übergeordnetes Sicherheits-Leitbild geben?

Die Durchsetzung der Sicherheitspolitik muss vom Management kommen.
Ein übergeordnetes Leitbild schafft den Rahmen für detaillierte Anweisungen.

Für welche Themen und Bereiche sollen Richtlinien erstellt werden?

- für welche Abteilungen des Unternehmens sollen Sicherheits-Richtlinien erstellt werden?
- für welche Systeme? (Z. B. Nutzung best. IT-Systeme, Nutzung des Internets, Umgang mit Virenschutz)
- für welche Informationen? (Z. B. Daten ab einer gewissen Vertraulichkeits-Einstufung)
- für bestimmte Tätigkeiten/Vorgänge (Z. B. Umgang mit Email, Datenarchivierung, Datenlöschung)
- für besondere Situationen (Z. B. Notfallplan, Wiederherstellung)
- für wen? (Z. B.: für alle Mitarbeiter einer Abteilung, für bestimmte Rollen [Führungskräfte, IT-Verantwortliche, externe Mitarbeiter])

Welche Arten von Dokumentation soll es geben?

Z. B.: Richtlinien, Arbeitsanweisungen

Welche sicherheitsrelevanten Abläufe sollen mit Prozessen hinterlegt werden?

Welche Sicherheits-Ziele sollen erreicht werden?

Welche "Leitwerte" sollen durch die Richtlinien abgesichert werden?

(Leitwerte: z. B. Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Zurechenbarkeit)
Z. B. Sensibilisierung der Mitarbeiter, Darstellung nach außen - Vertrauen schaffen

4.1.2. **Aufgaben und Verantwortlichkeiten**

Wie soll die Sicherheitsorganisation aussehen?

Rollen, Zuständigkeiten & Verantwortlichkeiten müssen definiert werden

Wo, wie und von welcher Rolle sollen die Sicherheits-Richtlinien veröffentlicht werden?

Wann, wie häufig und von welcher Rolle sollen Updates erfolgen?

Soll ein Schulungsprogramm aufgesetzt werden?
→ *siehe hierzu Kapitel 5 „Schulungen“*

Wie sollen die Mitarbeiter zur Einhaltung der Richtlinie verpflichtet werden?
Z. B. durch Unterschrift oder durch regelmäßige Prüfungen

Wie soll die Einhaltung der Sicherheits-Richtlinien geprüft werden?
Z. B. durch unabhängige Sicherheits-Audits

Wie sollen Verstöße gegen die Regeln geahndet werden?

4.1.3. **Strategie und Inhalte der Sicherheits-Richtlinien**

Wie sollen die Ziele erreicht werden?

Soll die Sicherheitspolitik sich an einem Standard/einer Norm orientieren?

Welche Maßnahmen sollen verpflichtend vorgeschrieben werden?
→ *siehe hierzu auch die Themen aus Kapitel 3*

4.2. Monitoring und Angriffserkennung

Voraussetzung für Monitoring und Angriffserkennung:
der reguläre Betrieb, die typischen Datenflüsse, die üblichen Netzwerkaktivitäten und das typische Nutzerverhalten sind bekannt.
die Netzwerkarchitektur erlaubt eine Überwachung und die Netzwerksegmentierung ist sinnvoll gewählt.
die Zugriffsrechte sind definiert.

Grundsätzlich sollte eine Überwachung nicht nur an einer Stelle erfolgen (kein "Burgmauer-Konzept"), sondern es sollte eine verteilte Überwachung aufgebaut werden.

4.2.1. **Was soll überwacht werden?**

Woran ließen sich Indikatoren für eine Unregelmäßigkeit festmachen?
Z. B.: an auffälligen Zugriffen (von Maschinen, Personen, Applikationen), an einem untypischen Nutzerverhalten, an gespeicherte Daten, an Besonderheiten im Datenverkehr, am Ressourcenverbrauch, an der Leistung, an der veränderten Geschwindigkeit, an der Konfiguration, an der fehlenden Verfügbarkeit

4.2.2. **Wie und wo soll überwacht werden?**

Soll ein Logging/Aufzeichnung von Daten erfolgen?
Welche Daten sollen aufgezeichnet werden?
Achtung bei der Aufzeichnung von personenbezogenen Daten!
Wie kann sichergestellt werden, dass das Logging nicht manipuliert oder verfälscht wird?
Externes Logging oder Blockchain
Wie lange sollen Daten aufgezeichnet werden?
Zeitraum der Aufnahme
Aufbewahrungsdauer der gespeicherten Daten

Können Monitoringfunktionen im Leitstand integriert werden?

Soll permanent, periodisch oder in Stichproben überwacht werden?

Soll eine Signaturprüfung durchgeführt werden?
Vom Programm? Von der Kommunikation? Von Emails?

Soll ein Virenscanner installiert werden?
Achtung:
Die Installation eines Virenscanners darf nicht die Funktion beeinträchtigen.
Wenn die Steuerung ein proprietäres System ist, muss geprüft werden, ob es einen Virenscanner gibt, welcher darauf installiert werden kann.
Das Installieren eines Virenscanners führt unter Umständen zum Erlöschen der Gewährleistung des Herstellers.

An welcher Stelle im System/Netzwerk soll ein Monitoring eingerichtet werden?

Was muss an welcher Stelle überwacht werden?

4.2.3. **Analyse und Auswertung**

Soll die Auswertung automatisiert erfolgen?
Z. B.: mit einem Tool, Datamining, KI

Soll eine Anomalieerkennung durchgeführt werden? (siehe Voraussetzung)
Vergleich mit "normalen" Daten
Vergleich mit "normalem" Verhalten

Sollen Angriffe auf Basis von Angriffsmustern erkannt werden?
Nachteil: Nur bekannte Angriffsmuster können erkannt werden

Sollen Tools eingesetzt werden?
Z. B.: IDS Intrusion Detection Systems, SIEM

4.2.4. **Warnung und Alarm**

In welchen Situationen soll eine Warnung oder ein Alarm ausgelöst werden?

Wie soll eine Warnung oder ein Alarm aussehen?
Z. B.: E-Mail, Warnton, Warnleuchte

An wen ist die Warnung oder der Alarm gerichtet?
Z. B.: Maschinen-Bediener, Administrator …
Soll es verschiedene Eskalationsstufen geben?

Was ist im Fall einer beobachteten Unregelmäßigkeit zu tun?

Was ist im Fall einer Warnung oder eines Alarms zu tun?

4.3. Wiederherstellungsplan

Ein Wiederherstellungsplan legt fest, mit welchen Mitteln und Maßnahmen Systeme und Funktionen nach einem Störfall/Sicherheitsvorfall wiederhergestellt werden müssen. Ziel ist es, die Arbeitsfähigkeit rasch und mit einem definierten, konsistenten Datenstand wieder zu erlangen.

4.3.1. **Mögliche Gefahren**

Für welche Szenarien muss die Wiederherstellbarkeit gewährleistet sein?

Z. B.: Hardwareausfall, Hardware-Defekt, Stromausfall, Überhitzung, Ausfall Klimaanlage, Feuer, Ausfall des zentralen Servers, Ausfall eines besonders kritischen Servers, Ausfall des Kommunikationssystems, Ausfall der Steuersoftware, Ausfall Zutrittssystem, Produktionsdaten nicht verfügbar, Datendiebstahl, Datenverlust, Sabotage, Terror, Wiederherstellung nach fehlgeschlagenem Update, Wiederherstellung nach Installation neuer Komponenten

→ *siehe auch Ergebnisse der Risikoanalyse oder Business Impact Analyse*

4.3.2. **Szenarien für die Wiederherstellung**

Ein Recovery-Szenario beschreibt im Einzelnen, was, wann, wie und von wem getan werden muss, um die Auswirkungen des Störfalls zu beheben. Abhängig von den möglichen Störfällen kann es mehrere verschiedene Recovery-Szenarien geben.

Was muss wiederhergestellt werden?

Welche Anlagen? Welche Systeme? Welche Server? Welche Festplatten? Welche Hardware?
Welche Applikationen oder Steuerungssoftware? Welche Daten/Informationen/"Rezepte"?

Muss ein Notbetrieb definiert werden?

Welche Prioritäten gelten bei der Wiederherstellung?

Was muss zuerst wiederhergestellt werden?

abhängig von Unternehmenszielen, schützenswerten Objekten, Anforderungen an Geschäftskontinuität, Service Level

Welche Abhängigkeiten müssen berücksichtigt werden?

Z. B.: technische Abhängigkeiten, Schnittstellen zu IT, zu Personalwesen, zu Kunden)
sind die Prioritäten abhängig von der Art oder der Zeit des Störfalls?

Wann und von wem wird das Ende der Wiederherstellung und der Übergang zum Normalbetrieb bekannt gegeben?

Wie können die Auswirkungen des Störfalls behoben werden?

Z. B.: durch Einspielen von Backups oder Auslieferungsständen, durch redundante Systeme, durch redundante Datenhaltung, durch dezentrale Datenhaltung, durch Neuinstallation von Applikationen, durch Beschaffung neuer Hardware

Welche Zeiten müssen eingehalten werden?

Wer muss eine Tätigkeit durchführen?

Z. B.: Abteilungsleiter, Servicetechniker

Wer muss benachrichtigt werden?

Wie soll die Benachrichtigung erfolgen?
Wie kann Erreichbarkeit sichergestellt werden?

Wie sieht eine Vertreter-Regelung aus?

4.3.3. Voraussetzungen und Vorbereitungen für die Wiederherstellung

Technisch:

Wie, wann und wie häufig sollen Backups erstellt werden?

Backup immer beim Start? Nach bestimmten Zeitintervallen?
Manuelle Backups? Automatische Backups? (Z. B. automatische Sicherung für Steuerrechner)
anwendungsabhängig
Inhalte eines Backups, Datenvolumen
redundante Backups, Backup vom Backup

Welche Backup-Systeme werden benötigt?

Z. B.: NAS Systeme (Network Attached Storage)

Welche Prüfungen müssen vor dem Einspielen eines Backups erfolgen?

Wie erfolgt die Verschlüsselung von Backups?

Auf welchem Medium werden die Backups gespeichert?

Die Lebensdauer von Medien beachten

Wer hat Zugriff (Berechtigungen) auf die Backups?

Es muss sichergestellt werden, dass ein Backup immer (auch wenn ein Mitarbeiter nicht da ist) eingespielt werden kann.

Wo werden die Backups aufbewahrt?

Sichere Ablage von Backups
→ *siehe hierzu Kapitel 4.8 „Konfigurationsmanagement“*

In welchen Abständen müssen die Backups überprüft werden?

Sollen Hardware-Ersatzteile bereitgehalten werden? Welche?

Welche Arbeitsanweisungen (Dokumentation) müssen zur Wiederherstellung verfügbar sein?

Was muss getestet werden?

Test von Backups: ist Wiederherstellung möglich?

Wie häufig müssen Tests des Wiederherstellungsplans erfolgen?

organisatorisch:

Wo ist der Wiederherstellungsplan zu finden und für wen ist er zugänglich?

Wer ist der Verantwortliche (Owner) des Plans?

Wie wird sichergestellt, dass der Plan stets aktuell ist?

Z. B.: aktueller Stand der Systeme, Liste der ausgemusterten Systeme ist aktuell, Namen und Kontaktdaten der Zuständigen sind aktuell

Muss eine Abstimmung mit anderen Plänen erfolgen?
Z. B.: Wiederherstellungspläne anderer Anlagen und anderer Betreiber

Wer hat Zugriff zu Backups, benötigten Passwörtern, Schlüsseln, Ablageorten, …

Was soll zur Nachbereitung eines Störfalls getan werden?

4.4. Sicherer Produktlebenszyklus

Alle Maschinen/Anlagen befinden sich stets in einer Phase des System-Lebenszyklus:
Initiierung –> Entwicklung –> Inbetriebnahme –> Betrieb/Wartung –> Stilllegung.

Die Sicherstellung von Security ist mit der Entwicklung und Inbetriebnahme einer Maschine oder Anlage nicht abgeschlossen, sondern bedarf einer laufenden Pflege der Systeme und Komponenten. Security Requirements und deren Tests müssen daher integraler Bestandteil aller Phasen des Lebenszyklus sein.

Was muss in der Planungs-/Initiierungsphase einer neuen Maschine/Anlage berücksichtigt werden?
- Verantwortliche für Security benennen
- Risikoanalyse durchführen
- Business Impact Analyse erstellen
- Unternehmensrichtlinie, Best Practices, Gesetze heranziehen
- Schutzbedarf feststellen (was gilt es zu schützen?)
- Security Konzept erstellen und Security Maßnahmen planen
- Security Requirements und Security Testing definieren
- Security Richtlinien für Lieferanten festlegen
- Abnahmebedingungen für Security festlegen
- Schulungen planen und durchführen

Was muss in der Entwicklungsphase einer Maschine/Anlage berücksichtigt werden?
- Verantwortliche für Security benennen
- Entwicklung einer sicheren, resilienten Systemarchitektur
- Sicheres Programmieren
- Absicherung der Schnittstellen
- Schutz der Entwicklungs-/Testumgebung und des Codes
- Konfigurationsmanagement
- Security Gates analog zu Quality Gates
- Regelmäßige manuelle und automatisierte Security Tests und deren Dokumentation
- Ausbildung und Qualifikation der Mitarbeiter

Was muss in der Inbetriebnahmephase einer Maschine/Anlage berücksichtigt werden?
- Verantwortliche für Security benennen
- Durchführung der Security Tests
- Security Abnahme durch den Auftraggeber
- Übergabe und Konfigurationsmanagement der gelieferten Software Komponenten

Was muss in der Betriebs-/Wartungsphase einer Maschine/Anlage berücksichtigt werden?

- Verantwortliche für Security benennen
- Beobachtung von neuen Schwachstellen der beteiligten Systeme und Komponenten durch Auftraggeber und Auftragnehmer
- Beobachtung der Bedrohungslage durch Auftraggeber und Auftragnehmer
- Patch Management und Security Testing für bekannt gewordene Schwachstellen

Was muss bei der Stilllegung und Entsorgung einer Maschine/Anlage berücksichtigt werden?

Löschen aller Daten, Programme, … mit Nachweis

4.5. Schnittstellen

Produktionsmittel (Maschinen/Anlagen) können in Bezug auf Industrie 4.0 nicht isoliert betrachtet werden. Es gibt viele zusätzliche Systeme, mit denen Daten und Informationen bidirektional ausgetauscht werden müssen. Durch solche Kopplungen werden Systeme verwundbarer und es müssen geeignete Maßnahmen zur Gewährleistung der Sicherheit durchgeführt werden.

Wie soll sichergestellt werden, dass eine sichere Kommunikation mit weiteren Systemen erfolgt?

Festlegen eines Schnittstellenmanagers (CDO[1] bzw. ein Beauftragter dessen)
Klären, welche Kommunikation zwischen welchen Systemen überhaupt notwendig ist und unnötigen Datenaustausch vermeiden *(siehe hierzu Kapitel 3.6 „Sicherheit der Komponenten")*
Planen und Dokumentieren der Schnittstellen sowie des notwendigen Informationsflusses von und zu Fremdsystemen wie beispielsweise:
- Vor- und nachgelagerte Prozessschritte (Querkommunikation in der Produktion)
- MES-System (z. B. Auftragsdatenübernahme, Rückmeldungen ins ERP)

Planung und Dokumentation von Zugriffsrechten auf Schnittstellen *(siehe hierzu Kapitel 3.2 „Benutzerkonten")*
- Wer oder was darf überhaupt zugreifen?
- Wer oder was darf welche Informationen über die Schnittstelle beschaffen (Z. B.: unterschiedliche Akteure bekommen mehr oder weniger Daten)

Festlegen von Maßnahmen zur Erhöhung der Sicherheit wie beispielsweise:
- Überwachen sämtlicher Kommunikation auf Anomalien (Abweichungen gegenüber der Planung)

Überwachen der Maßnahmen auf Funktionsfähigkeit und Manipulation
Zyklische Überprüfung der Maßnahmen auf Aktualität und Wirkungsgrad
Zyklische Analyse der Risiken und Prüfung auf Notwendigkeit zu Änderung der Maßnahmen

Wie soll sichergestellt werden, dass personenbezogene Daten nur im rechtlich zulässigen Rahmen erhoben bzw. verarbeitet werden?

Klären, ob die zu koppelnden Einzelsysteme überhaupt personenbezogene Daten generieren oder verarbeiten und dadurch eine verhaltens- bzw. leistungsbezogene Auswertung ermöglicht und die Datenschutzgrundverordnung erfüllt werden kann.
Den Datenschutzbeauftragten des Unternehmens und evtl. den Betriebsrat frühzeitig in alle Vorhaben einbinden.
Festlegen von zusätzlichen Maßnahmen zur Sicherstellung der Einhaltung des Rechtsraumes (Gesetze, Verordnungen usw.)

[1] CDO = Chief Digital Officer: Als Teil der Führungs-Team derjenige Verantwortliche für die Digitalisierung bzw. digitale Transformation im Unternehmen

4.6. Sicherheitsanforderungen zwischen Hersteller und Betreiber

Wird eine Maschine/Anlage ausgeliefert, so liegt es sowohl im Interesse des Herstellers als auch im Interesse des Betreibers, Klarheit über den aktuellen Stand der Security des Liefergegenstandes zu haben. Der Hersteller muss nachweisen, dass er eine sichere Maschine/Anlage ausliefert und der Betreiber muss prüfen, dass die Maschine/Anlage seinen Security Anforderungen entspricht. Darüber hinaus müssen Vereinbarungen getroffen werden, wie und von wem die künftige Sicherheit der Maschine/Anlage gewährleistet wird.

4.6.1. Sicherheit aus Sicht des Betreibers

Wie soll Sicherheit aus der Sicht des Betreibers gewährleistet werden?
- Vorgaben durch den Betreiber (Liefervorschriften sind Bestandteil des Lastenhefts)
- Detaillierte Beschreibung des beabsichtigten Lieferumfangs und der (Security-) Konfiguration durch den Lieferanten (Pflichtenheft)
- Checkliste der Security-Funktionen für die Maschinenabnahme
- Technische Überprüfung der Security (Virenscan + Securityscan)

Wer soll vor der Auftragserteilung überprüfen, ob die im Pflichtenheft aufgeführten Security-Komponenten und -Konfigurationen den Anforderungen entsprechen?
- Wie soll verfahren werden, wenn die Security-Komponenten und –Konfigurationen nicht den Anforderungen entsprechen?

Wer soll welche Security-Hardware installieren und konfigurieren?
- Zu welchem Zeitpunkt soll die Security-Hardware eingebaut, konfiguriert und aktiviert werden?

Wer soll welche Security-Software installieren und konfigurieren?
- Zu welchem Zeitpunkt soll die Security-Software installiert, konfiguriert, getestet und aktiviert werden?

Soll der Lieferant Informationen über benötigte Security Patches bereitstellen?
- In welcher Form sollen Security Patches bereitgestellt werden?
- Sollen die Patches vom Hersteller/Lieferanten getestet und freigegeben werden?

Wie soll der Test der Security-Hard- und Software erfolgen?

Sollen Softwarelizenzen vom Lieferanten gekauft oder durch den Betreiber bereitgestellt werden?

Soll beschrieben werden, wie bei Änderungen oder Updates von Software und Hardware verfahren wird?

4.6.2. Sicherheit aus Sicht des Lieferanten

Soll festgelegt werden, welche Software nicht vom Betreiber geändert werden darf?

Soll festgelegt werden, welche Software vom Betreiber aktualisiert werden muss?

In welchem Zeitraum muss Software vom Betreiber aktualisiert werden?
- Z. B.: kritische Patches oder Fehlerbereinigungen

Soll es eine Absprache mit dem Betreiber geben, welche Virenschutz-Software (oder welche Alternative) verwendet werden soll?

Soll beschrieben werden, wie Sicherungen gemacht werden müssen?

Sollen Veränderungen an den Schnittstellen gemeldet werden?

Über welchen Zeitraum muss die Sicherheit der Maschine/Anlage gewährleistet werden? (Gewährleistung, Wartungsvertrag)

Welche Maßnahmen und Prozesse muss der Lieferant intern etablieren, um die gelisteten Anforderungen erfüllen zu können?

Z. B.: Patchmanagement

4.6.3. **Sicherheit aus Sicht des Empfängers**

Soll eine Security-Checkliste zur Maschinenabnahme erstellt werden?

Wie und wann soll geprüft werden, ob die Liefervorschriften bzgl. Security eingehalten wurden?

Wie und wann soll geprüft werden, dass die komplette Dokumentation vorliegt?

Wie und wann soll geprüft werden, dass die Lizenzen geliefert und dem Lizenzmanagement gemeldet wurden?

Wie und wann soll geprüft werden, dass alle für den Fall einer Wiederherstellung benötigten Anleitungen, Software und Backups vorliegen?

Wie und wann soll geprüft werden, dass Backup und Wiederherstellung erfolgreich getestet wurden?

Wie und wann soll geprüft werden, dass die Security Patches auf aktuellstem Stand sind?

Wichtig: wie soll verfahren werden, wenn die Security Patches nicht auf dem neuesten Stand sind?

Wie und wann soll die Virenfreiheit der Maschine überprüft werden?

Soll ein Security Scan durchgeführt werden?

Wie wird mit gefundenen Securityproblemen umgegangen?

Soll geprüft werden, ob Software installiert ist, die nicht benötigt wird und hierdurch die Maschine gefährdet?

4.7. Dokumentation

Der Begriff Dokumentation bedeutet weit mehr als die einfache Beschreibung einer (Maschinen-) Funktion oder eines Prozessablaufs. Mit einer nachhaltigen Dokumentation lassen sich Fragen für jeden Mitarbeiter auf einfache Weise klären sowie Reproduzierbarkeit und Handlungssicherheit gewährleisten.

Warum muss dokumentiert werden?

Z. B. um einen hohen Wissenstand in der Belegschaft aufrecht zu halten, um eine Nachweispflicht ggf. einer Behörde zu erfüllen, um die Wartung einer Maschine/Anlage zu gewährleisten

Wie soll sichergestellt werden, dass jedem Mitarbeiter die benötigten Informationen auf einfache Weise zur Verfügung stehen?

Z. B.: Dokumentenmanagementsystem, Schulung des Mitarbeiters im Umgang mit Dokumentation

Welche Dokumentation muss erstellt werden?

Z. B.: Organisatorisch
- Risikoanalyse -> *siehe hierzu Kapitel 2 „Risikoanalyse“*
- Prozesse und Rollen im Unternehmen
- Sicherheitsvorfälle
- Strategie und Schutzmaßnahmen z. B. für Sicherheitsvorfälle

Z. B.: Technisch
- Assetmanagement: Was ist verbaut, was wurde wann geändert, …
- Schnittstellen, Ports, Protokolle -> *siehe hierzu Kapitel 3.1 „Netzsegmentierung“ und 3.3 „Sichere Protokolle“*
- Handbücher und Datenblätter
- Backup- und Wiederherstellungsstrategie -> *siehe hierzu Kapitel 4.3 „Wiederherstellungsplan“*

Wie soll eine durchgängige Dokumentation gewährleistet werden?

Wie soll sichergestellt werden, dass die Dokumentation fortlaufend versioniert und gepflegt wird?

4.8. Konfigurationsmanagement

"Konfigurationsmanagement ist ein Managementprozess zur Herstellung und Erhaltung einer Übereinstimmung der Produktleistungen sowie der funktionalen und physischen Eigenschaften des Produktes mit den Anforderungen, dem Produktdesign und den operativen Informationen während des gesamten Produktlebenszyklus." [ANSI/EIA]

Warum soll Konfigurationsmanagement durchgeführt werden?

Z. B. muss bei Bekanntwerden von Sicherheitslücken nachvollzogen werden können, in welchen Maschinen und bei welchen Kunden einzelne Softwarebibliotheken (Open Source, kommerziell) im Einsatz sind.

Welche Konfigurationsstände sollen gespeichert bzw. dokumentiert werden?

Alle an einen Kunden gelieferten bzw. beim Kunden geänderten Konfigurationsstände

Z. B.: Mechanik, Elektrik, Elektronik, Hydraulik, Embedded Software, Maschinen-Software, Industrie 4.0, IoT Komponenten

Wie sollen Konfigurationsstände für physische Komponenten dokumentiert werden?

Die verbauten physischen Komponenten sollten in Form von strukturierten Stücklisten dokumentiert werden.

Was soll im Konfigurationsstand einer Software enthalten sein?

Z. B.: Version, alle verwendeten Bibliotheken mit Version, Build-Datum

Warum ist ein Konfigurationsmanagement für physische Komponenten notwendig?

Hat eine physische Komponente ein bekanntes Sicherheitsproblem, so kann geprüft werden, welche Maschinen davon betroffen sind.

5. Schulungen

Schulungen sind ein wichtiges Mittel, um Personen in die Bedeutung von Security einzuführen und zu vermitteln, welche Maßnahmen von welcher Rolle ergriffen werden können, um Security im jeweiligen spezifischen Umfeld zu gewährleisten.
Security Incidents können alle Bereiche einer Firma betreffen. Daher genügt es nicht, ausschließlich technisches Personal zu schulen. Z. B. sollten auch Mitarbeiter aus der Verwaltung eine grundlegende Einführung erhalten.

Welche Ziele soll eine Security-Schulung erfüllen?

- Bewusstsein schaffen (Awareness) für:
  - Risiken, steigende Vernetzung durch I4.0 => deutlich höhere IT Risiken, Social engineering, Fehlbedienung
- Kosten/Nutzen belegen: IT-Sicherheit kostet Geld; IT-Sicherheit ist ein Wettbewerbsvorteil
- Weiterbildung (durch Industrie 4.0 ist IT-Know How in jedem Beruf erforderlich)
  - IT-Grundlagen
  - Grundkonzepte der IT-Sicherheit
- Ausbildung
  - Um den geänderten Anforderungen der Arbeitswelt künftig gerecht zu werden, muss IT-Security auch in den Ausbildungsplänen der Auszubildende verankert werden.
- Einarbeitung neuer Mitarbeiter

Soll ein Schulungs-Verantwortlicher und Anbieter für die Auswahl fachspezifischer Schulungen benannt werden?

Sollen Schulungspläne entsprechend den Rollen erstellt werden?

Soll eine konsequente Schulungsplanung und Durchführung für das gesamte Unternehmen geplant werden?

Welche Personengruppen sollen an welchen Schulungen teilnehmen?

- Z. B. Konstrukteure, Entwickler, Anlagenplaner, Projektierer, Verantwortliche für Produktschutz, Geschäftsführung, Management, Controlling, Produktionsverantwortliche, Instandhalter, IT Mitarbeiter, Auszubildende und Sekretariate

6. Verifikation und Validierung von Security Requirements

Security Requirements müssen nicht nur erhoben und geplant, sondern auch wirksam umgesetzt werden. Andernfalls wären sie wertlos.
Abhängig davon, ob es sich um technische oder um organisatorische Security Requirements handelt, werden Methoden der Verifikation oder der Validierung eingesetzt um nachzuweisen, dass die Maschine/Anlage gegen Security Incidents geschützt ist.

Bei der **Verifikation** handelt es sich um eine dynamische Methode, die durch Test oder Messung prüft, ob die erwartete Reaktion eintritt. Während die Maschine läuft, wird ein konkreter Testfall oder eine Messung durchgeführt, um nachzuweisen, dass das Verhalten genau dem Security Requirement entspricht.

Bei der **Validierung** wird z. B. durch ein Audit nachgewiesen, dass die geforderten Prozesse befolgt und die Richtlinien eingehalten wurden. Die Validierung ist eine statische Methode und setzt analytische Mittel zum Nachweis der Security Requirements ein.

Wie soll die Erfüllung der Security Requirements verifiziert werden?

- Z. B.: Durch Testing (dynamische Ausführung von Testfällen zur Laufzeit der Software), durch Automatisierte Vulnerability Scans mit Tools, durch Penetration Tests

Wie soll die Erfüllung der Security Requirements validiert werden?

- Security Audits (statische Analyse ohne Ausführung der Software)
- Z. B. Nachweis der Anforderungen zur Compliance mit BSI Grundschutz, ISO 27001, IEC 62443, firmeninternen Security Richtlinien
- Sind Trainings durchgeführt worden?
- Sind die Prozesse eingehalten worden?
- Security Assessments
- Security Reviews

Der Anspruch dieses Kapitels ist, aufzuzeigen, dass zu einer sicheren Maschine nicht nur Security Requirements gehören, sondern zwingend auch deren korrekte Umsetzung, die mit Tests oder Analyse Methoden, nachgewiesen werden muss. Eine detaillierte Beschreibung der Verifizierungs- und Validierungsmethoden würde den Rahmen dieses Whitepapers sprengen. Daher sei an dieser Stelle auf die Fachliteratur verwiesen.

7. Fazit und Ausblick

Dieses Whitepaper hat in den vorangegangenen Kapiteln gezeigt, dass eine allumfassende Security-Lösung für alle Maschinen- und Anlagenbauer nicht existieren kann, sondern für jede Maschine/Anlage ein individuelles Konzept erstellt werden muss. Zwar sollen bewährte Best Practices und Werkzeuge übernommen werden, aber schlussendlich kann das eigene Unternehmen beziehungsweise die eigene Maschine/Anlage nur dann optimal geschützt sein, wenn der eigene Schutzbedarf, die spezifischen Risiken und die individuell eingesetzte Technologie analysiert wurden und auf dieser Basis Schutzmaßnahmen ergriffen und regelmäßig überprüft werden.

Der Aufbau eines wirksamen, nachhaltigen und weitreichenden Sicherheitssystems ist eine ausgesprochen fordernde Aufgabe, die mit großer Sorgfalt erledigt werden muss, um eine gut gesicherte Maschine/Anlage zu betreiben und dadurch Haftungsrisiken auszuschließen. Allerdings bietet eine einmalige Erstellung und Überprüfung eines Sicherheitskonzepts lediglich einen temporären Schutz.

Die zunehmende Vernetzung von Systemen durch neue Technologien, die fortschreitende Digitalisierung der industriellen Abläufe und eine immer stärker auf den Nutzer zentrierte Sichtweise, schaffen viele neue Herausforderungen, die durchaus zu Sicherheitsrisiken werden können. Eine Maschine/Anlage, die heute bestmöglich geschützt ist, kann morgen angreifbar sein. Aus diesen Gründen ist eine stetige Überprüfung und Neubewertung der Risiken ein essenzieller Bestandteil der Wartung vernetzter Maschinen/Anlagen.

Zudem muss das Sicherheitssystem des gesamten Unternehmens fortwährend gepflegt, erweitert und auf den neuesten Stand gebracht werden. Jede Veränderung – sei es im Unternehmen, beim Lieferanten oder in der Technologie – kann aufgrund des hohen Vernetzungsgrades unvorhergesehene Auswirkungen haben.
Dieses Bewusstsein für Zusammenhänge und Gefahren muss bei allen Mitarbeitern intensiv gefördert und die Risikoanalyse zu einer kontinuierlichen Aufgabe werden, die bei jeder Veränderung die möglichen Folgen für die Security gewissenhaft untersuchen. Nur so lässt sich dauerhaft die Wirksamkeit des aufgebauten Securitysystems aufrechterhalten.

8. Literatur

[ANSI-EIA]	ANSI-EIA-649 National Consensus Standard for Configuration Management
[Enisa15]	Enisa, Definition of Cybersecurity, Gaps and Overlaps in standardization V1.0, 2015
[link1]	https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05039.html
[statista1]	https://de.statista.com/statistik/daten/studie/154143/umfrage/umsatz-im-maschinenbau-2009-nach-laendern/
[statista2]	https://de.statista.com/statistik/daten/studie/77231/umfrage/produktionswert-und-umsatz-im-deutschen-maschinenbau-seit-2000/
[statista3]	https://de.statista.com/statistik/daten/studie/237376/umfrage/geschaetzter-umsatz-im-maschinenbau-weltweit/

9. Glossar

CDO	Chief Digital Officer; Als Teil der Führungsriege derjenige Verantwortliche für die Digitalisierung bzw. digitale Transformation im Unternehmen
ENISA	European Union Agency for Network and Information Security (www.enisa.europa.eu)
PDE	Produktionsdatenerfasser
DMZ	Demilitarisierte Zone; Eine eigene, besonders geschützte Zone im Netzwerk, welche keinen direkten Zugriff auf das Firmennetzwerk besitzt.
SDN	Software Defined Network; Ein Netzwerk, welches zentral gesteuert und programmiert werden kann.
SPS	Speicherprogrammierbare Steuerung
Maschinen-Netz	Netzwerk innerhalb einer Maschine/Anlage.
Produktions-Netz	Netzwerk, in dem eine oder mehrere Maschinen/Anlagen betrieben werden.
Office-Netz	Netzwerk, in dem normale PCs und Server für Mitarbeiter betrieben werden.

10. Abbildungsverzeichnis