Industrial Cyber Security Handbook

Pragmatischer Ansatz zur Erhöhung der Cyber-Sicherheit und Widerstandsfähigkeit für Unternehmen aus Industrie und Produktion

BearingPoint®

Vorwort

Am 1. Juli 2021 nimmt SalzburgMilch, Österreichs drittgrößte Molkerei, nach einem erfolgten Hackerangriff, nach über einer Woche Stillstand ihrer IT-Infrastruktur und Produktionsstätten, den Normalbetrieb wieder auf. Keine zwei Tage darauf, startete am ersten Juliwochenende einer der größten Hackerangriffe der vergangenen Jahre. Durch den Angriff auf den US-amerikanischen IT-Dienstleister Kaseya, dessen Software den Angreifern als Einfallstor zu weltweit über 1.000 Unternehmen diente. In Schweden mussten daraufhin 800 Supermarktfilialen für mehrere Tage schließen.

Wieder wenige Tage darauf, am 6. Juli 2021, attackierten Kriminelle das Computersystem eines Landkreises in Sachsen-Anhalt und legten das gesamte IT-System und damit kritische kommunale Arbeitsbereiche lahm. Unter anderem konnten keine Sozialleistungen mehr ausbezahlt werden. Daraufhin wurde zum ersten Mal in der Geschichte Deutschlands in einem Landkreis der Katastrophenfall aufgrund eines Cyberangriffs ausgerufen.

Die drei angeführten Beispiele aktueller Cyber-Vorfälle sind aus mehreren Gesichtspunkten interessant. Sie sind nur die Spitze des Eisbergs, denn der Großteil der Angriffe findet statt, ohne dass die Öffentlichkeit jemals davon erfährt, aber sie zeigen die Brisanz des Themas zum Zeitpunkt der Veröffentlichung unseres Whitepapers aus mehreren Perspektiven.

Alle drei Angriffe sind innerhalb von nur einer Woche passiert. Sie zeigen dabei aber keine zufällige Spitze, sondern einen stetig steigenden Trend. Wir hätten genauso gut Beispiele von einigen Wochen davor oder danach wählen können. Sie zeigen, dass es weder geografische noch branchenspezifische Grenzen gibt. So wurde beim ersten Fall ein mittelgroßes, österreichisches Unternehmen angegriffen, aus einer Branche, die man nicht zuallererst in Verdacht hätte, besonders anfällig für Cyberangriffe zu sein. Beim zweiten Fall wurde zwar ein amerikanisches Unternehmen angegriffen, aufgrund der globalen Lieferketten-Zusammenhänge waren aber weltweit Firmen betroffen und sogar Endverbraucher in Schweden haben die unmittelbarsten Auswirkungen zu spüren bekommen. Und das dritte Beispiel zeigt einen direkten Angriff auf unsere kommunalen, sozialen und gesellschaftlichen Systeme und Abhängigkeiten, und soll einen ungefähren Eindruck vermitteln was passieren kann, wenn sogenannte kritische Infrastrukturen beeinträchtigt werden. Auch wenn der Katastrophenfall beim Angriff auf das IT-System einer Kommune natürlich nicht vergleichbar ist mit dem Katastrophenfall, der beim Angriff auf ein Atomkraftwerk ausgerufen werden würde.

Cyber-Bedrohungen sind also im Bewusstsein der breiten Bevölkerung angekommen und werden in den nächsten Jahren noch sehr viel stärker in den Vordergrund rücken. Bei Unternehmen mit breiter IT-Nutzung stellen IT-Risiken schon seit langem eine immer größer werdende Herausforderung dar und mit rasantem Tempo steigt nun auch die Bedrohung für alle anderen Unternehmen, die bisher noch nicht so stark im Fokus von Cyber-Kriminellen standen. Und am stärksten, so scheint es aktuell, sind vor allem hochautomatisierte und stark vernetzte Produktions- und Industrieunternehmen ins Fadenkreuz der Angreifer gerückt. Werden sensible und geschäftskritische Produktionsstätten angegriffen und beeinträchtigt, fällt es vielen Unternehmen umso schwerer auf Lösegeldforderungen der Kriminellen nicht einzugehen.

Wir wollen mit unserem Whitepaper vor allem Verantwortliche aus Industrie und Produktion ansprechen. Seien dies Sicherheitsbeauftragte für IT (CISO's) oder für die Produktion (ISO-Prods), Produktions- oder IT-LeiterInnen, genauso wie Finanzverantwortliche (CFO's), Betriebsverantwortliche (COO's) und Verantwortliche aus dem Risk Managment (CRO's). Im Prinzip alle jene, die sich für das Thema IT und noch viel mehr für das Thema OT-Sicherheit interessieren. Dabei sehen wir das Whitepaper als eine Art Handbuch, das einen einfachen und pragmatischen Einstieg in das Thema, auf der einen Seite zwar möglichst umfassend, auf der anderen Seite aber auch möglichst konkret und effektiv, ermöglichen soll.

Das Handbuch startet mit einem Abriss des bekanntesten und gleichzeitig auch spannendsten Industrie Cyber-Angriffs der Geschichte. Zum einen zeigt dieser Angriff wie ausgeklügelt Angreifer vorgehen, wenn ihnen genügend Ressourcen und die notwendige Motivation bereitstehen, zum anderen auch, dass es keine vollständig von der Außenwelt abgeschotteten Insel-Lösungen gibt. Danach wollen wir kurz den aktuellen Stand im Bereich IT/OT-Umgebungen beleuchten und was dazu geführt hat, dass diese ursprünglich voneinander abgetrennten Technologien immer mehr zusammenwachsen und welche Schlüsse man daraus ziehen kann.

Die besten Lösungen und Ideen entstehen, wenn man fundiertes Grundlagenwissen mit praktischer Erfahrung zusammenbringt. Aus diesem Grund wollen wir ein wenig theoretischen Background in zwei Kapiteln über zwei ausgewählte Sicherheitsframeworks geben. IEC 62443 ist ein sehr umfassendes industriespezifisches Framework und beschreibt gleichzeitig einige sehr konkrete und praxisrelevante Konzepte, die bei eigenen Lösungen unbedingt Berücksichtigung finden sollten.

Mit dem CIS Security Framework haben wir darüber hinaus noch ein allgemeineres, für IT als auch OT gültiges, Best-Practice Framework aufgenommen, dass mit 20 sehr konkreten Handlungsempfehlungen zum pragmatischen Vorgehen einladen möchte.

Danach folgen zwei Kapitel mit Erfahrungen, Handlungsempfehlungen und konkreten Tipps aus der Praxis. Wir zeigen dort ein Schritt-für-Schritt Vorgehen für Unternehmen, auf unterschiedlichen Reifegraden ihrer Sicherheitslösungen, genauso wie ganz gezielte und effektive Lösungen für konkrete Herausforderungen und Problemstellungen.

Zwischen den einzelnen Kapiteln haben wir zwei anonymisierte Fallbeispiele (Case Studies) aus eigenen beziehungsweise Projekten unserer Technologie-Partner eingebaut, die das Whitepaper etwas auflockern und detaillierte Einblicke in konkrete Kundenherausforderungen geben sollen.

Um den Kreis zu schließen, wollen wir am Ende ein Fazit ziehen, ob es mit den in diesem Whitepaper beschriebenen Ansätzen, Technologien und Maßnahmen möglich wäre, auch einen hochgradig ausgeklügelten und mit umfassenden Ressourcen geplanten Angriff – wie dem im Einstiegskapitel beschriebenen – wirkungsvoll abzuwehren.

Vor allem LeserInnen mit wenig Vorkenntnissen in der Thematik, können das Handbuch Kapitel für Kapitel, vom Beginn bis zum Ende lesen. Wir haben so gut es geht versucht, Fachbegrifflichkeiten zu vereinfachen, zu erklären oder ganz wegzulassen, wenn sie für das Verständnis nicht notwendig sind. LeserInnen mit bereits viel Erfahrung im Bereich OT-Security, empfehlen wir insbesondere die konkreten Tipps und Empfehlungen in den letzten beiden Kapiteln und die Case Studies, um diese mit ihren eigenen Theorien und Erfahrungen zusammenzubringen.

Ich wünsche Ihnen viel Spaß beim Lesen und freue mich auf Feedback!

Markus Seme

Inhaltsverzeichnis

1

Das Ende einer Ära

Wie ein gezielter Angriff die Welt für immer veränderte

Das Ende einer Ära

Wie ein gezielter Angriff die Welt für immer veränderte

Als am 17. Juni 2010 der weißrussische Sicherheitsforscher Sergey Ulasen einen neuartigen Computervirus, den er vor einigen Tagen zur Analyse von einem Unternehmen mit Computerproblemen aus Teheran übermittelt bekommen hatte, in seinem Blogeintrag mit den Worten „Current malware should be added to very dangerous category“ beschrieben hat, ahnte noch niemand die Tragweite, die seine Entdeckung für die Welt der Cyber-Sicherheit und im Speziellen, für die der Industriellen Security haben sollte.

Sergey hatte gerade die erste autonome Cyberwaffe in der Geschichte der Menschheit vor sich, die es ermöglichte, einen gezielten und hochkomplexen Cyberangriff auf eine militärisch gesicherte und netzwerkseitig vollständig isolierte Industrieanlage durchzuführen.

Ulasen hatte erkannt, dass der ihm vorliegende Virus, wenn er einmal einen Rechner über einen infizierten USB-Stick befallen hatte, sich selbstständig im daran angeschlossenen Netzwerk verbreitet und in weitere Computer eindringt. Dazu nutzt er eine bis dahin noch unbekannte Schwachstelle des Windows Betriebssystems von Microsoft. Einen sogenannten Zero-Day-Exploit.

Das Besondere daran: Virenscanner und damals gängige Sicherheitslösungen können dagegen nichts ausrichten, genauso wie ein auf den letzten Softwarestand gebrachtes System dagegen schutzlos wäre.
Warum: Da weder der Hersteller des Betriebssystems noch der des Antivirenprogrammes bisher noch mit dem Virus konfrontiert worden ist, konnte weder ein Softwareupdate mit Fehlerbehebung entwickelt, noch das Antivirenprogramm mit einer passenden Signatur trainiert werden.

So ein Zero-Day-Exploit ist, je nach Ausrichtung, relativ selten und deshalb auch sehr wertvoll. Verwendet man ihn nicht für eigene Zwecke, könnte dieser am Schwarzmarkt um 100.000 bis 250.000 Dollar verkauft werden.

Der später unter der Bezeichnung Stuxnet zu weltweiter Bekanntheit erlangte Virus, hatte vier solcher Zero-Day-Exploits eingebaut!

Das Besondere an der neuartigen Malware war, dass sie sich nach der Infektion der Rechner vollständig passiv verhielt und keinerlei auffällige Aktionen durchgeführt wurden.

Erst einige Zeit später gelang es dem, auf Produktionsanlagen und kritische Infrastrukturen spezialisierten deutschen Sicherheitsexperten Ralph Langner mit seinem Team, die Payload – also den eigentlichen Schadcode – zu entschlüsseln. Nämlich, als sie den Virus in ihrem, mit Industrie-Steuerungssystemen (SPS) der Marke Siemens ausgestatteten, Labornetzwerk freigesetzt hatten. Erst dort erwachte Stuxnet zum Leben und begann seinen hochkomplexen und ausgefeilten Angriff auf, wie später durch Langner noch bestätigt werden konnte, die in der iranischen Urananreicherungsanlage Natanz betriebenen Zentrifugen.

Abbildung 1: Über mobile Datenträger wie USB- Sticks, lassen sich auch netzwerkseitig komplett abgeschottete Systeme erreichen.

Um den Angriff, der die sensiblen Zentrifugen-Teile physisch zerstören sollte, möglichst unentdeckt und über einen längeren Zeitraum durchführen zu können, zeichnete Stuxnet den Normalbetrieb der Anlage vor dem Angriff auf. Dadurch konnte während des aktiven Angriffs die Überwachungsanlage des Betriebspersonals mit einem korrekten Betriebszustand getäuscht werden, während im Hintergrund Drehzahlen und Gasdruck in den Zentrifugen manipuliert wurden.

Lange Zeit konnte nicht mit absoluter Sicherheit bestätigt werden, dass es sich beim Angriffsziel wirklich um das iranische Natanz handelt.

Langner lieferte auch hierzu einen letzten schlüssigen Beweis. Es gelang ihm spezifische Teile des entschlüsselten und dekompilierten Codes von Stuxnet, welche an verschiedensten Stellen immer wieder auftauchten, einem Pressefoto des offiziellen iranischen Fernsehens zuzuordnen.

In folgendem Code Fragment (einer Anweisungsliste der SPS Steuerungen), findet man zum Beispiel, beim Setzen eines Zählers (Laden eines Merkers) für einen Schleifendurchlauf, dass dieser mit dem Wert 164 belegt werden soll.

Anders gesagt, soll in späterer Folge eine Programmschleife 164-mal durchlaufen werden und irgendeine Aktion ausführen.

```
M117:L     LWO
     L     164
     <=I
     SPBN  M101
```

In Abbildung 2 sieht man am unteren Bildrand den Ausschnitt eines Überwachungssystems (Monitoring) der Zentrifugenanlage. Die grünen Punkte stellen dabei die einzelnen Zentrifugen dar. Über diesen Bildausschnitt konnte ermittelt werden, dass es sich dabei um exakt 164 Einzelzentrifugen, einer sogenannten IR 1 Kaskade, handeln musste. So wurde die erste Version der iranischen Anreicherungsanlage, eines Zusammenschlusses von Zentrifugen, mit dem Ziel Uran anzureichern, genannt.

Diese 164 Einzelzentrifugen waren noch dazu in 15 sogenannten Anreicherungsstufen aufgeteilt. Jeder Stufe war eine unterschiedliche Anzahl an Zentrifugen zugeordnet. Diese Zuordnung konnte mittels einer Bildanalyse des Pressefotos nachträglich erstellt werden und ergab ein einzigartiges und auf das Angriffsziel abgestimmtes Muster, welches völlig identisch an mehreren Stellen im Code von Stuxnet wiederzufinden war.

Abbildung 2: Der iranische Präsident Ahmadinejad betrachtet die Visualisierung des Kaskadenschutzsystems. [1]

Das Geheimnis von Stuxnet war gelöst, zumindest ein Teil davon. Auch wenn sich bisher noch niemand offiziell dazu bekannt hat hinter dem ausgefeilten Angriff zu stecken, zeigen Faktenlage und Handschrift in eine eindeutige Richtung, was die potenziellen Akteure, die hinter Stuxnet gestanden haben könnten, betrifft.

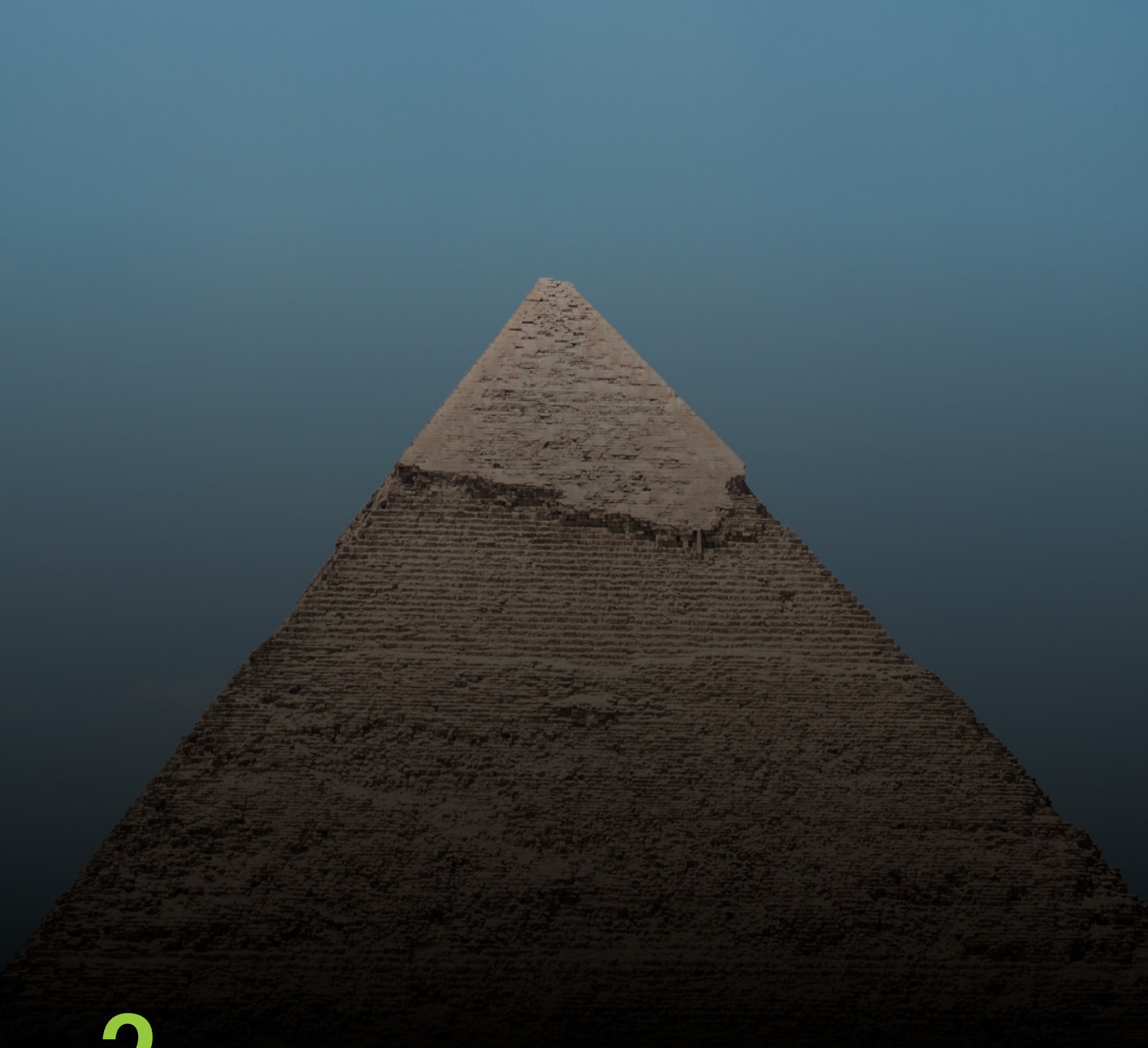
Wie auch immer man das politisch oder gesellschaftlich bewerten mag, aus der Sicht von Industrie- und Produktionsautomatisierung und der, wie man solche Anlagen effektiv absichern kann, hat Stuxnet zum ersten Mal in der Geschichte gezeigt, dass jedes physische System, das in irgendeiner Form automatisiert ist, angreif- und manipulierbar ist, auch wenn es netzwerktechnisch vollkommen isoliert zu sein scheint. Die dabei einzigen begrenzenden Faktoren sind die Motivation der Angreifer und die Ressourcen, mit denen jene ausgestattet sind.

Jene, die sich für noch mehr Details im Zusammenhang mit Stuxnet interessieren, sei der äußerst detaillierte und hochinteressante Report von Ralph Langner – *„Stuxnet und die Folgen“* [2] – ans Herz gelegt.

Und los geht's

Die oben beschriebene Geschichte soll Verantwortlichen und Interessierten nicht den Mut nehmen, dass ein wirksamer Schutz gegen potente Angreifer ohnehin nicht möglich ist, sondern vielmehr aufzeigen, dass ein Wiegen in falscher Sicherheit oder ein Verlassen auf einzelne, scheinbar unüberwindbare Sicherheitsmaßnahmen und Hürden, fatale Folgen haben kann.

Gleichzeitig wollen wir den LeserInneneinen möglichst umfassenden und trotzdem überschaubaren Überblick sowie einen sehr praktischen und pragmatischen, trotzdem aber mit theoretischen Ansätzen und Konzepten angereicherten Leitfaden an die Hand geben, der zeigen soll, dass man durch das systematische Setzen von bereits wenigen, effektiven Maßnahmen, eine Vielzahl an Cyberangriffen erfolgreich abwehren kann und sich mitunter sogar vor einem gezielten und besonders ausgeklügelten Angriff, einem sogenannten „Advanced Persistent Threat“ (APT), effizient schützen kann.



2

Pyramiden haben ausgedient

Industrie 4.0, die komplette Vernetzung und der Verlust des Air Gaps

Pyramiden haben ausgedient

Industrie 4.0, die komplette Vernetzung und der Verlust des Air Gaps

Produktivitätssteigerung und Senkung der Produktionskosten, sind zwei der maßgeblichen Treiber für Automatisierungsbestrebungen in industriellen Produktionsanlagen.

Die ehemals oft vollständig isolierten Operational Technology Netzwerke (OT-Netzwerke) werden dadurch zunehmend von außen zugänglich gemacht und mit vorhandenen Information Technology Netzwerken (IT-Netzwerken) und Technologien verbunden.

Der Mythos vom vollständigen Air Gap, der kompletten physischen Trennung der Systeme zwischen Prozess- und Betriebsleitebene, kommt dadurch immer mehr ins Bröckeln.

Die proprietären Protokolle der Industrial Automation and Control Systems Umgebungen (IACS-Umgebungen), werden immer mehr von offenen Protokollen aus dem IT-Umfeld verdrängt. Das bisher typische Schichtenmodell der klassischen Automatisierungspyramide, wie sie im *"Purdue Reference Model"* [3] beschrieben ist, in der die Kommunikation zwischen Komponenten der unterschiedlichen Schichten sehr strukturiert und kontrolliert abläuft und überwacht und gesichert werden kann, weicht immer mehr einem Modell, das eher einem unstrukturierten Automatisierungsnetzwerk ähnelt.

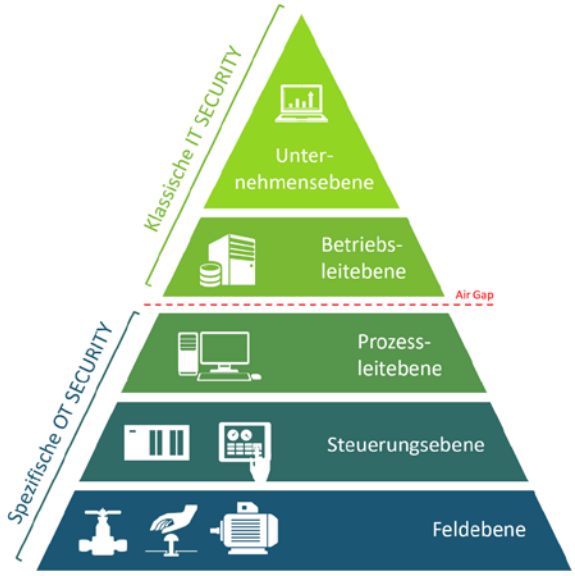


Abbildung 3: Klassisches Schichtenmodell der Automatisierungspyramide

Systeme aus den IT-Netzwerken oder der Betriebsleitebene, kommunizieren plötzlich direkt mit Komponenten wie Sensoren oder Aktoren auf der Feldebene und werden nicht mehr wie bisher, von den SPS- und SCADA Systemen der Steuerungs- und Prozessleitebene abstrahiert und geschützt.

Durch diese zunehmend horizontal, als auch vertikal miteinander vernetzten Systemkomponenten, entstehen neue Formen von Risiken und Herausforderungen, mit denen moderne und zukünftige Industrie 4.0 Produktionsumgebungen konfrontiert sind.

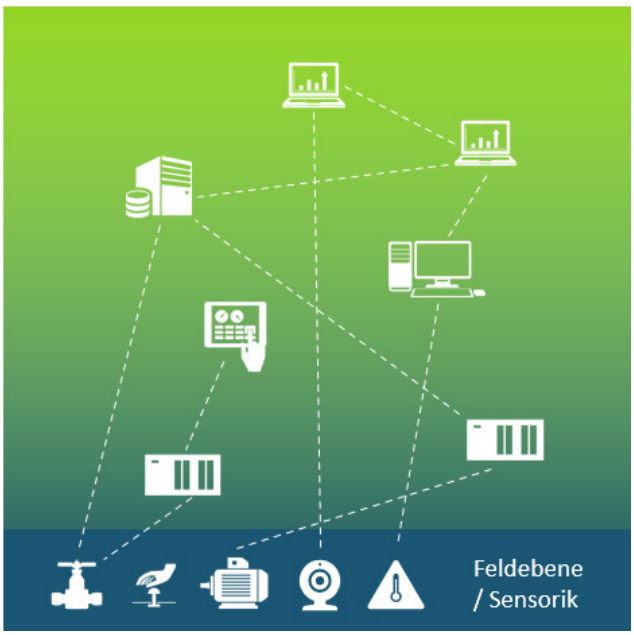


Abbildung 4: Automatisierungsnetzwerk mit direkt miteinander kommunizierenden Systemkomponenten

Besondere Herausforderungen

Um den unterschiedlichen Risiken und Herausforderungen bestmöglich begegnen zu können, macht es Sinn diese zuerst einmal zu strukturieren.

Dazu gibt es in der Literatur in den unterschiedlichen Sicherheitsstandards und Best Practice Vorgehensmodellen, ähnliche Herangehensweisen, auf die im weiteren Verlauf noch näher eingegangen wird.

Bei der einen Herangehensweise nähert man sich über unterschiedliche Domänen, etwa den operativen Zielen wie der Verfügbarkeit der Anlage oder der Gewährleistung der Funktionen oder den funktionalen Zielsetzungen wie etwa Echtzeitkommunikation oder dem Umstand, dass in OT-Umgebungen Systeme und Applikationen oft bis zu 20 Jahre eingesetzt werden, ohne die Möglichkeiten zu haben, diese regelmäßig zu aktualisieren.

Wieder andere Modelle strukturieren eher nach der Art und Weise möglicher Risiken und Präventionsmöglichkeiten. Beispielsweise die Unterscheidung zwischen technischen und organisatorischen oder prozessualen Möglichkeiten, den Anlagenschutz zu erhöhen. Wichtig dabei ist, dass man in der Herangehensweise Maßnahmen auf verschiedenen Ebenen berücksichtigt und sich nicht nur auf einzelne Schwerpunkte, wie etwa technische Security-Lösungen, konzentriert.

Eine pragmatische Herangehensweise bietet etwa das Center for Internet Security (CIS) in Zusammenarbeit mit dem SANS-Institute, mit ihren „20 Critical Security Controls (CSC) for Effective Cyber Defense“ (CIS CSC) an, auf das im Folgenden noch genauer eingegangen wird. Auch hier wird grob zwischen technischen und organisatorischen Maßnahmen unterschieden.

Geht man davon aus, dass es keinen vollständigen Schutz gegen gezielte Angriffe geben kann, macht es außerdem Sinn eine Resilienz-Strategie in sein Cyber-Security-Konzept mitaufzunehmen. Die Maßnahmen daraus, müssen ein schnelles Wiederhochfahren beziehungsweise ein Minimieren des Schadens, nach einem erfolgreichen Angriff, sicherstellen können.

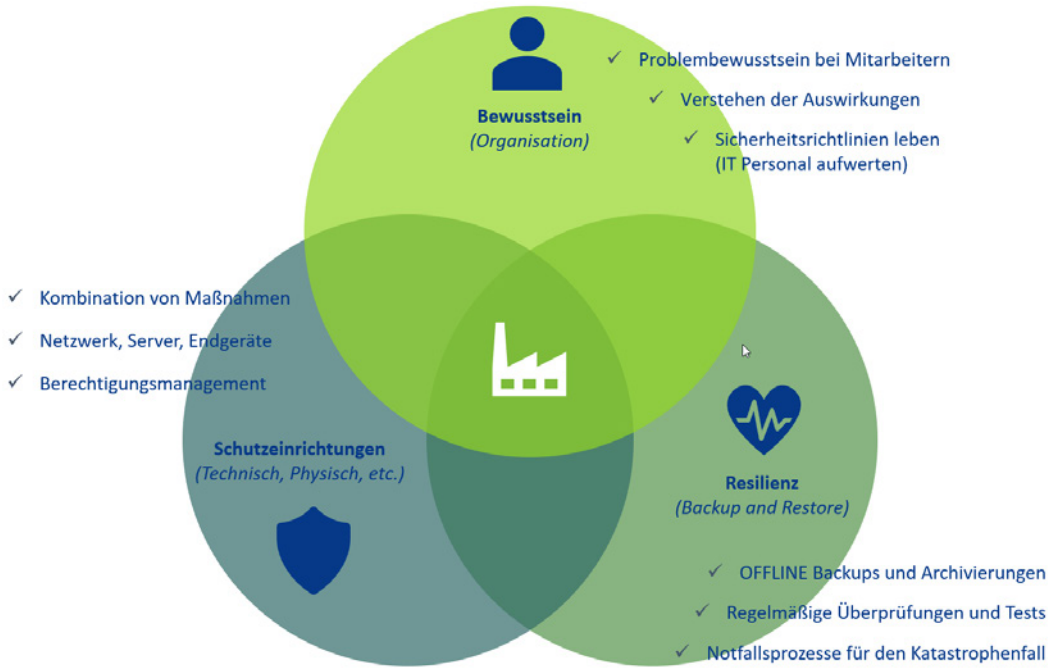


Abbildung 5: Ein Umfassendes Konzept beinhaltet immer Maßnahmen unterschiedlichster Blickrichtungen

Customer Case study

Absicherung der Legacy Systeme für internationalen Anlagenbauer

Der Kunde ist ein international tätiger Anlagenbauer, welcher weltweit hochautomatisierte Lagersysteme plant, fertigt und teilweise für Kunden betreibt. Die Systeme bestehen sowohl aus OT-Komponenten, also Automatisierungstechnik, als auch IT-Komponenten, wie Datenbank- und Applikationsservern und Software zur Ablaufsteuerung.

Auf Grund der langen geplanten Einsatzdauer der Anlagen, diese können durchaus 15-20 Jahre in Verwendung sein, und der geänderten Bedrohungslage hinsichtlich Cyber-Security, ergeben sich einige Herausforderungen um diese Anlagen ausreichend vor modernen Bedrohungen zu schützen.

Herausforderungen

Da die Anlagen mit einem freigegebenen Betriebszustand betrieben werden, sind Änderungen an den einzelnen Komponenten, beispielsweise Patching oder Upgrades auf neuere Versionen, nur schwer umzusetzen und mit hohem Aufwand und möglichen Risiken verbunden.

Neuere Anlagen wurden hingegen bereits so konzeptioniert, dass Upgrades und Patching ohne erheblichen Aufwand möglich sind. Die Vorgehensweise von BearingPoint zielt daher besonders auf ältere Anlagen ab und soll diese gegen kritische Angriffsvektoren schützen und die Verfügbarkeit sicherstellen.

Weiters soll eine mögliche Security-Lösung eigenständig und unabhängig von den verbauten Komponenten laufen, und beispielsweise nicht als Software auf den bestehenden Servern installiert werden, um im Falle einer Fehlfunktion negative Auswirkungen auf die Anlage und Software auszuschließen.

Bei einer gesamtheitlichen Betrachtung der Anlagen wurden mehrere mögliche Angriffsvektoren und Schwachstellen identifiziert, die mit modernen Cyber-Security-Technologien und entsprechenden Konzepten entschärft werden können.

1. Teilweise besteht auf Netzwerkebene keine Trennung beziehungsweise Absicherung zwischen dem Business-IT-Netzwerk und dem Automatisierungsnetzwerk. Dies ermöglicht einem Angreifer oder einer automatisierten Schadsoftware einfach vom IT-Netz auf die Produktionsanlage überzugreifen.

2. Einige der IT-Komponenten werden bereits seit Jahren nicht mehr supportet und erhalten daher auch keine Security-Patches mehr von den Herstellern. Dies macht sie angreifbar, da davon auszugehen ist, dass Schwachstellen und möglicherweise Exploits existieren.

3. Auf Grund der oftmals älteren Softwareversionen der Ablaufsteuerungssoftware nutzen deren Frontends keine modernen, sicheren Protokolle mit ausreichender Verschlüsselung. Dies erleichtert einem Angreifer die Analyse und Manipulation der Datenströme und den Versuch sich erweiterte Berechtigungen zu verschaffen.

4. Die Datenströme und Kommunikation am Übergang zwischen dem Business-IT-Netzwerk und der Automatisierungslösung werden nicht auf Anomalien und Securityevents wie beispielsweise Command & Control Traffic oder Schadsoftwaren überwacht und so können Daten unkontrolliert zwischen den Netzen auf beliebige Komponenten übertragen werden.

5. Zugriffe auf und Datenströme zu Komponenten innerhalb des Automatisierungsnetzwerks werden nicht gesteuert und auf Securityanomalien oder Schadsoftware überwacht.

6. Wartungszugriffe auf die Automatisierungslösung, sowohl auf IT als auch auf OT, erfolgen teilweise über einen Jumphost in einem separaten Wartungsnetzwerk. Dieser Jumphost hat Zugriff auf alle Komponenten, aber der Zugriff darauf ist häufig nicht ausreichend gesichert und verdächtiger Netzwerk-Traffic oder Schadsoftwaren können nicht erkannt werden.

7. Es besteht keine vollständige und automatisierte Erfassung aller verbauten Assets und deren Schwachstellen und die Erkennung von Anomalien oder verdächtiger Kommunikation ist nicht möglich. Weiters besteht keine Möglichkeit einer granularen Steuerung von Zugriffen auf OT-Komponenten und Kommunikation zwischen diesen.

Zielsetzung

Ziel war die Erstellung eines Konzeptes zur Absicherung älterer Anlagen, Überprüfung der Wirksamkeit in einem Proof-of-Concept sowie die Implementierung und der Betrieb in Kundenanlagen in unterschiedlichen Ausprägungen.

Die Lösung hatte in jedem Fall autark zu funktionieren und durfte im Falle einer Fehlfunktion keine signifikanten Auswirkungen auf den Anlagenbetrieb haben. Weiters sollten modernste Security-Technologien zum Einsatz kommen, welche die Anlagen auch in den kommenden Jahren vor neuen Bedrohungen zu schützen vermochten. Den Betrieb der Lösung sollte BearingPoint übernehmen, wobei ein voller Managed-Service mit 24/7 Verfügbarkeit und schnellen Reaktions- und Reparaturzeiten gefordert war.

Lösung

Nach einer Evaluierung der technischen Anforderungen der verschiedenen Anlagentypen (Größe, Netzwerk-Traffic, Vulnerabilities, eingesetzte Hard- und Software, Schnittstellen, Protokolle, etc.) entschieden wir uns für den Einsatz von modernsten Next-Generation-Firewalls sowie einer spezialisierten Lösung für OT-Assetmanagement und Bedrohungserkennung.

Zum Einsatz kamen dabei Firewalls vom Hersteller Check Point, da diese die benötigten Technologien bieten, um alle technischen Anforderungen zu erfüllen und zudem ein sehr hohes Schutz- und Serviceniveau sowie lange Supportlaufzeiten bieten.

Die Firewalls wurden so implementiert, dass sie am Übergang zwischen Business-IT-Netzwerk und dem Automatisierungsnetzwerk den gesamten Traffic kontrollieren und so vor Bedrohungen schützen können. Damit etablierten wir eine zusätzliche Verteidigungsschicht, mit der wir weitere Herausforderungen lösen konnten.

Durch das Feature Virtual Patching können Zugriffe auf nicht ausreichend gepatchte Komponenten so modifiziert werden, dass Sicherheitslücken eliminiert werden und für Angreifer oder Schadsoftwaren nicht mehr sichtbar sind. Der Versuch diese Sicherheitslücken trotzdem auszunützen, wird von der Firewall verhindert.

Über ein entsprechendes Feature wurde für die Nutzer der Weboberfläche der Steuerungssoftware verschlüsselte Kommunikation (https) eingeführt und erzwungen, obwohl die dahinterliegende Software diesen Standard nicht unterstützt. Außerdem wurde dies nicht nur für die Benutzer aus dem IT-Netz forciert, sondern auch für Benutzer, die aus dem Automatisierungsnetzwerk zugreifen, indem diese Zugriffe von innen ebenso über die Firewall geleitet wurden.

Indem nun sämtliche Zugriffe auf und Kommunikation mit Komponenten, sowohl von innen als auch aus dem Business-IT-Netzwerk über die Firewall laufen, kann der Traffic auf verdächtige Daten und Kommunikation überprüft werden. Malware, Command & Control Traffic, Botnetkommunikation, Port Scans und viele weitere Angriffstechniken werden nicht nur erkannt, sondern zuverlässig verhindert.

Weiters wurde der Zugriff auf den Jumphost zu Wartungszwecken ebenso über die Firewall geschleust, wodurch zum einen auch dieser sensible Traffic kontrolliert und geschützt werden kann und zum anderen auch weitere Sicherheitsmechanismen wie Multi-Factor-Authentifizierung eingeführt werden konnten.

Durch die Einführung der spezialisierten OT-Security-Lösung von Claroty werden nun erstmalig sämtliche Assets im Automatisierungsnetzwerk automatisch erfasst und auf Schwachstellen und mögliche Bedrohungen überwacht. Dadurch konnte in vielen Fällen das Asset Management auf Papier oder in Excel durch eine moderne Lösung ersetzt werden, die noch dazu erlaubt die Security der Anlagenkomponenten signifikant zu erhöhen und Bedrohungen rasch zu erkennen.

3

IEC 62443

Der Cyber-Security-Standard für Industrie und Produktion

IEC 62443

Der Cyber-Security-Standard für Industrie und Produktion

Der IEC 62443 Standard ist gleich aus mehreren Gesichtspunkten ein wichtiger Baustein, der in jedem Cyber-Security-Konzept eines Unternehmens aus dem Industriebereich oder mit einem Produktionsfokus berücksichtigt werden sollte.

Es werden hier nicht nur fundamentale Konzepte wie etwa das des Defense-in-Depth, also der Verteidigungsmechanismen, welche über mehrere Schichten abgebildet werden und das Unterteilen von OT-Netzen in Zonen zwischen denen ein Kommunikationsfluss nur sehr eingeschränkt erlaubt ist beschrieben.

Die Verfasser folgen auch dem Ansatz, dass erfolgreiche Cyber-Security-Maßnahmen mehr umfassen als rein technische Vorkehrungen.

Der Standard richtet sich nicht nur an Anlagenbetreiber, sondern auch an Lieferanten und Produkthersteller, wie auch an System- und Lösungsintegratoren und deckt damit das volle Spektrum zum Thema Cyber-Security im Umfeld von Industrieautomatisierung und -steuerung ab.

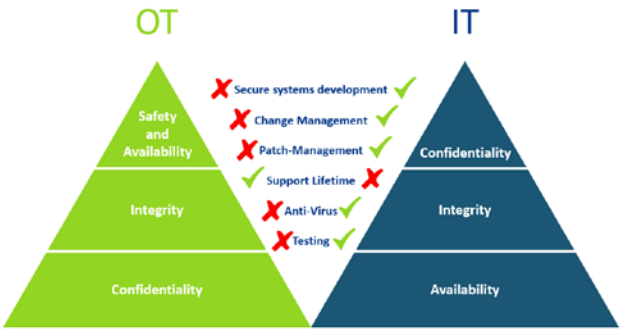


Abbildung 6: Unterschiedliche Anforderungen und Herausforderungen in OT und IT

Auch wenn viele der im IT-Umfeld gängigen Security-Praktiken im OT-Bereich mittel- bis langfristig Einzug finden werden müssen, gibt es doch starke Unterschiede der Anforderungen betreffend oder auch in Bezug auf die möglichen Maßnahmen in einem OT-Netzwerk, verglichen mit dem was man aus der IT-Welt gewohnt ist, wie Abbildung 6 beispielhaft beschreibt.

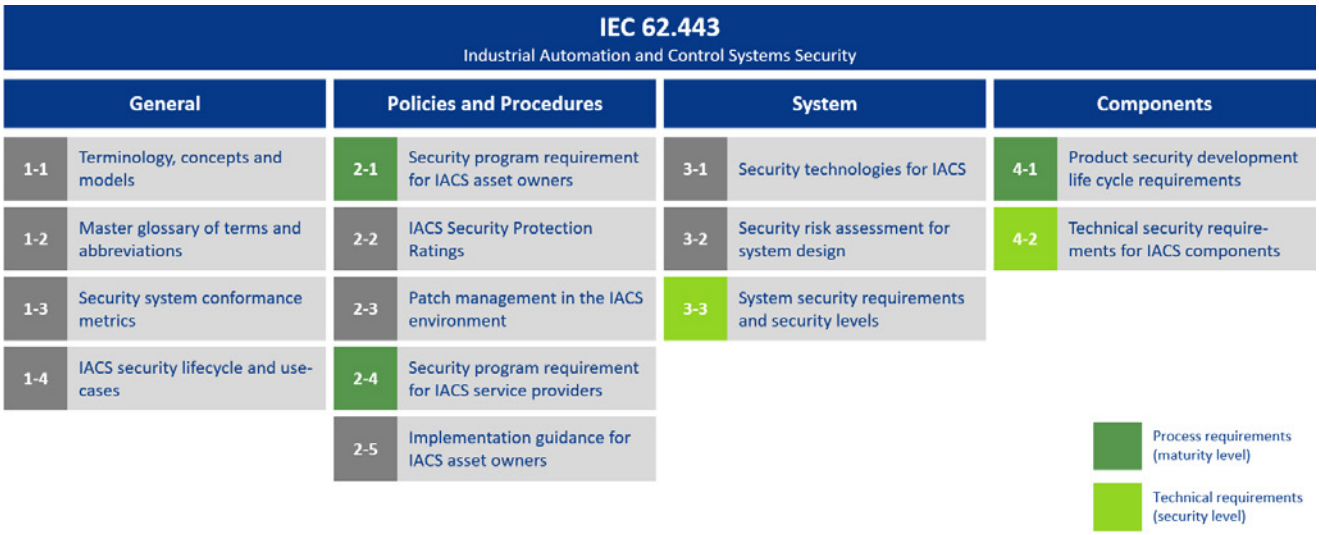


Abbildung 7: Der IEC 62443 Standard ist spezialisiert auf industrielle Automatisierung und deckt neben technischen Vorkehrungen auch Prozessverbesserungen ab.

Defense-in-Depth

Das sogenannte Defense-in-Depth-Prinzip findet nicht nur im OT-Umfeld Anwendung, sondern überall dort, wo man es Angreifenden möglichst schwer machen will, an wertvolle Daten oder Assets zu kommen.

Der Grundgedanke dahinter ist, ähnlich wie bei einer Burgfestungs-Anlage mit mehreren Sicherungsringen, (Wassergräben, Burgmauern, etc.) Angreifende daran zu hindern, beim Einnehmen eines Sicherungsringes, die zentrale Burg, umgelegt auf IT/OT, die wertvollen Daten oder Assets einzunehmen.

Im Cyber-Security Bezug, nennt man diese Sicherungsringe Layer.

Die Layer sollten das zu schützende Gut, meistens Daten, im OT-Umfeld zum Beispiel der eigentliche Produktionsprozess, schützend umschließen. Vergleichbar mit einer Zwiebel, legen sich Schicht für Schicht, also mehrere schützende Schalen, um den eigentlichen Kern und erschweren einem potenziellen Eindringling somit den Zugriff darauf.

Im Englischen spricht man deshalb vom sogenannten Onion Approach.

Optimalerweise ist dann noch jeder Layer mit individuellen Schutzmechanismen versehen, so dass beim Aufbrechen eines Layers, die dabei gewonnenen Erkenntnisse nicht dafür genutzt werden können, den nächsten Layer zu überwinden.

Das mehrschichtige Sicherheitsmodell in Abbildung 8 beschreibt den klassischen Ansatz des Defense-in-Depth-Konzeptes. Die Schichten werden in den unterschiedlichen Technologien und physischen Bereichen des Gesamtsystems eingezogen und können dadurch auch mit unterschiedlichen, auf den jeweiligen Technologiebereich ausgerichteten, Maßnahmen abgesichert werden.

So unterscheiden sich die Möglichkeiten einen Netzwerk-Ring zu sichern, von jenen Möglichkeiten, die einem im Applikations-Bereich zur Verfügung stehen. Die Angreifenden können dadurch gewonnene Informationen beim Überwinden einer Schicht nicht automatisch beim Überwinden der nächsten Schicht weiterverwenden.

Die klassischen Layer und Schutzmethoden in einem solchen Defense-in-Depth-Konzept sind beispielsweise die Folgenden:

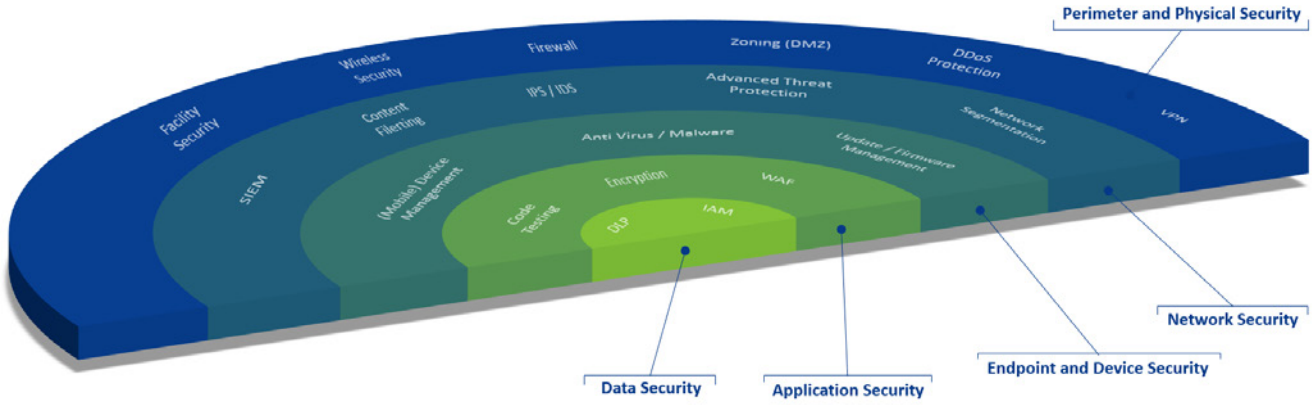


Abbildung 8: Defense-in-Depth beschreibt ein mehrschichtiges Sicherheitsmodell, vergleichbar mit einer Burgfestung und mehreren Sicherungsringen.

Data Layer — Meist der zu schützende Kern mit sensiblen Daten, die durch Verschlüsselung oder spezielle Zugriffsrechte geschützt werden können.

Application Layer — Auf Daten wird meist mittels Standards oder individuellen Applikationen zugegriffen. Diese sollten durch ein durchgängiges Patchmanagement immer auf dem letzten Stand gehalten und dadurch bekannte Sicherheitslücken zeitnah geschlossen werden.

Endpoint and Device Layer — Die Applikationen und dafür benötigten Softwarekomponenten laufen in der Regel auf einer physischen Plattform (Server, PC, Mobile oder Embedded Device) und auf dem dazugehörigen Betriebssystem (Unix, Windows, etc.). Diese Einheit aus Hardware und Software sollte ebenso zentral erfasst (inventarisiert) und damit bekannt sein, um über entsprechende Maßnahmen geschützt zu werden (Antiviren oder Antimalware Lösungen, etc.).

Network Layer — Speziell im Netzwerk-Bereich gibt es eine Vielzahl an Möglichkeiten die Kommunikation von und mit einzelnen Devices zu überwachen, einzuschränken und im Bedarfsfall zu schützen. Klassische Maßnahmen sind hier etwa interne Firewalls, Segmentierung oder *Intrusion Prevention Systeme* (IPS).

Perimeter and Physical Layer — Die meisten Unternehmen fokussieren ihre Sicherheitsmaßnahmen auf den äußersten Ring, sichern diesen beispielsweise mit Perimeter-Firewalls und physischen Schutzeinrichtungen (Kameraüberwachung, Zutrittssysteme, etc.) und versuchen damit dem Eindringen externer Angreifer in ihre firmeninterne Infrastruktur einen Riegel vorzuschieben.

Leider enden die Maßnahmen dann nur allzu oft in diesem äußersten Perimeter und machen es damit Eindringlingen, die diesen überwunden haben, beziehungsweise einem Angriff, der bereits im Inneren eines Unternehmens-Netzwerkes startet, nur allzu leicht, weiter in dahinterliegende Systeme einzudringen.

Zonen und Security Levels

Ein weiteres, weit verbreitetes und in IEC 62443 beschriebenes Konzept, basiert ebenso auf dem Defense-in-Depth-Prinzip, also der Absicherung in mehreren Schichten und ist ebenso ein bewährtes Vorgehen in der klassischen IT, das sogenannte Segmentieren.

Während die reine Aufteilung von Netzwerken in mehrere Sub-Segmente anfänglich dazu verwendet wurde Netzwerk-Traffic (Broadcast Traffic, etc.) einzugrenzen, bildet es nun immer häufiger auch die Grundlage dafür, Sicherungsmaßnahmen beim Übergang von einem Segment in ein anderes aufzubauen.

Üblicherweise geschieht dies mit Firewalls. Es können dabei aber auch erweiterte, eher passive Funktionen wie Intrusion Detection oder aktive wie Intrusion Prevention eingebaut werden, die beispielsweise als sogenannte Features auf den Firewalls mitlaufen oder als eigene Appliances in den Übergängen implementiert werden.

Bei der Segmentierung versucht man Assets mit ähnlichen Security-Anforderungen in Zonen zusammenzufassen und diesen dann sogenannten Security Levels zuzuordnen.

Die Levels in Abbildung 9 beschreiben die Netzwerkschichten der Automatisierungspyramide des “Purdue Reference Model“. Trotz ähnlicher Bezeichnung entsprechen sie nicht den in IEC 62443 beschriebenen Security Levels, lassen sich aber beispielhaft dafür verwenden, um eine Vorstellung für eine solche Auftrennung in Levels zu bekommen.

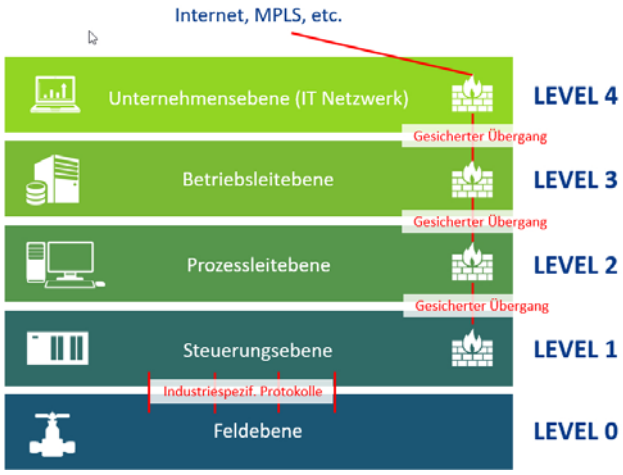


Abbildung 9: Beispiel typischer Zonen und gesicherter Übergänge in einer ICS-Architektur

Dringen Angreifer nun erfolgreich in das Unternehmensnetzwerk auf Level 4 ein, dann müssen diese sich erst noch durch weitere abgesicherte Zonen und Übergänge vorarbeiten, bevor sie mit der hochsensiblen Steuerungs- oder Feldebene in Kontakt kommen und dort physischen Schaden anrichten können.

Ebenso würde ein Ausbruch einer Malware auf Level 3, sich nicht automatisch auch auf das Unternehmensnetzwerk auf Level 4 oder die Prozessleitebene auf Level 2 auswirken.

Wichtig dabei ist, dass wirklich jeglicher Datenverkehr nur noch über die gesicherten Übergänge läuft und von diesen eingeschränkt und kontrolliert wird. Werden im Normalbetrieb, parallel dazu Schattennetzwerke und Übergänge aufgebaut, um die eingeschränkten und gesicherten Kommunikationswege zu umgehen, führt das dazu, dass das gesamte Sicherheitskonzept kompromittiert und ad-absurdum geführt wird.

Die jeweiligen Security Levels (SL1 bis SL4) werden in IEC 62443 mit einem Anforderungsprofil beschrieben, in dem genau festgelegt ist, mit welchen Skills, welcher Motivation und welchen Ressourcen potenzielle Angreifer ausgestattet sein müssen, um in den jeweiligen Security Level vorzudringen.

Diese Beschreibung hilft bei der Einteilung dafür, welche Assets sich in welchem Level befinden sollten und ebenso welche Sicherheitsmaßnahmen in den jeweiligen Levels getroffen werden müssen, um diese abzusichern.

Prozesse und Maturity Levels

Wie eingangs erwähnt umfasst IEC 62443 nicht nur technische Anforderungen, sondern begreift ein vollständiges Security-Konzept als Zusammenspiel von technischen und menschlichen, also auch prozessualen Komponenten.

Während die vorher beschriebenen Security Levels die Anforderungen an technische Sicherheitsmaßnahmen definieren, beschreiben die sogenannten Maturity Levels die Anforderungen an den Reifegrad von Prozessen, die Service Provider und Asset Owner implementieren und erfüllen müssen.

Dabei wird, ähnlich den Security Levels, nach vier Stufen unterschieden, von „Level 1 – Initial“, mit einem sehr niedrigen Reifegrad bis zu „Level 4 – Improved“ mit dem höchsten Reifegrad.

Zusammenfassung und Tipps

Kurz zusammengefasst sind die wichtigsten Punkte, die man als Denkanstoß bei der Entwicklung eines umfassenden Security-Konzeptes aus IEC 62443 mitnehmen sollte, die Folgenden:

Gesamtheitliche Betrachtung — Um Cyber-Sicherheit vollumfänglich abzudecken, müssen alle Beteiligten im Boot sein und Security-Maßnahmen bereits im Design und in der Grundkonfiguration mitbedacht und berücksichtigt werden.

Das spielt zum einen eine Rolle, wenn Systemintegratoren Komponenten auswählen und zusammenschalten, die von einem oder unterschiedlichen Lieferanten hergestellt werden, dann aber vom Asset Owner betrieben werden müssen.

Zum anderen aber auch, wenn technische Maßnahmen für einen Teil der Sicherheit Sorge tragen, viele andere Teile aber nur über Prozesse und letztendlich dem Verständnis und der Awareness von Menschen abgedeckt werden können.

Defense-in-Depth — Das Konzept von mehrschichtigen Sicherungsringen ist ein zentraler Punkt beim Aufbau von Cyber-Security-Architekturen und kann in vielerlei Hinsicht angewendet werden. Sei es, indem man die unterschiedlichen Technologien (Netzwerk bis Daten) als eigens abzusichernde Schichten betrachtet oder indem man Assets gemäß ihrer Sicherheitsanforderungen zusammenfasst und in verschiedenen Schichten voneinander abtrennt und absichert.

Strukturieren und Priorisieren — Das Konzept der Zonen und Sicherheitslevel zeigt auch wie wichtig es ist, sich Gedanken darüber zu machen, ob wirklich alle Assets gleich wichtig sind und deshalb gleich priorisiert werden sollten. Das macht auch aus betriebswirtschaftlicher Sicht Sinn, da zur Verfügung stehende Mittel so effizienter eingesetzt werden können und es dabei hilft den Fokus und Überblick zu behalten.

4 Critical Security Controls

Nur 5 Maßnahmen reduzieren erfolgreiche Cyberangriffe um 85 %

CIS Critical Security Controls

Nur 5 Maßnahmen reduzieren erfolgreiche Cyberangriffe um 85 %

Dem „Industrial Cybersecurity Survey“ Report 2020 von TrendMicro [4] zufolge, bei dem weltweit mehr als 500 Unternehmen, 200 davon aus Deutschland, befragt wurden, setzen Industrie und produzierende Unternehmen, vor allem im deutschsprachigen Raum, sehr stark auf das *CIS Controls Framework*. Ein Anreiz dafür dürfte der sehr pragmatische Ansatz mit den konkreten Handlungsempfehlungen sein, den man mit den CIS Controls geliefert bekommt.

Es gibt neben den CIS Controls zwar noch weitere Frameworks, wie das NIST CSF (Cyber Security Framework), wo der Umfrage nach, noch mehr Unternehmen die Notwendigkeit einer Entsprechung sehen, deren Umsetzung aber mit einem ungleich höheren Aufwand einzustufen ist.

Der sehr pragmatische und zielgerichtete Ansatz der CIS Controls führt einer Studie [5] zufolge dazu, dass 85 % der erfolgreichen Cyberangriffe verhindert werden, wenn man nur die ersten fünf Basic Maßnahmen der CIS Controls implementiert.

Implementiert man alle 20 Maßnahmen, so können sogar 97 % der Angriffe abgewehrt werden.

Obwohl die meisten Maßnahmen der bisher gültigen Version 7 der CIS Controls – seit 2021 ist die Version 8, mit kleineren Veränderungen released – auf technische Maßnahmen abzielen, berücksichtigt CIS, wie auch die meisten anderen Security-Frameworks, ebenso organisatorische Vorkehrungen.

Wir wollen beispielhaft hier die ersten fünf Maßnahmen anführen um den, aus unserer Sicht sehr guten Ansatz der CIS Controls zu verdeutlichen. Das vollständige und aktuellste Framework bekommt man kostenlos auf der CIS-Security-Website [6] zum Download angeboten.

CIS Critical Security Controls
Center for Internet Security – Version 7.1

Basic		Foundational		Foundational		Organizational	
1	Inventory and Control of Hardware Assets	7	Email and Web Browser Protections	12	Boundary Defense	17	Implement a Security Awareness and Training Program
2	Inventory and Control of Software Assets	8	Malware Defenses	13	Data Protection	18	Application Software Security
3	Continuous Vulnerability Management	9	Limitation and Control of Ports, Protocols and Services	14	Controlled Access based on the Need to Know	19	Incident Response and Management
4	Controlled Use of Administrative Priviledges	10	Data Recovery Capabilities	15	Wireless Access Control	20	Penetration Tests and Red Team Exercises
5	Secure Configuration for HW and SW on Devices and Server	11	Secure Configuration for Network Devices	16	Account Monitoring and Control		
6	Maintenance, Monitoring and Analysis of Audit Logs						

Abbildung 10: Die 20 CIS Controls unterteilt in die drei Hauptgruppen Basic, Foundational und Organizational

1. Inventory and Control of Hardware Assets

Ein sogenannter Attack-Vector in ein abgesichertes Netzwerk führt oft über ein manipuliertes oder schlecht abgesichertes, vielleicht nicht auf den letzten Softwarestand gepatchtes, Hardware Device. Das kann sowohl klassisch ein PC oder Server sein, genauso gut und dabei meist viel weniger beachtet, sind das aber Embedded Devices wie WLAN-Accesspoints, schlecht gesicherte Webcams oder andere IoT-Devices.

Um einen Überblick darüber zu haben, mit welchen Geräten man als Unternehmen überhaupt konfrontiert ist, neue und möglicherweise unautorisierte Devices zu erkennen, unsichere Systeme zu entfernen und ein flächendeckendes Patchmanagement zu implementieren, ist es deshalb unerlässlich eine umfassende Inventarisierung aller seiner Hardware-Assets durchzuführen und diese laufend auf dem letzten Stand zu halten. Dies erfordert eine entsprechende Automatisierung im Hintergrund.

Neben der reinen Inventarisierung bekommt man über verschiedenste Technologien hinaus die Möglichkeit, unbekannte oder unsichere Hardware, die erlaubt oder unerlaubt, in das Netzwerk eingebracht wurde, zu erkennen und entsprechend rasch Maßnahmen dagegen zu ergreifen.

2. Inventory and Control of Software Assets

Vergleichbar mit dem ersten CIS Control, der Inventarisierung von Hardware, muss natürlich auch die darauf laufende Software erfasst und kontrolliert werden.

Genauso wie bei der Hardware, sollte auch bei der Software, egal ob es sich um Betriebssysteme, Firmware oder sonstige Applikationen handelt, automatisiert vorgegangen werden, um immer über eine aktuelle Datenbasis zu verfügen. Da auf jeder Hardware eine Vielzahl an Software-Produkten laufen kann, ist es hier noch viel wichtiger zu wissen, welche Software auf welcher Hardware läuft.

Neben den bereits unter Punkt 1 genannten Vorteilen, bietet die Inventarisierung von Software auch die Möglichkeit einen Gesamtüberblick über die Landschaft zu bekommen, Software und Services zu priorisieren, beispielsweise nach Kritikalität, als auch nach verschiedensten Gesichtspunkten zu kategorisieren, beispielsweise nach Aktualität, Unsicherheitsfaktoren, etc.

So kann die, durch die Inventarisierung erstellte Datenbasis zum einen zu einer Risikobewertung herangezogen werden und zum anderen können aufgrund dieser Daten auch Überlegungen angestellt werden, ob wirklich alle Softwarepakete benötigt werden, welche davon regelmäßig upgedatet oder getestet werden müssen beziehungsweise ob und welche Möglichkeiten es gibt eine Software zu schützen, wenn diese veraltet ist und nicht mehr upgedatet werden kann.

3. Continuous Vulnerability Management

Wie unter Punkt 2 beschrieben, ermöglicht erst eine vollständige Datenbasis über die eingesetzte Hard- und Software einen Überblick und das Management von möglichen Schwachstellen.

Die zur Verfügung stehenden Möglichkeiten, um sich über Schwachstellen einen Überblick zu verschaffen, sind vielfältig. Es ist ein lebendiger Prozess, der niemals abgeschlossen ist.

Zum einen deshalb, weil sich durch Wartungsfälle oder Erneuerungen eingesetzter Hard- und Software

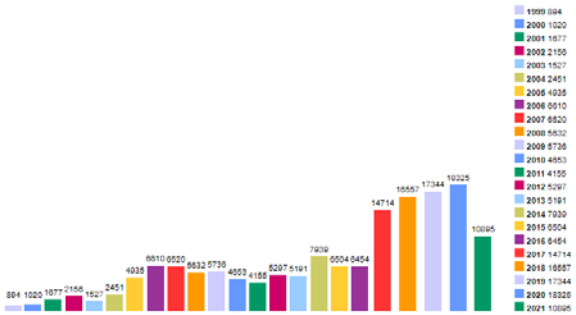


Abbildung 11: Jährlich werden an die 20.000 neue Schwachstellen offiziell gemeldet [10]

Versionsänderungen ergeben können. Zum anderen aber auch deshalb, weil auch Jahre später immer wieder neue Schwachstellen von produktiver Hard- und Software gemeldet werden.

Während man mit, zum Teil sogar kostenlosen, Open-Source-Tools wie *OpenVAS* [7] oder dem kommerziellen, größeren Bruder *Nessus* [8] technisch relativ leicht bestehende Systeme auf bekannte Schwachstellen überprüfen kann, sollten für das fortlaufende Schwachstellen-Management auch bekannte Internet-Quellen mit ihren RSS-Feeds und Mailinglisten, wie „Mitre CVE Database“ [9] oder verschiedener Hard- und Software Vendoren herangezogen werden.

Was in der reinen IT-Welt noch relativ einfach bewerkstelligt werden kann, ist im Umfeld von Produktionsumgebungen und Industrienetzen, sprich in der OT-Welt, nur mehr eingeschränkt, oft auch gar nicht möglich.

So können etwa einfachste aktive Scanning Methoden oder Schwachstellen Analysen in manchen Fällen dazu führen, dass ältere oder proprietäre Systeme gestört werden oder in einen Systemcrash laufen.

Zusatzinfo zu interessanten Tools

Über das als Open Source verfügbare „Metasploit Framework“ [11] ist es relativ einfach möglich, dedizierte Exploits für bekannte Schwachstellen auszuführen, das heißt diese aktiv auszunutzen.

Für viele der bekannten Schwachstellen, der sogenannten Common Vulnerabilities and Exposures (CVEs), gibt es bereits entsprechenden Schadcode (Exploits), der beispielsweise über die im Internet frei zugängliche Exploit Database [12] verfügbar ist.

4. Controlled Use of Administrative Privileges

Dieses CIS Control zielt auf eine, leider viel zu häufig erlebbare, Problematik ab. Nämlich dass für alltägliche oder sehr spezielle Aufgaben häufig Accounts mit viel zu weitreichenden Rechten wie beispielsweise Administratoren- oder Superuser-Accounts verwendet werden, obwohl diese Aufgaben auch mit sehr viel eingeschränkteren Rechten ausführbar wären.

Fällt ein solcher Admin-Account in die Hände von Angreifern, ist es diesen nicht nur möglich sich auf ein System Zugriff zu verschaffen, sie können meistens auch auf ein sehr umfangreiches Tool Set und auf tiefgreifende Konfigurationsmöglichkeiten am System zugreifen.

Dies erlaubt nicht nur die Installation von betriebsfremder Software, die für weitere Angriffe verwendet werden kann, sondern birgt weiters auch die Gefahr, dass im Hintergrund unbemerkt verschiedenste Überwachungs-software (Keylogger, Netzwerk-Sniffer, etc.) zum Einsatz kommen, mit denen die Angreifer an weitere sensible Informationen gelangen können.

Letztendlich ist es den Angreifern damit auch leicht möglich Logfiles zu löschen und Spuren des Einbruchs oder der Manipulation zu beseitigen.

Deshalb sollte es vor allem für sensible Systeme ein nachvollziehbares Berechtigungskonzept geben und BenutzerInnen immer mit einem möglichst niedrigen Rechteset und personalisierten Userprofilen ausgestattet werden.

Zusätzlich sollten Rechte, soweit möglich, zentral und automatisiert verwaltet und regelmäßig auf Angemessenheit überprüft werden. Dies bietet dann in weiterer Folge die Möglichkeit Passwortrichtlinien auszurollen und durchzusetzen (enforcen) oder Accounts, von aus dem Unternehmen ausgeschiedenen Mitarbeitern, automatisiert zu deaktivieren.

5. Secure Configuration for Hardware and Software

Dieses Security Control betrifft jegliche Form von Devices, wie Laptops, Workstations, Server, Mobile Devices aber auch Hardware, die oft nicht so sehr beachtet wird, wie netzwerkfähige Drucker, Webcams, Switches und andere Netzwerkgeräte.

Die meisten der oben angeführten Geräte werden mit Fokus auf Ease of Use konfiguriert und ausgeliefert, nicht mit dem Ziel möglichst eingeschränkter Nutzung oder höchstmöglicher Sicherheit.

Das führt dazu, dass keine oder dokumentierte Standard-Passwörter vergeben sind, Software installiert ist, die gar nicht genutzt wird oder Ports und Services offen sind, die unsicher, veraltet oder unbekannt und ungenutzt sind. Auch für nicht versierte Hacker ist das ein Einfallstor, das leicht genutzt werden kann, um in ein System oder Unternehmensnetzwerk einzudringen.

Wichtig ist also, dass man ebenso Konfigurationen, vor allem sicherheitsrelevante Konfigurationen, dokumentiert und verwaltet. Eine Grundüberlegung, anhand verschiedener Security- und Konfigurations-Richtlinien, sollte existieren und die Vorgabe für die Verwendung neuer und vorhandener Hard- und Softwarekonfigurationen darstellen.

Zusammenfassung und Tipps

Der zielgerichtete Ansatz der CIS Controls, ermöglicht auch Unternehmen, die sich bisher noch nicht so tief mit der Thematik Cyber-Security beschäftigt haben, einen schnellen und pragmatischen Einstieg.

Die 20 (in Version 8 nur noch 18) CIS Controls geben einen guten Überblick, auf welche Themenbereiche und Details man beim Aufbau eines Security-Konzeptes achten sollte und geben ganz konkrete Handlungsempfehlungen und Tipps.

Zusammengefasst sind dabei folgende Überlegungen von besonderem Wert:

80/20 Regel — Bereits mit überschaubarem Aufwand, nämlich durch die ersten fünf Controls, können über 80 % der Angriffe verhindert werden. Das bedeutet, dass mit jeder implementierten Maßnahme, sofort das Sicherheitslevel steigt, auch wenn das Gesamtkonzept noch nicht perfekt ist. Fazit: Erste Schritte machen und dranbleiben.

Überblick verschaffen — Man kann nur effektive Maßnahmen planen und durchführen, wenn man einen Überblick über seine Assets, Infrastruktur, Hard- und Software, Konfigurationen, User, etc. hat. Eine vollständige und aktuelle Datenbasis ist essenziell für weitere Schritte.

Unterstützung suchen — Man muss nicht alles selbst machen. Speziell bei den letzten vier organisatorischen Controls bieten sich einige Maßnahmen, wie etwa das regelmäßige Testen eigener Schutzmaßnahme oder Security-Teams geradezu an, dies von externen PartnerInnen durchführen zu lassen.

Customer Case study

Automaker Drives Towards Comprehensive OT Security with Claroty

As the scope of an auto manufacturer's operation grows, the complexity of its security requirements often increases exponentially. Struggling to gain a unified view into its operational technology (OT) security posture, this large automaker initially tapped Claroty for its comprehensive OT asset visibility offering.

This discovery led to a host of other benefits that ultimately helped the company improve availability, reliability, and safety across its entire OT environment.

Challenges

The company — like many others in its industry — sought a way to view, monitor and manage the security of its numerous production sites, each consisting of hundreds of assets, in order to proactively strengthen its OT security and more effectively manage the inherent risks.

1. **Complex and diverse attack surface:** Automakers typically have numerous factories, usually spread across a large geographic area, each comprising a wide range of networked devices. This poses a particular challenge in finding a scalable but consistent approach to OT security because the technical requirements for OT devices differ considerably across use cases and vendors.
2. **Unauthorized users and misconfigurations:** Operational complexity causes many automakers to struggle to effectively monitor and manage unauthorized remote access to OT environments. Furthermore, many also struggle to prevent unauthorized changes to OT assets, leading to misconfigurations and operational downtime.
3. **Lack of production-related alerting:** OT security incidents are often difficult to detect until after they have already begun to impact production, which has a cascading effect on operations. Precise and automated alerting are necessary to allow staff to respond quickly and keep the plant operational.

Customer Quote

"We have a few dozen factory sites across two continents. That translates thousands of assets in our entire manufacturing operation, so you can imagine the challenge of establishing a confident OT cybersecurity posture. Even just getting simple visibility of everything in our ecosystem is a huge challenge, and most solutions can't even do that basic thing very well. Of all the platforms we evaluated, only Claroty's was capable of giving us the unified view and total control we were looking for, and they did it with zero downtime. There honestly wasn't even a close second."

The Solution

After a comprehensive evaluation process, The Claroty Platform was chosen and deployed across an automobile manufacturing operation spanning more than 40 factories across two continents. Platform components utilized include:

Continuous Threat Detection (CTD) for full-spectrum OT asset visibility, continuous security monitoring, and real-time risk insights with zero impact to operational processes and underlying devices.

Secure Remote Access (SRA) to safeguard OT networks from threats introduced via potential misconfigurations and unauthorized users, including third-party contractors.

Enterprise Management Console (EMC) to simplify management overall, consolidating data from across The Claroty Platform and providing a unified view of assets, activities, and alerts across multiple sites. The platform also integrates seamlessly via the EMC for IT security infrastructure, wherever appropriate.

Outcomes

CTD immediately profiled all assets in the company's network and provided a depth and volume of detail on each asset that was unmatched by any other vendor evaluated. This process was achieved without disruption to operational processes.

SRA eliminated direct interactions between remote users and network assets by enforcing a secure, single-access pathway for remote diagnostics and maintenance operations. This elimination of direct interaction led to a dramatic increase in security best practices across the entire OT surface.

By giving the company a unified view of all devices in the ecosystem, even legacy devices in use since before modern cybersecurity was a primary design consideration are identified, monitored and secured. This comprehensive OT visibility and real-time threat detection empowered the company to be proactive about protection against a much wider range of threats.

About Claroty

Claroty bridges the industrial cybersecurity gap between information technology (IT) and operational technology (OT) environments. Organizations with highly automated production sites and factories that face significant security and financial risk especially need to bridge this gap.

Armed with Claroty's converged IT/OT solutions, these enterprises and critical infrastructure operators can leverage their existing IT security processes and technologies to improve the availability, safety, and reliability of their OT assets and networks seamlessly and without requiring downtime or dedicated teams. The result is more uptime and greater efficiency across business and production operations.

Backed and adopted by leading industrial automation vendors, Claroty is deployed on all seven continents globally. The company is headquartered in New York City and has received $100 million in funding since being launched by the famed Team8 foundry in 2015.

Contact

contact@claroty.com

5 Vorgehensweise und Empfehlungen aus der Praxis

Schritt für Schritt zu mehr Cyber-Sicherheit und Resilienz

Vorgehensweise und Empfehlungen aus der Praxis

Schritt für Schritt zu mehr Cyber-Sicherheit und Resilienz

Viele Standards und Normen beschreiben eine theoretische und ganzheitliche Herangehensweise bei der Entwicklung eines Cyber-Security-Konzeptes. Das ist auch gut so, weil dadurch mögliche blinde Flecken aufgedeckt werden und man einen guten Überblick über ein sinnvolles, zukünftiges Gesamtbild bekommt.

In der Praxis sehen sich die meisten Unternehmen jedoch mit ganz konkreten Herausforderungen konfrontiert.

Es gibt bereits gewachsene Infrastrukturen und vorhandene Sicherheitslösungen, IT- und OT-Netzwerke sind maximal gefordert, mit aktuellen technischen Weiterentwicklungen oder neuen Anforderungen aus dem Business Schritt zu halten. Nebenbei setzt auch der permanente Fachkräftemangel, welcher nicht nur in den Kerngeschäftsbereichen, sondern vor allem bei IT-nahen Berufsbildern vorherrschend ist, viele Unternehmen zusätzlich unter Druck.

Kommen dann, durch Digitalisierung und veränderte Kundenanforderungen, auch noch die klassischen Geschäftsmodelle unter Druck und erfordern zusätzliche Aufmerksamkeit, bleiben Risiko- und Zukunftsthemen wie Cyber-Resilienz, die keinen unmittelbaren ROI liefern, nur allzu oft auf der Strecke.

Umso wichtiger ist es, mit pragmatischen und effektiven Maßnahmen in kleineren Schritten eine permanente Weiterentwicklung der Cyber-Sicherheit voranzutreiben. Dadurch kann auch sehr agil auf neue Bedrohungsarten und Herausforderungen reagiert werden, statt mit umfangreichen Konzepten und weitreichenden Infrastrukturänderungen in der Planungsphase hängenzubleiben.

Gleichzeitig sollte jeder dieser einzelnen Schritte und Verbesserungsmaßnahmen ein stimmiger Teil einer letztendlich mehrschichtigen und auch mehrdimensionalen Security-Architektur sein, die größtmögliche Sicherheit gewährleistet und deren Betrieb und Weiterentwicklung nur auf diese Weise effizient möglich ist.

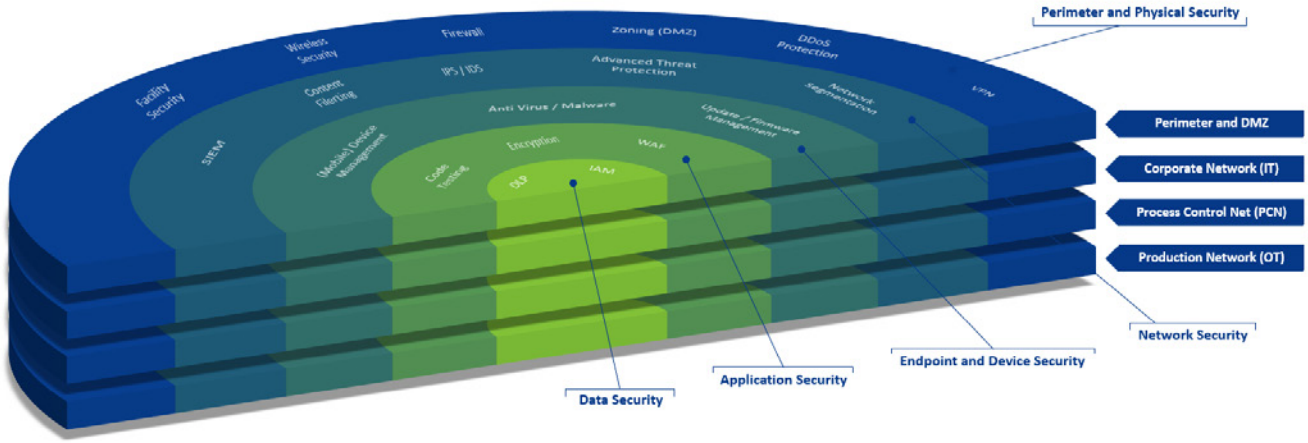


Abbildung 12: Defense-in-Depth-Konzept, in mehreren Schichten und mehreren Dimensionen, bietet größtmöglichen Schutz, muss aber auch effizient betreib- und weiterentwickelbar sein

Jede Reise beginnt mit dem ersten Schritt

Während bei geografischen Reisen der Startpunkt meistens klar ist und sich die Planung auf das Ziel und die eigentliche Reiseaktivität beschränkt, spielt beim Weg zu mehr Cyber-Sicherheit, auch die Bestimmung der aktuellen Position und des derzeitigen Reifegrades eine wichtige Rolle.

Manche Unternehmen wissen sehr gut darüber Bescheid, wie es um die Sicherheit Ihrer Produktionsumgebungen, Daten oder der des Unternehmens selbst bestellt ist. Bei manch anderen zeigt ein aktueller Vorfall auf, dass Handlungsbedarf besteht, und wieder andere sehen sich durch Dritte (Auditoren, Kunden, rechtliche Anforderungen, etc.) dazu gezwungen, sich mit dem Thema Cyber-Security näher zu beschäftigen.
In vielen Fällen macht es aber Sinn, sich einen verlässlichen Partner mit Erfahrung ins Boot zu holen, der speziell bei der Einschätzung der Ist-Situation und Risikobewertung (Stichwort: Penetration Testing und Sicherheitsaudits), bei der Evaluierung der aktuellen und zukünftigen Anforderungen, sowie bei der Konzeptionierung und möglicherweise bei der Implementierung erster Schritte beraten und begleiten kann.

Bei kleineren Unternehmen, ohne eigene IT-Einheiten oder IT-Security-Teams, könnte auch die Auslagerung von Teilen oder der gesamten Cyber-Security-Infrastruktur eine überlegenswerte Möglichkeit darstellen.

People first

Nach wie vor spielen Menschen eine entscheidende Rolle, wenn es darum geht, dass Sicherheitsmaßnahmen funktionieren, beziehungsweise erfolgreich umgangen werden konnten.

Die Awareness von MitarbeiterInnen, warum es bei bestimmten Prozessen und Vorgaben keinen Spielraum gibt und das Verständnis dafür, in welchen Situationen sie adäquat reagieren müssen, ist essenziell dafür, dass Cyber-Security-Maßnahmen funktionieren und Angriffe verhindert werden können und findet sich deshalb auch in jedem Konzept und Leitfaden wieder.

Das raffinierteste Maßnahmenpaket, das MitarbeiterInnen im Unternehmen vor Schadsoftware und anderen Gefahren schützt, ist unter Umständen wirkungslos, wenn sich beispielsweise MitarbeiterInnen mit ihren Firmennotebooks in einen öffentlichen, unsicheren WLAN-Hotspot einloggen.

Gleichzeitig entsprechen Investitionen in Sensibilisierung und Training von MitarbeiterInnen, dem zuvor im Kapitel CIS – Critical Security Controls beschriebenen Ansatz der 80:20 Regel. Da mit einem sehr überschaubaren finanziellen Aufwand, sehr rasch ein positiver Effekt zu mehr Sicherheit erreicht werden kann.

Abbildung 13: Beispiele technischer Möglichkeiten für Endpoint und User Protection

Schritt 1: OT Isolation

Auch wenn mit neuen technologischen Möglichkeiten und Entwicklungen wie verschiedensten Cloud Services, IoT Devices und neuen „DataDriven“ Geschäftsmodellen, OT- und IT-Welt zunehmend verschmelzen, besteht doch weiterhin Einvernehmen darüber, dass eine mehr oder weniger strikte Trennung der beiden Netzwerke, zumindest aus Security-Sicht, dringend notwendig ist.

Voraussetzung dafür, dass man das OT-Netz isolieren beziehungsweise vom IT-Netz abgrenzen kann ist, dass es separate Netzwerk-Segmente sind. Hier finden sich in der Praxis immer wieder auch Beispiele von gewachsenen Systemen, wo diese Trennung nicht von Grund auf geplant und durchgängig durchgeführt worden ist.

Aufgrund einzelner Anforderungen mag es Gründe geben, die Verbindungen zwischen dem IT- und OT-Netzwerk notwendig machen. Die Grundregel sollte jedoch immer sein, dass zumindest in Richtung OT-Netz keine Daten fließen beziehungsweise kein Verbindungsaufbau möglich sein sollte.

Egal welche Restriktion beim Übergang von IT zu OT umgesetzt werden soll; in der Regel wird dies über klassische Firewalls oder Security Gateways realisiert.

Entsprechend der Kritikalität der zu schützenden Assets, der benötigten Ausfallssicherheit und weiterer Anforderungen wie Datenübertragungsraten und Betriebsfähigkeit reicht das Spektrum von Low-End Appliances oder Software Firewalls, die auf Standard-Betriebssystemen laufen, bis hin zu hoch performanten und skalierbaren High-End Firewall-Clustern, die zentral verwaltbar sind und eine Vielzahl an zusätzlichen Sicherheitsfeatures mitbringen.

So können zum Beispiel auch Funktionen eines Intrusion Prevention System (IPS) oder Next-Generation Threat Prevention Features wie Threat Extraction, Sandboxing und vieles mehr, von einer Firewall mitübernommen werden.

Bricht dann etwa im IT- beziehungsweise Enterprise-Netzwerk eine, über ein unsicheres Device eingeschleppte, Malware aus oder infiziert eine bisher noch unbekannte Schadsoftware Rechner im Büro-Netzwerk, so bleibt dieser Schaden begrenzt und kann nicht in die sensiblen Produktionsnetze übergreifen.
In kritischen Infrastrukturen, wie zum Beispiel Atomkraftwerken, kann es sogar sein, dass für sogenannte Critical Digital Assets (CDA‘s) von den einschlägigen Regulatorien [13] vorgeschrieben ist, diese mittels AirGap, also einer vollständigen galvanischen Trennung von anderen Netzwerken und Devices zu isolieren.

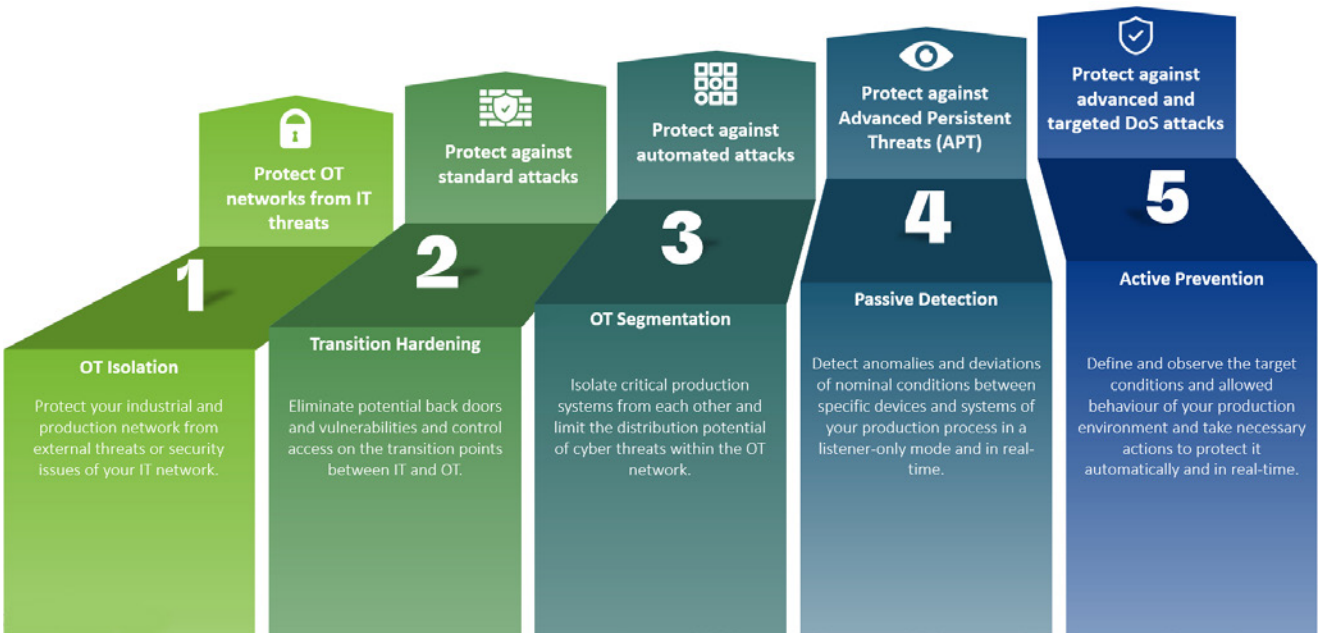


Abbildung 14: Evolutionsstufen von technischen Sicherheitsmaßnahmen, die sehr gezielt und pragmatisch, nacheinander beschritten werden können.

Hier setzt man etwa auf – in der IT-Welt eher unbekannte – Daten-Dioden, welche Datenströme nur in eine Richtung ermöglichen sollen und eine Manipulation sogar physisch unmöglich machen.

Schritt 2: Transition Hardening

Eine der Hauptherausforderungen vor denen Industrie- und produzierende Unternehmen im Angesicht von Industrie 4.0 und Industrial-IoT-Bestrebungen heute stehen ist, dass eine Vielzahl von Datenaustausch- und Zugriffsmöglichkeiten in Produktionsnetze existieren, die in über Jahre hinweg gewachsenen Systemen und Strukturen aufgebaut wurden.

Aus ERP-Systemen werden Daten an Produktionssteuerungssysteme übertragen, Wartungspersonal greift remote auf Maschinenkonfigurationen zu und über herstellerspezifische Kontrollstationen werden Logistiksysteme angesteuert, genauso wie Produktionsdaten aus IoT-Sensoren in die Cloud übertragen und dort ausgewertet werden.

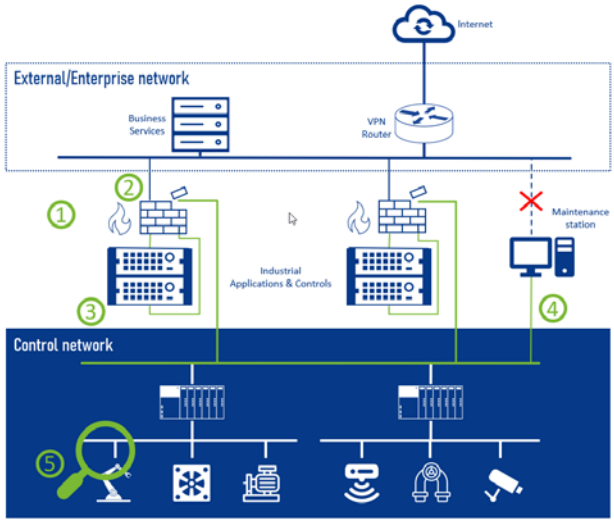


Abbildung 15: Beispiele von Möglichkeiten zur Absicherung des Übergangs von IT zu OT

Die Anforderungen und Möglichkeiten sind vielfältig und erfordern oft spezielle Lösungen. Vielen gemein ist aber, dass einmal implementierte Hard- und Software meistens nicht mehr aktualisiert wird und mit der Zeit veralten und somit ungeschützt, eine immer größer werdende Gefahr für Angriffe darstellen.

Spätestens wenn dann im Zuge von Zertifizierungen oder rechtlichen Vorschriften notwendige Sicherheitsaudits oder Penetrationstests im IT-Netzwerk durchgeführt werden, schlagen die kritischen Schwachstellen (die sogenannten Vulnerabilities) solcher Systeme ganz oben in den Management-Reports auf.

Auch wenn es nicht immer möglich ist Legacy Systeme auf den aktuellsten Stand zu bringen, gibt es eine Vielzahl an Möglichkeiten die Sicherheit dieser Systeme massiv zu erhöhen beziehungsweise sie durch vorgelagerte Sicherheitslösungen zu schützen wie Abbildung 15 zeigt.

Hier wurde ein Konzept entwickelt wie ein weltweiter Anbieter von Produktionssystemen die Legacy-Systeme in den Netzen seiner Kunden schützen kann, ohne diese austauschen oder upgraden zu müssen.

NextGen Security Gateways — können am Übergang von IT- zu OT-Netzwerk eingesetzt werden, um den Netzwerk-Traffic zu regulieren und auf Anomalien zu prüfen.

Authentifizierung und Verschlüsselung — können mitunter von veralteten Legacy-Systemen nicht mehr auf einem technisch zeitgemäßen Stand zur Verfügung gestellt werden. Dies kann aber von einer vorgeschalteten NextGen Firewall, wie beispielsweise der unter Abbildung 16 dargestellten, problemlos übernommen werden. Zusätzlich können damit auch Features wie 2-Factor-Authentication (2FA) relativ einfach eingeführt werden.

OT interner Netzwerk-Traffic – kann ebenso über das Security Gateway am Übergang gelenkt werden, um somit die dort verfügbaren Features wie Intrusion Prevention oder Intrusion Detection zu nutzen.

Unsichere Verbindungen verhindern — indem es keine direkten oder indirekten, zum Beispiel über veraltete Wartungsstationen, die als Gateway dienen, Verbindungen mehr in das Produktionsnetzwerk gibt. Auch solche Verbindungen werden kontrolliert über die Firewall und den dort aktivierbaren Sicherheitsmechanismen geführt.

Abbildung 16: NextGen Firewall zugeschnitten auf Anforderungen mittelständischer Unternehmen [14]

Schritt 3: OT Segmentation

Netzwerke zu gliedern und zu segmentieren ist nicht nur im IT-Umfeld gelebte Praxis, sondern entspricht im Wesentlichen auch dem im Kapitel über IEC 62.443 beschriebenen Konzept des mehrschichtigen Security Modells.

In den einzelnen Segmenten sollten Assets, einer im Vorhinein festgelegten, zugehörigen Logik folgen. Etwa die Aufteilung nach Security Levels oder entsprechend der Funktionen in der Automatisierungspyramide.
Der Übergang von einem Netzwerk-Segment in ein anderes muss dann immer über ein Security Gateway beziehungsweise eine Firewall abgesichert sein.
Dies gewährleistet, dass Angreifer, die sich bereits in ein Segment vorgearbeitet haben, nicht automatisch auch Zugriff auf den Rest der Assets haben. Noch viel wichtiger dabei ist aber, dass der Ausbruch einer Schadsoftware in einem Segment sich nicht sofort automatisch auch auf alle anderen Segmente ausbreitet, sondern in der Regel im Ausgangssegment isoliert werden kann.

Wie beim Übergang zwischen IT- und OT-Netz sollten auch zwischen den Segmenten klare Regeln zur Steuerung und Regulierung des Traffics definiert und umgesetzt werden.
Die Segmentierung von OT-Netzen ist absolut sinnvoll und klingt meist recht unspektakulär. In der Praxis werden dabei aber, aufgrund von Bequemlichkeit, Unwissenheit oder Mangels benötigter Hardware, oft Kompromisse eingegangen.

Dabei sind spezielle, auf industrielle Umgebungsbedingungen ausgelegte, Industrie-Firewalls wie beispielsweise die Rugged Appliance, die in Abbildung 17 zu sehen ist, relativ kostengünstig und bieten alle Features einer modernen Firewall mit zusätzlichen Möglichkeiten der Einbindung über LTE oder andere Mobilfunk oder Wireless Standards.

Industrielle Security Gateways können je nach Anwendungszweck auch ganz spezielle Aufgaben erfüllen und beispielsweise, in Form kleiner, gehärteter Appliances direkt vor einem Legacy Produktionssystem oder veralteten Steuerungsrechner eingebaut werden, um die Sicherheit des dahinterliegenden Systems zu gewährleisten.

Dabei werden unter anderem gezielt die jeweiligen Schwächen und Vulnerabilities des zu schützenden Systems abgesichert. Das dahinterliegende System muss nicht upgedated werden und genießt dennoch vollen Schutz. Diese Vorgehensweise bezeichnet man auch als Virtual Patching.

Abbildung 17: Spezielle Industrie-Firewall für den Einsatz unter härteren („rugged“) Bedingungen [15]

Schritt 4: Passive Detection

Während die in den ersten drei Schritten beschriebenen Maßnahmen eigentlich in jedem Unternehmen, in der einen oder anderen Form berücksichtigt oder bereits umgesetzt worden sein sollten, beschreibt Schritt 4 ein Thema, das in den letzten Jahren mehr und mehr Beachtung insbesondere auch bei produzierenden Unternehmen findet. Vor allem wenn sich diese aktiv mit dem Thema Cyber-Sicherheit auseinandersetzen.

In klassischen IT-Umgebungen finden Monitoring und Überwachung unter der Bezeichnung Security Information and Event Management (SIEM) immer mehr Anwendungsgebiete.

Der Grund dafür ist, dass moderne – mit leistungsstarken KI's (Künstliche Intelligenzen) ausgestattete SIEM-Systeme mehr und mehr in der Lage sind, mit einer geringen Anzahl an False-Positives in großen Datenmengen, Auffälligkeiten zu finden und so in Echtzeit selbstständig Angriffe und Ausbrüche von Schadsoftware erkennen und diese rund um die Uhr melden können.

Eine wichtige Ergänzung dieser passiven, aber dafür flächendeckenden Dauerüberwachung ist die regelmäßige Durchführung von Penetration-Tests, wo durch aktives Angreifen von Systemen Schwachstellen und Hintertüren erkannt und so rechtzeitig geschlossen werden können. Was in der IT-Welt immer mehr zur gelebten Praxis wird, ist in industriellen Umgebungen häufig noch undenkbar und würde, zumindest was automatisierte Gegenmaßnahmen angeht, wohl noch von den wenigsten Produktionsverantwortlichen genehmigt oder gern gesehen werden.

Was auch verständlich ist, wenn man bedenkt, dass die Verfügbarkeit und ungestörte Funktion des Produktionsbetriebes an oberster Stelle steht und nicht durch Aktionen wie der Suche nach Schwachstellen oder durch Maßnahmen zur vermeintlichen Abwehr eines Eindringlings in Gefahr gebracht werden darf.

Das ist auch der Grund, warum die allerwenigsten Produktionsunternehmen aktive oder automatisierte Scans oder Prozesse einsetzen und vorläufig lieber mit passiven Methoden und Werkzeugen arbeiten, um sich einen Überblick über die Komponenten und die Kommunikation ihrer Produktions-Infrastrukturen zu verschaffen und diese dauerhaft zu überwachen. Abbildung 18 zeigt die Ausgabe einer auf OT-Komponenten und Industrienetze spezialisierten Lösung, die nach einem ersten passiven Scan des Netzwerk-Traffics, eine Auflistung aller gefundenen Assets, mit den dazugehörigen Vulnerabilites oder Standardpasswörtern findet und bewertet.

Darüber hinaus kann die Lösung die hersteller- und industriespezifischen Kommunikations-protokolle (ProfiNet, Modbus, OPC UA, MQTT, etc.) erkennen und

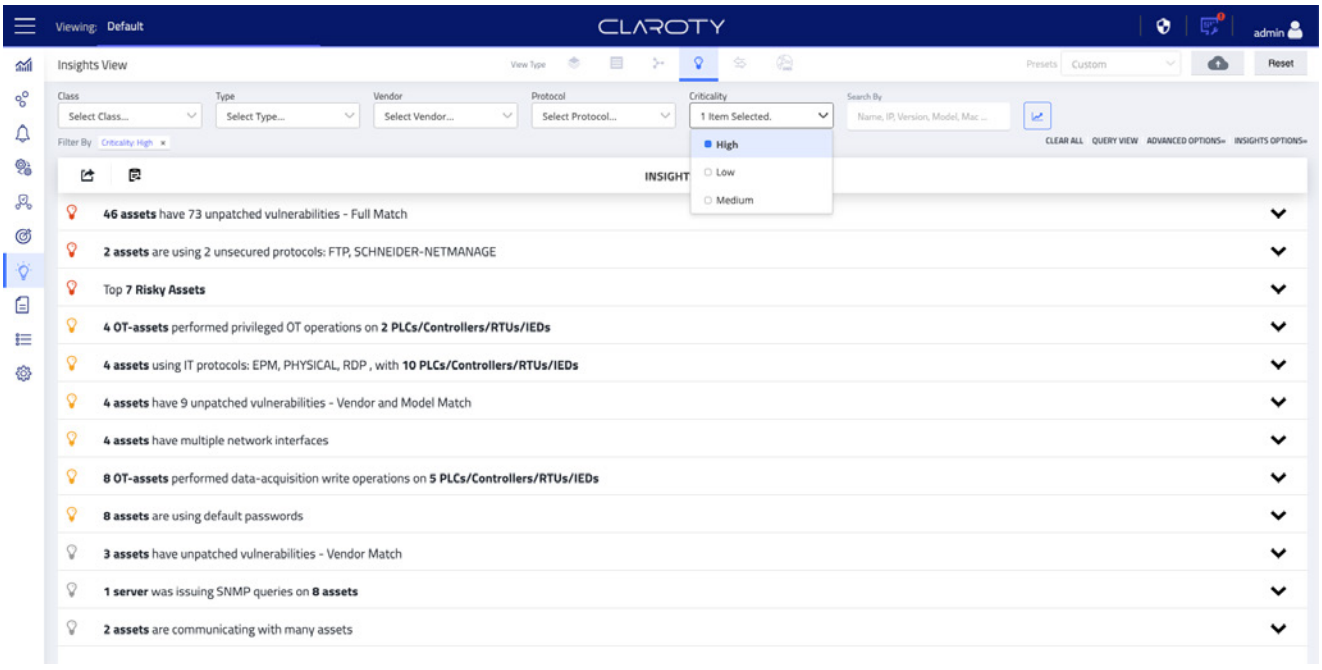


Abbildung 18: Auflistung der über passive Methoden gefundenen Assets, Schwachstellen und auffälligen Kommunikationen [16]

decodieren und ist dadurch in der Lage, ein Abbild aller Geräte im Netzwerk und der dazugehörigen Netzwerkkommunikation automatisiert zu erstellen. Man bekommt dadurch einen umfassenden Komponenten-Überblick, entdeckt Schatten-Infrastruktur und bisher unbekannte Kommunikationspfade genauso wie schlecht konfigurierte oder veraltete Hard- und Software.

Das ersetzt zwar nicht die Dokumentation, die in jedem OT-Betrieb genauso wie in der klassischen IT vorhanden sein sollte, liefert aber wichtige und bisher vielleicht nicht in der Form bekannte Zusatzinformationen.

Und, genauso wichtig, liefert eine automatisierte Inventorisierung, Informationen über nicht bekannte oder nicht dokumentierte Infrastruktur.

Damit ist die Grundlage geschaffen, zum einen pragmatische und schnell umsetzbare Maßnahmen zur unmittelbaren Verbesserung der Sicherheit zu setzen wie zum Beispiel den Austausch von bekannten Default-Passwörtern durch individuelle und damit sichere Passwörter. Zum anderen hat man damit aber auch den für die Planung weiterer Schritte oder zusätzlicher Konzepte, notwendigen Informationsstand geschaffen.

Schritt 5: Active Prevention

Unser letzter Schritt klingt für viele noch nach Zukunftsmusik und tatsächlich können sich nur wenige, vor allem mit bestehenden Produktionsumgebungen ausgestattete Unternehmen, vorstellen, das im Folgenden Beschriebene auch in vollem Umfang in der Praxis umzusetzen.

Die Rede ist davon, dass neben der unter Schritt 4 beschriebenen passiven Überwachung des Netzwerkverkehrs und den daraus gewonnenen Erkenntnissen, eine Art Normalzustand des Gesamtsystems erlernt wird. Das geht sogar so weit, dass es möglich wäre, genau vorzugeben mit welcher Drehzahl ein Motor angesteuert werden darf und welche Kommandos beziehungsweise Parameter vom Leitsystem an eine SPS geschickt werden dürfen.

Alles was nun nicht diesem gewohnten Normalzustand entspricht oder alles was über die vorab definierten Schwellwerte hinausgeht, wird nun nicht mehr nur als Warnung gemeldet, sondern zusätzlich in Echtzeit vollautomatisch auf der Netzwerkebene blockiert.

In IT-Umgebungen sind solche Mechanismen bereits seit Jahren in Form von Intrusion Prevention Systemen (IPS) oder auf IT-Endgeräten durch, auf Machine Learning Algorithmen basierenden, Anti-Malware-Schutzprogrammen im Einsatz.

Ja vielmehr, ist ein Security-Konzept ohne Vollautomation, das nur darauf basiert, dass wenn ein Sicherheitsvorfall auftritt, dieser gemeldet wird und jemand manuell eine Aktion durchführen muss, in der IT-Welt insbesondere in größeren oder komplexeren Umgebungen gar nicht mehr denkbar.

Dort ist aber auch wie bereits öfters erwähnt, eine zwischenzeitige Nichtverfügbarkeit eines Services, einem kritischen Security Vorfall in den meisten Fällen vorzuziehen und zieht andersherum in den seltensten Fällen einen nachhaltigen schweren Schaden nach sich. Besonders nicht von physischen Assets oder Menschen wie das in OT-Umgebungen der Fall sein könnte.

Im Moment noch würde im industriellen Umfeld, ein vollautomatisches Eingreifen in Produktions-prozesse in absoluten Widerspruch mit den hochkritischen Anforderungen der Safety Prozesse des einmal freigegebenen Betriebszustandes einer Produktionsanlage stehen und auch nicht den Anforderungen der EU Maschinenrichtlinie entsprechen.

Doch wird in den nächsten Jahren, vor allem bei neuen Projekten, immer öfter Security by Design und Security by Configuration mitbedacht und implementiert werden müssen. In diesem Zusammenhang können Lösungen wie die in diesem fünften Schritt beschriebenen, in Zukunft vielleicht dazu beitragen, dass zuvor festgelegte Rahmenbedingungen auf Netzwerkebene – also losgelöst von Applikation und Hardwarekomponenten – überwacht und durchgesetzt (enforced) werden und so Maschinen und Anlagen vollautomatisiert geschützt werden können.

6 Zusammenfassung und Empfehlungen

Ganz konkrete Tipps und Taktiken zum Loslegen

Zusammenfassung und Empfehlungen

Ganz konkrete Tipps und Taktiken zum Loslegen

Die bisherigen Seiten sollten einen guten Überblick über die theoretischen Konzepte, praktischen Anwendungen und konkreten Möglichkeiten gegeben haben.
Zum Abschluss ergeben sich aus dem bisher Gesagten also Tipps und Taktiken, die unabhängig vom gesetzten Ziel, dem eingeplanten Zeitrahmen oder dem zur Verfügung stehenden Budget, in jedem Fall Berücksichtigung finden sollten.

Denken Sie vielschichtig – Verstehen Sie Defense-in-Depth als zentrales Konzept, das Sie überall einsetzen können und sollten. Sei es im Einsatz unterschiedlicher Sicherheitslösungen in den unterschiedlichen Technologieschichten wie im Kapitel über IEC 62443 beschrieben, in Form von Segmentierung und Zoning der einzelnen Netzwerke und Assetklassen oder indem Sie Ihr Sicherheitskonzept möglichst breit denken und aufstellen. Dies reicht vom physikalischen Schutz Ihrer Gebäude, Produktionslinien und Einzelkomponenten, über die zahlreichen technischen Möglichkeiten, bis hin zu Prozessen und Menschen in Form von Guidelines, Trainings und regelmäßigen Überprüfungsszenarien.

Zentralisierung, Standardisierung und Automatisierung – Die meisten Unternehmen stehen vor dem Problem, Jahr für Jahr weniger Personal, für immer mehr Regeltätigkeiten zu haben. Um dabei langfristig nicht zu verlieren, hilft nur eine Strategie. Versuchen Sie so viel als möglich zu zentralisieren und zu standardisieren. Je weniger individuelle Prozesse, Tools und Tätigkeiten, desto mehr Zeit, Geld und Nerven sparen Sie.

Der Aufwand und die Kosten für Cyber-Security ihrer Produktionsstandorte darf sich nicht mit der Anzahl der Standorte multiplizieren, sondern muss effizient, zentral verwaltet werden können. Genauso dürfen Sie nicht den Überblick verlieren, nur weil immer mehr Notwendigkeiten bestehen, Wartungspersonal und Lieferanten von außen auf interne Systeme zugreifen zu lassen. Abbildung 19 zeigt, dass es für diese und viele andere Herausforderungen bereits Standardtools gibt, die Ihnen Überblick, zentrales Management und maximale Transparenz und Nachvollziehbarkeit bieten.

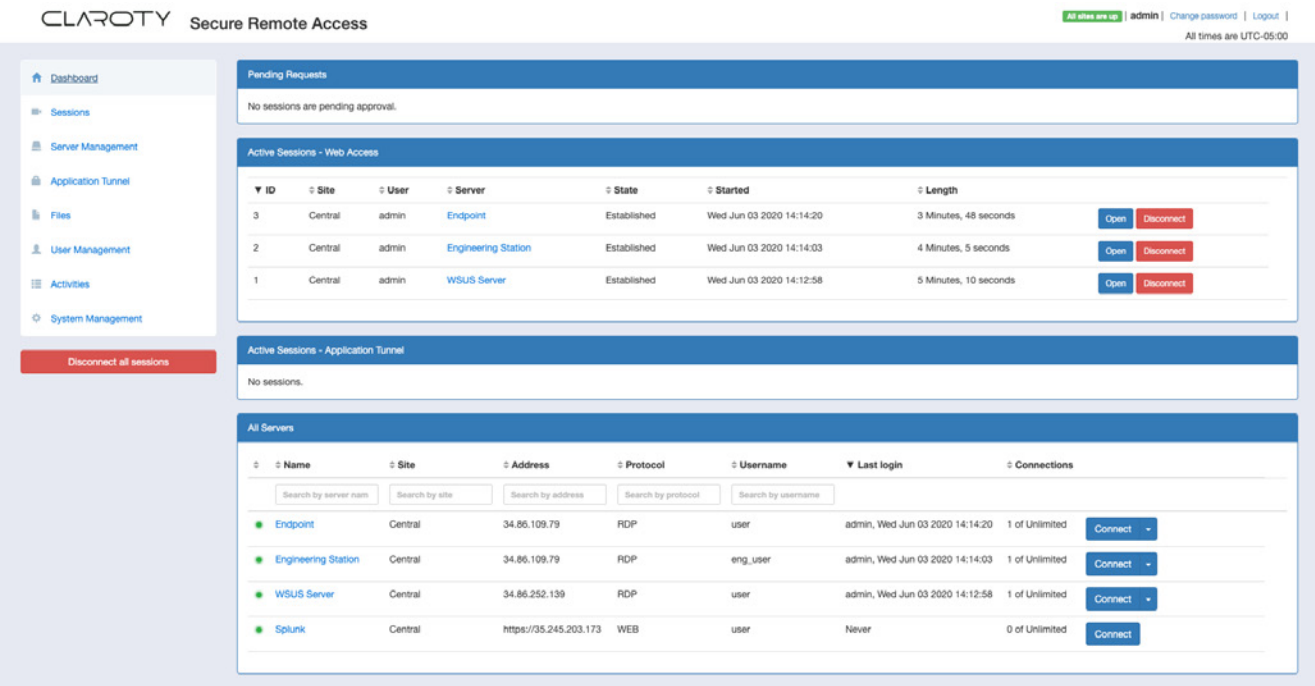


Abbildung 19: Lösung für Lieferanten- und Fernwartungszugänge, mit zahlreichen Möglichkeiten diese zentral zu verwalten und gezielt einzuschränken und zu überwachen

Konfigurations- und Asset-Management — Auch wenn Sie gerade, aus Ihrer Sicht wichtigere Maßnahmen geplant haben, ein tragfähiges Konfigurations- und Asset-Management zählt zu den wichtigsten Aspekten, wenn es um Themen wie strukturierte Weiterentwicklung und Absicherung von Leit- und Automatisierungstechnik geht.

Gerade bei größeren und komplexeren Umgebungen stößt eine Verwaltung mittels Excel oder eine, die rein auf manueller Erfassung basiert, schnell an ihre Grenzen oder skaliert schlichtweg nicht mehr.

Noch dazu sind die Vorteile einer detaillierten und permanent aktuellen System- und Konfigurationsdokumentation nicht nur wichtig bei der Absicherung der Systeme. Auch Regeltätigkeiten wie Systemwartung, notwendige Ausbauten und erste Schritte in Richtung Industrie 4.0 sind ohne diese Daten-Basis nur schwer oder mit großem Risiko zu stemmen.

Wie der eingangs beschriebene Stuxnet Angriff deutlich macht, bauen komplexere, cyber-physikalische Angriffe immer auf nicht-autorisierte Konfigurationsänderungen auf. Dabei sind oft nicht einmal Sicherheitslücken notwendig, sondern es wird Standardfunktionalität der Automatisierungstechnik quasi für ursprünglich nicht so vorgesehene Anwendungsfälle missbraucht. Wer also solche nicht-autorisierten Konfigurationsänderungen erkennen oder verhindern kann, kann sich auch vor solchen Angriffen wirksam schützen.

Moderne, auf Leit- und Automatisierungstechnik spezialisierte Konfigurations- und Asset-Management-Lösungen, bieten neben dem automatisierten Erkennen von unautorisierten Konfigurationsänderungen oder dem Einbringen von nicht autorisierter Hardware in das überwachte Netzwerk, auch noch viele andere Features an.

So werden zum Beispiel auch ungewöhnliche Zugriffe oder Datenflüsse auf Komponenten des Steuerungssystems gemeldet oder es können Wartungszugriffe von außerhalb, detailliert überwacht und eingeschränkt werden.

Systematisch pragmatisch — Da sich Technologien, Infrastrukturen und damit einhergehende Angriffsmöglichkeiten permanent weiterentwickeln, muss ein nachhaltiges Sicherheitskonzept ebenso kontinuierlich verbessert und auf vielen Ebenen angepasst werden.

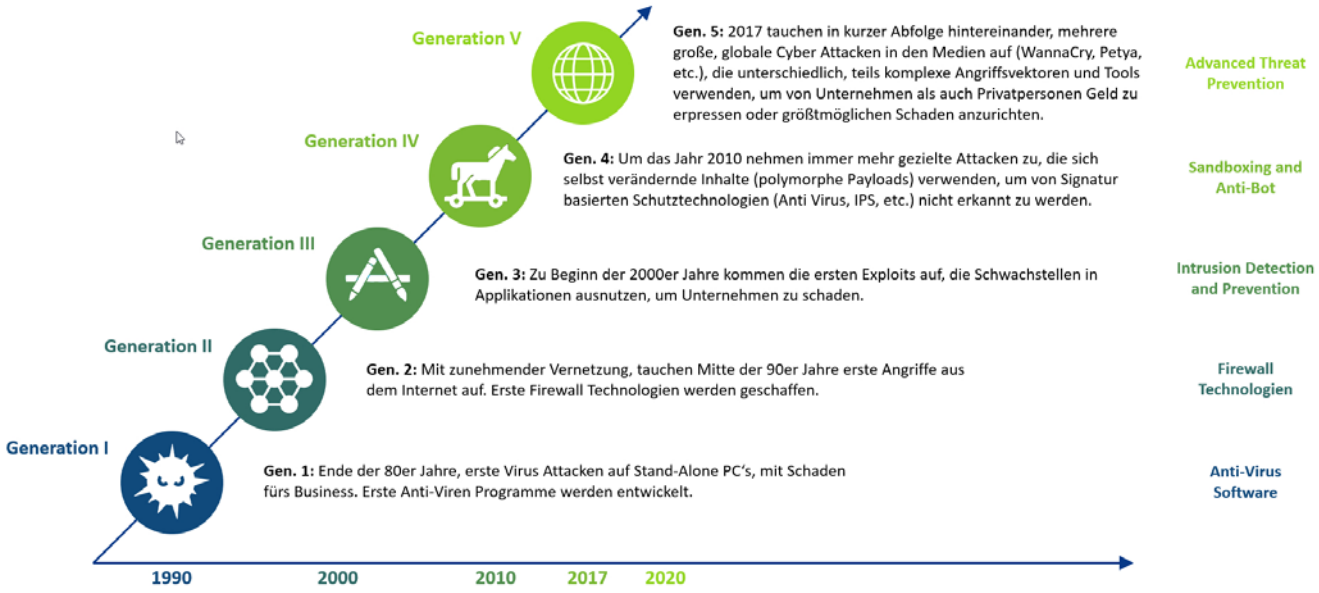


Abbildung 20: Die Evolution von Cyber-Bedrohungen und dagegen entwickelten Sicherheits-Technologien zeigt, dass Cyber-Security einer permanenten Weiterentwicklung unterliegt.

Zahlreiche Normen und Sicherheitssysteme wie auch die in diesem Artikel erwähnte IEC 62443 oder das allgemeinere ISO 27001 adressieren genau diese Herangehensweise, der ganzheitlichen und kontinuierlichen Verbesserungszyklen, sind aber relativ aufwändig in der Umsetzung, wenn man die enthaltenen Empfehlungen und Vorgaben in der vollen Breite mit praktischer und noch dazu betriebswirtschaftlicher Sinnhaftigkeit umsetzen möchte.

Wie bei vielen anderen Ansätzen zeigt sich auch hierbei, dass eine Kombination von langfristiger und systematischer Planung, mit pragmatischem, betriebswirtschaftlich sinnvollem Vorgehen am effizientesten ist.

Damit ist gemeint, dass man Zeit und Geld primär dort einsetzen sollte, wo man gemäß der 80/20 Regel, am schnellsten, die größtmögliche Verbesserung an Sicherheit schafft. Bestenfalls lässt sich diese Verbesserung dann sogar quantitativ oder qualitativ messen.

Gleichzeitig sollen diese Einzelmaßnahmen, sich gegenseitig ergänzend, gut in ein nachhaltiges Gesamtkonzept passen.

Personelle Verantwortung und dediziertes Budget — Der letzte und vielleicht sogar wichtigste Tipp ist: Richten sie eine dedizierte personelle Verantwortung für die Cyber-Sicherheit ihrer Produktionsstätten ein. Wo diese Person oder dieses Team organisatorisch angesiedelt ist, ist nicht so wichtig wie die Anforderung, dass sie unbedingt, zumindest grundlegende Kenntnisse in der Leit- und Automatisierungstechnik mitbringen muss.

Darüber hinaus sollte es sich um eine dedizierte Stelle (Teil- oder Vollzeit) handeln, das heißt um jemanden, der 100 % seiner verfügbaren Zeit dieser Tätigkeit widmen kann. In der Praxis funktionieren Aufteilungsschlüssel, wo jemand einen Teil seiner Zeit für ein bestimmtes Thema zuständig ist, meistens nur sehr mäßig, da im Tagesgeschäft fast immer etwas wichtiger ist als die systematische Weiterentwicklung von strategischen Themen.

Fazit

Würde man die wichtigsten, in diesem Dokument beschriebenen Konzepte und konkreten Schutzmechanismen implementieren, so ließe sich mit hoher Wahrscheinlichkeit sogar ein Angriff wie der, des im ersten Kapitel beschriebenen Stuxnet Virus, verhindern.

Die meisten Angriffe, auch auf Industrieanlagen, sind aber weit weniger komplex oder mit weit weniger Fachwissen und Ressourcen ausgestattete Attacken. Gegen solche Gefahren ist man auch mit Basismaßnahmen, wie sie etwa die CIS Security Controls empfehlen, schon recht gut abgesichert. Da sich ein individuelles Security Konzept in jedem Fall immer erst Schritt für Schritt entwickeln und vor allem auch weiterentwickeln muss, ist die Kombination von Basismaßnahmen, auf die dann entsprechend fortgeschrittenere Methoden aufgebaut werden können, ein sinnvoller Ansatz.

Das Wichtigste aber ist: Setzen Sie einen ersten Schritt und bleiben Sie dran!

Wir unterstützen Sie gerne dabei.

Kontakt

Unser Team für Ihre Anliegen

Markus Seme

Geschäftsführer BearingPoint Österreich
markus.seme@bearingpoint.com
https://www.linkedin.com/in/markus-seme-6bb67b15b/

Bernd Koberwein

Service Line Leader – Cyber Security
bernd.koberwein@bearingpoint.com
https://www.linkedin.com/in/bernd-koberwein/

Thomas Rossmann

Network and Security Architect
thomas.rossmann@bearingpoint.com

Erlend Depine

Head of Advanced Threat Inspection
erlend.depine@bearingpoint.com
https://www.linkedin.com/in/erlend-depine-5869082/

Quellenverweise

Interessante Quellen zum Nachlesen

[1] https://www.langner.com/wp-content/uploads/2017/08/Stuxnet-und-die-Folgen.pdf

[2] https://www.langner.com/wp-content/uploads/2017/08/Stuxnet-und-die-Folgen.pdf

[3] https://en.wikipedia.org/wiki/Purdue_Enterprise_Reference_Architecture

[4] https://resources.trendmicro.com/Industrial-Cybersecurity-WP.html

[5] https://www.tripwire.com/state-of-security/security-data-protection/security-controls/cis-top-20- critical-security-controls/

[6] https://www.cisecurity.org/controls/v8/

[7] https://www.openvas.org/

[8] https://de.tenable.com/products/nessus

[9] https://cve.mitre.org/index.html

[10] https://www.cvedetails.com/browse-by-date.php

[11] https://www.metasploit.com/get-started

[12] https://www.exploit-db.com/

[13] https://www.nrc.gov/docs/ML1801/ML18016A129.pdf

[14] https://www.checkpoint.com/de/products/midsize-enterprise-security/

[15] https://www.checkpoint.com/quantum/next-generation-firewall/industrial-control-systems-appliances/

[16] https://www.claroty.com/continuous-threat-detection/

Österreichs größtes Technologieberatungsunternehmen

Mit mehr als 500 Mitarbeiterinnen und Mitarbeitern in Österreich entwickeln wir innovative Strategien für neue und bestehende Geschäftsmodelle und konzipieren und implementieren digitale Lösungen und Services für führende Unternehmen und öffentliche Institutionen.

Vor allem in den Bereichen Software Entwicklung, Cloud- und Plattform Technologien und besonders im Bereich Cyber-Security, zählen wir im deutschsprachigen Raum zu den führenden Anbietern und erfahrensten Partnern an der Seite unserer Kunden.

Zu unseren Partnern zählen die Branchenleader unterschiedlichster Technologiebereiche. Im Cyber-Security-Umfeld liefern wir von der Konzeption über die Implementierung bis hin zum Betrieb von Gesamtlösungen für den Schutz von Endgeräten, genauso wie Netzwerk- und Cloud-Infrastruktur bis hin zur Absicherung sensibler Automatisierungs- und Steuerungstechnik aus Industrie und Produktion.

Zu den Kunden von BearingPoint zählen die führenden Unternehmen und Organisationen Österreichs. Das globale BearingPoint-Netzwerk mit mehr als 10.000 Mitarbeiterinnen und Mitarbeitern unterstützt Kunden in mehr als 75 Ländern und engagiert sich aktiv für messbare und nachhaltige Geschäftserfolge.

Für mehr Informationen besuchen Sie unsere Website: besecure.bearingpoint.com, bearingpoint.services oder www.bearingpoint.com

BearingPoint®