DURCH DEN DSCHUNGEL DER INDUSTRIELLEN CYBERSICHERHEIT

Ein Wegweiser

AUTOREN

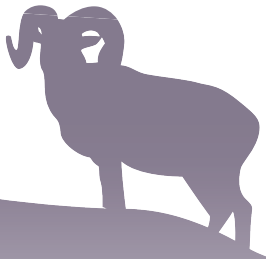
Gary DiFazio
Kristen Poulos
Gabe Authier
Keith Blodorn

PRÄSENTIERT VON

Tripwire
Belden
ProSoft Technology

HOPF
PARTNER | SOLUTIONS | COMPONENTS

INHALTSVERZEICHNIS



EINFÜHRUNG

Nahezu jeder Bereich unseres täglichen Lebens ist von dem störungsfreien Betrieb industrieller Steuersysteme (Industrial Control Systems, ICS) abhängig. Sie sorgen dafür, dass wir stets sauberes Trinkwasser haben, das Licht einschalten und andere kritische Infrastrukturen nutzen können. ICS werden nicht nur in Strom-, Energie- und diversen Ver- und Entsorgungsunternehmen eingesetzt, sondern auch bei der Herstellung von Computern, Autos und weiteren Gegenständen, die wir jeden Tag nutzen.

Der Schutz der ICS vor Cybersicherheitsvorfällen – sowohl versehentlichen als auch absichtlichen – hat oberste Priorität, denn die physischen Folgen solcher Angriffe stellen eine ernste Bedrohung für die Sicherheit der Öffentlichkeit dar und würden den Betrieb und die Wettbewerbsfähigkeit der Industrieunternehmen erheblich beeinträchtigen.

Allerdings lassen sich die Best Practices für die Cybersicherheit in der Informationstechnologie (IT) nicht einfach auf die Automatisierungstechnologie (Operational Technology, OT) übertragen, denn IT- und OT-Umgebungen bestehen aus völlig unterschiedlichen Anlagen und Netzwerkstrukturen. Zudem gibt es in der OT ganz andere Risiken und Bedrohungen.

WAS IST EIN INDUSTRIELLES STEUERSYSTEM?

„Industrielles Steuersystem" (Industrial Control System, ICS) ist ein allgemeiner Begriff, der verschiedene Arten von Steuersystemen umfasst, zum Beispiel SCADA-Systeme (Supervisory Control and Data Acquisition), verteilte Steuerungssysteme (Distributed Control Systems, DCS) und andere wie speicherprogrammierbare Steuerungen (SPS). Diese Systeme werden in der diskreten Fertigung, der Prozessautomatisierung, in der Energiebranche und im Transportwesen eingesetzt, die häufig auch kritische Infrastrukturen betreiben. Ein ICS setzt sich aus verschiedenen Steuerkomponenten zusammen (z. B. elektrischen, mechanischen, hydraulischen und pneumatischen), die gemeinsam einen physischen Prozess durchführen und kontrollieren (beispielsweise in den Branchen Automobil, Fertigung, Petrochemie, Öl und Gas, Lebensmittel, Pharmazie, Wasserversorgung/-entsorgung, Transport und Stromerzeugung/-übertragung/-verbreitung)

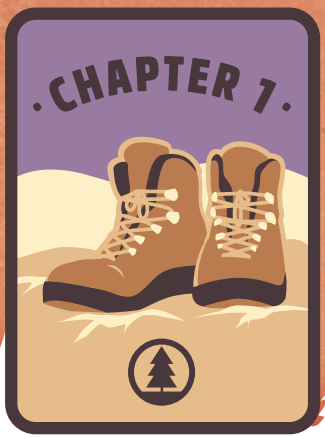
Immer mehr ICS-Anlagen verfügen über Ethernet-Verbindungen, doch damit werden sie auch anfälliger. Die meisten Industrieunternehmen sind nur unzureichend auf die Konvergenz von IT- und OT-Umgebungen vorbereitet. Neue verbundene Geräte werden schneller implementiert als die erforderlichen Sicherheitsmaßnahmen.

Anlagen, die bisher rein mechanisch betrieben wurden, müssen jetzt mit dem dynamischen industriellen Internet der Dinge (Industrial Internet of Things, IIoT) Schritt halten. Intelligente Geräte steigern zwar die Effizienz, aber ohne angemessene Sicherheitsmaßnahmen bieten sie Cyberkriminellen auch Ansatzpunkte für den Remote-Zugriff und ganz neue Angriffstechniken.

Das sind nur einige der Themen, die wir in diesem Leitfaden abdecken. Wir beginnen mit den Grundlagen der Cybersicherheit für industrielle Steuersysteme und geben schrittweise Anleitungen zum Schutz vor den schwerwiegendsten neuen Cyberbedrohungen. Dieser Leitfaden bietet nur einen allgemeinen Überblick, aber damit erhalten Sie einen Eindruck von den größten Herausforderungen für die industrielle Cybersicherheit.

„IT-Technologien werden zunehmend für industrielle Steuersysteme eingesetzt und damit werden auch Bedrohungen relevant, die bisher nur den IT-Teams bekannt waren. Unternehmen müssen sich umstellen und ihre OT-Umgebungen besser vor diesen Bedrohungen schützen. Außerdem sind viele Mitarbeiter immer noch der Ansicht, dass das IT-Team für die Sicherheit verantwortlich ist. Regelungs- oder Wartungstechniker fühlen sich dafür häufig nicht zuständig. Doch das stimmt so nicht ganz. In diesen Unternehmen besteht noch erheblicher Schulungsbedarf in Bezug auf die industrielle Cybersicherheit.“

– Nick Shaw, Senior Systems Engineer bei Tripwire



ERKUNDUNG DER UMGEBUNG

Grundlagen der industriellen Steuersysteme

Zwar müssen sowohl IT- als auch OT-Teams ihre Systeme und Daten vor Angriffen schützen, doch die OT-Sicherheitsexperten verfolgen dabei einen anderen Ansatz, da sie ganz andere Prioritäten haben.

So zögern Regelungstechniker manchmal ein Upgrade für ihre Anlagen möglichst lange hinaus, selbst wenn es die Cybersicherheit verbessern würde. Das liegt daran, dass konstante Verfügbarkeit und die Messung von Leistungswerten wie der Gesamtanlageneffektivität für sie höhere Priorität haben als die Installation der neuesten und besten Firmware. Die folgenden drei Punkte sind in der OT-Cybersicherheit ausschlaggebend:

1. **Schutzmechanismen** *Cyberangriffe oder menschliche Fehler können in einer ICS-Umgebung physische Schäden verursachen. Ein Einzelhändler muss bei einem Datenleck eventuell Millionen an Strafgebühren zahlen und mit einer Rufschädigung rechnen, aber körperliche Verletzungen der Mitarbeiter oder Kunden sind dabei kaum zu befürchten. In industriellen Umgebungen haben Schutzmechanismen höchste Priorität. Dazu gehört sowohl der Schutz der Mitarbeiter in den Produktionsstätten als auch die Sicherheit der Kunden, die die Erzeugnisse eines bestimmten ICS erhalten. Diese reichen von der Lieferung unbelasteter Produkte aus einem Lebensmittelbetrieb bis zum Einbau eines funktionierenden Airbags in der Automobilfertigung.*

2. **Qualität** *In einer industriellen Umgebung ist Konsistenz das A und O. Ist die Qualität der Erzeugnisse bedroht, kann dies finanzielle Verluste nach sich ziehen. Auch Cyberangriffe ohne Verletzungsrisiko können Industrieunternehmen schädigen, wenn beispielsweise Produkte aufgrund von Qualitätsmängeln zurückgerufen oder vernichtet werden müssen. Die Möglichkeit, qualitätsgefährdende Anomalien zu erkennen und zu beheben, ist für die Integrität der ICS-Prozesse entscheidend.*

3. **Verfügbarkeit** *Cyberangriffe können verschiedene finanzielle Schäden für Industrieunternehmen nach sich ziehen und reichen von dem Diebstahl geistigen Eigentums bis zur zeitweiligen Stilllegung von Teilen des Steuersystems durch*

einen DoS-Angriff (Denial of Service). Der Stellenwert der Verfügbarkeit wird deutlich, wenn man sich vor Augen führt, dass sich die Verluste aufgrund von ungeplanten Ausfallzeiten in der Fertigungsbranche jährlich auf 50 Milliarden US-Dollar belaufen.[1]

In vielen Industrieanlagen werden noch ältere, äußerst anfällige Windows-Versionen verwendet, die nicht gehärtet oder gepatcht wurden. Die Betreiber trauen sich nicht, die Systeme für Routinewartungsarbeiten und Sicherheitsupdates herunterzufahren, da die Anlagen für den Betrieb der Produktionsstätte oder die Bereitstellung der Services unentbehrlich sind.

Außerdem haben sie Sorgen, dass ein Upgrade oder Update die Abläufe stören könnte. In einigen Fällen würden die Schwachstellenanalysen aus dem IT-Bereich die OT-Umgebungen zu stark beeinträchtigen und können daher nicht verwendet werden. In vielen ICS-Umgebungen werden sogar noch spezielle industrielle Protokolle und Anlagen eingesetzt, die kein TCP/IP verwenden (das gängigste Kommunikationsprotokoll für IT-Netzwerk- und Sicherheitstools).

Selbst wenn die Unternehmen diese Hindernisse überwinden, bleibt Cybersicherheit eine relativ neue Disziplin für Ops-Teams in ICS-Umgebungen. Möglicherweise verzögern sie die Bearbeitung von Sicherheitsproblemen, da sie tatsächlich Bedenken in Bezug auf die Schutzmechanismen, die Qualität und die Verfügbarkeit haben. Das ist zwar durchaus nachvollziehbar, doch Cyberangriffe auf kritische Infrastrukturen nehmen rasant zu.

KRITISCHE INFRASTRUKTUREN

Nicht alle industriellen Steuersysteme werden für die kritischen Infrastrukturen eines Landes eingesetzt, aber häufig ist dies der Fall. Wie der Name schon sagt, sind kritische Infrastrukturen für das Funktionieren des Gemeinwesens und die Bereitstellung grundlegender Versorgungsleistungen wie Wasser und Strom von großer Bedeutung.

Laut dem National Infrastructure Protection Plan des U.S. Department of Homeland Security (Ministerium für Innere Sicherheit

SEKTOREN KRITISCHER INFRASTRUKTUREN

1. Chemie
2. Gewerbe
3. Kommunikation
4. Kritische Fertigung
5. Dämme
6. Rüstungsindustrie
7. Notfalldienste
8. Energie
9. Finanzwesen
10. Behörden
11. Ernährung und Landwirtschaft
12. Gesundheitswesen und medizinische Versorgung
13. Informationstechnologie
14. Kernkraftwerke, Werkstoffe und Entsorgung
15. Transportwesen
16. Wasser- und Abwassersysteme

„In unserer zunehmend vernetzten Welt reichen kritische Infrastrukturen über nationale Grenzen und globale Lieferketten hinweg. Durch diese Abhängigkeiten und die diversen Bedrohungen steigen auch die potenziellen Folgen von Angriffen."

– U.S. Department of Homeland Security

der Vereinigten Staaten)[3] werden kritische Infrastrukturen in separate Sektoren unterteilt: „Es gibt 16 Sektoren kritischer Infrastrukturen, deren physische und virtuelle Ressourcen, Systeme und Netzwerke von so großer Bedeutung für die USA sind, dass ihr Ausfall oder ihre Zerstörung die Sicherheit, nationale wirtschaftliche Stabilität, den Schutz oder die medizinische Versorgung der Bevölkerung oder eine Kombination dieser Faktoren nachhaltig beeinträchtigen würde."

Doch auch die vielen ICS-Unternehmen, die nicht zum Schutz der Öffentlichkeit beitragen, benötigen effektive Sicherheitsmaßnahmen. Typische Branchen sind die Automobilfertigung, Stromerzeugung, -übertragung und -verteilung, Öl und Gas, Pharmazie und die Wasserversorgung bzw. Abwasserentsorgung.

DIE KLUFT ZWISCHEN IT UND OT

Lange Zeit waren unterschiedliche Netzwerktypen wie Ethernet und Feldbus nicht kompatibel. Heutzutage sind industrielle Steuersysteme zunehmend mit IT-Geräten und Geschäftsprozessen verzahnt, wodurch sich das Risiko für die Befehlsfunktionen vervielfacht.

Die erforderliche IT-/OT-Konvergenz wirft auch einige Fragen für die Abteilungsleiter auf, zum Beispiel: Wer ist für die ICS-Cybersicherheit verantwortlich – der Produktionsstättenbetreiber oder das SOC (Security Operations Center) der IT-Abteilung?

Die Antwort lautet natürlich: Die Verantwortung muss geteilt werden. Doch vielen Unternehmen fehlen die internen Organisationsstrukturen, um bereichsübergreifend Aufgaben zu verteilen und Rollen und Zuständigkeiten durchzusetzen.

In einem gemeinsamen Cybersicherheitsprogramm für IT und OT können diverse technische Probleme auftreten, wenn sie versuchen, beide Seiten unter einen Hut zu bringen. Das liegt daran, dass ältere ICS-Anlagen aufgrund der zunehmenden Verbreitung des IIoT inzwischen zwar Ethernet-Verbindungen herstellen können, aber ursprünglich nicht auf eine sichere Datenübertragung ausgelegt waren. Das U.S. Department of Homeland Security[2] hat folgende Unterschiede zwischen den Sicherheitsmaßnahmen in Produktionsstätten und IT-Abteilungen ausgemacht.

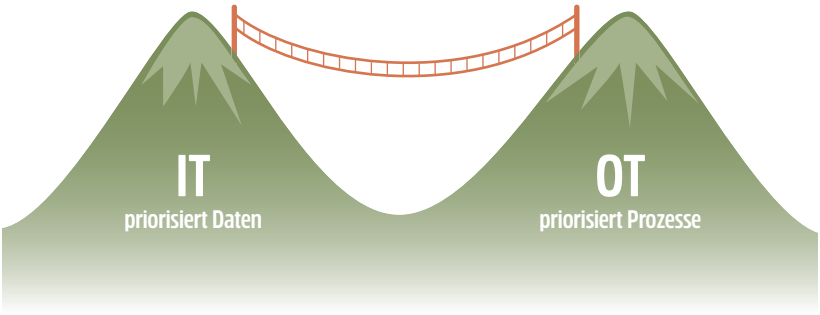
Unterschiede bei der Cybersicherheit in IT- und OT-Umgebungen

Thema	Informationstechnologie (IT)	Automatisierungstechnologie (OT)
Antivirensoftware und mobiler Code	Üblich; einfache Bereitstellung und Aktualisierung. Können ressourcen- oder unternehmensbasiert sein; Benutzer können Anpassungen vornehmen	Mögliche Beeinträchtigung des ICS-Betriebs durch die Speicheranforderungen; Unternehmen können ältere Systeme nur mit Aftermarket-Lösungen schützen; in der Regel sind Ordner für Ausnahmen erforderlich, damit wichtige Dateien nicht isoliert werden
Patch-Management	Einfach festzulegen; unternehmensweit; per Fernzugriff kontrollierbar und automatisiert	Lange Vorlaufzeit für eine erfolgreiche Patch-Installation; herstellerspezifisch; kann den ICS-Betrieb erheblich beeinträchtigen; Ressourceninhaber müssen ein akzeptierbares Risiko festlegen
Supportlaufzeit für Technologie	2–3 Jahre; mehrere Anbieter; umfassende Upgrades	10–20 Jahre; meist nur ein Anbieter; Sicherheitsbedenken am Ende des Produktlebenszyklus
Tests und Audit-Methoden	Moderne Methoden; Systeme sind in der Regel widerstandsfähig und stabil genug für Bewertungen	Tests müssen auf das System abgestimmt werden; moderne Methoden sind eventuell ungeeignet; Geräte können während der Tests ausfallen
Änderungsmanagement	Regelmäßig und geplant; auf die Mindestnutzungsdauer abgestimmt	Strategische Planung; aufgrund der Auswirkungen auf die Produktion ein komplexer Prozess
Ressourcenklassifizierung	Üblich und jährlich durchgeführt, Ergebnisse führen zu neuen Anschaffungen	Durchführung nur, wenn vorgeschrieben; meist keine präzisen Inventarlisten für nicht kritische Ressourcen; kein Bezug zwischen Ressourcenwert und angemessenen Abwehrmaßnahmen
Incident-Response-Maßnahmen und Forensik	Einfache Entwicklung und Bereitstellung; einige gesetzliche Vorschriften; in die Technologie eingebettet	Fokus auf Neustart des Systems; forensische Maßnahmen noch unausgereift (keine Wiederherstellung der Ereignisse); gute Zusammenarbeit von IT und ICS erforderlich
Physische Schutzmaßnahmen und Umgebungssicherheit	Reicht von „minimal" (Bürosysteme) bis zu „ausgezeichnet" (kritische IT-Systeme)	Für kritische Bereiche in der Regel ausgezeichnet; Reifegrad variiert je nach Stellenwert/Kultur am Standort
Sichere Systementwicklung	Fester Bestandteil des Entwicklungsprozesses	Ursprünglich kein fester Bestandteil des Entwicklungsprozesses; Reifegrad der Anbieter steigt, allerdings langsamer als bei der IT; grundlegende/wichtigste ICS-Lösungen lassen sich kaum nachträglich mit Sicherheitsfunktionen ausstatten
Sicherheits-Compliance	Präzise Vorgaben durch Behörden je nach Sektor (und nicht für alle Sektoren)	Spezifische Leitfäden je nach Sektor (und nicht für alle Sektoren)

„Die IT setzt gern sofort die neuesten Technologien ein, während die OT versucht, Upgrades so lange wie möglich hinauszuzögern, um den Produktionsbetrieb nicht zu stören. Manchmal wirkt es, als würden die Teams sogar verschiedene Sprachen sprechen. Wenn man ihnen beispielsweise sagt, sie sollen darauf achten, dass die neue Netzwerkmanagementsoftware mit ‚sip' kompatibel ist, denken die OT-Experten an das ‚Common Industrial Protocol' (CIP) und die IT-Experten an das ‚Session Initiation Protocol' (SIP). Und beide Teams sind davon überzeugt, die Anweisung richtig verstanden zu haben."

– Jeremy Friedmar, Business & Channel Development Manager bei Belden

Die Kluft zwischen IT und OT



DIE DREI ARTEN VON ICS

Industrieunternehmen stehen verschiedene Automatisierungsmethoden zur Verfügung. In bestimmten Fällen müssen beispielsweise verteilte Systeme eingesetzt werden, um Anlagen an externen Standorten zu steuern. Andere sind lokal und überwachen mehrere Untersysteme für zahlreiche Kontrollpunkte, die sich in unmittelbarer Nähe befinden. Die meisten ICS nutzen eine der folgenden Systemarten:

1. **Verteilte Steuerungssysteme:** *Verteilte Steuerungssysteme (Distributed Control Systems, DCS) verwalten und automatisieren Tausende Kontrollpunkte in einem Prozess. Sie werden üblicherweise in großen lokalen Unternehmen wie Öl- und Gasraffinerien, Pharma-Werken und Stromerzeugungsanlagen verwendet. Verteilte Steuerungssysteme bestehen häufig aus verschiedenen Komponenten, zum Beispiel Controllern, E/A-Geräten und Servern.*

2 **Speicherprogrammierbare Steuerungen:** *Eine speicherprogrammierbare Steuerung (SPS) ist eine Art Industriecomputer und sozusagen das Gehirn des Betriebs. Die SPS analysiert die eingehenden Daten der Sensoren und trifft dann mithilfe logischer Programmierung angemessene Entscheidungen, z. B. einen Motor einschalten oder Druck ablassen. SPS werden in allen industriellen Automatisierungsprozessen eingesetzt und können auch Teil eines größeren Systems sein, beispielsweise eines DCS.*

3 **SCADA-Systeme:** *Ein SCADA-System (Supervisory Control and Data Acquisition) verwaltet und überwacht Remote-Feldgeräte, die oft auf einer Fläche von Tausenden Quadratkilometern verteilt sind. Es kann diese auch eingeschränkt steuern, um bei Warnmeldungen oder Benachrichtigungen bestimmte Aktionen durchzuführen, zum Beispiel ein Ventil öffnen oder ein Schütz schließen. In Umgebungen, die sich über eine große geografische Fläche erstrecken, wie Erdgaspipelines oder Umspannwerken, wird das SCADA-System auch zur Steuerung und Verwaltung der Anwendungen genutzt.*

> ***TIPP VON TRIPWIRE:*** **Die Best Practices für die Cybersicherheit (wie die Zertifizierung für und Einhaltung von IEC 62443) gelten für nahezu alle industriellen Steuersysteme. Für die Integrität des ICS sind die Erkennung/Inventur, Verwaltung und Überwachung der Ressourcen notwendig. Die einzelnen Prozesse hängen von der spezifischen Hardware und Software im ICS ab.**

DAS PURDUE-MODELL

Zu Beginn der IT-/OT-Konvergenz wurde deutlich, dass eine Referenzarchitektur benötigt wurde, um die spezifischen Rollen und Funktionen der Anlagen zur Steuerung physischer Prozesse und die relevanten untergeordneten Geräte und Abläufe zu definieren. 1990 wurde daher zu diesem Zweck das Purdue Enterprise Reference Model entwickelt, das heute meist einfach „Purdue-Modell" genannt wird.

Das Modell wurde im Laufe der Jahre weiterentwickelt, aber es dient immer noch der hierarchischen Einordnung der physischen Prozesse in einzelne Verwaltungsbereiche. Es gilt inzwischen als Standard für die Netzwerksegmentierung. (Das bezieht sich auf die Segmentierung von Netzwerken, um die verschiedenen Ebenen des Modells mithilfe von Firewalls abzugrenzen. Dort wird der gesamte Datenverkehr für die Ebenen des Purdue-Modells blockiert, sofern er nicht ausdrücklich genehmigt wurde.)

Mit den zunehmenden Verbindungen zwischen den Produktionsanlagen und den IT-Netzwerken der Unternehmen wurde dem Purdue-Modell mit der demilitarisierten Zone (DMZ) eine neue Trennlinie zwischen industriellen Steuernetzwerken und Unternehmensnetzwerken hinzugefügt. Das aktuelle Purdue-Modell umfasst sieben Ebenen, einschließlich der DMZ auf Ebene 3.5.

Die Ebenen des Purdue-Modells

- *EBENE 0:* E/A-Feldgeräte
- *EBENE 1* Steuerung: SPS und RTU (Fernbedienungsterminals)
- *EBENE 2* Prozess: MMS, Bedien- und Kontrollstationen
- *EBENE 3* Betrieb: Data-Historian-Software, Netzwerkservices und hochentwickelte Steuerungen
- *EBENE 3.5* DMZ
- *EBENE 4* Unternehmensnetzwerk
- *EBENE 5* Unternehmens-IT

Die spezifischen Industrieanlagen und -geräte befinden sich näher an den physischen Prozessen auf Ebene 0. Zu den Ebenen 0 und 1 zählen Geräte wie Sensoren, Aktoren, Laufwerke, SPS und DCS. Je weiter man sich von diesen beiden Ebenen entfernt, desto mehr herkömmliche, standardisierte IT-Systeme (wie Engineering-Workstations, Mensch-Maschine-Schnittstellen (MMS), Data-Historian-Software zur Prozessdatenerfassung und SCADA-Systeme) finden sich. Diese werden unter gängigen Betriebssystemen wie Linux oder Microsoft Windows ausgeführt.

Da die Automatisierungssysteme weiterentwickelt werden, müssen dem Purdue-Modell auch in Zukunft neue Ebenen hinzugefügt werden. Allerdings werden diese unter Umständen nicht so deutlich abgegrenzt sein wie im aktuellen Modell. Die Entwicklung der Automatisierungssysteme wird ähnlich wie die der IT-Systeme verlaufen und sich aufgrund von Virtualisierung, dienstgestützten Netzwerken, Anwendungscontainern und Cloud-Umgebungen von den physischen Anlagen lösen.

Die ersten Cybersicherheitslösungen sollten ein – wenn nicht sogar das größte – Problem der industriellen Cybersicherheit beheben: Wie schützt man sich vor etwas, das nicht bekannt oder sogar unsichtbar ist? Die Lösungen wurden erst dann als nützlich eingestuft, als sie Geräte auf den Ebenen 0 und 1 des Purdue-Modells identifizieren konnten, da diese Geräte nicht über herkömmliche IT-Protokolle kommunizieren, sondern über industrielle Protokolle wie Ethernet/IP, Modbus und Profinet.

MANCHE ICS haben DEN ANSCHLUSS VERPASST

Als vor über 30 Jahren die ersten industriellen Steuersysteme entwickelt wurden, war Cybersicherheit noch kein Thema. Industrieunternehmen müssen neben der IT-/OT-Konvergenz noch einige andere Herausforderungen bewältigen, wenn sie die erforderlichen Cybersicherheitsprogramme zum Schutz vor Fehlern und Angriffen implementieren möchten.

Der Wechsel zu neuen Netzwerktechnologien verbessert die Datenerfassung und die Automatisierung, steigert die betriebliche Effizienz und verkürzt die Markteinführungszeiten, aber er bringt aufgrund der folgenden Faktoren auch neue Risiken mit sich:

- **Nicht integrierte Technologien:** *Viele ICS sind zweckgebunden, proprietär und wurden zu einem Zeitpunkt entwickelt, als Cybersicherheit noch keine Priorität hatte.*

- **Flache Netzwerke:** *Viele ICS-Netzwerke sind flach, d. h., jedes Gerät hat Zugriff auf alle anderen. In einer flachen, nicht segmentierten Netzwerkarchitektur kann sich Malware nach dem Angriff auf ein einziges Gerät ungehindert in der Umgebung ausbreiten.*

- **Fachkräftemangel:** *Aufgrund der alternden Belegschaft und der immer schnelleren Einführung von IT-Technologien in industriellen Steuersystemen kommt es in Bezug auf die ICS-Sicherheit zu einem Fachkräftemangel. Bis 2021 werden schätzungsweise 3,5 Millionen Stellen in der Cybersicherheit unbesetzt bleiben[4], sodass der Fachkräftemangel zu einem ernsten Problem wird.*

TIPP VON TRIPWIRE: Um die Kluft zwischen IT und OT zu überbrücken, sollten Industrieunternehmen eine neue Position einführen: den ADX-Techniker (Automation and Data Exchange, Spezialist für Automatisierung und Datenaustausch). Dieser arbeitet eng mit den IT- und OT-Teams zusammen und stellt sicher, dass die Betriebsprozesse funktionieren und die Daten an die IT-Abteilung weitergeleitet werden, damit fundierte Geschäftsentscheidungen getroffen werden können.

„In den nächsten fünf bis zehn Jahren werden Internetverbindungen in industriellen Systemen immer wichtiger, da das IoT in der Branche an Einfluss gewinnt und diese Systeme auch mit 5G-Mobilfunknetzen verbunden werden, die die Kommunikationsverzögerungen zwischen Geräten minimieren sollen. Die Standardsicherheitsfunktionen von IoT-Geräten sind in der Regel nicht sehr zuverlässig, daher wird die Verwaltung zahlreicher IoT-Geräte in industriellen Systemen eine große Herausforderung.“

– Justin Sherman, Cybersecurity Policy Fellow bei New America

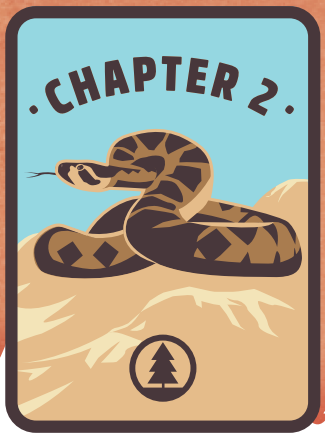
WICHTIGE BEGRIFFE UND DEFINITIONEN

Hier sind einige Begriffe und Definitionen aus dem Bereich der industriellen Cybersicherheit, die für den Rest des Leitfadens hilfreich sind.

Physische Systeme	
ICS (Industrial Control System, industrielle Steuersysteme)	Unter diesem Begriff werden verschiedene Arten von Steuersystemen zusammengefasst. ICS bestehen aus diversen Steuerkomponenten (z. B. elektrischen, mechanischen, hydraulischen und pneumatischen), die für ein bestimmtes Ziel (wie Fertigung, Transport von Feststoffen oder Energieverteilung) kombiniert werden. Industrielle Steuersysteme sind für den Betrieb kritischer Infrastrukturen entscheidend, oft eng verzahnt und voneinander abhängig.
SCADA (Supervisory Control and Data Acquisition)	Dieses Steuersystem wird in verteilten Systemen verwendet, um Remote-Feldgeräte, die oft über eine große geografische Fläche verbreitet sind, zentral zu verwalten und zu überwachen. Die Geräte erfassen Felddaten und übertragen sie dann, damit sie in der zentralen Konsole analysiert werden können.
Feldbus	Feldbus ist ein Kommunikationssystem für Eingabe- und Ausgabegeräte. Damit muss nicht jedes Gerät eine Verbindung zum Controller herstellen.
DCS (Distributed Control System, verteilte Steuerungssysteme)	Verteilte Steuerungssysteme verwalten und automatisieren Tausende Kontrollpunkte in einem Prozess. Sie setzen sich häufig aus verschiedenen Komponenten zusammen, zum Beispiel Controllern, E/A-Geräten und Servern.
SPS (speicherprogrammierbare Steuerung)	Die SPS ist eine Art Industriecomputer und sozusagen das Gehirn des Betriebs. Sie analysiert die eingehenden Daten der Sensoren und trifft dann mithilfe logischer Programmierung angemessene Entscheidungen, z. B. einen Motor einschalten oder Druck ablassen.
MMS (Mensch-Maschine-Schnittstelle)	Hardware oder Software – von physischen Steuereinheiten bis zu einem Industriecomputer, auf dem spezielle Software ausgeführt wird. Mitarbeiter können den Prozessstatus überwachen, die Einstellungen und Ziele ändern und automatische Steuerprozesse manuell überschreiben.
Begriffe aus der industriellen Cybersicherheit	
Kritische Infrastrukturen	Physische und Cyber-Systeme, die für ein Land von großer Bedeutung sind und deren Ausfall oder Zerstörung den Schutz oder die medizinische Versorgung der Bevölkerung nachhaltig beeinträchtigen würde
Kritische Ressourcen	Ein bestimmtes Mittel, das eine so hohe Priorität hat, dass ein Ausfall oder die Zerstörung das Funktionieren des Gemeinwesens eines Landes nachhaltig beeinträchtigen würde
IIoT (Industrial Internet of Things, industrielles Internet der Dinge)	Unter diesem Begriff werden diverse Hardware-Produkte zusammengefasst, die miteinander verbunden sind und die Fertigungs- und Industrieprozesse verbessern sollen.

Einige Definitionen stammen aus der *NIST Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security.*

Zone	Eine Gruppe von Objekten, die eine Systempartition darstellen und aufgrund ihrer funktionalen, logischen und physischen Beziehungen (einschließlich Standort) zusammengefasst wurden
Conduit	Die logische Gruppierung von Kommunikationskanälen, die mindestens zwei Zonen mit gleichen Sicherheitsanforderungen miteinander verbinden
Cybersicherheitsvorfall	Ein Sicherheitsvorfall, der die Integrität, Vertraulichkeit oder Verfügbarkeit einer Informationsressource beeinträchtigt
Datenleck	Ein Sicherheitsvorfall, bei dem tatsächlich (nicht nur potenziell) Daten für nicht autorisierte Dritte freigegeben werden
Defense-in-Depth-Ansatz	Eine mehrstufige Technik, bei der mindestens zwei sich überschneidende Sicherheitsmechanismen eingesetzt werden, um die Folgen bei dem Ausfall eines dieser Mechanismen zu minimieren. Dazu zählen häufig Firewalls, demilitarisierte Zonen, Mitarbeiterschulungen, Incident-Response-Maßnahmen und physische Schutzmechanismen.
Phishing	Eine Strategie, mit der Einzelpersonen zur Herausgabe personenbezogener Daten verleitet werden sollen. Dabei werden in elektronischer Kommunikation vertrauenswürdige Unternehmen imitiert.
Social Engineering	Die psychologische Manipulation von Personen, damit diese Informationen herausgeben (z. B. ein Passwort) oder Aktionen durchführen (beispielsweise Geld überweisen). Diese Taktiken können auch für Angriffe auf Systeme oder Netzwerke eingesetzt werden.
Malware	Software oder Firmware, die einen nicht autorisierten Prozess ausführen soll, um die Vertraulichkeit, Integrität oder Verfügbarkeit eines Informationssystems zu beeinträchtigen
Zero-Day-Angriff	Ein Angriff, bei dem eine bisher unbekannte Sicherheitslücke ausgenutzt wird, für die entweder noch kein Patch vorhanden ist oder die die Anwendungsentwickler nicht kannten
SCM (Security Configuration Management)	Die Verwaltung und Kontrolle von Sicherheitskonfigurationen eines Informationssystems zur Steigerung der Sicherheit und Minimierung der Risiken
FIM (File Integrity Monitoring, Überwachung der Dateiintegrität)	Auch Änderungsüberwachung genannt. Bei diesem Prozess werden die Dateien untersucht und es wird festgestellt, ob und wann sie geändert wurden, was geändert wurde, wer sie geändert hat und wie sie wiederhergestellt werden können, falls die Modifizierungen nicht autorisiert worden waren.
Schwachstellenmanagement	Das Durchsuchen von Netzwerken auf bekannte Sicherheitslücken oder CVEs (Common Vulnerabilities and Exposures). Anschließend werden diese Schwachstellen nach Risikograd priorisiert und behoben.
Positionen in der ICS-Sicherheit	
CISO (Chief Information Security Officer)	Eine Führungskraft, die üblicherweise für die Gestaltung der Strategie und die Implementierung und Pflege des Sicherheitsprogramms verantwortlich ist, mit dem Informationsressourcen und -technologien geschützt werden sollen.
ADX-Techniker (Automation and Data Exchange, Spezialist für Automatisierung und Datenaustausch)	Ein neuer Titel für Cybersicherheitsexperten, die sich überwiegend mit der Überbrückung der Kluft zwischen IT und OT beschäftigen.



POTENZIELLE GEFAHREN

Cyberbedrohungen für industrielle Steuersysteme

Betreiber industrieller Steuersysteme müssen die gängigen Angriffstechniken wie Phishing und Malware kennen und über neue Taktiken auf dem Laufenden sein, die speziell für ICS entwickelt werden. Obwohl viele industrielle Steuersysteme proprietäre Geräte und Software einsetzen, wird immer häufiger Malware gezielt für ICS-Umgebungen entwickelt. Ein bekanntes Beispiel dafür ist Stuxnet.

Laut dem *2019 Data Breach Investigations Report von Verizon*[5] haben die finanziell motivierten Angriffe auf die Fertigungsbranche in den letzten Jahren zugenommen, aber auch die Spionage bleibt ein wichtiges Motiv. Bei den meisten Angriffen wurden Phishing-Kampagnen und gestohlene Anmeldedaten genutzt. Von den 352 Sicherheitsvorfällen und 87 Datenlecks, die in dem Bericht genannt werden, gehören finanzielle Absichten (68 Prozent) und Spionage (27 Prozent) zu den Hauptmotiven der Angreifer.

Wie verschaffen sich Angreifer Zugriff auf ein anfälliges industrielles Steuersystem? Das hängt von dem Reifegrad des Cybersicherheitsprogramms ab. Wenn das Cybersicherheitsprogramm eines Industrieunternehmens beispielsweise keine grundlegende Änderungsüberwachung umfasst, haben Angreifer relativ leichtes Spiel. Sie können sich unbemerkt im Netzwerk aufhalten, Daten ausschleusen und sich Zugriff auf Konten mit umfassenden Rechten verschaffen. Verwendet ein Unternehmen allerdings ein ausgereiftes Programm zur Überwachung der Geräte und Netzwerke, ist das Risiko für Angreifer größer, da ihr Zugriff und das erste Ausspähen erfasst werden, bevor sie Schaden anrichten können.

„Wenn Sie in Ihrem Unternehmen ein industrielles Steuersystem verwenden, sollten Sie die Sicherheitsmaßnahmen für diese Umgebung evaluieren. Industrieunternehmen ist inzwischen bewusst, dass digitale Bedrohungen schwerwiegende Folgen haben können. Dazu haben vielleicht auch die letzten Angriffe beigetragen, die speziell zur Störung physischer Prozesse entwickelt wurden und damit Erfolg hatten."

– Tim Erlin, VP of Product Management and Strategy bei Tripwire

ABSICHTLICHE oder VERSEHENTLICHE UND INTERNE oder EXTERNE BEDROHUNGEN

Wenn Sie eine Schlagzeile zu einem Cyberangriff auf eine kritische Infrastruktur lesen, denken Sie vermutlich zuerst an einen koordinierten staatlich gesponserten Angriff. Diese stellen zwar durchaus ein Risiko für die Öffentlichkeit dar, aber nicht alle Cyberangriffe auf ICS laufen wie in einem Actionfilm ab.

Laut dem *2019 DBIR* ließen sich 30 Prozent der Cybersicherheitsvorfälle auf interne Bedrohungen zurückführen. Das können Insider sein, die für Spionageaktivitäten bezahlt werden, oder unzufriedene Mitarbeiter, die das Unternehmen finanziell schädigen oder den Betrieb stören wollen. In vielen Fällen war die Ursache für einen Cybersicherheitsvorfall aber auch einfach ein menschlicher Fehler. Zu den versehentlichen internen Bedrohungen zählt beispielsweise ein Mitarbeiter, der den falschen Switch konfiguriert und damit eine Anlage außer Betrieb setzt oder der unabsichtlich ein Passwort offen liegen lässt, sodass vertrauliche Informationen gestohlen werden können.

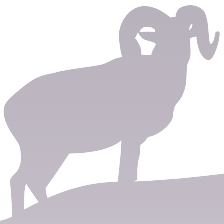
TYPISCHE ICS-SICHERHEITS-VERLETZUNGEN

1. Vernichtung von Daten
2. Manipulation von Daten
3. Datendiebstahl
4. Denial-of-Service-Angriffe
5. Identitätsmissbrauch
6. Ausweitung der Zugriffsrechte
7. Menschlicher Fehler
8. Geräteausfall

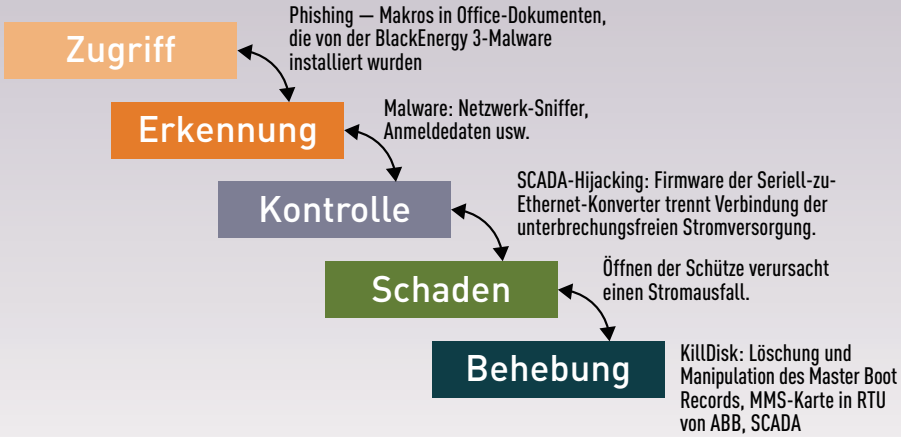
BEISPIEL FÜR EINEN REALEN ANGRIFF AUF EIN ICS

An einem kalten Winterabend im Dezember 2015 fiel in mehr als 230.000 ukrainischen Haushalten in drei verschiedenen Regionen plötzlich der Strom aus. Ein einziger koordinierter Angriff hatte 30 öffentliche Umspannwerke lahmgelegt.

Er kam vielleicht für das Versorgungsunternehmen überraschend, war aber das Ergebnis sechs Monate langer sorgfältiger Planung der Cyberkriminellen. Sie nutzten eine Kombination aus Phishing, Keylogger, VPN-Hijacking, Denial of Service, Firmware-Modifizierung und anderen Techniken.



Ablauf eines Angriffs auf das ukrainische Stromnetz



Schwerwiegende Cybersicherheitsvorfälle in der Industriebranche

Jahr	Angegriffene(s) Unternehmen	Taktik	Ergebnis
2010	Iranisches Kernkraftwerk	Der Stuxnet-Wurm wurde über einen USB-Stick in das Werk eingeschleust und griff dann die Steuerungssoftware an, mit der die Zentrifugen zur Uran-Anreicherung programmiert wurden.	Stuxnet störte das iranische Atomprogramm, da ungefähr 20 Prozent der Zentrifugen ausfielen.
2011	Energiebranchen in den USA, der Schweiz und der Türkei	Die Hackergruppe DragonFly wurde 2011 gegründet, trat aber vor allem 2017 in Erscheinung. Sie nutzte RAT-Malware (Remote Access Tool) für Spear-Phishing-, Trojaner- und Watering-Hole-Angriffe.	DragonFly verschaffte sich nicht autorisierten Remote-Zugriff und konnte dadurch vertrauliche Informationen wie Passwörter aus den industriellen Steuersystemen ausschleusen.
2013	Mehrere industrielle Steuersysteme in der Energie- und Pharmabranche	Die Gruppe Energetic Bear nutzte Watering-Hole- und Phishing-Angriffe zur Spionage und Ausspähung.	Sie manipulierte außerdem SPS, indem sie mit der Havex-Malware Backdoors installierte.
2015	Ukrainisches Stromnetz	Industroyer ist eine Malware-Art, die zur Steuerung von Umspannwerken und Leistungsschaltern verwendet wurde.	Industroyer-Angriffe haben einen Stromausfall verursacht, von dem mehr als 230.000 Personen betroffen waren.
2017	Saudi-arabisches Petrochemiewerk	Hacker nutzten TRITON-Malware, um physische Schutzmechanismen zu umgehen. Die Angreifer konnten sich ein Jahr lang im Netzwerk ausbreiten, Dateien umbenennen und reguläre Prozesse imitieren, bis sie auf das Sicherheitssystem des ICS zugriffen.	Das Ziel der Angreifer war vermutlich eine Explosion in dem Werk, aber letztendlich konnten sie nur einige der Festplatten des Unternehmens löschen.
2018	Über 200.000 Unternehmen in der Energie-, Fertigungs-, Öl- und Gas-, Petrochemie-Branche und anderen Sektoren in mehr als 150 Ländern	Die Angreifer nutzten die Ransomware WannaCry, um eine Windows-Sicherheitslücke auszunutzen und Daten zu verschlüsseln.	Der Angriff hatte weltweit schwerwiegende Folgen. Einige Autohersteller mussten sogar vorübergehend den Betrieb einstellen.

NICHT OHNE KARTE

Die Vorteile von Industriestandards

In Branchen wie dem Gesundheitswesen, Finanzwesen und Einzelhandel gelten strikte Cybersicherheitsvorschriften, unter anderem HIPAA, PCI und SOX. Die Einhaltung dieser obligatorischen Standards wird durch akribische Audits überprüft und Unternehmen müssen bei Missachtung mit heftigen Geldstrafen rechnen. In der Industrie gibt es bisher noch keine derartigen branchenweiten Vorgaben, doch einige Sparten veröffentlichen Regelwerke als Leitfäden.

WAS SPRICHT FÜR EIN REGELWERK?

Weshalb sollten sich Unternehmen für ein Regelwerk entscheiden, wenn dies nicht gesetzlich vorgeschrieben ist? Der Grund ist ganz einfach: Ein optionales Regelwerk ist der beste Einstieg in ein Cybersicherheitsprogramm. Darin werden der Aufbau solider Abwehrmaßnahmen und die Sicherstellung des Betriebs erläutert. Unternehmen erhalten eine schrittweise Anleitung zur Minimierung der Risiken und vermeiden, dass sie aufgrund von Datenlecks Schlagzeilen machen.

Ein solches Regelwerk ist damit eine Investition in die zukünftige Stabilität und Rentabilität eines Unternehmens. Durch die zunehmende Verbreitung des IIoT wird es auch mehr Verbindungen und damit größere Cyberrisiken geben. Mit den grundlegenden Cybersicherheitsmaßnahmen der Compliance-Regelwerke machen Sie Ihre industriellen Steuersysteme zukunftssicher.

Standards wie IEC 62443, NIST SP 800-82 und NERC CIP geben Industrieunternehmen praxisnahe Anleitungen zum Schutz der Prozesse an die Hand und enthalten umfassendes Branchenwissen zur Einrichtung eines Cybersicherheitsprogramms.

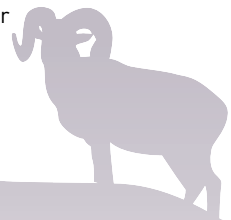
TIPP VON TRIPWIRE: Wie schnell können Sie einen Fehler erkennen und beheben? Die Integrität der Prozesse ist ein weiterer Vorteil eines guten Cybersicherheitsprogramms. Überwachungslösungen bieten Ihnen einen Überblick über Sicherheitsvorfälle, die die Prozessintegrität gefährden könnten. Sie funktionieren ähnlich wie ein Videorekorder, bei dem Sie die Aufnahme zurückspulen, um die Problemursache zu finden. Auf diese Weise soll die Zuverlässigkeit der Prozesse gewährleistet werden, damit die Abweichungen der Erzeugnisse minimal bleiben. Mit einer solchen Überwachungslösung können Sie schnell rückwirkend Fehler erkennen und beheben.

IEC 62443

IEC 62443 (ursprünglich ISA-99) wurde von der International Society for Automation (ISA) erstellt und von der International Electrotechnical Commission (IEC) übernommen. Es ist ein Cybersicherheitsstandard für Industrieunternehmen und ein Leitfaden zur Implementierung von Sicherheitslösungen.

In IEC 62443 wurden flexible Methoden für sichere Prozesse definiert. Höchste Priorität haben dabei der Schutz der Mitarbeiter sowie die Produktion, Verfügbarkeit, Effizienz und Qualität. Es ist ein weit verbreiteter Standard in Industriebranchen wie der diskreten Fertigung, Öl und Gas, Strom und Wasser/Abwasser.

Ein zentrales Konzept von IEC 62443 ist die Struktur aus Zonen und Conduits (Kommunikationskanälen), mit der die verschiedenen Ebenen des Purdue-Modells erstellt werden. Dies ist auch eine wichtige Komponente für die Defense-in-Depth-Methode, die in Kapitel 4 erläutert wird.



„Die ISA/IEC 62443-Standards, die von dem ISA-99-Komitee entwickelt und von der International Electrotechnical Commission (IEC) übernommen wurden, bieten ein flexibles Regelwerk zur Behebung und Vermeidung aktueller und zukünftiger Schwachstellen in industriellen Automatisierungs- und Steuersystemen (Industrial Automation and Control Systems, IACS). Das Komitee wurde von IACS-Sicherheitsexperten aus der ganzen Welt beraten, um Konsensnormen für alle Branchensektoren und kritischen Infrastrukturen zu entwickeln.“

– International Society for Automation

CIS CONTROLS

Viele der vertrauenswürdigsten Unternehmen in der Cybersicherheitsbranche nutzen zum Schutz ihrer Systeme die CIS Controls des Center for Internet Security. Die 20 Sicherheitsmaßnahmen sind nach Priorität aufgelistet und werden daher am besten der Reihe nach implementiert.

Grundlegende CIS Controls

1. Inventur und Kontrolle von Hardwareressourcen
2. Inventur und Kontrolle von Softwareressourcen
3. Kontinuierliches Schwachstellenmanagement
4. Kontrolle der Nutzung von Administratorrechten
5. Sichere Konfiguration von Hardware und Software auf mobilen Geräten, Laptops, Workstations und Servern
6. Wartung, Überwachung und Analyse von Auditprotokollen

Technische CIS Controls

7. Schutz von E-Mail-Systemen und Webbrowsern
8. Abwehr von Malware
9. Einschränkung und Kontrolle von Netzwerkports, Protokollen und Services
10. Funktionen für die Datenwiederherstellung
11. Sichere Konfiguration von Netzwerkgeräten, einschließlich Firewalls, Routern und Switches
12. Abwehrmaßnahmen an Netzwerkgrenzen
13. Datenschutz
14. Kontrollierter Zugriff nach dem Need-to-know-Prinzip
15. WLAN-Zugangskontrollen
16. Kontrolle und Überwachung von Konten

Organisatorische CIS Controls

17. Implementierung eines Programms zur Steigerung des Sicherheitsbewusstseins und Einführung von Schulungen
18. Sicherheitsfunktionen für Anwendungssoftware
19. Incident-Response-Maßnahmen und -Management
20. Penetrationstests und Red-Team-Übungen

„Viele Unternehmen sind von den modernen Cybersicherheits-umgebungen überfordert und wissen nicht, wie sie mit den zahlreichen neuen Informationen und Bedrohungen umgehen sollen. ... In den CIS Controls legen wir die Prioritäten fest und nutzen das Know-how einer großen Experten-Community, um wichtige Best Practices und konkrete Maßnahmen vorzustellen."

– Center for Internet Security

ERGÄNZENDER IMPLEMENTIERUNGSLEITFADEN FÜR CIS CONTROLS

Als Ergänzung zu den bekannten CIS Controls hat das Center for Internet Security einen Leitfaden speziell für Industrieunternehmen veröffentlicht: *CIS Controls Implementation Guide for Industrial Control Systems*. Das Dokument enthält detaillierte Anleitungen zu den 20 Sicherheitsmaßnahmen speziell für ICS-Umgebungen.

„Die Sicherheitsbedrohungen für industrielle Steuersysteme sind einer dieser Fälle, bei denen besondere Aufmerksamkeit gefordert ist. Viele der grundlegenden Sicherheitsprobleme aus IT-Systemen treffen auch auf ICS-Umgebungen zu. Die größte Herausforderung bei der Übernahme von Best Practices besteht darin, dass diese Systeme in der Regel Software und Hardware für die direkte Steuerung physischer Anlagen oder Prozesse verwenden."

– CIS Controls Implementation Guide for Industrial Control Systems

MITRE ATT&CK FÜR ICS

CIS bietet eine priorisierte Liste mit Maßnahmen zur Systemhärtung. MITRE hingegen geht bei seinem Regelwerk vom Standpunkt der Angreifer aus.

MITRE ist eine gemeinnützige Organisation, die staatlich geförderte Forschungs- und Entwicklungszentren betreibt. Ein Schwerpunkt ist die Cybersicherheitsforschung zur Stärkung nationaler Abwehrmaßnahmen. MITRE hat bisher zwei ATT&CK-Regelwerke (Adversarial Tactics, Techniques, and Common Knowledge) entwickelt, in denen weit verbreitete Cyberangriffsmethoden aus realen Angriffen aufgeführt werden. Das eine Regelwerk bezieht sich auf IT-Umgebungen in Unternehmen, das andere auf industrielle Steuersysteme.

Die Organisation möchte damit aufzeigen, wie Angreifer Cyberinfrastrukturen infiltrieren und ausnutzen, damit Unternehmen effektive Abwehrmaßnahmen entwickeln können. Mit dem ATT&CK-Regelwerk für ICS können sie Angriffe auf ein industrielles Steuersystem simulieren und die notwendigen Cybersicherheitsmaßnahmen implementieren, um potenzielle Schäden zu verhindern oder zumindest zu minimieren.

„Die Befehlsausführung in industriellen Steuersystemen hat direkte physische Auswirkungen. Wird sie manipuliert, drohen körperliche Verletzungen für Menschen und schwerwiegende Schäden für die Umgebung. Weitere Folgen können finanzielle Schäden durch Produktionsausfall, Beeinträchtigung der Wirtschaft eines Landes und die Offenlegung proprietärer Daten sein. In ATT&CK für ICS beschreiben wir die Aktionen der Angreifer, die genau dies zum Ziel haben."

– MITRE

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Das National Institute of Standards and Technology (NIST) hat das Regelwerk *Framework for Improving Critical Infrastructure Cybersecurity* veröffentlicht. Es ist vor allem für kritische Infrastrukturen unentbehrlich, da es das einzige Werk mit präzisen Best Practices zu den spezifischen Herausforderungen in OT-Umgebungen ist.

Das Regelwerk wird zwar von einer Bundesbehörde verwaltet, aber es gilt nicht nur für Behörden. *NIST Special Publication (SP) 800-82* ist vor allem für Industrie-

unternehmen wichtig. Darin werden konkrete Anweisungen zum Schutz von SCADA-Systemen, verteilten Steuerungssystemen und speicherprogrammierbaren Steuerungen beschrieben. Mithilfe der Schritte zur Beschränkung des nicht autorisierten Zugriffs auf das ICS können die einzelnen Komponenten geschützt und die Verfügbarkeit bei Angriffen sichergestellt werden.

„Cybersicherheit spielt bei der nationalen und wirtschaftlichen Sicherheit eine wichtige Rolle. Das optionale NIST Cybersecurity Framework sollte in allen Unternehmen als grundlegende Sicherheitsmaßnahme implementiert werden. Die Einführung von Version 1.1 ist ein Muss für alle CEO."

– Wilbur Ross, U.S. Secretary of Commerce

AMERICAN WATER WORKS ASSOCIATION

Die American Water Works Association veröffentlichte 2013 *Process Control System Security Guidance for the Water Sector*, da die Branche ein Regelwerk mit detaillierten Anleitungen zum Schutz der Prozesssteuerungsnetzwerke vor Cyberangriffen benötigte. Der Leitfaden war auch eine Antwort auf das Dekret des US-Präsidenten (U.S. Presidential Executive Order 13636) *Improving Critical Infrastructure*, das ebenfalls 2013 erlassen worden war. Darin wurde NIST aufgefordert, die Entwicklung eines Regelwerks zur Minimierung der Cyberrisken für kritische Infrastrukturen zu initiieren.

„Mit dem AWWA-Leitfaden möchten wir Inhabern und Betreibern von Einrichtungen im Wasser-/Abwassersektor konsistente und wiederholbare Empfehlungen an die Hand geben, mit denen sie Schwachstellen für Cyberangriffe reduzieren können, wie es in ‚ANSI/ AWWA G430: Security Practices for Operations and Management' und EO 13636 gefordert wird. Das Projekt soll auch alle Führungskräfte in dieser Branche auf den Stellenwert aufmerksam machen, den der Schutz der Prozessleitsysteme hat."

– American Water Works Association

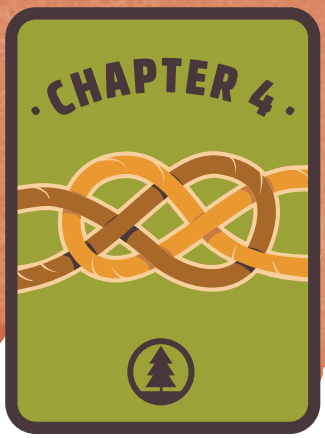
NERC CIP

Die North American Electric Reliability Corporation (NERC) ist eine internationale Regulierungsorganisation zur Minimierung der Risiken für Stromnetze. Sie entwickelt die Standards fortlaufend weiter und bietet Fortbildungen, Schulungen und Zertifizierungen für Beschäftigte der Branche an.

Im Gegensatz zu den anderen genannten Compliance-Verordnungen, die optional sind, ist die Einhaltung der NERC CIP-Anforderungen (Critical Infrastructure Protection, Schutz kritischer Infrastrukturen) in Stromnetzen und anderen kritischen Infrastrukturen verpflichtend. Die Compliance wird per Audit überprüft, daher fordern die Vorkehrungen den Energieunternehmen einen hohen Zeit-, Ressourcen- und Kostenaufwand ab.

„Das Electric Reliability Organization Enterprise ist ein Zusammenschluss der NERC und sechs regionaler Institutionen zum Schutz des nordamerikanischen Verbundnetzes. Unser Ziel ist die effektive und effiziente Risikominimierung für zuverlässige und sichere Stromnetze.“

– NERC



ÜBERLEBENS-TRAINING

Best Practices für ICS-Entscheidungsträger

Wenn Sie die Cyberbedrohungen für industrielle Steuersysteme kennen und wissen, mit welchen Standards und Regelwerken Sie Ihr ICS vor Cyberangriffen und Datenlecks schützen können, sind Sie bereit für die Implementierung einer Defense-in-Depth-Strategie mit grundlegenden Sicherheitsmaßnahmen.

DEFENSE-IN-DEPTH-ANSATZ

„Defense in Depth" ist ein Konzept, das wie die verschiedenen Verteidigungsebenen mittelalterlicher Burgen funktioniert. Damals schützten beispielsweise Burggraben, Brücken, Tore, interne und externe Mauern, auf denen sich Soldaten und Kanonen befanden, und Türme vor Angreifern.

Eine ähnliche Strategie kann auch zum Schutz von Netzwerken verwendet werden. Angreifer müssen dann erst mehrere Sicherheitsebenen überwinden, um zum Zentrum des Netzwerks vorzudringen, wo sie schwerwiegenden Schaden anrichten können. Dieser mehrschichtige Ansatz erschwert also den Zugang und bietet zudem Funktionen, mit denen ein Angriff erkannt und die Ausbreitung verhindert werden kann. Mithilfe von integrierten Redundanzen können Eindringlinge aufgespürt und daran gehindert werden, auf andere ICS-Bereiche zuzugreifen. So wird vermieden, dass sie sich lange unbemerkt im Netzwerk aufhalten.

Wie sieht ein Defense-in-Depth-Ansatz in einem industriellen Steuersystem aus? Stellen Sie sich Folgendes vor: Ihr Cloud-Netzwerk ist über Firewalls am Netzwerkperimeter mit den Produktionsstätten, Umspannwerken oder externen Anlagen verbunden. Diese sind wiederum mit einer weiteren DPI-Firewall (Deep Packet Inspection) verbunden, die vor die SPS geschaltet ist. Das ist ein Beispiel für Netzwerksegmentierung. Dieses Konzept werden wir in diesem Kapitel in Bezug auf die Defense-in-Depth-Strategie noch genauer betrachten.

Die Elemente einer Defense-in-Depth-Strategie[6]

Risikomanagement	» Bedrohungen identifizieren » Risiken definieren » Ressourceninventar pflegen
Cybersicherheitsarchitektur	» Standards/Empfehlungen » Richtlinien » Prozesse
Physische Schutzmaßnahmen	» Feldgeräte sind durch Schlösser gesichert » Zugangskontrollen an dem Kontrollzentrum » Videoüberwachung, Zugangskontrollen, Barrieren an externen Standorten
ICS-Netzwerkarchitektur	» Einheitliche Architekturzone » Demilitarisierte Zonen (DMZ) » Virtuelle LAN
Sicherheitslösung am ICS-Netzwerkperimeter	» Firewall/Einweg-Datendiode » Remote-Zugriff und -Authentifizierung » Jump-Server/Hosts
Hostbasierte Sicherheitslösung	» Patch- und Schwachstellenmanagement » Feldgeräte » Virtuelle Maschinen
Sicherheitsüberwachung	» Intrusion-Detection-Services » Protokollierung für Sicherheits-Audits » Überwachung von Sicherheitsvorfällen und -ereignissen
Anbietermanagement	» Lieferkettenmanagement » Managed Services/Auslagerung » Cloud-Services
Mitarbeiter	» Richtlinien » Prozesse » Schulungen und Sensibilisierung für das Thema

„Die Defense-in-Depth-Strategie stammt ursprünglich aus dem militärischen Bereich und bezieht sich auf Hindernisse, mit denen Eindringlinge aufgehalten werden sollten. So konnten ihr Vorgehen besser beobachtet und gleichzeitig angemessene Abwehrmaßnahmen ausgewählt und eingesetzt werden. In der Cybersicherheit bezieht es sich auf entsprechende Maßnahmen, mit denen Cyberkriminelle am Zugriff gehindert werden sollen, damit das betroffene Unternehmen den Angriff erkennen und abwehren kann. Das Ziel ist es, die Folgen eines Angriffs zu minimieren und einzudämmen.“

– U.S. Department of Homeland Security

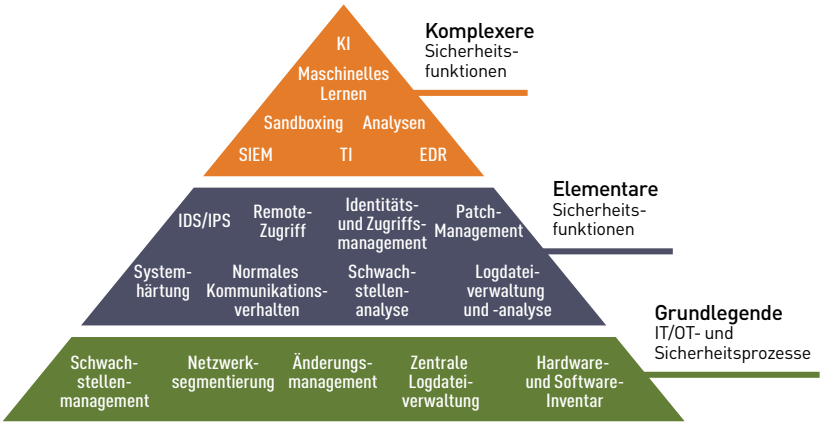
GRUNDLEGENDE SICHERHEITSMASSNAHMEN FÜR ICS

In Kapitel 3 haben sich einige Gemeinsamkeiten bei den branchenüblichen Standards von Organisationen wie IEC, NIST und CIS herauskristallisiert. Mit diesen Regelwerken müssen sich Unternehmen keine Sorgen mehr um die „grundlegenden Sicherheitsmaßnahmen" machen, wie Tripwire sie nennt.

WAS SIND GRUNDLEGENDE SICHERHEITSMASSNAHMEN?

Grundlegende Sicherheitsmaßnahmen sind einfache Cybersicherheitstechniken, wie Netzwerksegmentierung, Schwachstellen-, Konfigurations- und Änderungsmanagement, die den Kern eines erfolgreichen Cybersicherheitsprogramms bilden.

Nachdem Sie diese grundlegenden Sicherheitsmaßnahmen implementiert haben, können Sie sich den komplexeren Strategien widmen. Um die meisten Risiken zu minimieren und optimal von den Sicherheitslösungen zu profitieren, müssen Sie sicherstellen, dass diese grundlegenden Sicherheitsmaßnahmen implementiert und die Prozesse befolgt werden.



Die Pyramide der grundlegenden Sicherheitsmaßnahmen

DIE FÜNF WICHTIGSTEN GRUNDLEGENDEN SICHERHEITSMASSNAHMEN

Diese grundlegenden Sicherheitsmaßnahmen bilden die Best Practices für ICS-Cybersicherheit, die Sie unbedingt in Ihr Cybersicherheitsprogramm aufnehmen sollten. Sie werden in allen Standards und Regelwerken für industrielle Cybersicherheit aufgeführt, die wir zuvor genannt haben.

1 Hardware- und Software-Inventur

Es ist eigentlich selbstverständlich: Einer der ersten Schritte zum Schutz einer Umgebung ist die Inventur. Sie können schließlich nur schützen, was Sie kennen. Falls Sie noch keine besitzen, sollen Sie daher zuerst eine Inventarliste mit allen Hardware- und Software-Ressourcen erstellen. Diese Liste müssen Sie kontinuierlich pflegen. Die Technologien in den Automatisierungssystemen werden fortlaufend weiterentwickelt und auch die Bedrohungen verändern sich. Die Inventarliste ist daher ein Grundpfeiler des Cybersicherheitsprogramms und Voraussetzung, um die anderen grundlegenden Sicherheitsmaßnahmen für diese Ressourcen effektiv zu implementieren.

Am schnellsten lässt sich die Inventur mit einem Tool durchführen, das passiv Daten von jedem verbundenen Gerät in dem industriellen Steuersystem erfasst. Es kann nicht nur die im Netzwerk vorhandenen Geräte auflisten, sondern auch das Normalverhalten der Netzwerkkommunikation ermitteln, einschließlich des Industrieprotokolls. So können Sie dann Abweichungen erkennen. Dieses Normalverhalten bildet die Grundlage für einen Prozess für das Änderungsmanagement, da Sie Änderungen der Prozesskonfiguration erkennen und entsprechend reagieren können.

In einer Ölraffinerie ist beispielsweise das System zur Temperaturregelung die anfälligste Ressource. Ein Hacker greift über ein mit dem Internet verbundenes Gerät auf einen E-Mail-Server zu. Doch wie gelangt er vom E-Mail-Server zu seinem Ziel? Er wird von einem anfälligen, leicht zu hackenden Gerät zum nächsten springen und sich so einen Weg vom IT- zum OT-System bahnen. Aus diesem Grund benötigen ICS-Betreiber eine detaillierte Netzwerkübersicht, in der die Konfigurationen und Schwachstellen aller Geräte vermerkt sind. Mithilfe dieser Informationen können Sie sicherstellen, dass ein Conduit den Pfad des Hackers zu den sensibelsten Zonen und Ressourcen blockiert.

2 Änderungsmanagement

Wie wollen Sie die Integrität der industriellen Prozesse gewährleisten, wenn Sie keinen Prozess für das Änderungsmanagement implementiert haben? Ein solcher Prozess sollte nicht nur vorgeben, wie Änderungen dokumentiert, genehmigt, getestet und implementiert werden, sondern es sollten auch alle Änderungen von der Konfiguration einer Firewall oder eines Switches bis zum Upload eines neuen

Steuerungsprogramms in eine SPS erfasst werden. Idealerweise wird er mit einer Erkennungsfunktion kombiniert, die alle Änderungen hervorhebt. Dann wissen die Regelungstechniker, dass ihre Aktivitäten autorisierten Arbeitsaufträgen oder Änderungsanfragen zugeordnet werden.

Nicht autorisierte Konfigurationsänderungen oder autorisierte Änderungen, die am falschen Gerät vorgenommen werden – sei es versehentlich oder absichtlich – können schwerwiegende Folgen für den Betrieb haben. Dazu zählen nicht nur ungeplante Arbeiten zur Fehlerbehebung, sondern eventuell auch erhebliche Kosten durch Ausfallzeiten oder Rückrufe von Produkten.

Außerdem können Änderungen auch die gehärtete Konfiguration eines Geräts in Bezug auf Standards wie IEC 62443 beeinträchtigen. Das Gerät ist dann wesentlich anfälliger für Malware und andere Angriffe. Ein Beispiel dafür ist die Aktivierung eines USB-Ports, wenn im Standard die Deaktivierung aller USB-Ports vorgeschrieben ist. Um die Angriffsfläche zu verkleinern, müssen Sie wissen, ob eine Änderung die sichere Konfiguration eines Geräts gefährden würde.

3 Zentrale Logdateiverwaltung

Lösungen für die Logdateiverwaltung funktionieren ähnlich wie Data-Historian-Software. Damit lassen sich Prozessereignisse und Sensormesswerte für industrielle Prozesse erfassen und abrufen. Die Logdateien aller Geräte werden in einem zentralen Repository in dem ICS gespeichert.

Sie geben Aufschluss über den Cybersicherheitsstatus und die -prozesse im ICS und werden von Netzwerkgeräten (Switches, Router, Firewalls usw.), Betriebssystemen wie Windows und Linux, Anwendungen wie SCADA und MMS sowie Controllern und DCS erstellt. Auch Lösungen für den Remote-Zugriff, VPN und Authentifizierungssysteme wie Active Directory speichern Logdateien.

Die Dateien enthalten diverse Informationen zum Betrieb des Systems oder Geräts, zum Beispiel Angaben zum Ausfall der Stromversorgung oder zu Cybersicherheitsereignissen wie fehlgeschlagenen Anmeldeversuchen. Diese Daten dürfen nicht ignoriert werden, denn sie eignen sich für eine vorausschauende Wartung, sodass Ausfallzeiten und ungeplante Arbeiten vermieden werden können.

4 Schwachstellenmanagement

Bei dem Schwachstellenmanagement wird ermittelt, welche öffentlich bekannten Sicherheitslücken oder Schwachstellen, auch CVEs (Common Vulnerabilities and Exposures) genannt, im Netzwerk vorhanden sind. Die meisten Angriffe mit Ransomware und Malware lassen sich auf bekannte CVEs zurückführen, die nicht rechtzeitig gepatcht oder behoben wurden.

Allerdings können die meisten älteren ICS-Anlagen in OT-Umgebungen die Analysen herkömmlicher Technologien für das Schwachstellenmanagement nicht

verarbeiten. Je weiter Sie sich von den Unternehmensnetzwerken auf Ebene 4 und 5 entfernen und den Produktionsstätten auf Ebene 0 und 1 nähern, desto weniger Ressourcen werden für aktive Scans infrage kommen. MMS, Data-Historian-Server und Engineering-Workstations auf den Ebenen 2, 3 und 3.5 (DMZ) eignen sich in der Regel besser dafür, da diese Geräte auf herkömmlicher IT-Technologie basieren.

Solange Sie die Ebene berücksichtigen, werden die meisten ICS-Ressourcen von einer umfassenden Schwachstellenanalyse profitieren. Tools für das Schwachstellenmanagement stufen Sicherheitslücken gemäß dem Risiko ein, damit Sie besser erkennen, welche zuerst behoben werden müssen.

5 Netzwerkzonen und -segmentierung

Bei der Netzwerksegmentierung wird ein Netzwerk in einzelne Zonen unterteilt. Diese setzen sich aus Gruppen von Systemen mit einem ähnlichen Risikoprofil und einer ähnlichen Funktion zusammen. Ein Conduit bildet die Grenze zwischen den Zonen und blockiert ein- und ausgehende Kommunikation, sofern sie in den Firewalls oder Zugriffskontrolllisten nicht ausdrücklich genehmigt wurde.

Wird ein Gerät wie eine MMS von Ransomware manipuliert, sind nur Geräte mit ähnlichen Funktionen in derselben Zone gefährdet, da der Conduit die Ausbreitung der Ransomware verhindert. Dies ist ein wichtiger Faktor der Defense-in-Depth-Strategie.

In dem IEC 62443-Standard wird für industrielle Steuersysteme die Netzwerksegmentierung mit Zonen und Conduits empfohlen.

Zone: *Eine Gruppe logischer oder physischer Ressourcen, die ähnliche Sicherheitsanforderungen in Bezug auf ihre Bedeutung und Verfügbarkeit aufweisen*

Conduit: *Bildet die Grenze zwischen Zonen und blockiert ein- und ausgehende Kommunikation, sofern sie nicht ausdrücklich zugelassen wurde. Er bildet einen Netzwerkpfad zwischen den Zonen, in dem Sicherheitsmaßnahmen netzwerkbasierte Angriffe abwehren, andere Netzwerksysteme schützen und die Integrität und Vertraulichkeit des Netzwerk-Datenverkehrs gewährleisten können.*

> ***TIPP VON TRIPWIRE:*** Die Überwachung und Konfiguration von Conduits ist in der Regel wesentlich günstiger als das Upgrade jedes einzelnen Geräts oder Computers in einer Zone, um die jeweiligen Anforderungen zu erfüllen.

PASSIVE oder AKTIVE SCANS UND AGENTBASIERTE oder AGENTLOSE ÜBERWACHUNG

In einigen Netzwerkbereichen müssen passive Scans durchgeführt werden, um die Störung älterer sensibler Systeme zu vermeiden. Bei passiven Scans werden der Netzwerkverkehr überwacht und Geräte per Fingerprinting-Verfahren erfasst.

Auf diese Weise können ein Ressourceninventar erstellt, Kommunikationsmuster ermittelt, Netzwerkeverbindungen erfasst und Schwachstellen erkannt werden.

Bei aktiven Scans hingegen werden Abfragen direkt an ein bestimmtes Gerät gesendet, um weitere Informationen zu erhalten. Die Kombination aus aktiven und passiven Scans liefert die zuverlässigsten Daten. Doch auch bei den passiven Scans gibt es Einschränkungen. So haben beispielsweise manche Netzwerk-Switches nicht genügend Ports, um einen für die Spiegelung bereitzustellen.

Eventuell reicht auch die Leistung eines Switches nicht aus, sodass er die Spiegelung nicht parallel zu den anderen Aufgaben ausführen kann. Prüfen Sie daher sorgfältig, ob die Switch-Fabric die Spiegelung unterstützt und die Anforderungen zur Datenerfassung für Cybersicherheit und Ressourceninventar erfüllt werden können.

> ***TIPP VON TRIPWIRE:*** **Wenn Sie aktiv Daten von einem Gerät abfragen, sollten Sie sicherstellen, dass die Scan-Lösung dieselbe Sprache wie die Ressource unterstützt (zum Beispiel Modbus TCP oder Ethernet/IP CIP). Andernfalls riskieren Sie eine Betriebsstörung, wenn die Verbindung zum Gerät unterbrochen wird.**

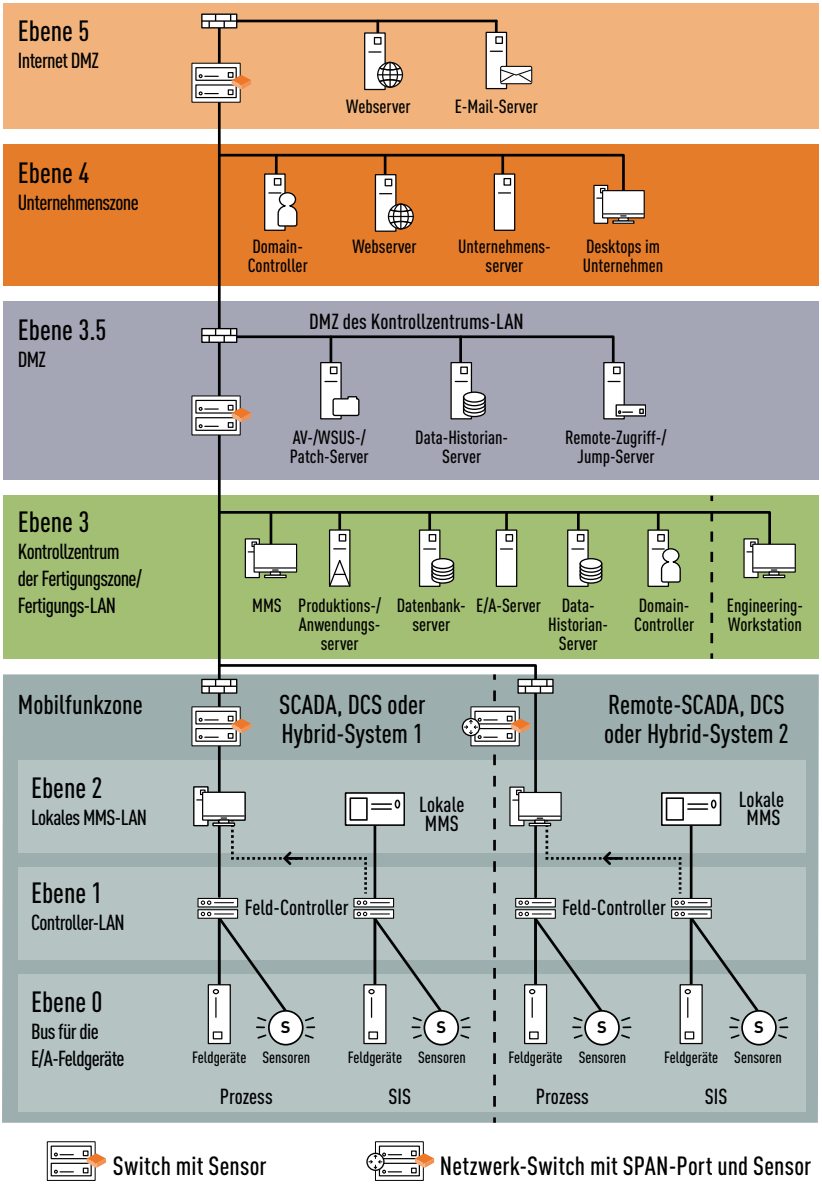
Außerdem müssen Sie wissen, in welchen Fällen Sie Agents für die Datenerfassung einsetzen sollten. Agents liefern umfassende Informationen, aber sie werden lokal auf dem Gerät installiert. Vergewissern Sie sich daher vorab, dass Ihr Automatisierungsanbieter die Installation von Drittanbieter-Agents auf den MMS oder Engineering-Workstations unterstützt.

Mit agentlosen Scans können Sie Daten von Geräten erfassen, auf die Sie authentifizierten Zugriff haben. Es gibt zahlreiche Möglichkeiten, Daten agentlos zu erfassen. Wählen Sie am besten eine Lösung, die sowohl OT- als auch IT-Protokolle unterstützt und daher die größte Flexibilität bietet. Es empfiehlt sich eine strategische Kombination aus agentlosen und agentbasierten Scans.

RISIKOMANAGEMENT HAT PRIORITÄT

Lassen Sie sich von dem Arbeitsaufwand, der für die Implementierung aller fünf grundlegenden Sicherheitsmaßnahmen in das Netzwerk erforderlich ist, nicht abschrecken. Jeder fängt mal klein an – und zwar in der Regel damit, sich einen Überblick über die Geräte im Netzwerk und deren Kommunikationsmuster, Schwachstellenstatus, Konfigurationen und Logdateien zu verschaffen.

Standard-Purdue-Modell für eine industrielle Netzwerkarchitektur



TIPP VON TRIPWIRE:

Ebene 0–2: Passive Scans sowie aktive und passive agentlose präzise Protokoll-Scans

Ebene 3–5: Aktive agentlose Scans

BEREIT FÜR DAS ABENTEUER

Ihr Aktionsplan für die ICS-Cybersicherheit

Die Auseinandersetzung mit den relevanten Regelwerken und grundlegenden Sicherheitsmaßnahmen für das ICS ist nur der erste Schritt. Wesentlich schwieriger kann es werden, Entscheidungsträger im Unternehmen von der Notwendigkeit dieser Sicherheitsmaßnahmen zu überzeugen.

WIE KÖNNEN SIE BESSER AUF DIE BEDEUTUNG DER CYBERSICHERHEIT AUFMERKSAM MACHEN?

68 Prozent der ICS-Experten sind der Ansicht, dass sich die Unternehmensführung erst nach einem Sicherheitsvorfall davon überzeugen ließe, in angemessene Maßnahmen zu investieren. Doch mit einer proaktiven Herangehensweise und effektiven Gesprächen mit den wichtigsten Stakeholdern müssen Sie nicht erst auf den Ernstfall warten.

> ***TIPP VON TRIPWIRE:*** Wenn Sie mit Ihrem CISO und/oder CTO über ICS-Sicherheitsmaßnahmen sprechen, stellen Sie das Risikomanagement in den Mittelpunkt (siehe Kapitel 4).

TIPPS ZUR ÜBERZEUGUNG DER UNTERNEHMENSFÜHRUNG

Erstellen Sie einen Zeitplan für die Sicherheitsmaßnahmen

Eine Möglichkeit, um die Verbesserung des Cybersicherheitsstatus anzustoßen, ist die Erstellung eines Entwicklungszeitplans, den Sie den wichtigsten Stakeholdern vorlegen können. Idealerweise vermerken Sie darin alle Programme, die Sie initiieren oder optimieren müssen, um die fünf grundlegenden Sicherheitsmaßnahmen zu implementieren.

ERGEBNISSE DER TRIPWIRE-UMFRAGE ZU ICS

Tripwire hat eine Umfrage unter 263 IT- und OT-Sicherheitsexperten durchgeführt. Alle Befragten waren direkt für die Sicherheit der ICS in Energie-, Fertigungs-, Chemie-, Damm-, Wasser-, Lebensmittel-, Auto- oder Transportunternehmen mit mehr als 100 Mitarbeitern verantwortlich.

» 88 Prozent machen sich Sorgen um ICS-Cybersicherheitsangriffe. Die größten Bedenken hatten die Fachkräfte im Energie- und Öl-/Gassektor.

» Industrieunternehmen haben Bedenken über die physischen Folgen von Cyberangriffen geäußert. Die Stilllegung des Betriebs und Ausfallzeiten werden am meisten gefürchtet. Zwei Drittel (66 Prozent) sind der Ansicht, dass ein ICS-Angriff katastrophale Folgen haben könnte.

» Beinahe zwei Drittel (61 Prozent) vermuten, dass sie in den nächsten zehn Jahren Opfer eines ICS-Angriffs werden könnten.

» Nur 12 Prozent waren äußerst zuversichtlich, dass sie Beeinträchtigungen des Betriebs durch einen Cyberangriff vermeiden können.

» 77 Prozent haben in den letzten zwei Jahren in Cybersicherheitsmaßnahmen für ihre Industrieumgebung investiert.

» 50 Prozent gaben an, dass ihr Unternehmen nicht ausreichend in ICS-Cybersicherheitsmaßnahmen investiert.

» Davon waren 68 Prozent der Ansicht, dass es erst zu einem schwerwiegenden Angriff kommen muss, bevor mehr investiert wird.

» Nur etwa die Hälfte (52 Prozent) haben mehr als 70 Prozent der Ressourcen in einer Inventarliste erfasst.

» Etwa ein Drittel der Unternehmen hat weder einen Vergleichswert für normales Verhalten der OT-Geräte noch eine zentrale Lösung für die Logdateiverwaltung.

» Nur ein Drittel (34 Prozent) hat eine Sicherheitsbewertung für industrielle Umgebungen durchführen lassen, aber mehr als die Hälfte (55 Prozent) zieht sie in Betracht.

» Die meisten Unternehmen (79 Prozent) gaben an, dass sie ihre Teams in Bezug auf OT-Sicherheit besser schulen müssen.

2 Lassen Sie eine Cybersicherheitsbewertung für Ihr ICS durchführen

Wenn Sie der Unternehmensführung einen Überblick über den Zeitaufwand und die Kosten zur Implementierung von Sicherheitslösungen bieten möchten, empfiehlt es sich, zuerst eine Sicherheitsbewertung für das industrielle Steuersystem erstellen zu lassen. Beauftragen Sie damit einen vertrauenswürdigen Drittanbieter. Mithilfe der gewonnenen Daten können Sie dem CISO das aktuelle Risikoprofil in Bezug auf Sicherheit, Produktivität und Qualität präsentieren. In Rahmen dieser Bewertung kann auch eine Bedrohungsanalyse erstellt werden, in der die Wahrscheinlichkeit eines Cyberangriffs und die potenziellen Folgen für den Betrieb aufgezeigt werden.

3 Unterstützen Sie proaktiv die Zusammenarbeit der IT- und OT-Teams

Fördern Sie die interne Zusammenarbeit durch bereichsübergreifende Teams, denen sowohl IT- als auch OT-Experten angehören. Legen Sie spezielle Rollen und den Aufgabenbereich für Sicherheitsinitiativen fest und berücksichtigen Sie dabei, dass IT- und OT-Teams in der Regel unterschiedliche Sichtweisen haben. Das erfordert viel Fingerspitzengefühl bei der Kommunikation. Auch interne Workshops können dabei helfen, einen gemeinsamen Plan zu entwickeln.

4 Wählen Sie einen Standard als Leitfaden aus

Ein Industriestandard wie IEC 62443 kann äußerst hilfreich sein, wenn Sie der Unternehmensführung vermitteln möchten, welche Bedeutung die Branche ICS-Sicherheitsmaßnahmen beimisst. Anhand der darin gegebenen Empfehlungen zur Netzwerkarchitektur, -konfiguration und -überwachung können sich die wichtigsten Stakeholder in Ihrem Unternehmen einen besseren Eindruck von den Prioritäten verschaffen.

LEITFADEN FÜR KÄUFER: ICS-LÖSUNGEN FÜR GRUNDLEGENDE SICHERHEITSMASSNAHMEN

Nachdem Sie wissen, wie Sie mit den grundlegenden Sicherheitsmaßnahmen Ihr industrielles Steuersystem schützen, müssen Sie die passenden Tools auswählen. Einige Lösungen decken mehrere Sicherheitsmaßnahmen ab. Manche wurden speziell für industrielle Umgebungen entwickelt, mit anderen wiederum lässt sich problemlos die Kluft zwischen IT und OT überbrücken. Auf diese Funktionen sollten Sie bei der Auswahl der Lösungen für die fünf grundlegenden Sicherheitsmaßnahmen aus Kapitel 4 achten:

» Für die Hardware- und Software-Inventur

Wählen Sie eine Lösung, die passiv die Echtzeitverbindungen

„Es ist unglaublich wichtig, dass IT- und OT-Netzwerktechniker die Anforderungen und Strategien des jeweils anderen Teams verstehen, da sie sich erheblich unterscheiden. ... Wenn sich die Teams austauschen und die Unterschiede besprechen, bevor Sicherheitsrichtlinien implementiert werden, ist die IT-/OT-Konvergenz einfacher zu stemmen.“

– Scott Kornblue, Field Application Engineer bei Belden

des gesamten ICS-Netzwerks erfasst und eine Inventarliste aller verbundenen Geräte erstellt. In ICS-Umgebungen müssen Sie an diese Informationen gelangen, ohne den Betrieb zu stören. Achten Sie daher darauf, dass die Lösung nicht nur passiv Daten erfassen kann, sondern auch aktiv über die industriellen Protokolle (wie Modbus TCP, Profinet und Ethernet/IP) kommuniziert, um die Ressourcen zu erkennen und ein Inventar zu erstellen.

» Für das Änderungsmanagement

Ein effektives Änderungsmanagement ist nur mit einer strikten Überwachung der Dateiintegrität (File Integrity Monitoring, FIM) und SCM (Security Configuration Management) möglich. Tools mit diesen Funktionen geben einen umfassenden Überblick über den Status der Systeme und zeichnen alle Abweichungen vom Normalverhalten auf. Diese grundlegenden Prozesse sind die beste Abwehrmaßnahme gegen Eindringlinge in das Netzwerk. Mit SCM können Sie zudem auch Abweichungen von Compliance-Richtlinien und -Vorschriften erfassen.

» Für die zentrale Logdateiverwaltung

Wählen Sie ein Tool für die Logdateiverwaltung, das die Daten vor der Übertragung an das SIEM verarbeitet. Diese Tools helfen auch bei der Ressourceninventur, da sie passiv Geräte erkennen, die mit der ICS-Umgebung verbunden werden. Sie müssen in Ihrem zentralen Logdatei-Repository nachvollziehen können, welche Daten die Geräte generieren. Nur mithilfe dieser Informationen können Sie die Leistung optimieren und sicherstellen, dass das Steuersystem voll funktionsfähig bleibt. Das Tool für die Logdateiverwaltung agiert damit als Cyber-Data-Historian für das ICS.

» Für das Schwachstellenmanagement

Bei der Auswahl eines Tools für das Schwachstellenmanagement in industriellen Umgebungen ist äußerste Sorgfalt geboten. In den meisten Fällen wird ein Tool benötigt, dass für Schwachstellenanalysen sowohl agentlose als auch agentbasierte Techniken verwendet. Das ist besonders hilfreich, wenn einige Geräte in der Umgebung nur gelegentlich verbunden werden. Achten Sie auch darauf, dass die Risikoeinschätzung detailliert genug ist, damit Sie wissen, welche Probleme zuerst behoben werden müssen. Wenn Sie zahlreiche Warnmeldungen zu kritischen Sicherheitslücken ohne Priorisierung erhalten, ist das Tool nicht effektiv.

» Für Netzwerkzonen und -segmentierung

Die wichtigste Anweisung aus ISA 99/IEC 62443 ist die Erstellung separater Zonen und Conduits. Sie sollten beispielsweise eine Firewall verwenden, die die industriellen Protokolle erkennt und als Conduit zwischen den Zonen agieren kann. Zonen sind Gruppen von Geräten und sollen die Auswirkungen von Cyberangriffen für das gesamte industrielle Netzwerk minimieren.

TIPP VON TRIPWIRE: Vollständige Transparenz lässt sich vermutlich nur erreichen, wenn Sie Rohdaten auf verschiedene Weise verarbeiten können. Suchen Sie nach Lösungen, die nicht nur aktiv oder passiv Daten erfassen, sondern auch Hybrid- und integrierte Funktionen bieten. „Hybrid" bedeutet, dass die Lösung Daten mit Anwendungen von Drittanbietern austauschen kann, die diese bereits erfasst haben. „Integriert" bezieht sich darauf, dass die Netzwerk-Hardware über eingebettete Sensoren oder Virtualisierungsfunktionen zur Datenerfassung genutzt werden kann.

LÖSUNGEN VON TRIPWIRE FÜR DIE GRUNDLEGENDEN SICHERHEITSMASSNAHMEN

Die meisten gängigen Bedrohungen für industrielle Steuersysteme lassen sich durch die grundlegenden Sicherheitsmaßnahmen und die damit verbundenen Prozesse abwehren. Das liegt daran, dass die meisten Angreifer den Weg des geringsten Widerstandes gehen und daher häufig bekannte Faktoren wie nicht überwachte Systeme, nicht gepatchte Schwachstellen, flache Netzwerke und falsch konfigurierte Ressourcen ausnutzen. Die industriellen Lösungen von Tripwire wurden speziell für die genannten fünf grundlegenden Sicherheitsmaßnahmen entwickelt:

Tripwire® Enterprise für Industrieanlagen erkennt Konfigurationsänderungen auf diversen Geräten und kann die Konfiguration mit den Vorgaben bestimmter Cybersicherheitsstandards abgleichen.

Tripwire Industrial Visibility bietet ICS-Betreibern einen umfassenden Überblick über die Geräte und Aktivitäten im Netzwerk. Dank des Änderungsmanagements, der Ereignisprotokollierung und den Bedrohungsmodellen können Sie Ihre sensiblen Ressourcen vor Angriffen schützen.

Tripwire Log Center™ erfasst, analysiert und korreliert Logdaten von Netzwerkgeräten, Controllern, SCADA-Systemen, Servern und Anwendungen.

Tofino Xenon Security Appliance für industrielle Umgebungen schützt Ihre Daten, da das Netzwerk in einzelne Sicherheitszonen segmentiert wird.

TRANSPARENZ IST EIN MUSS

ICS-Betreiber müssen einen umfassenden Überblick über die Kommunikation zwischen dem industriellen Steuersystem und dem IT-Netzwerk haben, einschließlich der Remote-Zugriffe über VPN und Mobilfunk. Außerdem müssen sie das Ressourceninventar erfassen und verwalten, die Kommunikation zwischen Ressourcen (wie MMS und SPS) über industrielle Protokolle nachvollziehen und die Konfigurationen abrufen können. Mithilfe dieser Informationen können sie ein akkurates Diagramm der Netzwerktopologie erstellen, das Normalverhalten ermitteln und potenzielle Schwachstellen erkennen.

DER TRIPWIRE-ANSATZ FÜR ICS-SICHERHEIT

Tripwire wandelt Rohdaten industrieller Steuersysteme in praxistaugliche Informationen um. Unsere Tools decken die gesamten IT- und OT-Umgebungen ab. Dank der zahlreichen Technologieintegrationen und anbieterunabhängigen Lösungen können ICS-Betreiber das Automatisierungssystem auswählen, das am besten zu ihrem Unternehmen passt.

Tripwire bietet mit diversen eng verzahnten Produkten umfassende Transparenz. Auf diese Weise können ICS-Cyberbedrohungen und Sicherheitsverletzungen erkannt und zukünftige Vorfälle durch die Ermittlung und Priorisierung der Risiken verhindert werden. Dank der kontinuierlichen Überwachung ist das Sicherheitsprogramm immer auf dem neuesten Stand.

Viele Industrieunternehmen beschäftigen nicht die nötigen Fachkräfte, um strikte ICS-Sicherheitsmaßnahmen zu implementieren und zu verwalten. Tripwire bietet verschiedene Dienstleistungen, die speziell auf industrielle Umgebungen zugeschnitten sind, zum Beispiel Sicherheitsbewertungen, Penetrationstests und Unterstützung durch einen Techniker vor Ort.

Die Hälfte der Fortune 500-Unternehmen vertraut auf unsere Lösungen. Tripwire und sein Mutterunternehmen Belden bieten seit über 20 Jahren führende Cybersicherheitslösungen an und unterstützen schon seit mehr als 100 Jahren die größten Industrieunternehmen weltweit.

WICHTIGSTE PUNKTE: TRANSPARENZ, SICHERHEITSMASSNAHMEN, KONTINUIERLICHE ÜBERWACHUNG

Bei der Wahl der Lösungen für Ihr Cybersicherheitsprogramm sollten Sie vor allem diese drei Punkte beachten:

1. **Transparenz** *Sie müssen genau wissen, was in Ihrem Netzwerk vor sich geht, und daher eine Inventarliste der gesamten Hardware und Software erstellen. Sie brauchen Antworten auf die Fragen, mit wem die Geräte kommunizieren, ob die Konfigurationen geändert wurden, welche Schwachstellen das Netzwerk und die Geräte betreffen und welche Informationen die Logdateien enthalten. Der erste Schritt ist die Erstellung einer Inventarliste aller Ressourcen, doch für vollständige Transparenz können zahlreiche andere Methoden zur Ermittlung des Risikoprofils industrieller Netzwerke eingesetzt werden.*

2. **Sicherheitsmaßnahmen** *Anschließend können die erforderlichen Sicherheitsmaßnahmen für die diversen Ebenen (nach dem Purdue-Modell)*

implementiert werden. Zwei der Sicherheitsmaßnahmen sind obligatorisch: 1) Netzwerksegmentierung und 2) Gerätehärtung.

3 **Kontinuierliche Überwachung** *Wenn Sie alle Komponenten kennen, überwachen Sie sie. Dazu sind mehrere parallel ausgeführte Prozesse erforderlich: Schwachstellenmanagement, SCM (Security Configuration Management), Logdateiverwaltung und Überwachung der Dateiintegrität.*

HÄUFIG GESTELLTE FRAGEN ZUR CYBERSICHERHEIT IN industriellen Steuersystemen

Frage: Welche Geräte in meinem ICS stellen eine potenzielle Gefahr dar?

Antwort: In der Vergangenheit hätte ein Angreifer sich durch Social Engineering Zugang zur Produktionsstätte verschafft, um die Anlagen eines Steuersystems physisch zu manipulieren. Eventuell hätte er auch einen mit Malware infizierten USB-Stick auf dem Parkplatz platziert und darauf gehofft, dass ein neugieriger Mitarbeiter ihn verwendet. Doch im Zeitalter des IIoT stellen alle verbundenen Geräte ohne entsprechende Sicherheitsmaßnahmen eine potenzielle Gefahr dar.

Frage: Wie kann ich sicheren Remote-Zugriff auf das ICS anbieten?

Antwort: Die Kontrolle des Remote-Zugriffs ist ein wichtiger Aspekt zum Schutz des ICS. Sie sollten alle Remote-Verbindungen zum Netzwerk (wie den Zugriff von Anbietern über Telefonmodems, VPN und Mobilfunk) nachvollziehen und dokumentieren. Industrieunternehmen können auch mit entsprechenden Lösungen die Multi-Faktor-Authentifizierung für externe Mitarbeiter einrichten und alle Aktivitäten protokollieren.

Frage: Wo soll ich am besten mit der Risikominimierung für die physischen Prozesse ansetzen?

Antwort: Die Erstellung und Pflege einer akkuraten Inventarliste aller Komponenten des industriellen Netzwerks ist ein guter Anfang. Sie können schließlich nur schützen, was Sie kennen. Doch Transparenz sollte sich nicht nur auf das Ressourceninventar beziehen, sondern auch andere wichtige Elemente umfassen, wie Konfigurationsänderungen, Ausgangswerte für die Kommunikationsmuster der Geräte, Änderungen der Netzwerktopologie und Daten aus den Diagnose-Logdateien. So können Sie potenzielle Störungen der industriellen Prozesse schnell erkennen und verhindern.

Frage: Muss ich auch Phishing-Angriffe berücksichtigen?

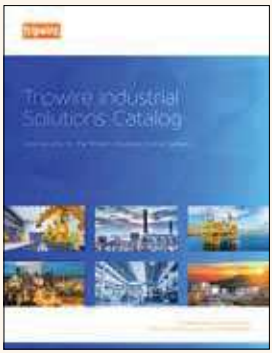
Antwort: Ja. Phishing ist eine gängige Angriffsmethode, um sich über E-Mails, Anrufe oder SMS Zugriff auf das IT-Netzwerk eines Unternehmens oder den Laptop eines Regelungstechnikers zu verschaffen. Über dieses Einfallstor können sich die Angreifer dann im industriellen Netzwerk ausbreiten. Die Sensibilisierung und Schulung der Mitarbeiter in Bezug auf Phishing-Techniken ist ein wichtiger Teil der Defense-in-Depth-Strategie.

Frage: Sollte ich ein Regelwerk für die Cybersicherheit berücksichtigen, auch wenn mein ICS keinen Branchenstandards unterliegt?

Antwort: Auch wenn diese Regelwerke nicht obligatorisch sind, helfen sie doch bei der Entwicklung und Verwaltung eines Cybersicherheitsprogramms und der Risikominimierung im Falle von Cyberangriffen. Allerdings erfordert die Einhaltung dieser Vorgaben Investitionen in Fachkräfte und Technologien und diese Änderungen lassen sich nicht sofort vornehmen. Verwenden Sie die Regelwerke daher zuerst als Leitfaden und implementieren Sie sie schrittweise. Überstürzen Sie nichts, sondern planen Sie die einzelnen Schritte sorgfältig.

Frage: Muss ich auch die Cloud berücksichtigen?

Antwort: Unbedingt. Die Verbreitung der Cloud ist nicht mehr aufzuhalten und einige industrielle Anwendungen wurden bereits ausgelagert, aber es ist noch Vorsicht geboten. Die Einführung cloudbasierter Lösungen für industrielle Netzwerke ist nur noch eine Frage der Zeit und es werden immer schneller immer mehr IT-Technologien und -Lösungen verwendet und angepasst. SCADA-Lösungen und einige Überwachungslösungen bekannter Automatisierungsanbieter wurden bereits in die Cloud migriert. Die Kostenvorteile werden die Einführung weiter vorantreiben. Vertrauen Sie nicht darauf, dass Cloud-Lösungen sicher sind. Übernehmen Sie die grundlegenden Sicherheitsmaßnahmen auch für die Cloud und wenden Sie dieselben Prinzipien wie für die anderen Technologien an.



Sie möchten gern mehr erfahren?

Dann laden Sie den Katalog von Tripwire mit Lösungen für die Industriebranche herunter.

tripwire.me/TISC

AUTOREN

Gary DiFazio

Gary DiFazio ist Strategic Marketing Director for Industrial Cybersecurity bei Tripwire. Er hat langjährige Erfahrung im Technologiebereich mit Systemen, Anwendungen, Netzwerken und Cybersicherheit in diversen Branchen wie Telekommunikation, Fertigung, Einzelhandel, Behörden, Finanzwesen, Energie und Logistik/Distribution. Nach der Übernahme von Tripwire durch Belden im Jahr 2015 war DiFazio Mitglied eines Teams, das industrielle Cybersicherheitslösungen sowohl für Kunden von Tripwire als auch von Belden vermarktete. Er hat einen Bachelor of Science in Industrial Engineering der Clemson University.

Kristen Poulos

Kristen Poulos ist Vice President und General Manager für die Industrie-Cybersicherheitssparte von Belden, einschließlich Produkten, Services und Lösungen unter den Marken Tripwire und Hirschmann. Zuvor leitete sie die globale Marketingabteilung für die Enterprise-Sparte von Belden, nachdem sie in mehreren Führungspositionen in Marketing- und Produktbereichen gearbeitet hatte. Sie mag die schnelllebige und kooperative Cybersicherheits-Community, die versucht, durch Technologiepartnerschaften und -integrationen den Bedrohungen immer einen Schritt voraus zu sein.

Gabe Authier

Gabe Authier ist Director of Product Management bei Tripwire. Er hat über 20 Jahre Erfahrung in den Bereichen Produktmanagement und Informationstechnologie sowie Zertifizierungen für agile Softwareentwicklung und pragmatisches Marketing. Authier hat einen BS in Systems Engineering der University of Arizona und einen Executive MBA der University of Oregon.

Keith Blodorn

Keith Blodorn ist Director of Product Management für ProSoft Technology, ein Tochterunternehmen von Belden. Er hat mehr als 20 Jahre in der industriellen Automatisierung gearbeitet und verschiedene Techniker- und Produktmanagementpositionen inne. Wie die meisten OT-Experten begeistert ihn neue Technologie – solange sie mindestens zehn Jahre in der Praxis getestet wurde.

QUELLEN

[1] Aberdeen Group, Asset Performance Management: Blazing a Better Path to Operational Excellence, November 2017.

[2] Department of Homeland Security National Cybersecurity and Communications Integration Center (NCCIC) and Industrial Control Systems Cyber Emergency Response Team (ICS–CERT), Recommended Practice: Improving Industrial Cyber Security with Defense In-Depth Strategies, 2016.

[3] Department of Homeland Security. (2019). Critical Infrastructure Sectors. [online] Verfügbar unter: https://www.dhs.gov/cisa/critical-infrastructure-sectors.

[4] Morgan, S. (2019). Cybersecurity labor crunch to hit 3.5 million unfilled jobs by 2021. [online] CSO Online. Verfügbar unter: https://www.csoonline.com/article/3200024/cybersecurity-labor-crunch-to-hit-35-million-unfilled-jobs-by-2021.html.

[5] Verizon Data Breach Investigations Report. (2019). Manufacturing Data Breaches & Cybersecurity. [online] Verfügbar unter: https://enterprise.verizon.com/resources/reports/dbir/2019/manufacturing/.

[6] Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies. (2016). U.S. Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team.

ÜBER TRIPWIRE

Tripwire, Inc. schützt führende Organisationen auf der ganzen Welt vor Sicherheitsverletzungen und Cyberangriffen – und weil Hacker immer raffinierter werden, entwickeln auch wir unsere Technologien seit mehr als 20 Jahren ständig weiter. Unsere Lösungen sind sowohl On-Premises als auch in der Cloud verfügbar, wo sie Ihre digitale Infrastruktur schützen sowie Bedrohungen aufdecken und abwehren, ohne den Geschäftsbetrieb oder die Produktivität zu beeinträchtigen.

Weitere Informationen erhalten Sie unter www.tripwire.com.

ÜBER BELDEN

Belden, Inc. ist ein Marktführer für hochwertige und hochverfügbare Datenübertragungslösungen in der Industriebranche. Sein umfassendes Portfolio beinhaltet Produkte für die Netzwerkinfrastruktur und industrielle Cybersicherheit in der Industrie-, Unternehmens- und Medienbranche. Das Unternehmen wurde 1902 gegründet, hat seinen Hauptsitz in St. Louis und Fertigungsstätten in Nord- und Südamerika, Europa und Asien.

Weitere Informationen erhalten Sie unter www.belden.com.

ÜBER PROSOFT TECHNOLOGY

Das industrielle Internet der Dinge (IIoT) ist inzwischen in aller Munde und alle möchten neue Produktionsdaten für die Entscheidungsfindung erfassen. Bei ProSoft Technology konzentrieren wir uns schon seit der Entwicklung unseres ersten Kommunikationsmoduls im Jahr 1990 auf solche Verbindungen und achten dabei auf die Zuverlässigkeit, Sicherheit und Flexibilität, die industrielle Anwendungen erfordern.

Weitere Informationen erhalten Sie unter www.prosoft-technology.com.

DURCH DEN DSCHUNGEL DER INDUSTRIELLEN CYBERSICHERHEIT

Nahezu jeder Bereich unseres täglichen Lebens ist von dem störungsfreien Betrieb industrieller Steuersysteme (ICS) abhängig. ICS-Anlagen sind immer stärker vernetzt, doch damit werden sie auch anfälliger. Die meisten Industrieunternehmen sind nicht ausreichend auf die digitale Konvergenz der IT- und OT-Umgebungen vorbereitet. ICS-Betreiber brauchen ein zuverlässiges Cybersicherheitsprogramm – und das möglichst schnell. Deshalb stellen wir in diesem Leitfaden Anleitungen zur Implementierung von Industriestandards und grundlegenden Sicherheitsmaßnahmen, zur Annäherung der IT- und OT-Umgebung, zur Überzeugung der Unternehmensführung und die idealen Tools für diese Zwecke vor.