SIEMENS

Information

Wien, November 2020

Security-Maßnahmen in der Industrie – ein Überblick

Autoren:	Sandra Dominikus	Email: sandra.dominikus@siemens.com
	Adrian Pinter	Email: adrian.pinter@siemens.com
	Andreas Reiter	Email: andreasreiter@siemens.com
	Lukas Gerhold	Email: lukas.gerhold@siemens.com
Ansprechpartner:	Adrian Pinter	Mobil: +43 664 8011763861

Einleitung

Digitale Technologien halten schon seit mehreren Jahren Einzug in die Produktions- und Automatisierungswelt. Früher prägten – zum Teil proprietäre – Feldbusse die Automatisierung. Typische Anwendungen waren meist Insellösungen, deren Möglichkeiten zur Kommunikation beschränkt waren. Transparenz über die Gesamtsituation in der Produktion zu erlangen war mühsam und mit erheblichem, teils manuellem Aufwand, verbunden.

Heute werden standardisierte Netzwerktechnologien und Kommunikationsstandards, wie Ethernet, Profinet und OPC-UA in der Industrie eingesetzt, womit es zu einer immer stärkeren Integration mit den IT-Systemen der Unternehmen kommt. Beispielsweise werden Daten aus den Produktionssystemen in Planungs- oder Kundensysteme zurückgespielt, oder umgekehrt Aufträge digital an die Produktionssysteme durchgereicht. Auch die Anbindung an Dateiserver, Datenbanken, E-Mail- und Messaging-Dienste, Domain Controller, Zeitsynchronisationssysteme und weitere digitale Dienste, die wir aus der IT kennen, werden in der Produktion immer mehr zur Selbstverständlichkeit.

Es findet also eine Konvergenz der IT-Technologien mit den Produktionstechnologien statt, was viele Vorteile bringt: etwa mehr geteiltes Know-how, bessere Durchgängigkeit und Integration der Technologien, höherer Grad an Vernetzung, höhere Flexibilität und weniger Abhängigkeiten von Herstellern. Sie bildet also die Basis für die Digitalisierung im Unternehmen. Der damit einhergehende Komfort und ein Mehr an Funktionalität und Möglichkeiten birgt aber auch das Risiko von Cyberangriffen in sich. Mögliche Auswirkungen reichen vom Ausfall der Produktion, dem Verlust von Produktions- oder Engineering Daten, von Unternehmensgeheimissen (wie Verfahrensdaten) bis hin zum Vertrauensverlust bei den Kunden. Eine mögliche Erpressung – Verlust der Kundendaten – kann das Image des Unternehmens nachhaltig beschädigen.

Es ist daher sinnvoll und notwendig, sich dem Thema Security unter Berücksichtigung der speziellen Anforderungen der Produktion strukturiert zu widmen, um die Risiken zu minimieren. Dieser Artikel soll Ihnen einen Einblick in die Welt der Cyber Security in der Produktion geben und einen ersten Ansatz bieten, wie Sie sich dem Thema nähern können.

SIEMENS

KPMG-Studie über Awareness von Cyber Security in den Unternehmen

Die von KPMG durchgeführte Studie zur „Cyber Security in Österreich“[1] bietet Einblicke in heimische Unternehmen und welchen Stellenwert Cyber Security in der Industrie – quer durch alle Branchen – hat. Unternehmen sind mit technisch immer ausgereifteren Angriffen konfrontiert, wiegen sich dennoch in einer falschen Sicherheit, Angriffe schnell zu erkennen. Realistisch betrachtet stieg die Verweildauer von Angreifern in den angegriffenen Systemen in den letzten Jahren stetig an und ist mittlerweile laut Schätzungen und Untersuchungen bei 100 bis 170 Tagen angekommen. Hierbei spielt den Angreifern in die Karten, dass 27 % der befragten Unternehmen kein dediziertes Cybersecurity-Budget aufweisen können. Gegenüber der Geschäftsleitung fällt hier die Argumentation meist schwer, da Erfolge nur schwierig messbar sind. Dem könnte man mit einer geeigneten Definition von Cyber Security KPIs entgegenwirken.

Neben allen technischen Maßnahmen, die ergriffen werden können, um auf Cyberangriffe aufmerksam zu werden oder diese abzuwehren und eine möglichst geringe Angriffsfläche zu bieten, steht die Schulung der Mitarbeiterinnen und Mitarbeiter immer noch an oberster Stelle. 79 % der Unternehmen wurden durch geschulte und achtsame Mitarbeiterinnen und Mitarbeiter auf potenzielle Cyberangriffe aufmerksam gemacht – wie beispielsweise auf Phishing-Angriffe die auch in der Industrie als beliebtes Einfallstor fungieren. Mitarbeiterinnen und Mitarbeiter stehen bei einem Cyberangriff in der ersten Verteidigungslinie und sind essenziell, um Angreifer am Eindringen in ein System zu hindern bzw. diese frühzeitig zu erkennen.

Investitionen in Cyber Security sind wichtig, weil sie ein Unternehmen dabei unterstützen, seine eigentliche Funktion aufrecht zu erhalten, wenn Unvorhergesehenes passiert. Sie sind aber kein Garant für eine absolute Sicherheit. In diesem Zusammenhang fällt auch oft der Begriff der Cyber Resilienz: er beschreibt, wie widerstandsfähig ein Unternehmen in Bezug auf Cyberangriffe ist und wie es diese auch kompensieren kann. Cyber Security ist Teil des Qualitätsversprechens eines Unternehmens an seine Kundinnen und Kunden und wird somit in den nächsten Jahren immer wichtiger werden. In Österreich bestätigt sich ein weltweiter Trend: Cyberangriffe werden in den nächsten 10 Jahren als das zweitgrößte Risiko für die Wirtschaft eingestuft – gleich hinter Finanzkrisen.

Bedrohungen, mit denen wir derzeit rechnen müssen

Ganz allgemein gilt, neueste Erkenntnisse zu Fehlern oder Schwachstellen in Soft- und Hardware können innerhalb kürzester Zeit für Cyberangriffe genutzt werden. Daher ist es auch wichtig, die Bedrohungslage als Ganzes zu kennen, um insgesamt angemessen auf Cyberangriffe reagieren zu können. Die hier vorgestellten Angriffsszenarien stammen aus dem BSI Lagebericht 2019[2].

Identitätsdiebstahl
Prominentester Vertreter des Identitätsdiebstahls ist das Phishing, bei dem versucht wird, über „Social Engineering“-Methoden an sensible persönliche Informationen heranzukommen. Dabei werden den Opfern z. B. personalisierte Emails geschickt und sie werden aufgefordert, Passwörter, Zugangsdaten oder Accounts preiszugeben.

1 https://home.kpmg/at/de/home/insights/2020/05/studie-cyber-security-in-oesterreich-2020.html
2 https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html

Ransomware
Ziel des Angriffs mit Ransomware ist es, wie aus der Bezeichnung hervorgeht (Ransom engl. für Lösegeld), an Lösegeldzahlungen der Opfer zu kommen. Hierbei wird der Zugriff auf die Dateien oder auf den eigenen Rechner verwehrt oder eingeschränkt, um das Opfer anschließend zu erpressen. In den meisten Fällen wurde jedoch beobachtet, dass die Täter nach der Zahlung entweder gar nicht in der Lage waren den Zugriff wieder zu ermöglichen oder sogar weitere Forderungen stellten, bzw. einfach nicht mehr reagierten. Prominenter Vertreter einer solchen Ransomware war 2019 LockerGoga, der bei einem norwegischen Aluminium Konzern ca. 35 Mio. Dollar Schaden verursachte. Effektive Maßnahme dagegen sind unter anderem das Aufsetzen einer entsprechenden Patch Management- und Backup-Strategie.

Schadprogramme
Bei nahezu jedem Angriff sind Schadprogramme Bestandteil der Attacke. Darunter versteht man ganz allgemein Software/Programme, die schadhafte Funktionen ausführen können. Zu dieser Kategorie zählen unter anderem Viren, Trojaner oder Würmer. 2019 wurden 114 Mio. neue Schadprogramme registriert, im Durchschnitt also 320.000 neue Programme pro Tag! Kein Anti-Virenhersteller der Welt könnte so eine Anzahl an Schadprogrammen in seine Anti-Virensoftware aufnehmen, für einen Grundschutz sollten Sie aber – wo sinnvoll anwendbar – dennoch nicht auf Anti-Virensoftware verzichten. Ein besonders lästiger Vertreter der Kategorie Schadprogramme ist EMOTET, der ein APT (Advanced Persistent Threat) ähnliches Verhalten aufweist. Dabei wird der Computer in einer ersten Welle infiziert, um dann anschließend passendere Software nachzuladen, die dann erst die finale Attacke durchführt.

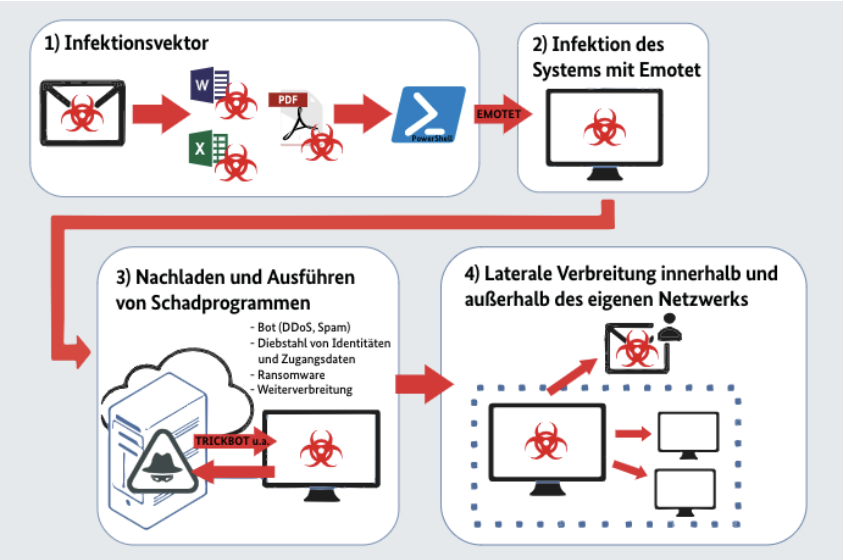

Abbildung 1: Angriffsvektor von EMOTET[3]

Distributed Denial of Service (DDoS)
Oftmals ist eine DDoS Attacke – also das Überlasten von Netzwerkdiensten durch eine große Anzahl von Anfragen – die Ursache, wenn Netzwerkdienste ausfallen, Webseiten nicht mehr erreichbar oder kritische Geschäftsprozess wegen Überlastung blockiert sind. Diese Angriffe werden meist durch eine Vielzahl von Computern oder Servern parallel ausgeführt, meist mit dem Ziel, kundenrelevante Internetdienste

[3] Grafik: https://www.fortinet.com/resources/icon-libary.html, Microsoft, Adobe

lahmzulegen oder von einer anderen Attacke abzulenken. 2018 wurde dadurch ein Gesamtschaden von ca. 4 Mrd. Euro verursacht.

Botnetze
Botnetze ermöglichen den Angreifern Zugriff auf eine große Anzahl fremder Systeme (Computer, Smartphones, Router, IoT Geräte, etc.), um diese für bösartige Zwecke zu missbrauchen. Dabei können persönlichen Daten aus den betroffenen Systemen abgegriffen und/oder die Ressourcen übernommen werden, um beispielsweise Cryptomining oder DDoS-Attacken durchzuführen. 2019 wurden Botnetze vorwiegend zum Abgreifen von persönlichen Daten genutzt, die zum Betrug beim Onlinebanking verwendet wurden. Generell konnte ein Anstieg an IoT-Botnetzen auf Basis internetfähiger Heimelektronik festgestellt werden.

Spam (oder unerwünschte E-Mails)
Klassischer Spam wird meist mit Produkt-, Wertpapier- oder Dienstleistungswerbung benutzt und gleichzeitig für Betrugsversuche eingesetzt. Opfer werden dabei animiert, Geld für eine Ware oder Dienstleistung im Vorhinein zu bezahlen, die dann später nie geliefert wird.

Beim Schadprogramm-Spam wird der Empfänger mit Schadprogrammen infiziert. Bei Phishing-Nachrichten werden die Benutzer dazu aufgefordert ihre Zugangsdaten (z.B. Internetbanking, soziale Netzwerke, Einkaufsportale, etc.) auf Webseiten einzugeben, die unter der Kontrolle der Angreifer stehen, die damit Daten abgreifen können.

Industrielle Sicherheitskonzepte und -lösungen

Aus den oben ausgeführten Bedrohungsszenarien ergeben sich eine Reihe von Security-Maßnahmen, die man abhängig von der tatsächlichen Gefährdungslage definieren muss. Die Auswahl, das Zusammenstellen und der Betrieb von Sicherheitslösungen kann für Anwender mitunter sehr komplex werden. Daher zielt Siemens darauf ab, dem Kunden möglichst automatisierte und durchgängige Lösungen anzubieten und ihn auf allen Ebenen zu unterstützen.

Eine Richtlinie, die dabei helfen kann, ein ganzheitliches Security-Konzept für Industriebetriebe zu erstellen, ist die IEC 62443. Sie definiert Sicherheitsmaßnahmen von der Prozessebene abwärts bis zur Produktebene. Auf der Prozessebene geht es vor allem um organisatorische Maßnahmen, wie die Awareness und das Aufsetzen von Security-Prozessen. Siemens unterstützt hier die Kunden mit Schulungen, Assessments und Consulting. Darüber hinaus bietet Siemens Servicedienstleistungen wie eine Security Hotline oder auch eine sogenannte Incident Response an.

Ein wichtiger Grundsatz auf der technischen Ebene ist das „Defense-In-Depth“-Prinzip. Es besagt im Grunde, dass die Verteidigung gegen Bedrohungen in Schichten (Zwiebelschalen-Modell) aufgebaut werden soll, in denen jeweils eigene Verteidigungsmechanismen implementiert sind. Wenn die Verteidigung einer Schicht gebrochen wird, gibt es immer noch weitere, die die wichtigen Assets schützen können.

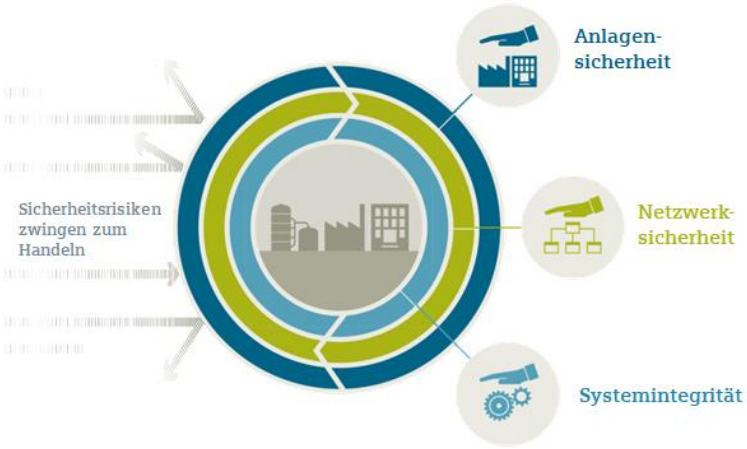

Abbildung 2: Defense-in-Depth Konzept @Siemens

Dieses Prinzip (siehe Abbildung 2) findet sich auch bei Security-Lösungen von Siemens wieder. Die Ebenen, auf denen hier Security betrachtet wird, sind:

→ Anlagensicherheit → Netzwerksicherheit → Systemintegrität

Für jede dieser Ebenen gibt es eine Reihe von Sicherheitslösungen. Wir wollen in diesem Artikel einige dieser Lösungen hervorheben, die durch Automatisierung auch ein besonderes Maß an Komfort für den Kunden bieten.

Anlagensicherheit

Um Angriffe auf der Anlagenebene zu erkennen, ist Monitoring ein wichtiges Instrument. Dazu wird der Datenverkehr in der Produktion analysiert und Abweichungen vom Regelverhalten werden festgestellt. Der erste Schritt ist hier die Erfassung aller Geräte, die in der Produktion verbaut sind, um das Regelverhalten zu definieren. Hierzu kann beispielsweise der über längere Zeit aufgezeichnete Netzwerkverkehr im OT-Bereich herangezogen werden. Damit lassen sich nicht nur die im Einsatz befindlichen Geräte bestimmen, sondern auch die Kommunikationsbeziehungen unter den Geräten sowie deren übliches Kommunikationsverhalten. Durch den Einsatz von industrieller Anomalie-Erkennungssoftware wird auf Ebene der Gerätebeziehungen, des Datentransfers aber auch über tiefergehende Protokollanalysen festgestellt, ob sich Geräte ungewöhnlich verhalten und somit potenziell kompromittiert sind. Im Falle eines Verdachts wird der Vorfall automatisiert bewertet und erkannt, welche Ereignisse zum aktuellen Zustand geführt haben (Root Cause Analysis). Unter anderem wird ein Alarm in einem SIEM (Security Incident and Event Management)-System ausgelöst. Durch die bereitgestellten Informationen kann ein Team im Security Operations Center (SOC) darauf effizient reagieren und einen möglichen Schaden abwenden. Siemens bietet hier sowohl eine speziell auf die Anforderungen der Industrie ausgelegte aktive Asset-Identifikation als auch eine passive Anomalie-Erkennung (Industrial Anomaly Detection) an.

Mit ihrer Erfassung geht auch die Übersicht über den Patching-Stand der einzelnen Geräte einher. Da laufend neue Schwachstellen, die bei Angriffen ausgenutzt werden könnten, gefunden werden, ist es essenziell, Geräte mit neuester Software auszustatten, um die Security einer Anlage auf einem hohen Niveau zu halten, z.B. durch das Einspielen von Updates. Dabei ist darauf zu achten, dass der Betrieb der Anlage nicht gestört wird. Siemens führt ein proaktives Security Monitoring seiner Produkte mit einem Team von anerkannten Security Experten bei ProductCERT durch. Entdeckte Schwachstellen in Siemens Produkten werden bewertet, Lösungen gefunden/vorgeschlagen und schlussendlich als Security Advisories

veröffentlicht. Kunden unseres Unternehmens werden damit über potenzielle Schwachstellen in ihren Systemen proaktiv informiert. Hierbei werden im Vorfeld die Auswirkungen von Schwachstellen auf Siemens Produkte und Lösungen unter Verwendung des CVSS Standards hinsichtlich verschiedener Metriken bewertet und schlussendlich in einen Score verpackt, der die allgemeine Verwundbarkeit angibt.

Darauf aufbauend hat Siemens den Industrial Vulnerability Manager entwickelt, der es ermöglicht, zielgerichtet für im Einsatz befindliche Komponenten, automatisiert Benachrichtigungen über Sicherheitslücken zu erhalten. Benachrichtigungen sind dabei nicht auf Siemens Komponenten bzw. Produkte beschränkt, sondern umfassen auch andere Components-off-the-shelf (COTS). Die Definition der zu überwachenden Softwarekomponenten muss dabei nicht manuell erfolgen, sondern kann automatisiert über die bereits im TIA-Portal oder auch SINEC NMS vorhandenen Daten realisiert werden. Der Industrial Vulnerability Manager bietet somit ein Schwachstellenmanagement, um den Überblick zu behalten, und liefert darüber hinaus detailliertere Informationen zu den gefundenen Schwachstellen sowie möglichen Patches. Die App zur Visualisierung der entdeckten Schwachstellen wird entweder in der Cloud als Mindsphere App oder direkt auf AWS betrieben. Um sensibleren Kundenanforderungen nachzukommen wird auch eine „on-premise“-Variante angeboten.

Netzwerksicherheit
Das Netzwerk ist eines der Haupteinfallstore für Cyberangriffe. Meist scannen die Angreifer nach offenen Ports und Diensten im Netz und den damit assoziierten Schwachstellen. Diese Scans erfolgen halb oder vollautomatisiert und liefern eine Liste aller Schwachstellen, die sich im Netz befinden. Anschließend können diese Schwachstellen attackiert werden.

Ziel muss es also sein, es den Angreifern so schwer wie möglich zu machen, d.h. der Zugriff auf Geräte, Netzwerke und Netzwerkkomponenten sollte nur über eine entsprechende Authentifizierung und Autorisierung möglich sein. Netzwerksicherheit umfasst auch die sichere und integre (wie zum Beispiel verschlüsselte) Kommunikation zwischen den Netzwerkteilnehmern. Vor allem dort, wo dem Netzwerk nicht vertraut werden kann.

Daher empfehlen wir für industrielle Netzwerke:

Netzwerktrennung und DMZ
Bei der Netzwerktrennung bildet man mit Firewalls, Routern und Switches voneinander getrennte Netzwerksegmente. In der IEC 62443 wird zusätzlich empfohlen, dass man für die Automatisierung ein physisch getrenntes Netzwerk mit einer eigenen Hardwareinfrastruktur schafft.

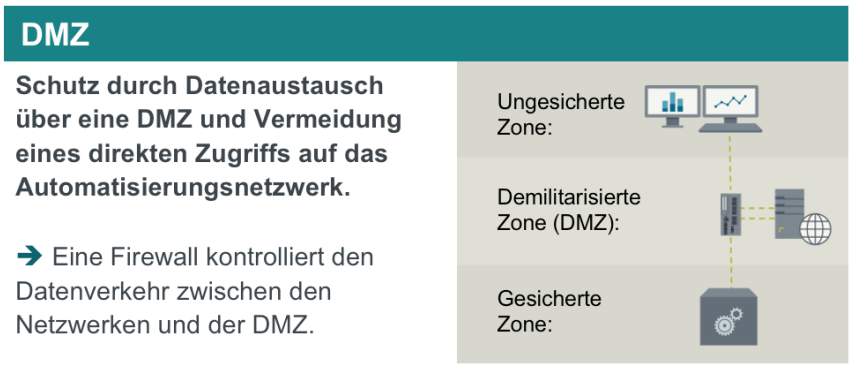

Abbildung 3: Netzwerktrennung und Demilitarisierte Zone @Siemens

Fernzugriff
Wartungszugriffe aus der Ferne müssen streng kontrolliert und im Unternehmen vereinheitlicht werden. Anlagen, die ihre eigene Lösung zur Fernwartung bereitstellen, müssen gemäß einer unternehmensweiten Fernzugriffsstrategie umgerüstet werden. Wichtige Anforderungen hierfür sind: zentrale Verwaltbarkeit, Übersicht über die aktuell laufenden Zugriffe von extern, sichere Kommunikation, eindeutige Identifizierung, Authentifizierung, Autorisierung und Nachvollziehbarkeit der Aktionen. Beliebiger Zugriff von Externen auf das Automatisierungsnetzwerk muss unterbunden werden.

Abbildung 4: Fernzugriff und Wartungszugänge @Siemens

Zellenschutz
Automatisierungszellen oder Anlagen sollen dort, wo möglich durch eine Firewall geschützt werden, um eine generelle direkte Kommunikation mit der Anlage oder der Zelle zu verbieten.

Eine Kommunikation soll nur durch klar definierte und überwachte Schnittstellen, Ports und Protokolle erlaubt werden. Ein regelmäßiges Review der erlaubten Kommunikation muss durchgeführt werden, um unerlaubte Kommunikation (die aber z.B. zur Fehlersuche, oder bei Wartungsarbeiten erlaubt wurde) wieder zu unterbinden.

Abbildung 5: Zellenschutz @Siemens

Systemintegrität
Die innerste Schicht der „Defense-In-Depth“-Verteidigungslinien ist der Schutz der Geräte selbst, die in einer Fertigung verbaut sind. Hier gibt es unterschiedliche Bereiche, die man schützen sollte. Ein Punkt, der in diese Kategorie fällt, ist der Kopier- und Know-how-Schutz von Software und Daten. Siemens bietet in zahlreichen Geräten Funktionalität an, um Kunden-Know-how zu schützen (z.B. Kopierschutz von Memory Cards, Passwortschutz für Funktionsblöcke, Binden von Funktionsblöcken an die Seriennummer einer Steuerung usw.).

Zugriffskontrolle
Auch die Zugriffskontrolle auf die Geräte spielt für die Systemintegrität eine wichtige Rolle. Nur authentifizierte Benutzer oder Geräte sollen Zugriff auf essenzielle Funktionen (z.B. Konfiguration, Lesen und Schreiben von Daten) von anderen Geräten haben. Mit der Benutzer- und Rechteverwaltung (UMAC) im TIA-Portal kann authentifizierter Zugriff auf Siemens-Geräte gewährleistet werden.

UMAC bedeutet “User Management and Access Control” und meint nicht nur die Authentifizierung von Benutzern, sondern auch die Zuweisung von Rechten aufgrund der Identität der Benutzer. Damit lassen sich Rechte sehr genau managen. Um den Komfort für den Kunden zu erhöhen, gibt es die Möglichkeit, eine bestehendes Windows Active Directory mit UMC zu kombinieren und so Benutzer zentral zu verwalten.

Hardening
Ein beliebtes Einfallstor für Angriffe sind Schwachstellen in der Software oder der Konfiguration. Durch verschiedene Maßnahmen, die sich unter dem Begriff System-Härtung (engl. Hardening) zusammenfassen lassen, kann die Angriffsfläche signifikant verringert werden. Dazu zählen vor allem ein restriktives Rechte-Management (least-privilege principle) und das Abschalten von Funktionalität oder Kommunikationskanälen, die für den angestrebten Einsatz eines Gerätes nicht erforderlich sind. Durch das sogenannte Whitelisting kann man beispielsweise jene Applikationen festlegen, die auf einem System laufen dürfen. Die Ausführung anderer, auch potenziell schädlicher Applikationen, wird automatisch blockiert.

Um dem Kunden ein sicheres Betreiben seiner Geräte zu ermöglichen, bietet Siemens nicht nur zahlreiche Konfigurationsmöglichkeiten, sondern stellt auch eine entsprechend detaillierte Dokumentation zur Verfügung. Darüber hinaus sind viele Produkte von Siemens schon ab Werk sicher vorkonfiguriert und werden im Zuge der Entwicklung – der Entwicklungsprozess folgt den Anforderungen der IEC 62443-4-1 Norm – durch zahlreiche Methoden gehärtet.

Sicherer Entwicklungsprozess
Sicherheit wird bei Siemens von Beginn der Entwicklung an mitbedacht – Security by Design – und startet schon mit der Planung. Dort werden die Security-Anforderungen für das Produkt festgelegt und eine Risikoanalyse kontinuierlich durchgeführt. Daraus resultierend wird ein Security-Konzept erstellt und Security-Maßnahmen abgeleitet, die dann während der Entwicklung umgesetzt werden. Dabei wird die Entwicklung durch umfangreiche Security-Test-Methoden unterstützt, die sicherstellen sollen, dass sich in Soft- und Firmware keine Schwachstellen befinden. Das schließt selbstverständlich auch Fremd-Software mit ein, die durch ein Monitoring Service immer wieder auf bekannte Schwachstellen geprüft wird, die dann vom Hersteller behoben werden müssen.

Wie schon erwähnt werden Siemens Produkte schon nach dem „Security-by-Default“-Prinzip ausgeliefert, d.h. es gibt eine Standardkonfiguration, die eine hohe Sicherheit bieten soll. Um sicher zu stellen, dass der Kunde tatsächlich die nach hohen Security-Anforderungen entwickelte Soft- und Firmware erhält, wird diese signiert. Damit kann der Ursprung verifiziert werden, darüber hinaus bieten einige Siemens-Geräte auch das Überprüfen der Firmware direkt beim Start des Gerätes („Secure Boot“).

Patching und Incident Handling
Patches und Updates werden bei Siemens zentral über den Siemens Industry Online Support (SIOS) ausgerollt. Falls, intern oder extern, Schwachstellen in den eigenen Produkten gefunden werden, kümmert sich auch hier eine zentrale Stelle um das weitere Vorgehen. Jeder Interessierte kann Schwachstellen beim Siemens CERT Service melden und sich auch benachrichtigen lassen, wenn neue Schwachstellen in Siemens-Produkten bekannt werden und erfahren, wie sie behoben werden können.

Durch die Integration von Sicherheits-Methoden schon ab dem Zeitpunkt der Planung, über die Entwicklung bis hin zum Betrieb der Geräte beim Kunden setzt Siemens ein ganzheitliches Sicherheits-Konzept um, das den Kunden schon auf Geräte-Ebene bestmöglich bei der Absicherung ihrer Produktion helfen soll.

Ausblick und Schlussfolgerung

Weder als Hersteller noch als Kunde oder Anwender darf man sich der Illusion einer absoluten Sicherheit hingeben. Bei Cyber Security geht es vor allem darum, den richtigen Kompromiss zwischen Aufwand und Nutzen zu finden. Fragen, die hier beantwortet werden müssen, sind z. B.: Welches Risiko bin ich bereit zu tragen, welches auf keinen Fall? Was sind die wichtigsten Assets, die ich schützen möchte? Der Schutz von Kundendaten und Betriebsgeheimnissen sowie das Aufrechterhalten der Produktionsfähigkeit stehen hier meist an oberster Stelle.

Aber auch Themen wie Usability spielen in der Umsetzung von Sicherheitsmaßnahmen eine wichtige Rolle, denn eine erfolgreiche Umsetzung wird stark von der Akzeptanz in der Belegschaft beeinflusst. Maßnahmen, die die Mitarbeiter an der Ausführung ihrer täglichen Arbeit behindern, werden von diesen auch nicht mitgetragen und können sich in weiterer Folge als nutzlos, wenn nicht sogar als kontraproduktiv erweisen.

Es ist nicht nur wichtig Maßnahmen zur Verhinderung von Cyberangriffen zu treffen, sondern auch, einen Angriff zu erkennen und eine Vorgehensweise zu definieren, wie man darauf entsprechend reagiert. D. h. für den unangenehmen Fall, dass ein Angreifer es geschafft hat ein System zu kompromittieren, sollten unbedingt Prozesse und Vorgehensweisen definiert sein, um effizient handeln zu können und sich möglichst schadlos zu halten.
Wir bei Siemens unterstützen unsere Kunden durch zahlreiche Lösungen und Maßnahmen dabei, eine „Defense-in-Depth“-Verteidigungsstrategie umzusetzen. Beginnend von der Anlagenebene, in der es z.B. um Monitoring-Lösungen und Schwachstellen-Scanner geht, über die Netzwerkebene, für die wir Geräte und Services für einen sicheren Netzwerkbetrieb bereit stellen können, bis hin zu unseren Geräten, die nach den Kriterien der IEC 62443 Norm für industrielle Sicherheit entwickelt werden.

Neben den technischen Maßnahmen vermitteln wir unseren Kunden auch unsere Expertise und organisatorische Hilfestellung in Form unseres Schulungs- und Consultingangebots. Darüber hinaus hat Siemens ein weltweit agierendes Team von Security-Experten, das auf neue Bedrohungen schnell reagieren und Kunden zeitnah informieren kann.

Durch die zunehmende Vernetzung und Digitalisierung von Produktionsanlagen werden auch sicherheitsrelevante Themen immer wichtiger. Siemens ist dafür mit einer umfassenden Sicherheitsstrategie ein guter Partner.