Whitepaper

Industrial Security

Warum eine ganzheitliche Security über die Office-Netzwerke hinausgeht

Erfahren Sie mehr über:

- die Bedeutung von Cyber Security für ein Unternehmen
- die Umsetzung von ganzheitlicher Security in der Automatisierung
- zentrale Handlungsfelder und erste Lösungsempfehlungen

PHOENIX CONTACT

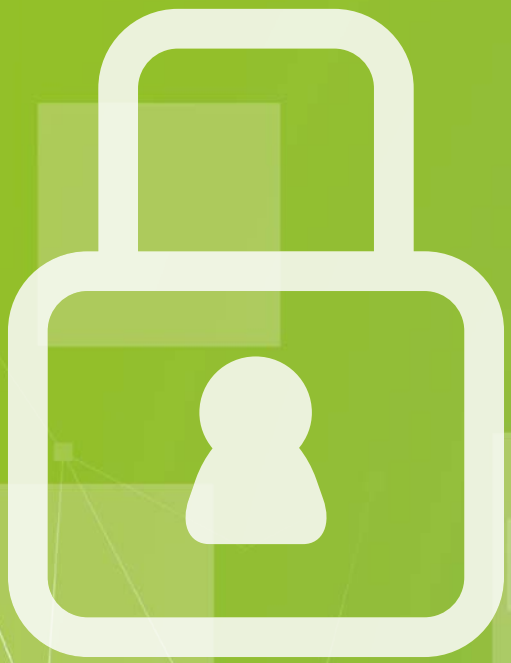
Einleitung

Die Wichtigkeit von Cyber Security in allen Bereichen eines Unternehmens ist in den letzten Jahren massiv gestiegen. Dabei kommen zwei Trends zusammen. Zum einen wird mit der zunehmenden Digitalisierung und Vernetzung die Angriffsfläche größer, zum anderen werden Angreifer und Angriffsmethoden professioneller. Entsprechend müssen Maßnahmen zum Schutz eines Unternehmens vor Cyber-Angriffen getroffen werden.

Dieses Papier beschreibt zuerst den Schutz der Wertschöpfung als Sicherheitsziel in Abschnitt 2 und die Besonderheiten der ICS-Umgebung in Abschnitt 3. Die wesentlichen Handlungsfelder werden mit ersten Lösungsempfehlungen in Abschnitt 4 aufgelistet.

Inhalt

1 Wertschöpfung als Sicherheitsziel



Die Wertschöpfung steht im Zentrum jedes Unternehmens. Ziel der Cyber Security ist es, die Wertschöpfung eines Unternehmens zu schützen. Daraus ergeben sich die individuellen Sicherheitsziele wie z. B. der Schutz von Know-how – etwa Entwicklungsergebnissen oder Vertragskonditionen – und die Einhaltung gesetzlicher Vorschriften, z. B. des Datenschutzes. In fertigenden Unternehmen ist die Produktions- und Lieferfähigkeit von offensichtlicher Wichtigkeit. Für kritische Infrastrukturen sind gesetzliche Vorgaben etabliert.

Besonderheiten von IT und ICS

Beim Vergleich der Bereiche IT und industrieller Automatisierungswelt (Industrial Control Systems, ICS) wird gern mit den unterschiedlichen Anforderungen beider Bereiche argumentiert (siehe Abbildung 1). In der Automatisierung steht der physische Prozess im Mittelpunkt: Es muss gebohrt, gestanzt oder gemessen werden. Die Anlagen werden betrieben, solange sie eine wirtschaftliche Herstellung ermöglichen.

ICS-Security	IT-Security
Prioritäten	
Verfügbarkeit Integrität Vertraulichkeit	**Vertraulichkeit** Integrität Verfügbarkeit
Eigenschaften	
Verfügbarkeit	
100 %	99 % ausreichend
Neustart	
Schwierig	Möglich
Patch-Management	
Große Herausforderung	Automatisiert möglich
Lebenszeit Hardware	
7 - 20 Jahre	3 - 5 Jahre

Abb. 1: Vergleich Security in IT- und ICS-Umgebungen

Die Lebensdauer ist dabei viel höher als in einer IT-Umgebung. Die weitergehenden Herausforderungen in der Automatisierung sind hinreichend erkennbar: Jede Störung führt zu verminderter Produktivität. Außerdem sind die Möglichkeiten zur Beseitigung von Schwachstellen eingeschränkt, da Neustarts nur bedingt realisierbar sind und jede Änderung an einem Automatisierungssystem das Risiko weiterer Fehlfunktionen nach sich zieht.

Die Auswahl und Umsetzung von Security-Maßnahmen unterscheiden sich in IT- und ICS-Umgebung. Für die Wertschöpfung werden aber sämtliche Elemente benötigt. Ob die Produktion wegen eines Cyber-Security-Vorfalls im Fertigungsprozess oder wegen des Ausfalls eines zentralen Dienstes – wie des ERP-Systems – stillsteht, ist im wirtschaftlichen Ergebnis nicht relevant.

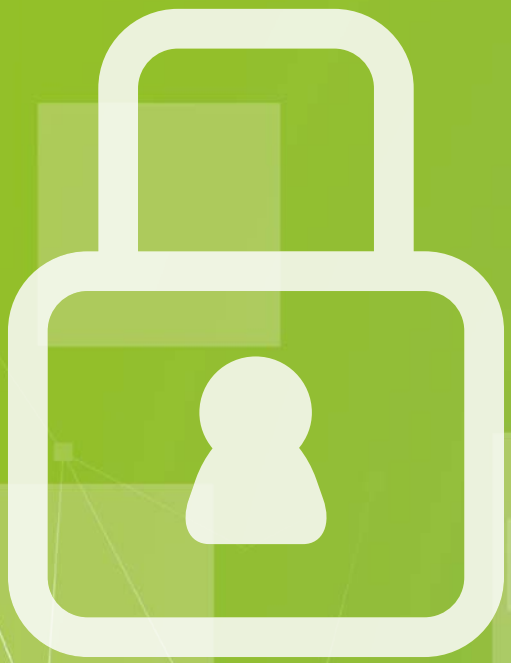
Gemeinsames Vorgehen/ Angepasste Maßnahmen

Entsprechend ist Cyber Security kein Thema, das mit isolierten Einzelkonzepten adressiert werden kann. Lediglich durch ein abgestimmtes gemeinsames Vorgehen lässt sich ein wirksamer und effizienter Ansatz erarbeiten.

Dies ist insbesondere deshalb wichtig, weil Security-Know-how in der IT-Umgebung vorhanden ist, in der Produktion jedoch häufig fehlt. Auf der anderen Seite müssen die speziellen Eigenheiten in der Produktion aber ebenso berücksichtigt werden.

Basis sollte ein Informationssicherheitsmanagementsystem sein, etwa nach ISO 27001 (1) oder IT-Grundschutz (2) vom Bundesamt für Sicherheit in der Informationstechnik, das zumeist ausgehend von der IT- in Richtung der ICS-Umgebung erweitert wird.

2 Umsetzung in der Automatisierung



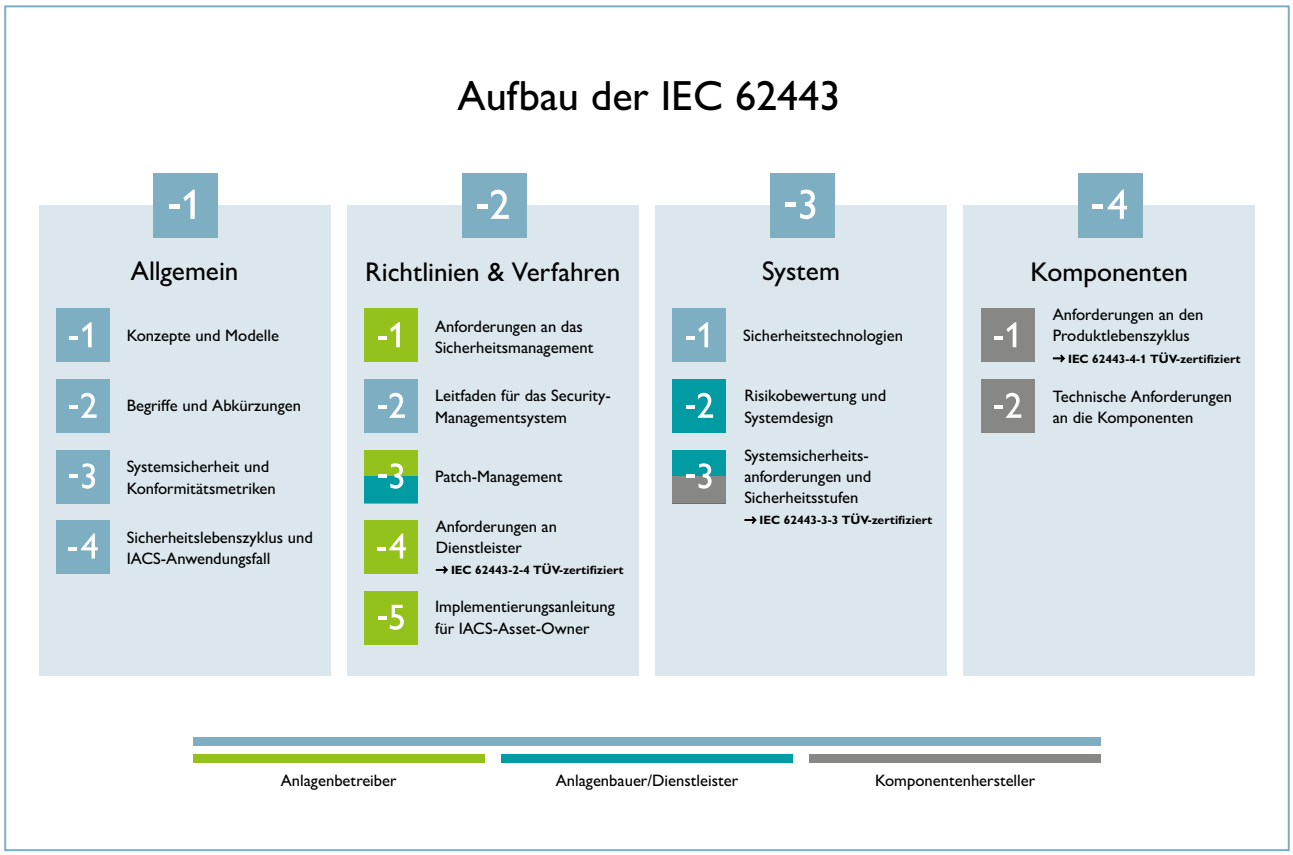
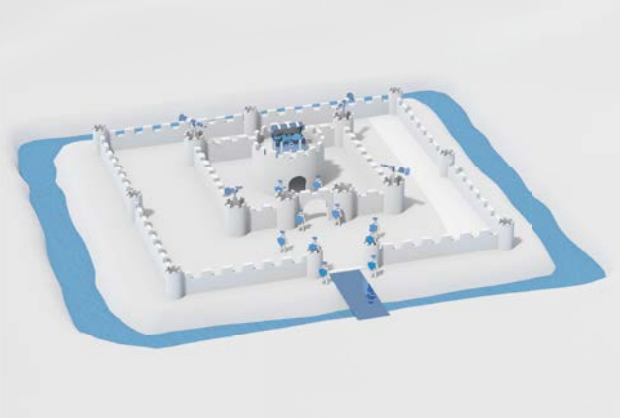


Abb. 2: Übersicht IEC 62443

Um die genannten Besonderheiten der ICS-Umgebung zu adressieren, wurde der Securitystandard IEC 62443 (3) erarbeitet. Er beschreibt und präzisiert das automatisierungsspezifische Vorgehen. Die in Abschnitt 4 aufgeführten Handlungsfelder orientieren sich an den in der IEC 62443 betrachteten Themen. Als besonderes Element der IEC 62443 ist der ganzheitliche Ansatz zu erwähnen, der von Anforderungen an die Betriebsprozesse über Anforderungen an die Systeme bis hin zu den Produkten reicht und sowohl prozessuale als auch technische Maßnahmen und Anforderungen darlegt. Im Folgenden werden die beiden wesentlichen Prinzipien, die der IEC 62443 zugrunde liegen, erklärt.

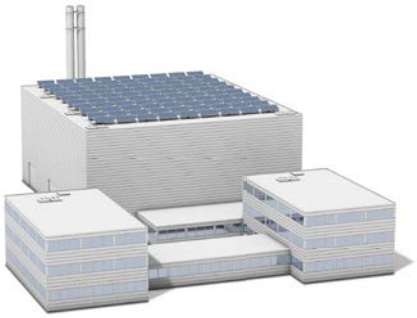
Defense in Depth

Ein entscheidendes Security-Konzept, das ebenfalls in der IEC 62443 verwendet wird, ist „Defense in Depth“, siehe Abbildung 3. Durch die Staffelung mehrerer Sicherheitsmechanismen hintereinander wird es dem Angreifer schwerer gemacht. So muss z. B. bei einem Angriff über das Netzwerk erst eine oder mehrere Firewalls überwunden werden, bevor der Angreifer an die Zielkomponente herankommt. Dort muss er eine Benutzeranmeldung bezwingen, um dann noch durch interne Sicherheitsmechanismen aufgehalten zu werden, siehe Abbildung 4. Wenn also ein Schutzmechanismus versagt, bricht nicht gleich das Sicherheitsmodell wie ein Kartenhaus zusammen.



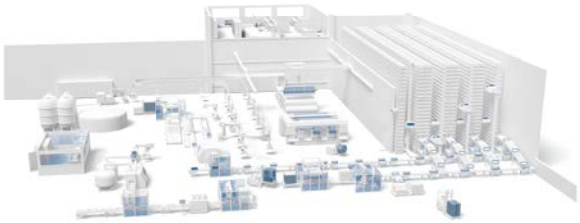
Das „Defense in Depth“-Konzept wird folglich durch das Zusammenwirken der verschiedenen Sicherheitsmechanismen realisiert. Es ist daher auch wichtig, alle Sicherheitsmechanismen im System zu betrachten.

Abb. 3: Konzept des Defense in Depth



Unternehmensebene

- Physische Maßnahmen
- Berechtigungskonzept (Zutritt, Zugang, Zugriff)
- Awareness-Schulungen
- ISMS-Prozesse



Netzwerkebene

- Netzsegmentierung (Zonen, Conduits)
- VPN
- Verschlüsselung
- Firewalls
- Angriffserkennung

Produktebene

- Security Features
- Systemhärtung
- „Security by Design“-Komponenten

Abb. 4: Defense in Depth umgesetzt

Betrachtung im System

Ein Spannungsfeld in der Bedrohungs- und Risikoanalyse ist das Zusammenspiel von Einzelaspekten im System. Für die Gestaltung eines sicheren Systems werden ebenfalls sichere Komponenten benötigt. Das erzielbare Security-Niveau hängt allerdings nur sehr indirekt von den Security-Eigenschaften der Komponenten ab. So lassen sich z. B. unsichere Komponenten ebenso in einem sicheren System betreiben, wenn diese durch vorgeschaltete Maßnahmen – wie eine Firewall – isoliert sind und lediglich von technischen oder organischen Maßnahmen gesichtet werden.

Umgekehrt ist es möglich, Komponenten mit hohem Security-Niveau unpassend einzusetzen und zu konfigurieren und anschließend ein unsicheres Gesamtsystem zu erhalten.

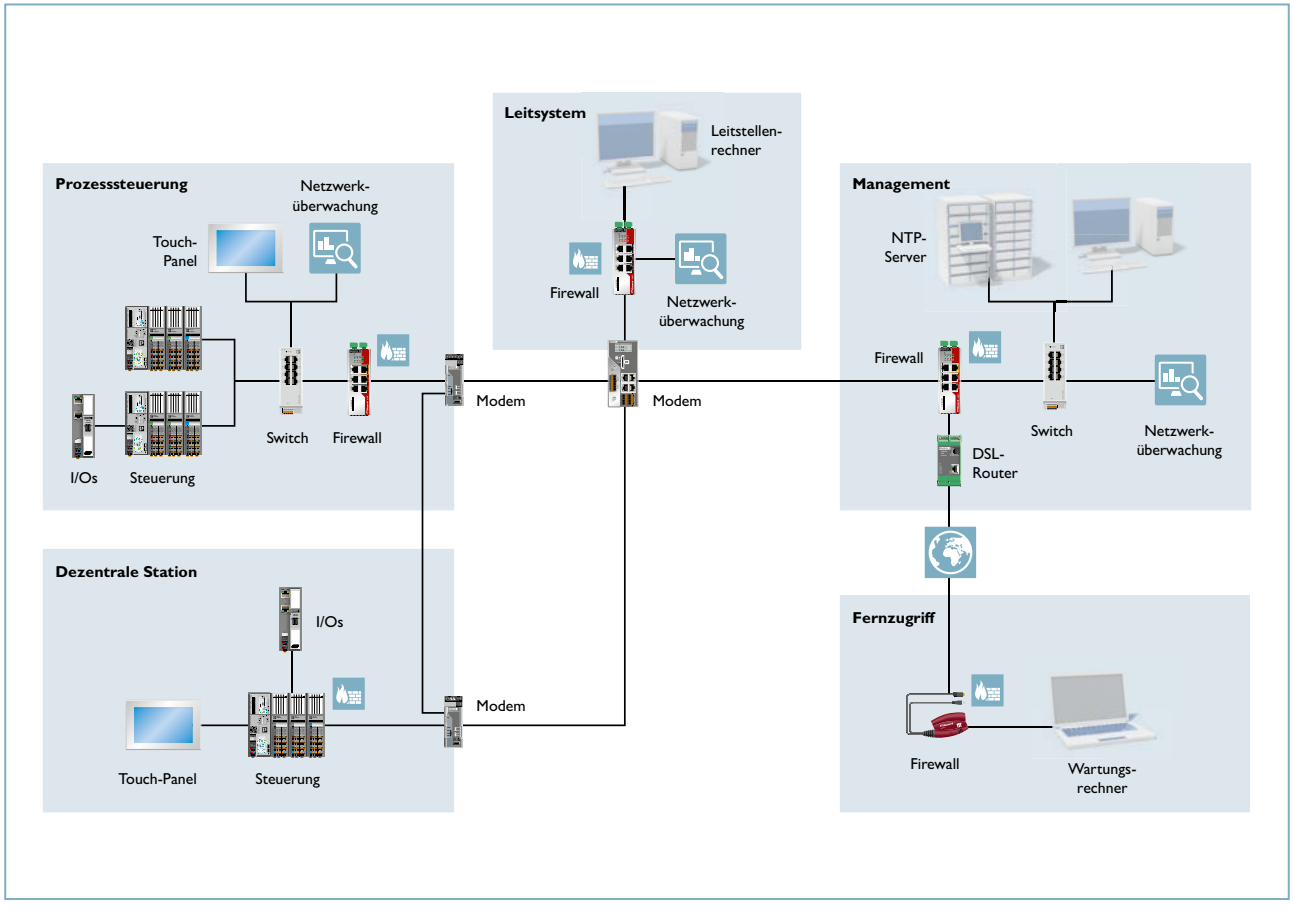
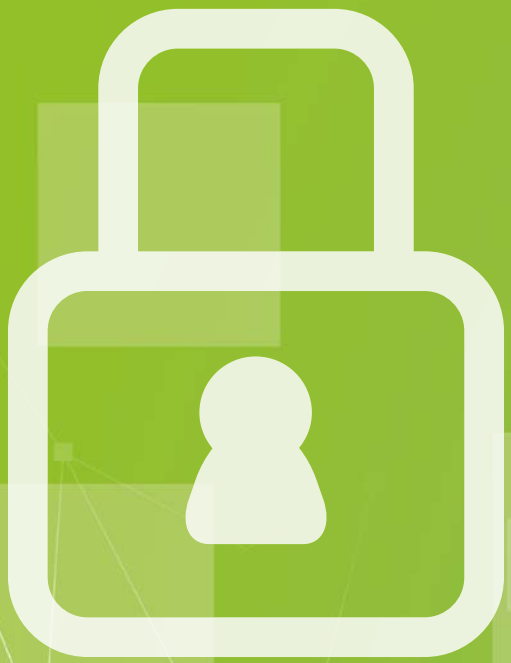


Abb. 5: Security in der Systembetrachtung

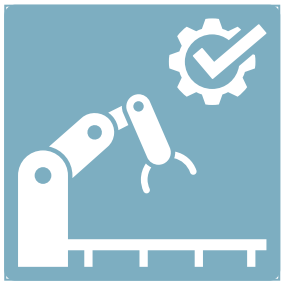
3 Handlungsfelder



Selbst, wenn sich beim Schutz des Automatisierungssystems immer individuelle Anforderungen und Maßnahmen für jeden Anwendungsfall ergeben werden, existieren zentrale Handlungsfelder, die für einen Großteil der Anwendenden vergleichbar sind. Diese werden im Folgenden beschrieben.

Datenverlust

Datenverlust kann durch unterschiedliche Ereignisse hervorgerufen werden. Neben mit Sachschäden verbundenen Naturkatastrophen können Systeme oder Datenträger defekt werden. Daten können auch versehentlich oder absichtlich gelöscht bzw. im Fall von Ransomware verschlüsselt werden.
Hier helfen, je nach Bedrohung, verschiedene Gegenmaßnahmen, die idealerweise kombiniert eingesetzt werden. Einfaches Hardware-Versagen lässt sich durch Redundanz (also das Speichern an mehreren Orten) abfangen. Eine geeignete Zugriffssteuerung, die enger eingrenzt wer Schreibzugriff benötigt, beschränkt Schäden durch Löschen oder Verschlüsselung. Backup-Datenspeicher sollten nicht dauerhaft an aktiven Systemen angeschlossen sein, der Datenspeicher im Schrank ist immun gegen Ransomware. Regelmäßiges Auslagern von Backups, z. B. in einen Banktresor, hilft gegen Großschäden in den eigenen Systemen. Und niemals zu vergessen, die Backups auf Wiedereinspielbarkeit prüfen.



Störungen aus fremden Systemen

Störungen im Produktionsnetzwerk können ebenfalls durch Zugriffe aus anderen Bereichen entstehen. Dies können sowohl weitere Einheiten des Unternehmens ebenso wie andere Fertigungsbereiche sein. Ursachen liegen z. B. in fehlerhaften Netzwerkeinstellungen oder auch versehentlichen oder nicht abgesprochenen Zugriffen.
Grundsätzlich empfiehlt es sich, Netzwerke nach Anwendungsbereichen zu segmentieren und nur die Verbindungen zu erlauben, die tatsächlich notwendig sind. So brauchen die meisten Bürobereiche keinen Zugriff auf die Produktion. Fertigungsbereiche oder Maschinen kommunizieren ebenfalls in den wenigsten Fällen direkt miteinander, sondern mit Leitsystemen und zentralen IT-Diensten, wie ERP-Systemen oder dem Benutzermanagement. Für die Segmentierung sollten IP-Netzwerke angelegt werden, die durch Firewalls, Router und Layer-3-Switches verbunden sind.

Schad-Software

Ein wichtiges Element ist der Schutz vor Schad-Software wie Viren und Trojanern. In der Automatisierungstechnik werden viele Windows-Systeme verwendet, auf denen Viren-Scanner die Automatisierungsfunktion stören könnten oder bei denen Updates von Viren-Pattern nicht oder lediglich schwer möglich sind. Insofern müssen andere Schutzkonzepte genutzt werden, die sich ebenso an den potenziellen Infektionswegen orientieren.

USB-Sticks/Notebooks

Zahlreiche Infektionen erfolgen über mobile Datenträger, wobei insbesondere USB-Sticks ein hohes Risiko aufweisen, da sie keinen Hardware-Schreibschutz bieten. Ein USB-Stick kann vom Anwendenden unbemerkt infiziert werden. Wenn nicht unbedingt erforderlich, sollte auf die Anwendung von USB-Sticks verzichtet und USB-Ports gesperrt werden. Werden USB-Sticks eingesetzt, sollten für jede Anwendung dedizierte Sticks verwendet werden, die für keinen weiteren Zweck genutzt werden. Der private Einsatz sollte grundsätzlich untersagt sein. Weiterhin besteht die Möglichkeit, USB-Sticks mit aktueller Viren-Software zu scannen. Extern eingebrachte USB-Sticks, etwa von Servicepersonal, sollten auf jeden Fall gescannt und durch das Servicepersonal nur bei expliziter Erlaubnis eingesteckt werden.
Ähnliches gilt auch für von Externen mitgebrachte Notebooks, die lediglich nach Viren-Scan und expliziter Freigabe an ein System oder das Unternehmensnetzwerk angeschlossen werden sollten.

Netzwerk

Sind Systeme in einem Netzwerk mit Schad-Software infiziert, ergibt sich das Risiko der Weiterverbreitung, z. B. durch Übertragung auf Netzlaufwerke oder aktive Verbreitung von einem System zum nächsten. Bei Webzugriffen könnte Schad-Software unbemerkt und ungewollt eingeschleppt werden.
In diesem Fall unterstützt die Netzwerksegmentierung gleichermaßen: Fertigungssysteme kommunizieren normalerweise nicht direkt miteinander. Mit einer Firewall kann der Datenaustausch auf notwendige Verbindungen beschränkt werden. Nicht erforderliche Dienste sollten deaktiviert sein.
Die wenigsten Automatisierungssysteme brauchen Zugriff auf das Internet. Dort, wo er benötigt wird, sollte nur die notwendige Verbindung möglich sein. Sofern für Mitarbeitende in der Produktion ein Web-Zugang erforderlich ist, kann dies über normale Arbeitsplatzrechner erfolgen, die dem Office-Segment zugeordnet werden.

Fernzugriffe

Fernwartung ist ein wichtiges Konzept zur Steigerung der Produktivität. Allerdings gehen von Fernzugriffen Risiken wie die Infektion mit Schad-Software aus. Es könnte ebenso technisch machbar sein, über das System im Fernzugriff Zugang zu anderen Ressourcen zu erhalten. Schließlich ist zu bedenken, dass der Bediener nicht vor Ort und insofern nicht im Bild über die Umgebungssituation ist. Er könnte z. B. durch den Eingriff aus der Ferne einen Unfall auslösen, weil er keinen Blickkontakt mit den Mitarbeitenden vor Ort hat.

Fernzugriffe sollten entsprechend nur „On Demand“ möglich sein. Häufig wird durch einen Schlüsselschalter in einen „Wartungsmodus“ geschaltet, in der eine Anlage lediglich unter besonderer Beachtung etwa der Betriebssicherheit operiert. Durch eine geeignete Firewall sollten für diesen Fall spezielle Regeln aktiviert werden, die den Rückgriff ins Produktionsnetzwerk blockieren. Auch hier sollte der Zugriff auf die notwendigen Schnittstellen begrenzt werden. Wird z. B. nur der Zugriff auf die Übertragung des Desktops beschränkt, reduziert sich das Risiko einer Infektion mit Schad-Software erheblich. Der Aufbau von (verschlüsselten) VPN-Verbindungen direkt zum Fernwartenden ist besonders kritisch zu betrachten, da keine Kontrolle über die Aktionen besteht.

Benutzermanagement

Bei Verwendung von Sammelaccounts mit bekannten Passwörtern werden Systeme angreifbar. Aktionen lassen sich nicht nachvollziehen.

Durch die Nutzung individueller Benutzer-Accounts und ihnen zugeteilten Rechten lassen sich die Risiken verringern. So brauchen die Bedienenden vielleicht kein Recht, Dateien zu schreiben und dies kann den Administrierenden überlassen werden. Vielleicht kann ein Passwortschutz für die reine Bedienung dann ebenfalls entfallen. Grundsätzlich sollte für individuelle Benutzer-Accounts auf eine zentrale Benutzerverwaltung gesetzt werden, über die sich auch die Aktualisierung von Passwörtern und das Sperren nicht mehr genutzter Benutzer-Accounts effizient regeln lässt.

Härtung durch sichere Parametrierung

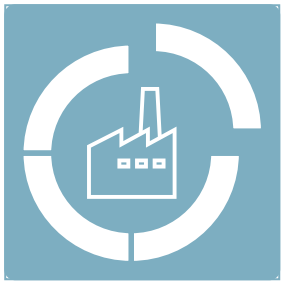
Oftmals werden Automatisierungssysteme nicht mit sicheren Voreinstellungen ausgeliefert, sondern mit vielen aktivierten Diensten und Einstellungen, die eine möglichst einfache Inbetriebnahme erlauben.

Es sollte daher eine Härtung durchgeführt werden, bei der alle unnötigen Benutzer-Accounts gelöscht oder gesperrt werden. Nicht verwendete Software sollte deinstalliert oder abgeschaltet und nicht verwendete Funktionen deaktiviert werden, so dass lediglich erforderliche Dienste laufen. Die Kontrolle auf unnötige Dienste kann mit einem Portscan zur Prüfung offener Kommunikationsschnittstellen unterstützt werden.

Schwachstellen- und Patch-Management

Die Risikobewertung für eine Komponente oder ein System kann sich sehr schnell verändern, wenn eine Schwachstelle gefunden wird. Ursache wird häufig ein Implementierungsfehler sein, es sind aber bereits Fehler in öffentlich empfohlenen Algorithmen und Protokollen entdeckt worden.

Hier gilt ebenso, dass eine Schwachstelle in einer Komponente nicht zwingend zur gleichen Bewertung auf Systemebene führen muss. So kann ein kritischer Fehler in einer Komponentenfunktion frei von Auswirkungen auf der Systemebene sein, sofern die Funktion selbst gar nicht relevant oder zugänglich ist. Dies ermöglicht den Anwendenden, die Anwendung eines Patches abzuwägen. Grundsätzlich sind Schwachstellen über die Zulieferkette zu verfolgen, die entstehenden Risiken zu evaluieren und Gegenmaßnahmen einzuleiten. Im Automatisierungsumfeld ist dabei immer das Risiko einer Fehlfunktion nach einem Patch mit zu betrachten.



Detektion und Reaktion

Da nicht davon auszugehen ist, dass die präventiven Maßnahmen alle Bedrohungen vollständig abwehren können, müssen Vorkehrungen zur Erkennung von Angriffen getroffen werden. Hierzu gehört das Sammeln von Aufzeichnungen (Log-Dateien) sowie die Installation von Systemen zur Anomalieerkennung, die über Log-Daten hinausgehende Informationen zusammentragen. Die Auswertung der Informationen kann hierbei durch Tools unterstützt werden, letztlich müssen aber auch Zeitreserven beim Personal eingeplant werden.
Abwehr und Wiederherstellung sollten für die wichtigen Szenarien vorgeplant, dokumentiert und, wenn notwendig, eingeübt sein. Können Systeme kurzfristig vom Netzwerk getrennt und isoliert werden? Wer sind die wesentlichen Ansprechpersonen? Gibt es Pläne und Backups für die Wiederherstellung?

Sicherheit der Laufzeitumgebung

Wird Software für Automatisierungsanwendungen installiert, ist diese auf die Sicherheit der Ausführungsumgebung angewiesen. Wird z. B. eine Engineering-Software auf einem PC verwendet, können Angriffe auf das Betriebssystem oder über andere Anwendungen erfolgen. Über die Engineering-Software auf dem kompromittierten PC sind dann Angriffe auf das Automatisierungssystem möglich. Zur Reduzierung dieses Risikos sollten die Härtungsempfehlungen der Hersteller von Software und Betriebssystem befolgt werden.

Awareness und Ausbildung

Um einen nachhaltig sicheren Betrieb zu ermöglichen, reichen die technischen Maßnahmen allein nicht. Die Mitarbeitenden müssen ein Security-Bewusstsein entwickeln. Viele Angriffe lassen sich nur durch die (unfreiwillige) Unterstützung von Mitarbeitenden ausführen, die Mailanhänge mit Schad-Software öffnen oder verseuchte Datenträger verwenden. Die Erkennung von Bedrohungen und Umsetzung von Security-Maßnahmen erfordert entsprechende Kenntnisse auf fachlichen Ebenen.

4 Zusammenfassung

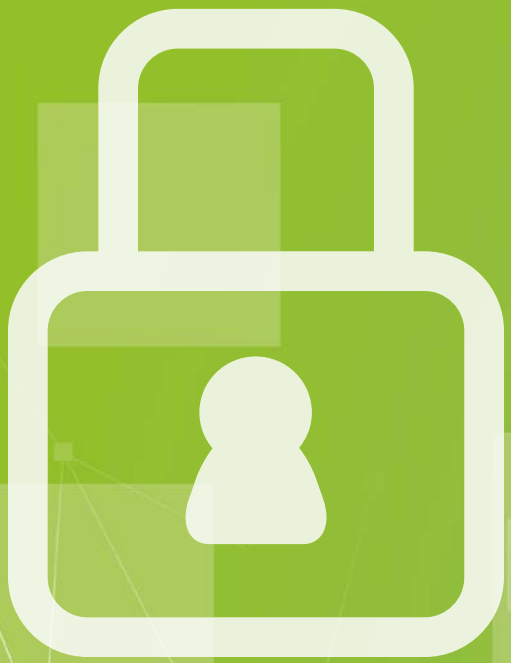


Abb. 5: 360°-Security-Ansatz

Cyber Security muss ein ganzheitlicher Ansatz sein. Er beginnt in den Köpfen des Managements und der Mitarbeitenden (Menschen). Neben technischen Maßnahmen, wie dem Einsatz von Security-Produkten (Technologie), dürfen organisatorische Maßnahmen nicht vernachlässigt werden.

Für nachhaltige Cyber Security ist ein Security-Management (Prozesse) zu etablieren, bei dem IT- und ICS-Welt zusammenarbeiten, um die Wertschöpfung zu sichern, ohne die Besonderheiten der beiden Bereiche zu ignorieren.

Literaturverzeichnis

1. Information technology – Security Techniques – Information Security Management System
   ISO/IEC 27000:2017

2. IT-Grundschutz-Kataloge: Bundesamt für Sicherheit in der Informationstechnik

3. Security for industrial automation and control systems
   IEC 62443

Kontakt

Wie sicher ist Ihr Unternehmen?

Wir helfen Ihnen, Ihre industriellen Netzwerke gegen unberechtigte Zugriffe und Schad-Software zu schützen. Sichern Sie sich jetzt einen Beratungstermin!

https://phoe.co/Cyber-Security

Bleiben Sie am Ball

- 360°-Security: Unser vollständiges Angebot ohne Kompromisse
- IEC 62443: Mit der Normenreihe IEC 62443 schützen Sie Ihre Anlagen vor Cyber-Sicherheitsrisiken
- Checkliste: Wo stehen Sie beim Thema Industrial Security?
  Unsere Checkliste hilft Ihnen, einen ersten Überblick über den Stand der Cyber-Sicherheit in Ihrer Anlage zu erhalten.

AI 03-21.004.L3