

4 Betrieb und Sicherheit vernetzter Systeme gewährleisten (Lernfeld 11d)



Enterprise Zone **Industrial Zone** **Area Zone** **Cell Zone** **Process**
Schutzbedarf **Systemstatus** **Dashboard** **Purdue-Modell** **Cyberkriminelle**
Cyberangriff **Überwachung** **Monitoring** **Gefahrenquellen** **IEC 62443**
Blacklist **Whitelist** **ICS** **Industrial Control System** **Operational Technology**

Darüber werden wir sprechen, uns kompetent und aktiv beteiligen, genauer im Arbeitsbuch folgende Lernsituationen/Lernarrangements bearbeiten:

Lernsituation 1: Wir kennen den Schutzbedarf von Operational-Technology-(OT-)Netzwerken und setzen Strategien der Ausfallsicherheit um.

Lernsituation 2: Wir sichern gemeinsam mit den Mitarbeitern der Produktion und der Automatisierungstechnik industrielle Maschinen und Anlagen nach international gültigen Standards ab.

Lernsituation 3: Wir überwachen den Systemstatus von cyber-physischen Systemen und vernetzten Maschinen und Anlagen.

In diesem Lernfeld der Fachrichtung „Digitale Vernetzung“ werden der Betrieb und die Sicherheit von vernetzten industriellen Produktionssystemen in den Blick genommen. Dabei wird nicht nur die Vernetzung im industriellen Umfeld betrachtet, vielmehr werden auch die Inhalte aus Kapitel 3 integriert.

Die Technologien in der Fertigungsindustrie entwickeln sich kontinuierlich und in schnellem Tempo weiter, nicht zuletzt durch die ständige Weiterentwicklung der Vernetzung von Produktionsmaschinen und Fertigungsprozessen. Durch den Fokus auf die Digitalisierung entstehen kontinuierlich auch komplett

Partnern, dass die IT-Sicherheit im Unternehmen ein wichtiges Unternehmensziel ist und das Unternehmen einer IT-Strategie mit festgelegten Zielen folgt. Eine Zertifizierung verschafft dem Prozess der IT-Sicherheit Transparenz. Es wird dadurch klarer, welche Schritte schon im Unternehmen etabliert sind und welche noch nötig sind, um den IT-Sicherheitsprozess zu ritualisieren.

Ohne wiederkehrende Überlegungen und verbesserte Maßnahmen findet keine Anpassung an die sich ständig ändernde Bedrohungslage statt. Bei allen getätigten Maßnahmen und Sicherheitsvorkehrungen muss immer bedacht werden, dass kein System sicher ist. Mit genügend Aufwand können Angreifer, z. B. durch Social Engineering, Zugang zu fast jedem System bekommen und Schaden anrichten.

Eine wichtige nicht technische Maßnahme ist die Schulung von Mitarbeitern. Nur durch eine stetige Schulung kann die Sensibilisierung der Mitarbeiter erreicht werden und es kann auf IT-Sicherheitsprobleme aufmerksam gemacht werden.

(2) Ausblick: Sicherheit denken

Für die Umsetzung einer effektiven und effizienten Sicherheitsstruktur innerhalb des Unternehmens ist die Verankerung des Themas IT-Sicherheit in der Organisationsstruktur von großer Bedeutung. Als Leitfaden sollte die Frage nach dem „Warum“ im Vordergrund stehen. Die Hauptgründe für die Umsetzung von Sicherheitsstrukturen sind zum einen die Einhaltung von Verträgen bzw. Gesetzesvorgaben (Compliance) und zum anderen die Reduktion von Risiken für die Erreichung der geschäftlichen Ziele. Eine Standardlösung für die Verankerung der Sicherheitsbeauftragten in der Unternehmensorganisation gibt es daher nicht.

In großen Unternehmen, z. B. Banken oder Versicherungen, bei denen oft umfangreiche gesetzliche Vorgaben beachtet werden müssen, ist eine zentrale und relativ nah an der Geschäftsführung angesiedelte Sicherheitsabteilung mit zusätzlichen Sicherheitsbeauftragten in den verschiedenen Abteilungen sinnvoll. In kleinen und mittleren Unternehmen (KMU) wäre ein solcher Überbau zu umfangreich und kaum finanzierbar. Hier sind eher an den Produktions- bzw. Wertschöpfungspunkten angesiedelte Sicherheitsbeauftragte sinnvoll.

Um Sicherheit dauerhaft im Unternehmen herzustellen, bedarf es der kontinuierlichen Überprüfung der Risiken wie auch der gegen diese Risiken umgesetzten Maßnahmen. Daher ist es unabdingbar, dies in das tägliche Geschäft fest zu integrieren. Sicherheitsaudits, die nur nach bestimmten Zeiträumen durchgeführt werden, sind zwar sinnvoll, um den akuten Handlungsbedarf zu identifizieren. Die Umsetzung der aus solchen Audits ermittelten Maßnahmen wird allerdings durch den punktuellen Charakter außerhalb des Tagesgeschäfts wesentlich erschwert.

Kompetenzcheck

- 1 Im Verlauf des Lernfeldes wurden Sie aufgefordert, Notizen in Ihrem Projektjournal anzulegen. Nehmen Sie diese Notizen zur Hand. Bilden Sie Gruppen und stellen Sie sich gegenseitig die erstellten Notizen vor. Nutzen Sie hierzu die folgenden Leitfragen.
 - a) Welche Informationen haben Sie sich notiert? Wurden die Notizen regelmäßig erstellt?
 - b) Haben Sie ausformulierte Sätze notiert oder nur Stichpunkte? Wie aussagekräftig sind Ihre Notizen?
 - c) Können Sie die Notizen inhaltlich noch zuordnen? Was müsste geändert werden?
 - d) Können Sie aus Ihren Notizen positive bzw. negative Erfahrungen ablesen?
 - e) Können Sie die Vorgehensweise nachvollziehen und daraus Rückschlüsse für zukünftige Aufgabenstellungen und Projekte ziehen?
 - f) Notieren Sie sich Punkte, die Sie bei einer nächsten Aufgabe anders umsetzen werden (positive oder negative Aspekte).

- 2 Bearbeiten Sie Aufgabe 1 der Lernsituation 6 im Arbeitsbuch.

neue Wertschöpfungsmodelle. Kundenspezifische Produkte können flexibel hergestellt werden und eine Vorhersage der Lieferzeiten ist durch die IT-Unterstützung entlang der Wertschöpfungskette sehr präzise möglich. Dadurch kann die Produktion genauer gesteuert und die Qualität sowie die Effizienz der Prozesse können optimiert werden. Durch rasante globale und geopolitische Veränderungen wird jedoch deutlich, dass bei stark gestörten Lieferketten eine genaue Vorhersage sehr schwierig ist.



Eine besondere Problemstellung der schnellen technologischen Weiterentwicklung und der intelligenten Vernetzungen ist die Tatsache, dass in manchen Industrie- und Handwerksunternehmen die notwendigen Sicherheitslösungen fehlen. Die richtigen Security-Maßnahmen einzusetzen, wird in Zukunft immer wichtiger. Gerade hochautomatisierte Produktionsanlagen bieten ein großes Potenzial für Cyberangriffe. Immer mehr Unternehmen erkennen das mittlerweile. Sie benötigen daher IT-Security-Lösungen, welche kostengünstig sind und gleichzeitig die Produktionsleistung nicht beeinträchtigen, damit die Vorteile der Vernetzung voll ausgeschöpft werden können, während das Risiko weitestgehend minimiert wird.

4.1 Strategien der Ausfallsicherheit für OT-Netzwerke umsetzen

S Sie sollen den Schutzbedarf von OT-Netzwerken kennen und Strategien zur Ausfallsicherheit erläutern können.

Bei der Betrachtung des Schutzbedarfs wurde bereits ausführlich auf die technischen und organisatorischen Maßnahmen (TOM) eingegangen (siehe auch Kapitel 3.1). Sie bilden für die industrielle Vernetzung eine wichtige Grundlage.

Systeme zur Fertigungs- und Prozessautomatisierung werden in sehr vielen Industriebetrieben eingesetzt. Angriffe auf Produktionsanlagen und kritische Infrastruktur wie Energieerzeugung, Wasserversorgung und Verkehrsleittechnik sind keine fiktionalen Gefahren mehr, sondern die Realität in unserem Leben und im Unternehmensalltag. Die Steuerungen von industriellen Maschinen und Anlagen sowie SCADA-Systemen (Supervisory Control and Data Acquisition) müssen immer häufiger Angriffen standhalten, wie sie schon in der konventionellen IT bekannt sind. Daher ist die Auseinandersetzung mit diesem Thema von höchster Wichtigkeit. Durch die erhöhte Anzahl an Angriffen werden auch immer mehr Schwachstellen aufgefunden und können ausgenutzt werden. Industrielle Cybersicherheit ist eine absolute Notwendigkeit geworden.

IT-Komponenten aus dem Büroumfeld (Büro-IT) sind immer verbreiteter in der Operational Technology zu finden und werden auch zunehmend vergleichbaren Risiken ausgesetzt. Diese Gefahr steigt zügig an, da diese Entwicklung durch die Industrie 4.0 immer stärker beschleunigt wird.

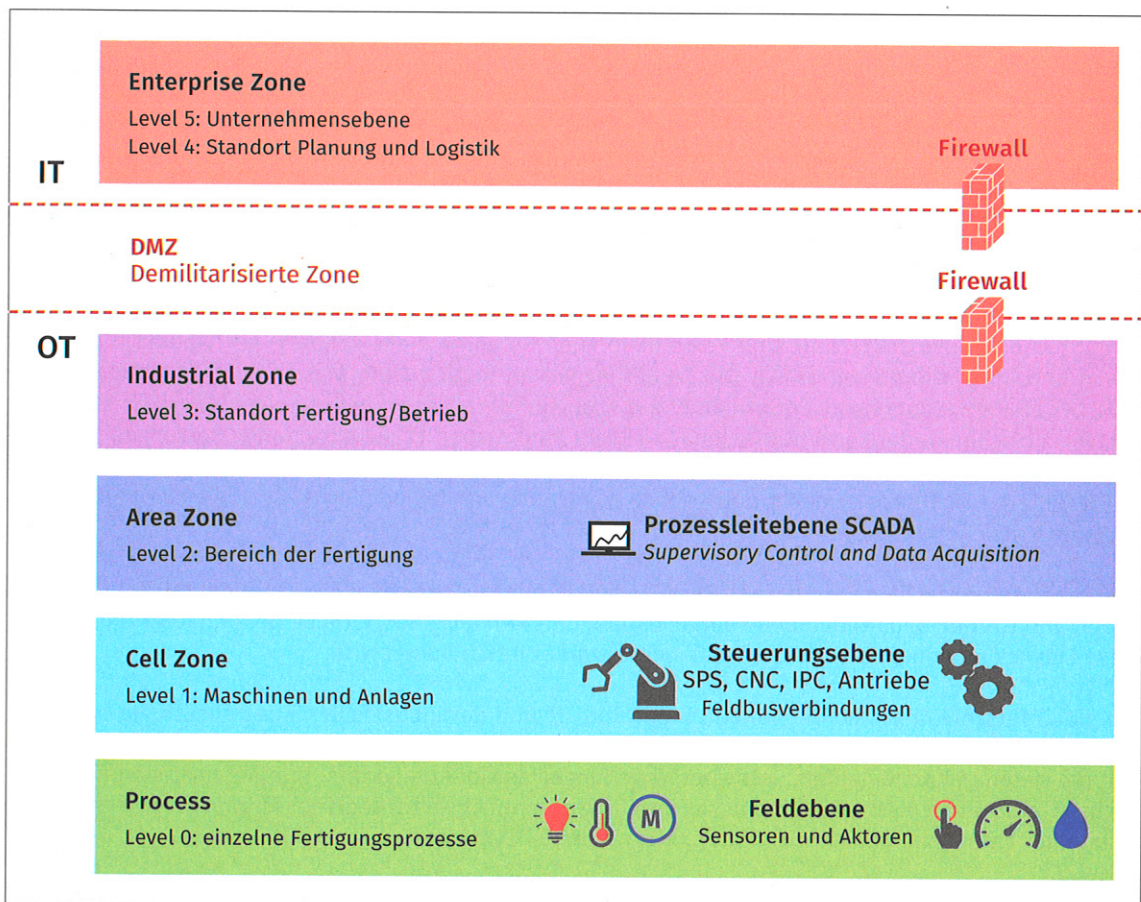
Um die unterschiedlichsten Komponenten der Büro-IT und der industriellen Kontrollsysteme besser zu kategorisieren, wurde schon Anfang der 1990er-Jahre das Purdue-Referenzmodell geschaffen. Das Modell teilt die vielen IT-Komponenten, Softwareanwendungen sowie Produktions- und Automatisierungssysteme in unterschiedliche Ebenen ein. Diese Einteilung entspricht weitgehend der Automatisierungspyramide und der entsprechenden horizontalen Integration der Systeme.

! Purdue-Referenzmodell

Das Purdue-Referenzmodell, das in den 1990er-Jahren in den USA entwickelt wurde, teilt die gesamte IT/OT-Infrastruktur in sechs hierarchische Ebenen ein (siehe Abbildung unten). Es betrachtet hierarchisch das gesamte Netzwerk von der obersten Büroebene (Level 5) bis zum niedrigsten Level 0, in dem sich die einzelnen Komponenten der industriellen Prozesse befinden.

- Level 4 und 5 sind die eigentliche IT-Umgebung in einem Unternehmen. In diesen Ebenen werden die wesentlichen IT-Systeme und -Funktionen betrieben.
- Level 3 ist die oberste Ebene der industriellen Automatisierungs- und Steuerungssysteme. Hier beginnt das OT-Netzwerk. In dieser Ebene ist auch das Manufacturing Execution System (MES) angesiedelt, welches u.a. die detaillierte Produktionsplanung sowie die Materialbedarfsplanung und -bereitstellung durchführt.
- Level-2-Systeme sind typischerweise SCADA-Leitstände oder HMIs (Human Machine Interfaces).
- Level 1 sind die Steuerungen von Maschinen und Anlagen, z.B. speicherprogrammierbare Steuerungen, Industrie-PCs oder Kleinststeuerungen.
- Level 0 beinhaltet die Sensorik und Aktorik von einzelnen Maschinen- und Anlagenelementen.

IT-Organisationen verwalten in der Regel die Unternehmensbereiche in den Levels 4 und 5. Die industriellen Produktionssysteme hingegen werden in den Unternehmen oftmals von der Betriebs- und Automatisierungstechnik installiert und gewartet. Zwischen den IT-Ebenen und den OT-Ebenen sollte eine Sicherheitszone (demilitarisierte Zone, DMZ) liegen (siehe auch Kapitel 2.2.4).



Unterschiedliche Ebenen des Purdue-Referenzmodells mit klarer Trennung zwischen IT und OT

4.1.1 Die Unterscheidungsmerkmale zwischen IT und OT beschreiben

S Sie können die wesentlichen Unterschiede zwischen IT- und OT-Systemen erläutern.

Zur Domäne der OT-Organisation gehören die Werkshalle, die Prozessautomatisierung und die Produktionssysteme. Wie im Schaubild zum Purdue-Referenzmodells ersichtlich wird, fokussiert sich die gesamte OT-Domäne auf die Ebenen 0 bis 3. OT-Teams kümmern sich primär um die Sicherheit und Verfügbarkeit ihrer physischen Maschinen und Anlagen, denn eine Unterbrechung kann zu menschlichen Schäden oder Produktionsausfällen führen. Die folgende Gegenüberstellung zeigt die Unterscheidungsmerkmale auf.

Unterscheidungsmerkmale zwischen IT und OT		
	IT	OT
Installation und Instandhaltung	IT-Fachpersonal	Betriebs- und Automatisierungstechnikpersonal
Einsatzbereich/-ort	Büroarbeitsplätze (teils klimatisiert)	sehr unterschiedlich; von rauen Umgebungen bis hin zum Reinraum
Netzwerk-Topologie	Sterntopologie	sehr maschinen- und anlagen-spezifisch (Ring-, Bus-, Sterntopologien kommen in unterschiedlichen Kombinationen vor)
Verfügbarkeit	Systemausfall im Sekunden- bis Minutenbereich „akzeptabel“	Systemausfall im Millisekunden-Bereich kann bereits sehr kritisch sein
Netzüberwachung	durch ausgebildetes IT-Fachpersonal	Bestandteil der Maschinen- und Anlagenüberwachung durch Schicht- oder Produktionsleitung
Outsourcing von Service und Support	weit verbreitet	eher selten
Patch-Management	sehr häufig/täglich	eher selten
Gerätedichte pro Switch	Managed Switches mit hoher Port-Anzahl	Switches mit wenigen Ports; dezentral in den Maschinen und Anlagen (Schaltschränken) platziert
Lebensdauer/-zyklus	durchschnittlich 3 bis 5 Jahre	sehr häufig 5 bis 15 Jahre (teils länger)

Kompetenzcheck

- 1 Vergleichen Sie das Purdue-Referenzmodell mit der Automatisierungspyramide und erläutern Sie, wie eine DMZ zwischen IT und OT realisiert werden kann.
- 2 Bearbeiten Sie Aufgabe 1 der Lernsituation 1 im Arbeitsbuch.


A1

4.1.2 Die Schutzprioritäten von IT und OT unterscheiden

S Sie können die unterschiedliche Priorisierung der Schutzziele benennen und erklären.

In der IT und OT wird der Ausdruck „Sicherheit“ unterschiedlich definiert. Im Englischen ist diese Unterscheidung eindeutiger, da hier zwischen „Security“ und „Safety“ unterschieden werden kann. In der konventionellen IT-Sicherheit (IT-Security) werden Vertraulichkeit, Integrität und Verfügbarkeit je nach Unternehmensschwerpunkt betrachtet. In der OT hat „Safety“ die oberste Priorität. Unter „Safety“ versteht man die Betriebssicherheit von Maschinen und Anlagen. Sowohl die Betriebssicherheit als auch der

Arbeitsschutz haben als oberstes Ziel, die Menschen und die Umwelt vor physischem Schaden zu schützen. Die IT-Sicherheit zielt darauf, die Daten von Menschen, Unternehmen und der Umwelt zu schützen. Die festgelegte Reihenfolge der Priorität in der OT ist folgendermaßen definiert: Die Betriebssicherheit steht an oberster Stelle, danach folgen Verfügbarkeit, Integrität und Vertraulichkeit.

Unterschiedliche Schutzprioritäten	
IT	OT
Die Priorität auf Personenschutz ist in der IT nicht explizit definiert.	1. Betriebssicherheit – Safety
Je nach Unternehmensschwerpunkt priorisiert:	2. Verfügbarkeit
	3. Integrität
	4. Vertraulichkeit
• Vertraulichkeit • Integrität • Verfügbarkeit	

Weshalb eine Gesamtbetrachtung beider Welten unvermeidbar geworden ist, zeigt sich in zurückliegenden Cyberangriffen.

Kompetenzcheck ✓

- 1 Beschreiben Sie die unterschiedlichen OT-Schutzprioritäten mit ihren eigenen Worten. Nutzen Sie dazu ein geeignetes Beispiel einer industriellen Maschine oder Anlage.
- 2 Bearbeiten Sie Aufgabe 2 der Lernsituation 1 im Arbeitsbuch.

A2

4.1.3 Gründe für die Verwundbarkeit der OT kennen

S Sie kennen die Hintergründe der zunehmenden Verwundbarkeit heutiger OT-Systeme.

Durch die Zusammenführung der Produktions-IT mit der internen IT bzw. Büro-IT sind inzwischen beide Bereiche sehr verwundbar und immer wieder Cyberattacken ausgesetzt. Die Gründe dafür hängen sowohl mit der Historie bestehender Produktionssysteme als auch der rasanten Digitalisierung zusammen. Die folgende Auflistung beschreibt die wesentlichen Veränderungen bei industriellen Kontrollsystemen.



Wandel bei industriellen Kontrollsystemen (Industrial Control Systems, ICS)

Externe Steuerung von Maschinen und Anlagen

Immer mehr Produktionsanlagen werden von außerhalb gesteuert und überwacht, z.B. greifen Techniker und Ingenieure per Fernwartungszugang auf die Anlagen zu.

Produktionsreports

Um Reports aus der Produktion in Echtzeit zu erhalten, ist eine permanente Onlineverbindung von IT-Netzen zur OT notwendig.

IoT wird zu IIoT

Basierend auf dem Internet der Dinge (IoT) entsteht unter dem Stichwort „Industrial Internet of Things“ (IIoT) die intelligente Smart Factory, welche über verschiedenste Endgeräte angesteuert werden kann.

Auf Basis dieser Kenntnisse und der Inhalte aus Kapitel 3.2 (Analyse des Schutzbedarfs in vernetzten Systemen) kann der gesamte Schutzbedarf für ein vernetztes System analysiert werden. Daher sollte auch bei der Fachrichtung Digitale Vernetzung das Kapitel 3.2 bearbeitet werden und die vielen unterschiedlichen Gefährdungen sollten betrachtet werden.

- 1 Erarbeiten Sie in Teams die unterschiedlichen Möglichkeiten zur Fernwartung von Maschinen und Anlagen.
- 2 Bearbeiten Sie Aufgabe 3 der Lernsituation 1 im Arbeitsbuch.

4.2 Absicherung von Industrieanlagen nach IEC 62443 sicherstellen

S Sie kennen die mögliche Absicherung von Industrieanlagen nach IEC 62443.

Die internationale Normenreihe IEC 62443 beschäftigt sich mit der Cybersicherheit von industriellen Kontroll- und Automatisierungssystemen. Das Ziel dieser IEC-Normenreihe ist, Verfahren und Informationen zur Verfügung zu stellen, um einen sicheren Betrieb von automatisierten Produktionsanlagen zu gewährleisten. Dabei wird sowohl Hard- als auch Software betrachtet. Die Normenreihe soll eine Hilfestellung und ein Leitfaden für die Entwicklung, die Implementierung und das Management von industriellen Maschinen und Anlagen in Bezug auf Cybersicherheit sein.

! IEC 62443

Die internationale Normenreihe IEC (Internationale Elektrotechnische Kommission) beinhaltet Grundkonzepte für die Cybersicherheit und grundlegende Sicherheitsanforderungen an die IT-Sicherheit von industriellen Kontroll- und Automatisierungssystemen sowie Leitfäden und Empfehlungen für die Umsetzung von IT-Security Maßnahmen.

4.2.1 Die notwendige Bestandsaufnahme von bestehenden Maschinen und Anlagen begründen können

S Sie können erklären, warum bei bestehenden Maschinen und Anlagen eine gründliche Bestandsaufnahme in Bezug auf Cyber-Sicherheitsstandards erfolgen muss.

Im Folgenden werden die wesentlichen Schwachstellen von bestehenden Maschinen und Anlagen in Bezug auf deren Gefährdungspotenzial aufgelistet:

- **Langlebige Produktionsanlagen und veraltete Systeme:** Klassische Produktionsanlagen haben nicht oftmals Laufzeiten von bis zu 15 Jahren (teils noch länger) und werden nicht – wie beispielsweise ein Smartphone – nach wenigen Jahren ausgetauscht. Häufig sind deren Betriebssysteme veraltet und Sicherheitsupdates (Patches) sowie der Support werden von den Herstellern nicht mehr angeboten.
- **Problematisches Patchen:** In einem Industrieumfeld zu patchen ist ein problematisches Unterfangen. Da Systeme dazu heruntergefahren werden müssen, ist die Produktionsanlage in dieser Zeit nicht verfügbar. Allerdings sind veraltete Systeme attraktive Ziele für Zero-Day-Attacken. Angriffe durch nicht geschlossene Sicherheitslücken in der Software verschaffen den Angreifern ebenfalls einen leichten Zugriff auf das System.
- **Mangelhafte IT-Sicherheitslösungen:** Der Grund für die fehlenden IT-Sicherheitsmaßnahmen von alten Produktionsanlagen liegt an dem Zeitpunkt der Herstellung der Anlage. In der Vergangenheit waren Cyberangriffe sehr selten bis unmöglich, daher wurden die Anlagen standardmäßig nicht mit Sicherheitslösungen ausgestattet. Ein Installieren von Antiviren-Scannern auf industriellen Kontrollsystemen ist im Nachhinein schwierig, denn in vielen Fällen führt dies zum Verlust von (Hersteller-)

Zertifikaten und -Garantien. Zusätzlich ist auch der Echtzeitscanner deaktiviert. Ein zeitnahes Installieren von Updates in den Scannern ist nicht immer möglich.

- **Unzureichendes Know-how in Bezug auf IT-Security:** Produktionsmitarbeiter, die für den Betrieb der Anlagen verantwortlich sind, wissen zu wenig über mögliche Angriffsmöglichkeiten und IT-Risiken. Insgesamt gibt es zu wenige IT-Fachkräfte mit Produktions- und Security-Know-how. Hierdurch wird indirekt auch das oberste Ziel der Betriebssicherheit gefährdet.

Kompetenzcheck ✓

- 1 Erstellen Sie eine Checkliste mit den Punkten, die Sie an einer Bestandsanlage prüfen würden. Diese Aufgabe kann auch im Tandem oder in einem Dreier-Team bearbeitet werden. Stellen Sie Ihre Vorgehensweise im Plenum vor.
- 2 Bearbeiten Sie Aufgabe 1 der Lernsituation 2 im Arbeitsbuch.

A1

4.2.2 Die häufigsten Gefahrenquellen für Maschinen und Anlagen erkennen

S Sie kennen die drei wichtigsten Bedrohungsarten bei Industrieanlagen.

Um den IT-Sicherheitsstatus von Maschinen und Anlagen gewährleisten zu können, ist es auch wichtig, die Mitarbeiter für die eigentlichen Bedrohungsarten zu sensibilisieren. Ein sehr großer Risikofaktor ist nämlich der Mensch selbst. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) publiziert jedes Jahr die zehn häufigsten Bedrohungen für industrielle Maschinen und Anlagen. Die folgende Tabelle zeigt die ersten drei Plätze.



Die häufigsten Bedrohungsarten nach Rangfolge	
Rang 1	Schadsoftware wird über Wechseldatenträger und externe Hardware in die Firmensysteme, Maschinen und Anlagen eingeschleust
Rang 2	Schadsoftware infiziert die Maschinen und Anlagen über eine direkte Vernetzung mit dem Internet (offene/ungeschützte Webserver)
Rang 3	Menschliches Fehlverhalten und gezielte Sabotage

Speziell bei Maschinen und Anlagen steht die Betriebs- und Arbeitssicherheit an erster Stelle. Eine Cyber-attacke kann als Ziel die Zerstörung einer Anlage oder die Gefährdung von Menschen haben. Selbst scheinbar unbedeutende Aktionen wie das Aufladen eines Smartphones an einem freien USB-Port eines Industrie-PCs kann verheerende Auswirkungen haben, wie das folgende Angriffsszenario zeigt.

Beispiel:

Mögliches Angriffsszenario auf eine Maschine oder Anlage

1. Eine ältere Bestandsanlage wird noch komplett unter Windows XP betrieben. Dabei handelt es sich um eine „Insellösung“, d.h. es besteht tatsächlich keine Verbindung zum Netzwerk.



2. Um dennoch Updates einzuspielen, besitzt die Anlage einen USB-Port.
3. Diese USB-Schnittstelle wird von Mitarbeitern zum Aufladen ihrer Mobiltelefone genutzt.
4. Die im Mitarbeiter-Handy eingesetzte SD-Card ist mit einer Malware befallen.
5. Die Malware gelangt nun beim Aufladen des Telefons in die Steuerung der Anlage und löst Fehlfunktionen aus.

Mögliche Folgen:

Die Fehlfunktionen können durch unkontrollierte Bewegungen der Maschine Menschen gefährden!

Die Fehlfunktionen können Werkstücke, Werkzeuge und auch die gesamte Maschine beschädigen und sogar zerstören!

Kompetenzcheck ✓

- 1 Erstellen Sie im Tandem eine Mindmap mit potenziellem menschlichem Fehlverhalten an industriellen Maschinen und Anlagen.
- 2 Bearbeiten Sie Aufgabe 2 der Lernsituation 2 im Arbeitsbuch.

A2

4.2.3 Schutzmaßnahmen für Maschinen und Anlagen beschreiben

S Sie können die grundlegenden Schutzmaßnahmen für industrielle Anlagen erläutern.

Zahlreiche Maßnahmen zur Erhöhung der Sicherheit in vernetzten Systemen wurden in Kapitel 3.3 thematisiert. So ist zum Beispiel der Einsatz der VLAN-Technik zur Einrichtung einer Sicherheitszone ein wichtiges Element möglicher Maßnahmen. Das BSI empfiehlt für industrielle Maschinen und Anlagen neben den in Kapitel 3.3 vorgestellten Maßnahmen vier wirksame Vorkehrungen, um Systeme gegen Cyberattacken zu schützen.

BSI-Empfehlungen

1. Restriktive Nutzung von Wechselmedien und mobilen Geräten

Um sich vor den Gefahren, die von Wechseldatenträgern und mobilen Endgeräten ausgehen, zu schützen, empfiehlt das BSI, diese vollständig zu verschlüsseln und zusätzlich allgemeingültige Regeln für deren Verwendung aufzustellen und bekanntzugeben. In einer industriellen Produktionsumgebung sollte die Nutzung weitestgehend eingeschränkt werden.

2. Schutz vor Schadprogrammen

Alle bedrohten IT-Systeme sowie die potenziellen Angriffswege, z. B. Außenschnittstellen oder Wechselmedien, müssen betrachtet werden. Außerdem muss ein Konzept zum Schutz vor Schadprogrammen sowie dessen Umsetzung erstellt werden.

3. Sensibilisierung und Mitarbeiterschulung

Das Betriebspersonal muss regelmäßig zu relevanten Sicherheitsbedrohungen im OT-Bereich informiert und sensibilisiert werden.

4. Überwachung, Protokollierung und Erkennung von Ereignissen auf den Endpunkten und Systemen

Betriebs- und sicherheitsrelevante Ereignisse müssen zeitnah identifiziert werden.

Kompetenzcheck ✓

- 1 Sie sollen den neuen Auszubildenden im ersten Ausbildungsjahr eine Einführung zu Sicherheitsbedrohungen im OT-Bereich geben. Erstellen Sie zwei Folien mit den wesentlichen Inhalten und praxisorientierten Beispielen.
- 2 Bearbeiten Sie Aufgabe 3 der Lernsituation 2 im Arbeitsbuch.

A3

4.3 Systemstatus eines CPPS überwachen

S Sie können den Systemstatus eines cyber-physischen Produktionssystems monitoren.

Nachdem die Gründe für die Verwundbarkeit von OT-Systemen bekannt sind und Schutzmaßnahmen für Maschinen und Anlagen beschrieben werden können, ist es außerdem notwendig, die Überwachung cyber-physischer Produktionssysteme (CPPS) in Echtzeit in den Fokus zu nehmen. Dabei ist zu beachten, dass Cyberkriminelle unterschiedliche Beweggründe für einen Angriff haben.

4.3.1 Die Motivation von Cyberkriminellen zum Angriff auf OT kennen

S Sie können die Motive von Cyberkriminellen beschreiben.

Der Industriesektor ist im Hinblick auf Cyberattacken besonders gefährdet, weil hier ein hoher Anspruch auf die Verfügbarkeit der Systeme sowie auf Betriebs- und Arbeitssicherheit (Safety) besteht. Manipulierte Anlagen, Maschinen, Roboter oder Transportsysteme können ein hohes Risiko für Menschen darstellen. Dazu kommt, dass in einem industriellen Produktionsprozess Ausfallzeiten sehr kritisch sind. Sollte eine Anlage wegen eines Angriffs stillstehen, führt dies sehr schnell zu hohen Kosten. Diese Voraussetzungen werden von Cyberkriminellen als Druckmittel verwendet, um ihre Ziele zu erreichen. Einige bekannte Beispiele aus der Vergangenheit sind nachfolgend aufgeführt.



Historische Cyberattacken

Cyberangriff auf Norsk Hydro

Der Cyberangriff auf den norwegischen Aluminiumhersteller Norsk Hydro legte wichtige IT-Systeme lahm. Die Erpressungssoftware/Ransomware befahl über das Office-Netz auch Produktionssysteme und behinderte die Fertigung. In der Folge sank die Aktie des Konzerns, der Preis für Metall stieg hingegen. Die IT-Katastrophe wurde von Norsk Hydro sehr offen kommuniziert.

TRISIS

Bei einem Vorfall in einer Chemieanlage in Saudi-Arabien wurde eine Schadsoftware entdeckt, die gezielt die Safety-Systeme befallen hatte. Diese war darauf ausgelegt, deren Funktion außer Kraft zu setzen. Die als TRISIS (2017) bezeichnete Schadsoftware zeichnete sich durch eine sehr hohe Spezialisierung auf das verwendete Safety-System einer Anlage aus. Nur durch einen Zufall wurde der Angriff entdeckt und es kam zu keinen weiteren Auswirkungen für Menschen oder die Umwelt.

Stuxnet

Der Computerwurm Stuxnet – ursprünglich gegen das iranische Atomprogramm eingesetzt – befiel Kontrollsysteme für Industrieanlagen und schädigte im Zuge seiner Verbreitung auch andere Industrieunternehmen.

Industroyer

Der Trojaner Industroyer legte das ukrainische Stromnetz lahm. Der Schadcode beherrscht mehrere Kommunikationsprotokolle, die von SCADA-Systemen (Supervisory Control And Data Acquisition) verwendet werden.

Kompetenzcheck ✓

- 1 Recherchieren Sie aktuelle Cyberattacken und diskutieren Sie im Plenum die Angriffsart, die Motivation der Täter, die Auswirkungen auf das Unternehmen und die möglichen Schutzvorkehrungen für einen vergleichbaren Angriff in Ihrem Unternehmen.
- 2 Bearbeiten Sie Aufgabe 1 der Lernsituation 3 im Arbeitsbuch.

A1

4.3.2 Ein Überwachungskonzept für Maschinen und Anlagen entwickeln

- S** Sie können ein Grundkonzept zur Überwachung von cyber-physischen Produktionssystemen erstellen.

Unterschiedliche Überwachungssysteme zur Erkennung von Eindringlingen und Angriffen (Intrusion Detection System, Intrusion Prevention System) wurden in Kapitel 3.5.2 bearbeitet. Auch für industrielle Maschinen und Anlagen baut das grundsätzliche Überwachungskonzept auf diesen Säulen auf. Ergänzt wird es durch ein strukturiertes und stringentes User- und Identitätsmanagement (siehe auch Kapitel 3.3.5 und 3.3.6).



Zusätzlich müssen für ein Überwachungskonzept von industriellen Anlagen folgende Punkte berücksichtigt werden.

Überwachungskonzept	
Maschinen- und Anlagensicherheit	Dies beginnt bereits mit dem klassischen Gebäudezutritt und wird bei einzelnen Maschinen und Anlagen fortgeführt. So können nur autorisierte Maschinen- und Anlagenführer sowie Servicetechniker an diesen Systemen arbeiten (User- und Identitätsmanagement).
Netzwerksicherheit	Schutz gegen unbefugten Zugriff auf Automatisierungssysteme, z. B. durch Schutzzonen (Firewalls), Netzwerksegmentierung (VLANs) und verschlüsselte Kommunikation.
Systemintegrität	Alle Funktionen einer Maschine oder Anlage müssen ein definiertes Verhalten besitzen. Sind unterschiedliche Funktionen optional, darf keine Option eine nicht spezifizierte Funktionsänderung herbeiführen.

Wird eine Maschine gewartet oder es besteht eine Störung, muss in die kontinuierliche Überwachung eingegriffen werden. Dazu wird mit dem folgenden Anwendungsfall ein möglicher Ablauf aufgezeigt.

Wartung bzw. Notfallzugriff bei einem industriellen Produktionssystem

Wartungsarbeiten an Software oder Netzwerkkomponenten müssen in einem sehr kurzen Zeitfenster durchgeführt werden können, um Ausfallzeiten von Maschinen und Anlagen zu reduzieren. Daher müssen solche Servicearbeiten ohne große Vorlaufzeiten möglich sein. Des Weiteren ist es notwendig, dass sicherheitsrelevante Veränderungen in den unterschiedlichen Steuerungen protokolliert und dokumentiert werden. Im Fall von bestehenden Block- oder Allowlists müssen die Änderungen ebenfalls eingepflegt werden.

Möglicher Ablauf bei der Software-Wartung einer Maschine oder Anlage

1. Eine Wartung der Software ist notwendig.

Dies kann durch eine Störung oder durch eine geplante Instandhaltungsmaßnahme ausgelöst werden.

2. Das industrielle Steuerungssystem (z.B. eine SPS oder ein Industrie-PC) wird entsperrt.

Die eigentliche Überwachung ist nun temporär nicht verfügbar oder eingeschränkt. Es kann „lokal“ oder „remote“ auf die Steuerung zugegriffen werden. In dieser Phase ist das System nicht komplett sicher und es sollten daher alle Aktivitäten systematisch protokolliert werden.

3. Die eigentliche Wartung wird durchgeführt.

Notwendige externe Datenträger werden temporär freigegeben. Die Applikation wird im Wartungsmodus aktualisiert und getestet.

4. Die Wartung wird beendet und die industrielle Steuerung wird wieder komplett abgesichert.

Die aktualisierte Systemsoftware ist im Sicherheitsprofil hinterlegt und kann nun ordnungsgemäß ausgeführt werden. Die eigentliche Überwachung ist wieder aktiv.

Kompetenzcheck ✓

- 1 Benennen Sie für jedes Überwachungskonzept jeweils eine weitere Maßnahme.
- 2 Bearbeiten Sie Aufgabe 2 der Lernsituation 3 im Arbeitsbuch.