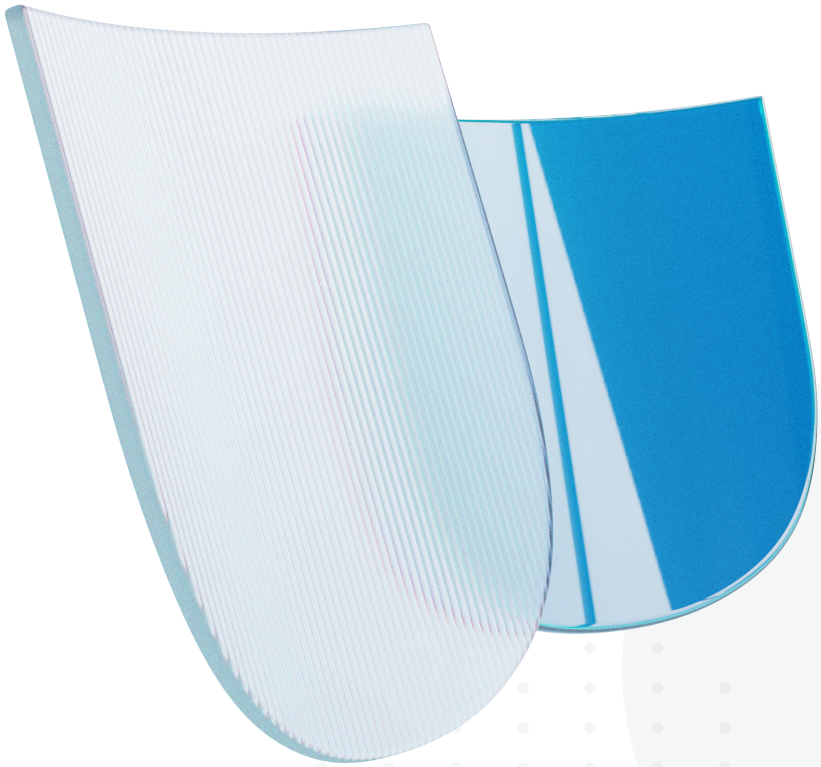
AUF DEM WEG ZUR SMART FACTORY MIT (I)OT SECURITY

Inhaltsverzeichnis



Abstract

Um Effizienz und Flexibilität der Produktion zu steigern, führen traditionelle Produktionsbetriebe derzeit verstärkt Systeme zur Produktionsoptimierung ein. Produktionsmanagementsysteme (MES), IoT-Anwendungen oder digitale Zwillinge stellen mit ihren Service-orientierten Kommunikationsanforderungen jedoch auch neue Anforderungen an die OT-Cybersecurity. Modernisieren heißt in diesem Zusammenhang nicht, ein paar Updates durchzuführen, sondern disruptive, neue Technologien und Prozesse einzuführen und die Produktion während dieser Transformation am Laufen zu halten, Mitarbeiter und ihre Skill-Sets auf diesem Weg mitzunehmen und gleichzeitig Cybersecurity nicht zu vernachlässigen.

Das Whitepaper beleuchtet Cyberrisiken und entsprechende Sicherheitsmaßnahmen in herkömmlichen, weniger vernetzten Produktionsumgebungen und vergleicht sie mit Risiken und Abwehrmaßnahmen in der *Smart Factory*.

Schließlich geht es um die Herausforderung, bestehende, oft über Jahrzehnte gewachsenen Produktionsanlagen bei laufender Fertigung zu modernisieren, ohne die Cybersicherheit aus den Augen zu verlieren. Am Beispiel einer Smart-Factory-Migrationsarchitektur wird aufgezeigt, wie dieser Übergang sicher gelingen kann.

Die „alte“ Welt

In der klassischen Produktion sind die Elemente der Produktionspyramide (siehe Abbildung) oft als zentrale, monolithische Großanlage implementiert und Produkte werden häufig an einem Standort produziert, auch wenn dies in mehreren Schritten und Gebäudeteilen stattfindet. Die Vernetzung dieser Anlagen beschränkt sich (zumindest in der diskreten Fertigung) meist auf SCADA Systeme, die „isolierte“ Maschineninseln steuern und für die Materialwirtschaft mit ERP-Systemen in der (lokalen) IT kommunizieren, auch wenn viele dieser Anlagen für Wartungszugriffe in Covid-Zeiten oder externe Datenanalyse mittlerweile mit einer Internetverbindung nachgerüstet wurden.

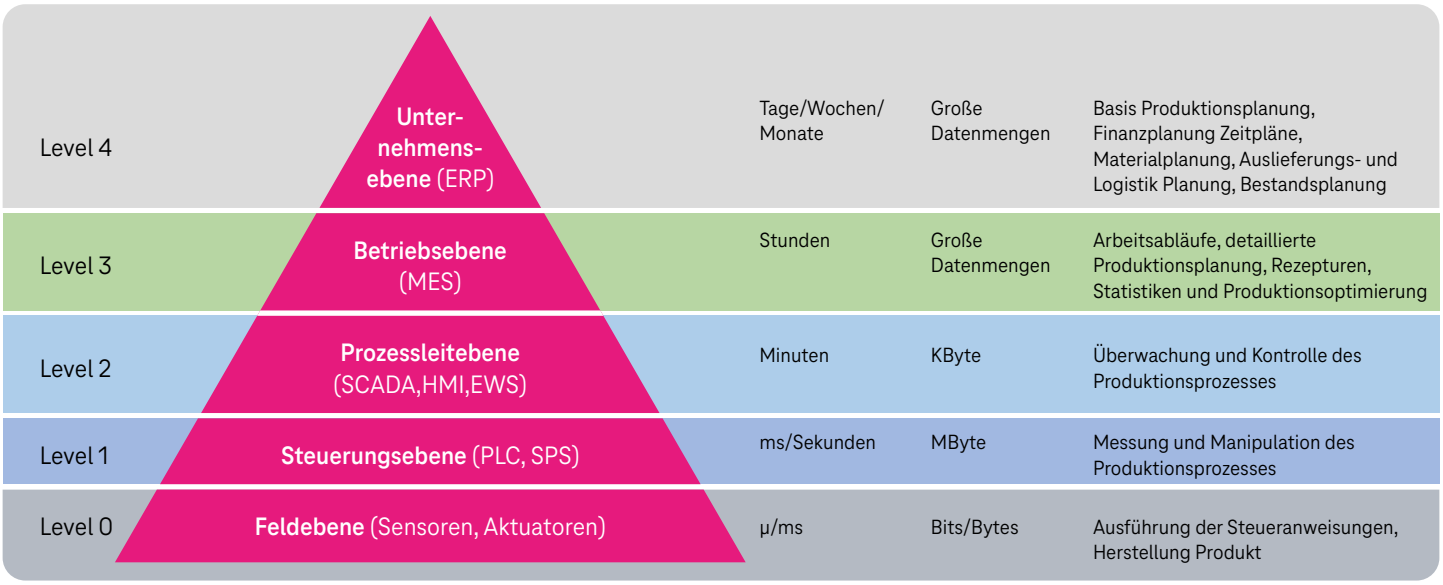


Abbildung: Klassische Automatisierungspyramide

Cyberrisikoprofil: Disruption

Die Risikobetrachtung im Umfeld der klassischen Produktion basiert stark auf unserem derzeitigen kollektiven Gedächtnis, also den Erfahrungen, die durch die Analyse vergangener Cyberangriffe gesammelt wurden. Diese so genannten Tactics Techniques and Procedures (TTPs) sind zum Beispiel in der MITRE ATT&CK® Matrix for ICS dokumentiert:

Initial Access	Execution	Persis-tence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
12 techniques	9 techniques	6 techniques	2 techniques	6 techniques	5 techniques	7 techniques	10 techniques	3 techniques	13 techniques	5 techniques	12 techniques
Drive-by Compromise	Change Operating Mode	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Command-Line Interface	Modify Programm	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Execution through API	Module Firmware		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	Spoof Reporting Message	Denial of View
External Remote Services	Graphical User Interface	Project File Infection		Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Detect Operating Mode		Block Reporting Mesage	Unauthorized Command Message	Loss of Availability
Remote Services	Modify Controller Tasking	Valid Accounts		Rootkit	Wireless Sniffing	Program Download	I/O Image		Block Serial COM		Loss of Control
Replication Through Removable Media	Native API			Spoof Reporting Message		Remote Services	Monitor Process State		Data Destruction		Loss of Productivity and Revenue
Rogue Master	Scripting					Valid Accounts	Point & Tag Identification		Denial of Service		Loss of Protection
Spearfishing Attachment	User Execution						Programm upload		Device Restart/ Shutdown		Loss of Safety
Supply Chain Compromise							Screen Capture		Manipulate I/O Image		Loss of View
Transient Cyber Asset							Wireless Sniffing		Modify Alarm Settings		Manipulation of Control
Wireless Compromise									Rootkit		Manipulation of View
									Service Stop		Theft of Operational Information
									System Firmware		

Abbildung: MITRE ATT&CK® Matrix für ICS

Die Spalten der MITRE ATT&CK® Matrix beschreiben die verschiedenen „Angriffsphasen“, die ein Angreifer erfolgreich durchlaufen muss, um sein letztendliches Ziel zur erreichen. Versteht man die letzte Spalte „Impact“ als das eigentliche Ziel des Angreifers – Welche Auswirkungen sollen erreicht werden? – so erkennt man hier einen Fokus auf die Störung des OT-Prozesses. Und so ist es wenig überraschend, dass das in diesem Kontext wahrscheinlichste Bedrohungsszenario die Verschlüsselung eines produktionsnahen Servers durch Ransomware ist. Dies hängt sicherlich auch damit zusammen, dass in solchen Umgebungen häufig veraltete Windows-Systeme mit nur geringen Endpoint-Protection-Maßnahmen ihren Dienst verrichten. Der Grund hierfür ist nicht die Nachlässigkeit der Betreiber, sondern die Inkompatibilität typischer IT-Endpoint-Schutzmaßnahmen mit den herstellerspezifischen Anwendungen auf diesen Systemen.

Typische Infektionswege sind verbundene IT-Systeme, welche durch Phishing-Attacken übernommen wurden, unsichere Remote-Zugänge, infizierte Engineering Workstations, Laptops oder mobile Datenträger. Stark zunehmend sind auch Lieferkettenangriffe, bei denen sich der Angreifer zum Beispiel nach einem erfolgreichen Angriff auf die Software eines Lieferanten Zugang zu dessen B2B-Kunden verschafft[1].

[1] Referenz Solarwinds

Schutzmaßnahmen im Kontext der „alten“ Welt

Im Zusammenhang mit diesen Bedrohungsszenarien haben sich in den vergangenen Jahren erfolgreiche Verteidigungsstrategien entwickelt. Umfangreiche Standards wie zum Beispiel IEC 62443 bilden die Leitplanken zur Umsetzung eines umfänglichen Cybersicherheitsprogramms für Komponentenhersteller, Integratoren und Betreiber von Produktionsanlagen. Die vollständige Umsetzung, speziell in einem Brownfield-Szenario, bei laufender Produktion, ist jedoch aufwendig und meist ein langwieriges Projekt. Muss man sich zunächst auf die wichtigsten Elemente eines solchen Schutzprogramms beschränken, sollten folgende fünf Themen priorisiert werden[2]:

Abbildung: Die fünf Säulen eines erfolgreichen ICS Cybersicherheitsprogramms

Incident Response Plan: Der Incident Resonse Plan sollte am Anfang des Security-Programms stehen, sodass zum Beispiel die Auswahl, Funktionen und Architektur des Angriffserkennungssystems zu seinen Anforderungen passen und nicht nachträglich angepasst werden müssen. Im IT-Umfeld liegt der Fokus der Reaktion typischerweise auf der Identifikation des Angreifers und der Eindämmung und Bereinigung von betroffenen Assets oder Daten. Im OT-Umfeld liegt die Priorität hingegen auf der Root-Cause-Analyse und der Aufrechterhaltung des Betriebs bzw. der Rückkehr zum sicheren und stabilen Betrieb.

Der Incident Response Plan sollte Szenarien behandeln, die auf Bedrohungsinformationen (Threat Intel) und Konsequenzen basieren. Szenarien sind besser dazu geeignet, ein gemeinsames Verständnis zwischen unterschiedlichen Fachbereichen und Entscheidern herzustellen, als detaillierte technische Beschreibungen. Außerdem vereint der Ansatz mit Bedrohungsinformationen und Konsequenzen zwei „Werkzeuge“, denen Prozessingenieure und Cybersecurityfachleute vertrauen[3]. Das macht es einfacher, beide Parteien an einen Tisch zu bekommen – zum Beispiel für eine gemeinsame Tabletop Übung (TTX). Szenarien benachbarter Branchen mit einzubeziehen kann helfen, sich proaktiv und fokussiert auf Situationen vorzubereiten, die man bisher nicht auf dem „Radar“ hatte, die aber dennoch relevant sind.

Ein OT-orientierter Incident Resonse Plan sollte folgende Elemente enthalten[4]:

- Eine Liste der wichtigsten Betriebsstätten und Produktionseinheiten (die „Kronjuwelen“)
- Die Top-Szenarien, die ein Risiko für das Unternehmen und den OT-Prozess darstellen
- Die Kernfragen, die in diesen Szenarien zeitnah beantwortet werden müssen, z.B. bezüglich operativer Sicherheit und Cyber Sicherheit, behördlichen Anforderungen, Kommunikation und finanziellen Aspekten
- Strategien, wie die notwendigen Informationen und Daten zur Beantwortung dieser Fragen und eine Root-Cause-Analyse erhoben, gespeichert und abgesichert werden können
- Rollen und Verantwortlichkeiten von Personen in der Organisation und bei Partnern

Auf dem Papier läßt sich ein solches OT-Security Resilienz Programm einfach umsetzten. Und längst wird Cybersecurity in der OT nicht mehr nur über das IT-Budget finanziert, sondern über Stakeholder aus der OT-Prozessverfügbarkeit oder der Betriebssicherheit (Safety) gesponsort. Geld wäre also da. Die Praxis hat aber gezeigt, das Unternehmen zur erfolgreichen Umsetzung von Cybersecurity im Produktionsumfeld einen Lernprozess (über mehrere Jahre) durchlaufen und einen gewissen Reifegrad erreichen müssen.

[2] https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls/
[3] https://www.weforum.org/agenda/2021/05/cybersecurity-safety-engineering/
[4] https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls/

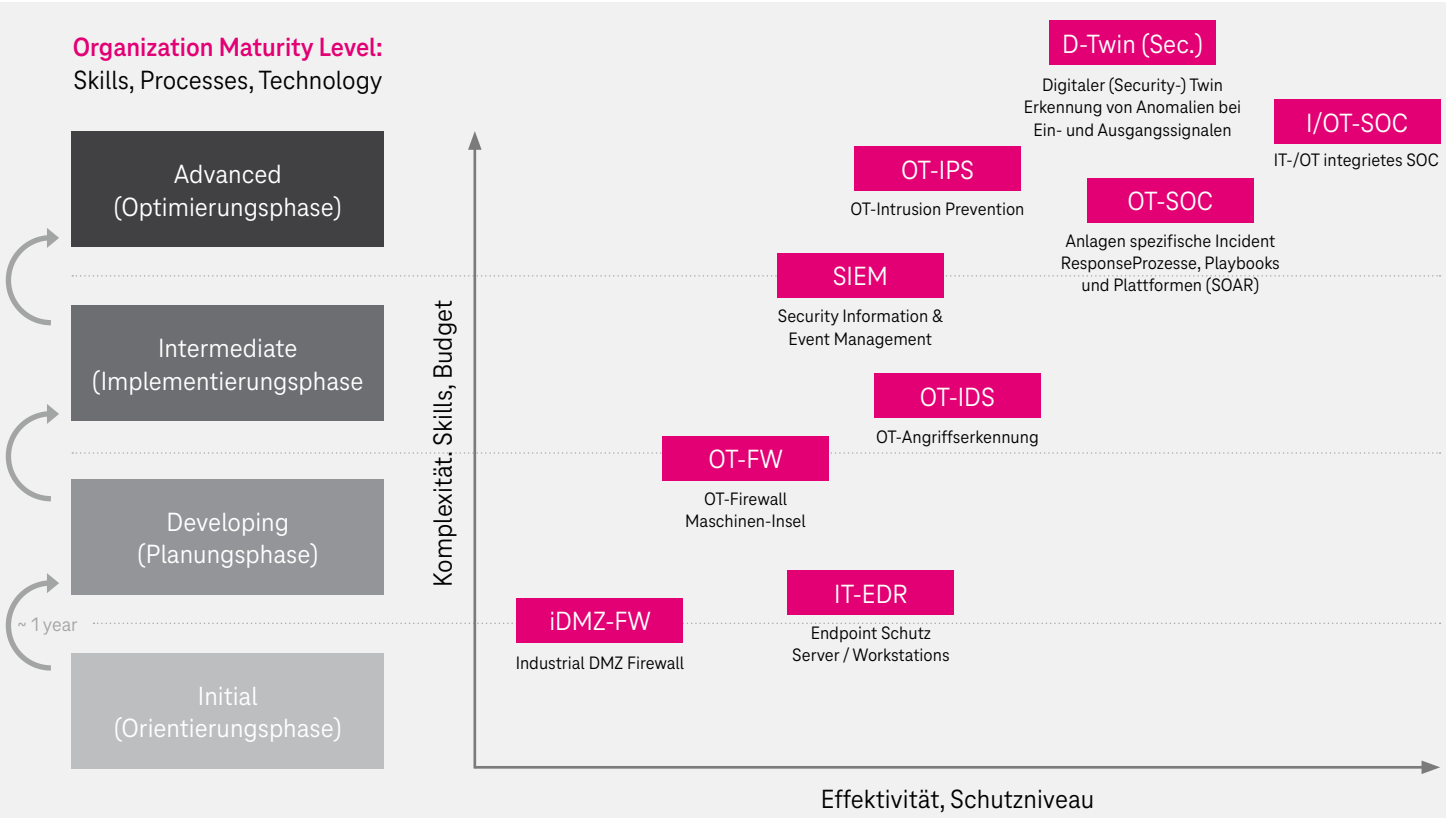


Abbildung: OT-Security Reifegradmodell

Wie in der Abbildung dargestellt, kann man am Anfang mit dem Vorhandenen Know-how und der IT-Firewall relativ einfach eine erste Segmentierung zwischen IT und OT implementieren, was das Schutzniveau moderat verbessert. Bis man jedoch in der Lage ist, ein integriertes OT-/IT-SOC zu betreiben, mit komplexer Technik, Korrelationsregeln, domainübergreifenden Playbooks und den zugehörigen Response-Prozessen, wird sich der Reifegrad deutlich erhöhen müssen.

Wehrhafte Netzwerkarchitektur: Denkt man an eine Netzwerkarchitektur, die man verteidigen kann, fallen einem sofort Aspekte wie Netzwerktopologie, Absicherung des Perimeters (falls noch vorhanden), Segmentierung, Zugriffskontrollen und ähnliche Aspekte ein. Was oft weniger Beachtung in diesem Bereich findet, ist die Verfügbarkeit von für die Verteidigung wichtigen Informationen (zum Beispiel über kritische Assets), die die Voraussetzung sind, um im Incident-Response-Fall überhaupt sinnvoll reagieren zu können. Dazu gehören insbesondere auch historische und aktuelle Ereignismeldungen innerhalb der OT-Infrastruktur, die helfen, die im vorangegangenen Abschnitt erwähnten „Kernfragen" des Incident Resonse Plans zu beantworten.

Deshalb muss eine wehrhafte Architektur das Sammeln von Informationen und den effizienten Zugriff auf diese Informationen unterstützen. In der IT denkt man hier sofort an System-Logs und SIEM-Systeme. In der OT kann es effizienter sein, Anomalie- oder Angriffserkennung über spezielle EDR-Agenten und spezialisierte, passive Netzsensoren zu implementieren. Im Idealfall kann man beides nutzen.

Moderne Netzwerktechnologien wie speziell für OT-Infrastrukturen optimierte Firewall- oder Switch-Systeme, oder Software-Defined-Networking-Ansätze (SDN) können helfen, diese Anforderungen umzusetzen – auch „Legacy" Anlagen können hiervon profitieren.

Angriffserkennung: Die dritte Säule einer robusten Verteidigungsstrategie ist die Schaffung von Transparenz darüber, was in meinem OT-Netzwerk passiert. Dies hilft nicht nur bei der frühzeitigen Erkennung von Cyberangriffen, sondern oft auch bei der Identifikation von Betriebsstörungen und deren Ursachen. Also eine Cybersicherheitstechnik, die auch dann nützlich ist, wenn gerade kein Angriff stattfindet. Aber eben auch zur Cyberabwehr, als zwingende Voraussetzung für die bisher besprochenen Themen Incident Response Plan und wehrhafte Netzarchitektur.

Die konkrete, effektive Umsetzung einer solchen Erkennung hängt stark von den Gegebenheiten der zu überwachenden Infrastruktur ab: Topologie und Segmentierungsgrad der Netze, Art der Endpunkte, Alter der verwendeten Betriebssysteme, Anwendungen und Hardware, verfügbare Netzwerkbandbreiten für Monitoring-Daten, erschließbare Datenquellen, Datenschutzanforderungen, vorhandene Schnittstellen, Knowhow und Prozesse.

Drei typische Datenquellen sind:

- **Log-Feeds:**
  Meist nur von moderneren, performanteren Geräten wie zum Beispiel: Switche, Firewalls, Windows ...
- **EDR-Lösungen:**
  Typischerweise auf Windows Hosts. Erfordert oft Ausnahmeregeln, um Fehlalarme zu vermeiden, ist dann aber sehr effektiv
- **Passive Sniffer mit Anomalie-Erkennungsalgorithmen:**
  Einfach zu installieren und effektiv

Auch ein „alter Bekannter“ ist dieser Tage wieder im Gespräch, wenn es um die Detektion von schwer zu erkennenden Angriffen (wie zum Beispiel Lieferketten-Angriffen) und deren Analyse geht: **Der Honeypot.**

Ein System, welches eigentlich keine Aufgabe im Kontext der Produktion im Netzwerk hat und von daher eigentlich nie kontaktiert werden dürfte. Sucht ein Angreifer aber nach Opfern und scannt das Netz, spielt der Honeypot ihm ein Produktionssystem vor und versucht, möglichst viele Daten über den Angreifer und sein Vorgehen zu erhalten. Wer dies einmal selbst ausprobieren möchte, sollte sich den **T-Pot**[5] ansehen. Mit so genannten „high-interactive“ Honeypots ist allerdings Vorsicht geboten. Platziert man diese in sensiblen Netzen und weisen diese dann eine Schwachstelle auf, könnte die Schutzmaßnahme als Angriffswerkzeug missbraucht werden.

Fernwartung: Ein großes Problem der Remote-Zugänge ist, dass provisorische Ad-hoc-Lösungen, die meist ein geringes Sicherheitsniveau aufweisen, zum Beispiel in Zeiten einer Pandemie schnell implementiert sind und dann gedankenlos weiter genutzt werden. Industrietaugliche Lösungen setzen Eckpfeiler wie Multi-Faktor-Authentifizierung, granulare Zugriffsrechte, Isolation des Fernwartungsziels während des Fernzugriffs, revisionssichere und datenschutzkonforme Aufzeichnung der Tätigkeiten und vertrauenswürdige Kryptographie um. Sie zu implementieren bedeutet eine monetäre Investition und Migrationsaufwand für Betreiber und Partner. Und anschließend müssen die alten, provisorischen Zugänge auch abgebaut werden, da gerade solche vergessenen Zugänge in der Vergangenheit als ein erfolgreicher Angriffspfad für den initialen Zugang genutzt wurden.

Risk Based Vulnerability Management: Risikobasiertes Vulnerability Management in der OT akzeptiert die Tatsache, dass es Systeme geben wird, die zu ihrer Lebzeit (10 - 100 Jahre) nicht gepatcht werden. Das können zum Beispiel Windows-Embedded-basierte Bedienpanels an der LKW-Wage sein oder Steuerungskomponenten von Herstellern, die es am Markt schon nicht mehr gibt. Bei diesen Systemen müssen andere Maßnahmen zur Risikominderung ergriffen werden. Dies sind zum Beispiel:

- Zugriffe auf diese Systeme führen über einen patchbaren Kontrollpunkt in einer überwachten Zone (iDMZ)
- Netzwerkdienste, die verwundbar sind, aber nicht benötigt werden, am Kontrollpunkt filtern
- Prozess-Whitelisting auf dem Zielsystem, falls möglich
- Virtuelles Patchen: Moderne Firewall-Systeme mit OT Awareness und robuster Erkennung von OT-spezifischen Angriffsmustern können gezielt Datenpakete, welche spezielle Schwachstellen ausnutzen, blockieren

[5] https://github.com/telekom-security/tpotce

Die „neue“ Welt

In der „neuen“ Welt lösen verteilte, virtualisierte Systeme die ehemals monolithischen Großanlagen ab. Teile des Produktionsprozesses werden als Service in der Cloud gehostet.

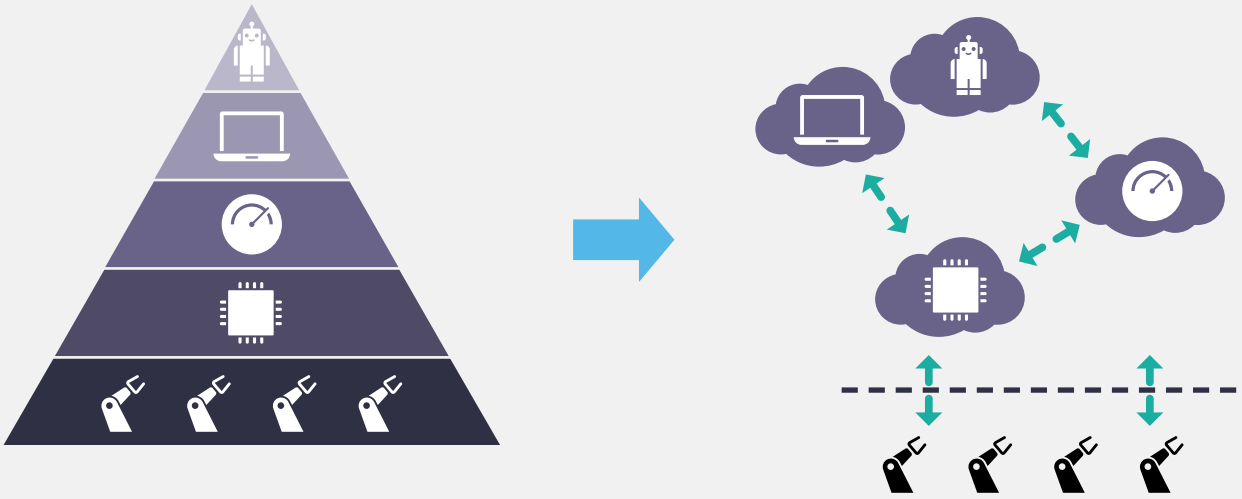


Abbildung: Auflösung der monolithischen Modelle hin zu verteilten Strukturen

Die Kopplung dieser Services (MES, Digital Twin, AI Analytics, ERP) erfolgt in diesen Modellen über einen Manufacturing Service Bus. Dieser Bus arbeitet als eine Art Dolmetscher zwischen den verteilten Systemen und verbindet sich mit den cyberphysischen Systemen (CPS) der Produktionsanlage unter Verwendung von Standardprotokollen wie zum Beispiel OPC-UA[6], MQTT, HTTP oder REST.

[6] OPC-UA ist eigentlich eine Architektur

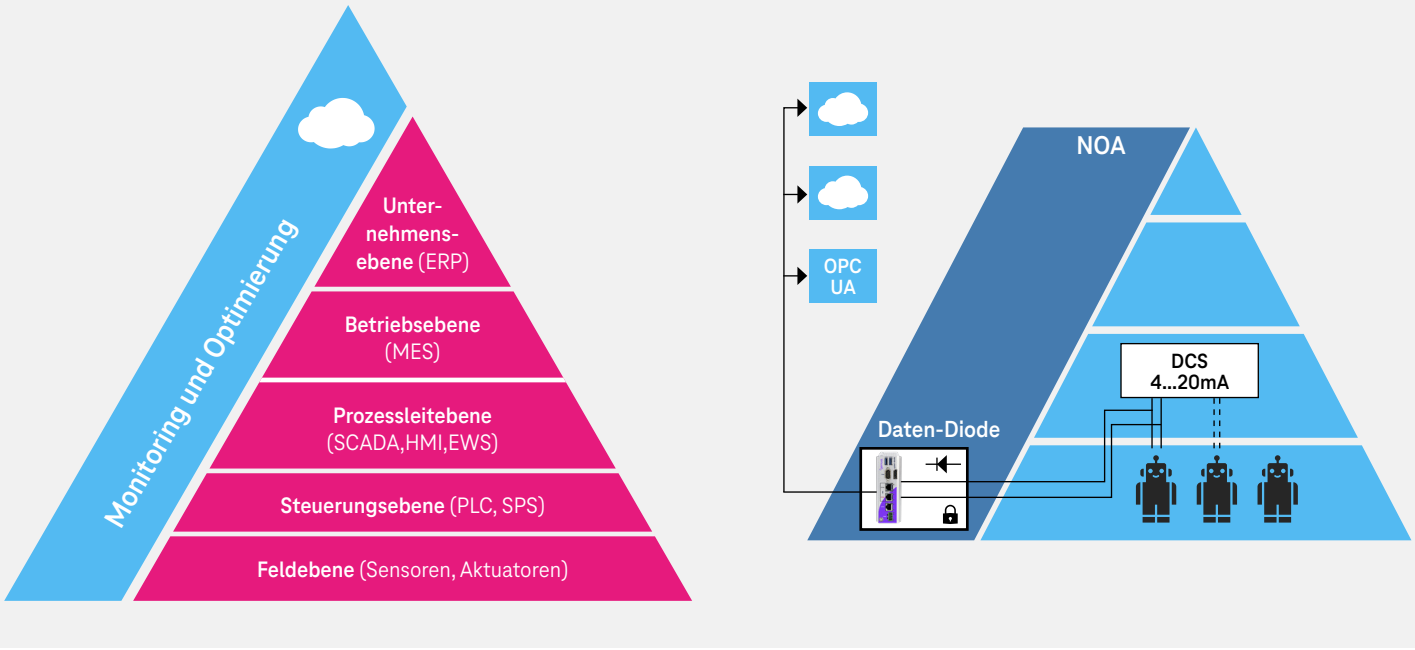


Abbildung: Erweiterung der Automatisierungspyramide

Dies führt zu einer Erweiterung der klassischen Automatisierungspyramide (siehe Abbildung). Die einzelnen Ebenen werden lateral um eine Monitoring- und Optimierungsschicht erweitert und kommunizieren direkt mit dem jeweiligen Cloud-Service. Was zunächst wie eine Umgehung der Segmentierung zwischen den Ebenen aussieht, ist aus Architektursicht als logische Verbindung zu verstehen. **In der technischen Umsetzung muss die Segmentierung in der Cloud fortgeführt und überwacht werden.**

Die rechte Seite der Abbildung illustriert die technische Implementierung eines solchen Modells. Die Daten der Ventile werden über eine so genannte Datendiode und ein Sicherheits-Gateway per OPC-UA-Protokoll[7] an die Analyseanwendung in der Cloud weitergleitet. Die Verwendung der OPC-UA-Architektur und -Protokolle erlaubt, im Gegensatz zu älteren, „traditionellen" Industrieprotokollen, unter anderem eine zertifikatsbasierte Absicherung der Maschinenidentitäten und -daten. Hier ersetzt die abgesicherte Maschinenidentität den „traditionellen" Netzwerk-Perimeter vor Ort.

[7] OPC-UA ist ebenfalls ein Architekturmodell, beschreibt aber auch Kommunikationsprotokolle in diesem Modell

Cyberrisikoprofil: Daten- und Kontrollverlust

Mit der Ausweitung der Service-orientierten Produktion (SOP) auf verteilte (Cloud-)Systeme, der einhergehenden Zunahme an externen Schnittstellen (netzwerk- und applikationsseitig), dem Einsatz von Virtualisierungssoftware, der Zunahme von Administrationsschnittstellen und der Menge der entstehenden und transportierten sensiblen Daten, vergrößert sich die potenzielle Angriffsfläche der Produktion für Cyberkriminelle und politische Akteure.

Neben dem weiterhin bestehenden Risiko der Produktionsstörung durch Angreifer verändert sich das Risikoprofil verstärkt in Richtung Daten- und Kontrollverlust durch externe Systeme oder Akteure. Wenn detaillierte Prozessdaten und Maschinenparameter zur Analyse an eine externe KI gesendet werden (Open-Loop-Szenario), müssen diese vor Diebstahl und unautorisierter Manipulation geschützt werden. Typischerweise entsteht aber auch eine Abhängigkeit bezüglich der Verfügbarkeit dieser (extern gespeicherten) Daten oder Funktionen. So ist es im Allgemeinen nicht sofort kritisch, wenn der Zugriff auf eine standortübergreifende Prozessoptimierungsanwendung in der Cloud für eine Stunden ausfällt, spätestens aber nach einem halben Tag dürfte die Situation in den meisten Fällen ernsthafte Auswirkungen mit sich bringen. Diese Zusammenhänge müssen vor der Migration in einer Risikoanalyse betrachtet werden.

Die nächste Stufe der Cloudifizierung der Produktion sind die Closed-Loop-Szenarien. Hier fließen nicht nur Daten in eine Richtung (von der Produktion in die Cloud), sondern Steuerungsfunktionen, bis hinunter auf die Maschinenebene, werden in die Cloud ausgelagert. Wir haben also eine bidirektionale Kommunikation mit Kontrollrechten auf Produktionssystem-Ebene. Neben dem offensichtlichen Risiko, dass potenzielle Angreifer die Kontrolle über diese Steuerfunktionen, zum Beispiel über eine Schwachstelle in der Cloud-, Netzwerk- oder Anwendungsplattform, übernehmen, existieren in diesem Fall auch erhöhte Anforderungen an Verfügbarkeit und Antwortzeiten. Das hängt natürlich davon ab, was gesteuert wird: Ein chemischer Prozess, die Herstellung eines Turnschuhs oder die Verteilung von Energie im Verteilernetzwerk. Hier können Edge-Architektur-Ansätze helfen, die Verfügbarkeit zu verbessern und besonders sensible Daten zu schützen.

Beispiel: Evil PLC

Um die vielleicht nicht so offensichtlichen Zusammenhänge einmal zu verdeutlichen, soll das Beispiel des „Evil PLCs“[8] betrachtet werden. Das Besondere an diesem Beispiel ist, dass eine Schwachstelle in der Firmware eines PLCs (Programmable Logic Controller) der Ausgangspunkt für die Übernahme der gesamten Cloud-basierten Remote-Management-Plattform ist, wodurch die Kontrolle über alle Steuerungssysteme möglich wird. Das Überraschende also: Der PLC und nicht die Cloud verursacht das Problem. Auch wenn dafür eine weitere Schwachstelle in der Remote-Management-Software selbst notwendig ist.

Der Angriff funktionierte vereinfacht folgendermaßen:

Schritt 1: Durch Schwachstellen in der PLC-Software[9] erlangt ein Angreifer Zugriff und Schreibrechte auf eine Datei auf dem PLC. Genauer genommen auf die WebVisu.html-Datei, eine Webseite, die für die Administration der PLC-Konfiguration genutzt werden kann. Hier fügt der Angreifer nun etwas ausführbaren JavaScript-Code hinzu und zieht sich zurück. Der PLC verrichtet seine Arbeit auch mit dieser Modifikation ohne Beeinträchtigung weiter.

Schritt 2: Zu einem beliebigen späteren Zeitpunkt greift ein Administrator für Wartungsarbeiten über die Cloud-basierte Remote-Zugriffsplattform auf den PLC zu. Hierbei ruft die Plattform zur Anzeige des Bedienpanels des PLCS die besagte WebVisu.html-Datei auf und der vom Angreifer angefügte JavaScript-Code wird mit den Rechten des angemeldeten Administrators ausgeführt.

Schritt 3: Da es sich bei dem Cloud-basierten Admin-Portal um eine Webanwendung mit einer weiteren Schwachstelle[11] handelt, kann der angefügte JavaScript-Code still und leise im Hintergrund einen neuen Admin User anlegen, der nur dem Angreifer bekannt ist (zumindest so lange, bis das hoffentlich regelmäßig durchgeführte Account Screening den neuen Account entdeckt und entfernt).

Schritt 4: Der Angreifer greift aus dem Internet regelmäßig auf das Remote-Management-Portal seines Opfers zu, um zu prüfen, ob sein Account schon angelegt wurde. Ist das der Fall, hat er nicht nur auf den PLC mit dem zuvor hinzugefügten Skript Zugriff, sondern, über einen offiziellen Admin Account, Fernzugriff auf die Plattform, sowie auf alle Produktionssysteme, die über diese Software weltweit administriert werden.

Zusammenfassend kann man sagen, der initiale Angriffsvektor ist eine Schwachstelle des PLCs. In Verbindung mit einer Webserver-Schwachstelle und dem Cloud-Nutzungsmodell entsteht in diesem Fall ein Hochrisiko-Szenario.

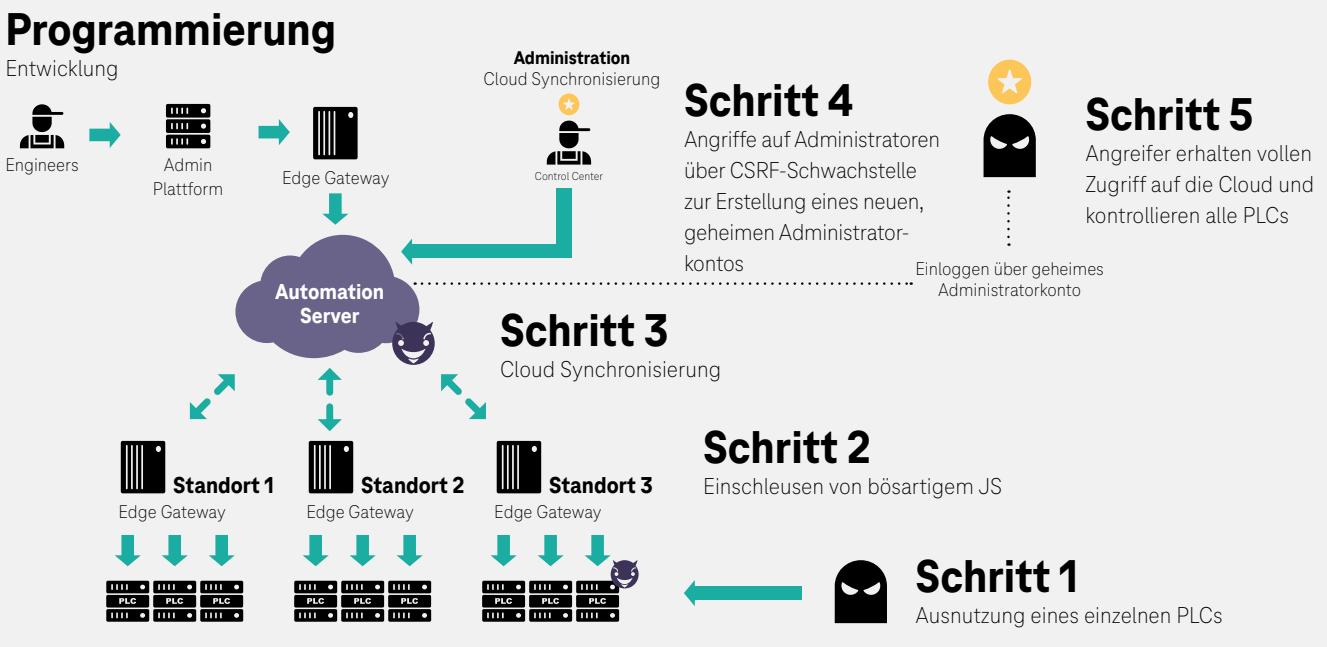


Abbildung: Übernahme der Cloud-Plattform durch PLC-Schwachstelle[10]

[8] https://claroty.com/team82/research/exploiting-vulnerabilities-in-the-ot-cloud-era
[9] CVE-2021-34566 bis -34569 [10] CSRF: CVE-2012-29238 [11] Whitepaper: Evil PLC Attack: Weaponizing PLC

Der Übergang

Der Übergang zwischen der „alten“ und der „neuen“ Welt ist insbesondere dann eine Herausforderung, wenn man nicht auf der grünen Wiese neu anfangen kann, sondern die Bestandsanlagen modernisieren muss – und zwar bei laufender Produktion. Dieses Szenario dürfte für die meisten der Normalfall sein. Hierbei ist die richtige Architektur nur ein Aspekt auf dem Weg zur sicheren Smart Factory. Genau so wichtig ist es, die Mitarbeitenden mit ihrem wertvollen Fachwissen in die neue Welt mitzunehmen.

Problematisch: Teilumbauten

In der Realität ist der Übergang zur smarten, vernetzten Produktion meist kein glatter Schnitt, sondern oft ein vereinzeltes Nachrüsten. Im Folgenden werden solche Teilumbauten, die oft in kleinen Schritten erfolgen, beispielhaft skizziert und die Sicherheitsrisiken, die damit einhergehen, thematisiert.

Das Unternehmen in diesem Beispiel fängt nicht bei Null an. Die Einführung einer Segmentierung und der teilweise Umbau der Produktionsnetze durch das Einbringen von VLANs und Firewalls wurde bereits erfolgreich umgesetzt, und das bei laufender Produktion. Die Veränderungen fielen relativ gering aus und die Modernisierung konnte schrittweise und kontrolliert erfolgen.

Der Umbau in Richtung Service Oriented Production (SOP), der grundlegender ist und disruptive Veränderungen mit sich bringt, begann hingegen unbemerkt bzw. ungeplant. Für einen bestimmten Produktionsschritt wurde ein Digitaler Zwilling ausprobiert, der sich als nützlich erwies. Damit der Versuchsballon funktionierte, wurden Maschinendaten von einem Hutschienen-IPC[12] in einem Abschnitt der Produktionsstraße per VPN-Tunnel an eine Cloud-Anwendung übertragen. Zuvor hatte man die Daten einer anderen Produktionseinheit zum Zweck der vorausschauenden Wartung an eine KI-Instanz des Herstellers in der Hersteller-Cloud gesendet. Und schon hatte der Kickoff für die Einführung eines extern gehosteten Manufacturing Execution Systems (MES) stattgefunden, ohne dass man sich dessen bewusst war.

Auch wenn in diesem Beispiel erst mal die gewünschten Funktionen der einzelnen Lösungen gegeben war, führt der Ansatz mittelfristig zu erhöhten Risiken bezüglich der Cybersicherheit aber auch der Stabilität und Wartbarkeit im Tagesbetrieb. Beispiele hierfür sind:

- Aufweichungen/Umgehen der Netzwerk-Segmentierung oder Zugriffskontrollen
- Schwächung/Umgehen der Netzwerküberwachung (Umgehung oder „Durchtunneln“ von Choke Points)
- Unbeabsichtigte Daten-Lecks durch fehlende, fehlerhafte oder schwache Verschlüsselung
- Einführung vieler neuer, u. U. proprietärer Insellösungen, die nicht in das normale Sicherheits- und Schwachstellen Management eingebunden sind
- Allgemeiner Anstieg der Komplexität und Abhängigkeit von verschiedenen Technologien, Plattformen und Prozessen

[12] Industrial PC

Die Lösung: Smart Factory (Migrations-) Architektur

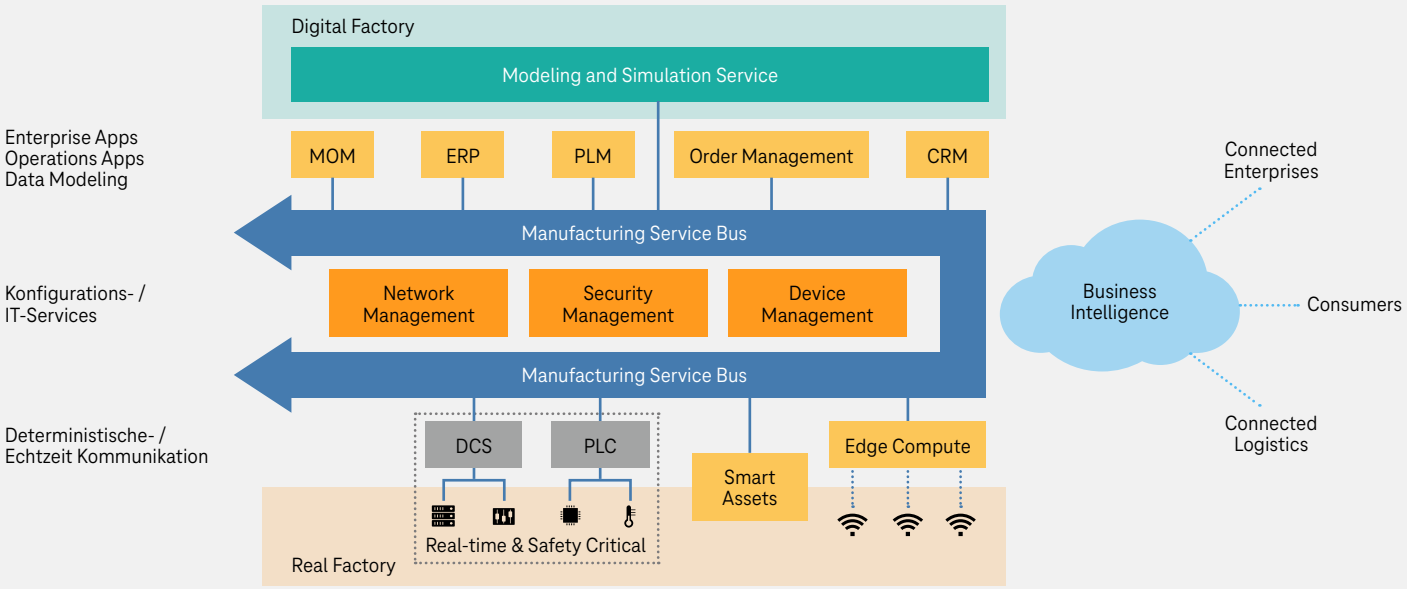


Abbildung: Vereinfachte NIST SOP Architektur[14]

Abhilfe kann hier die schrittweise Einführung eines Architekturansatzes bringen, wie er in der Abbildung dargestellt ist.

Zwei wichtige Elemente für den Start einer schrittweisen Migration sind die Schaffung eines (sicheren) Manufacturing Service Buses (MSB) und das Einrichten einer (sicheren) Cloud-Edge-Zone für die Produktion. Diese Elemente legen das Fundament für ein gestaffeltes Onboarding zukünftiger Use Cases, weil sie quasi die Verbindungsschicht oder Brücke zwischen der lokalen Maschinen- und der dezentralen, externen Cloud-Welt implementieren.

Beim Brückenbauen muss darauf geachtet werden, keine „Löcher" in die wehrhafte Architektur zu reißen. Dazu gehört zum Beispiel, dass logische, zonenübergreifende Datenverbindungen von der Maschine zur Cloud über geeignete Proxies oder Broker geführt werden. Diese gehören in geeignete DMZs (Demilitarized Zones) und bilden gleichzeitig gute Choke-Points zur zentralen Überwachung im Sinne der Cybersecurity. Moderne Angriffserkennungssystem können mit ihren Verhaltensmuster-Analysen an diesen Punkten zusätzlich das Risiko senken. Sie ersetzten aber nicht die Detektion in der Anlage selbst, zum Beispiel, um nur schwer zu erkennende Angreifer aufzudecken, die Zero-Day Schwachstellen in Anwendungs- oder Plattform-Software ausnutzen, oder den Software-Erstellungsprozess selbst unterwandern[13].

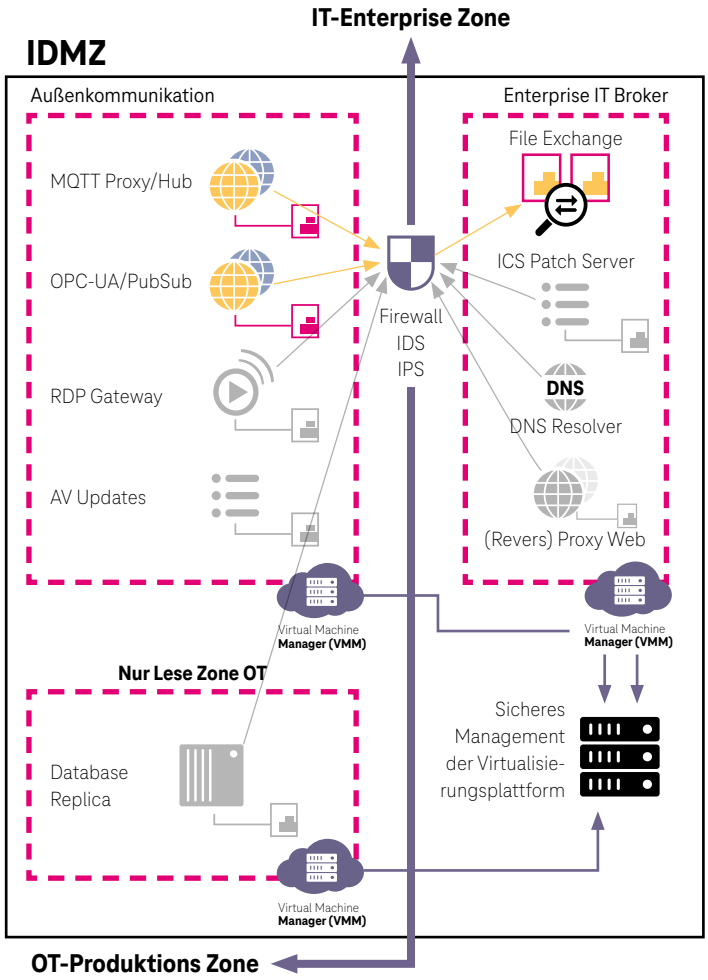


Abbildung: Proxy- und Broker-Zonen als Brücke zur Außenwelt

[13] Referenz Solarwinds
[14] The Paradigm Shift in Smart Manufacturing System Architecture

Big Picture: Schutzmaßnahmen

Betrachtet man das Gesamtbild einer Service-orientierten Produktion mit ihren verteilten Produktionsstandorten, Maschinen und Datensets, ihrer drahtlosen Vernetzung über drahtlose Campusnetze, vielfältiger Außenkommunikation über APIs, sowie der immer stärkeren Umstellung auf web-basierte Anwendung und deren Nutzung auf mobilen Endgeräten, so wird deutlich, dass sich das Cybersicherheitsmodell vom ursprünglichen Industrial-Control-System-Modell, hin zu einem Internet-of-Things-Modell entwickeln muss.

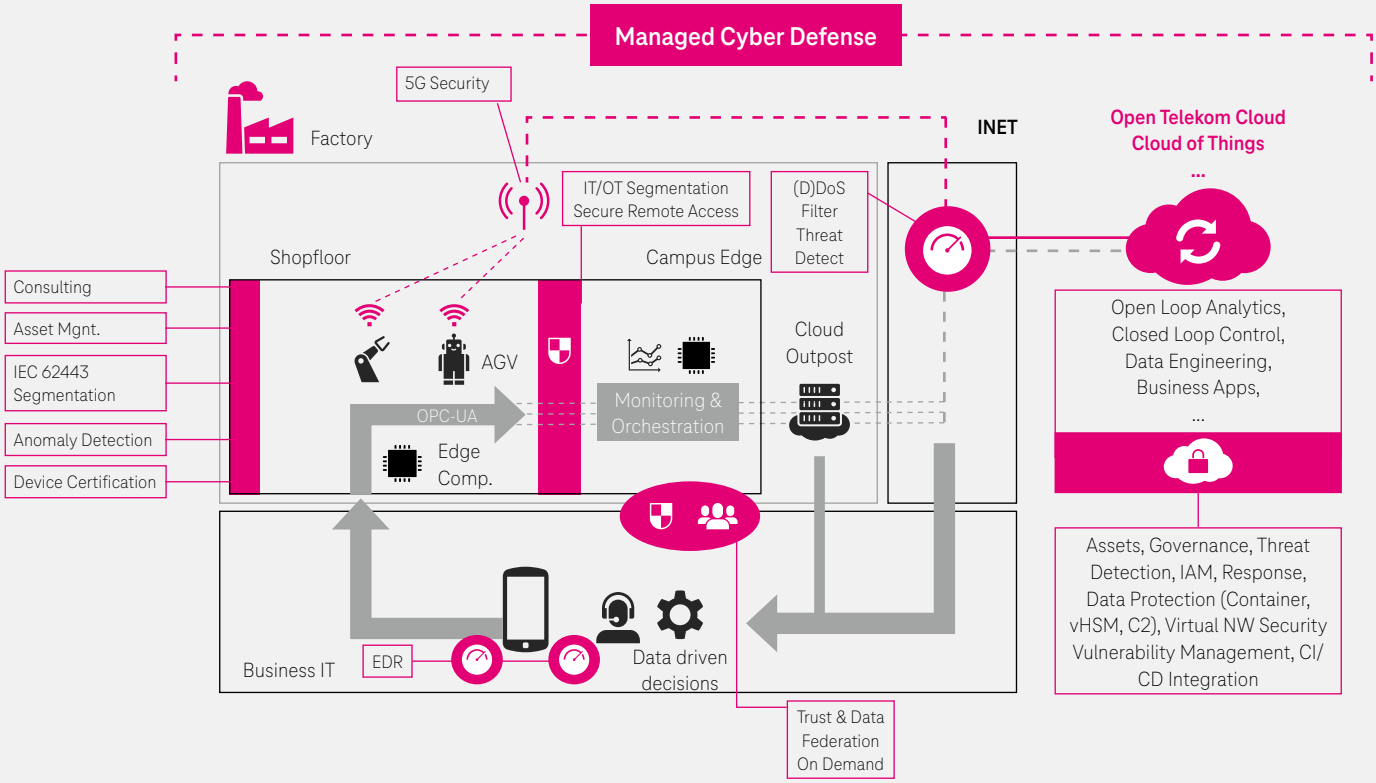


Abbildung: Ende-zu-Ende-Schutz für die smarte Produktion

Die Abbildung stellt den kontinuierlichen Datenkreislauf in diesem Modell und einige relevante Schutzmaßnahmen dar. Im Bereich 1 (Shopfloor) werden Waren mit Hilfe von Autonomous Guided Vehicles (AGVs), die über ein 5G-Campus-Netz angebunden sind, produziert. Zur Optimierung der Produktion werden sensible Prozessdaten in der Campus-Edge-Infrastruktur verarbeitet (2). Zusätzlich existieren digitale Zwillinge in einer externen Cloud-Umgebung, die über das Internet verbunden ist (3). Auf diese Daten haben externe Dienstleister und Maschinen Zugriff. Nach ihrer Verarbeitung fließen die Daten wieder zurück in die IT-Infrastruktur des Unternehmens (4), wo anhand dieser Informationen Entscheidungen zur Steuerung der Produktion gefällt werden, die dann wieder als Kontroll- und Steuerungsinformationen in Richtung Shopfloor fließen.

In diesem Kreislauf haben typischerweise eine Vielzahl von Parteien, Software-Instanzen, Maschinen oder Personen zu einem bestimmten Zeitpunkt ein bestimmtes Maß an Zugriff auf die Daten. **Daher kommt dem Management von Vertrauensstellungen und „starken", sicheren Identitäten (Personen und Maschinen), eine zentrale Rolle zu.**

Weitere Maßnahmen

Die Abbildung verdeutlicht auch, dass es zum Absichern einer SOP nicht mehr reicht, die speziellen Steuerungssysteme der Fertigungsanlagen abzusichern. Auch die normalen IT-Systeme wie Internetzugänge, Web-Proxies, Mobilgeräte und Cloud-Infrastruktur inklusive zum Beispiel eines dort beheimateten Active-Directory mit dessen Namensauflösungsservice (DNS) und Zeitgeber-Funktion (NTP), sind zusätzlich zu betrachten. Damit erweitert sich der OT-Security-Schutzmaßnahmenkatalog um Elemente wie:

- Wireless- und 5G-Sicherheit
- (D)DoS-Schutz der für die Produktion relevanten Internetverbindungen und -Anwendungen (Cloud, Web, Mail, DNS, APIs, Authentication Provider, MQTT Broker, MSB, MES, ...)
- Mobile-Device-Schutz (MDM, Sandbox, AV, ...)
- Starke Identitäten (PKI, Secure Elements, ...)

Key Takeaways

Bei der Migration von einem klassischen Automatisierungsmodell hin zu einer SOP ist es wichtig, die Risiken der Infrastrukturöffnung und der verteilten Verarbeitung von teils sensiblen Daten zu analysieren und zu verstehen. **Dies ist eine komplexe, interdisziplinäre Aufgabe, da hier Know-how bezüglich moderner Produktionsmethoden, IT, OT, Cybersecurity, Safety, Personalwesen und weiterer Fachbereiche notwendig ist.** Hierbei ist es besonders wichtig, die neuen Abhängigkeiten (von IT- oder externen Systemen und Prozessen) zu erkennen und zu berücksichtigen.

Darauf aufbauend kann eine robuste OT-/IT-Basisarchitektur (MSB, Edge) entworfen werden, die ein flexibles Onboarding und die Anbindung der existierenden und zukünftiger Produktions-Use-Cases erlaubt. Das Cybersicherheitskonzept muss stärker als bisher OT-/IT-übergreifend ausgelegt sein. Hier sind insbesondere eine übergreifende Angriffs- oder Anomalienerkennung und Vorfallsbehandlung herauszustellen, da sich die Angriffsfläche und die Lieferantenkette erweitert haben. Ein weiterer zentraler Aspekt in diesem Kontext ist die größere Bedeutung von gesicherten Identitäten und dem sicheren Delegieren von Vertrauen als neuem Perimeter in verteilten Systemen.

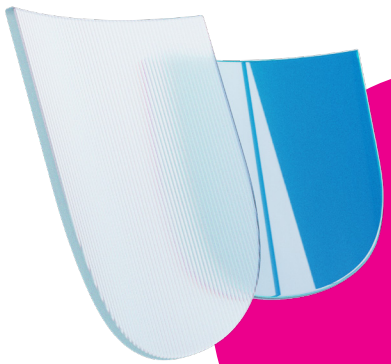
Aufgrund der Komplexität und Vielseitigkeit der Problemstellung ist es wahrscheinlich und auch wirtschaftlich sinnvoll, dass Unternehmen nicht immer alle Disziplinen mit eigenem Know-how abdecken. Mittelfristig ist es sinnvoll, eigene Fachkräfte im Bereich SOP auszubilden. In Disziplinen jenseits der eigenen Kernkompetenzen, wie etwa Cybersecurity, kann es sinnvoll sein, sich externe Hilfe zu holen.

Über den Autor

Bernd Jäger
Zu Karrierebeginn als Softwareentwickler auf Kernel-Ebene für Kommunikationsgeräte, fand Bernd schnell seinen Weg auf die Cyber Security Defender Seite des Lebens, wo er hochspezialisierte Sicherheitslösungen designte, ein SOC in London aufbaute, ein Beratungsteam für Security Penetrationstests leitete sowie ein Forschungsprojekt zur Cloud-Sicherheit unterstützte, bevor er Chief Information Security Architect wurde. Im Jahr 2016 wurde Bernd ein CSA Research Fellow und hat momentan Zertifizierungen für die Disziplinen Forensik, Intrusion Analyst, Reversing Malware, Web App Pentesting sowie Security Management. Und da er seit mehr als 20 Jahren im Bereich der Cybersicherheit tätig ist, war Bernd 2017 unter den ersten 120 SANS-zertifizierten "Industrial Defenders" (GRID). Bernd ist bei der Deutschen Telekom für die ICS/IoT Security zuständig um unseren Kunden bei der Sicherung ihrer ICS/IoT-Umgebungen zu helfen.

Abkürzungsverzeichnis

AGV	Autonomous Guided Vehicle
AI	Artificial Intelligence
CPPS	Cyberphysisches Produktionssystem
CPS	Cyberphysisches System
DDoS	Distributed Denial of Service
ERP	Enterprise Resource Planning
iDMZ	Industrial Demilitarized Zone
IPC	Industrial Personal Computer
IoT	Internet of Things
MES	Manufacturing Execution System
MSB	Manufacturing Service Bus
NTP	Network Time Protokoll
OT	Operations Technology
SDN	Software Defined Network
SOP	Service-orientierte Produktion
TTP	Tactics Techniques and Procedures
TTX	Tabletop Exercise
VLAN	Virtual Local Area Network



Kontakt
E-Mail: security.dialog@telekom.de
Web: security.telekom.de

Herausgeber
Deutsche Telekom Security GmbH
Office Port 1
Friedrich-Ebert-Allee 71–77
53113 Bonn

Connecting your world.

Deutsche Telekom Security GmbH | ore | 07/2024