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

Vorwort 1

1 Das Ende einer Ära 4

2 Pyramiden haben ausgedient 8

Customer Case study 11

3 IEC 62443 14

4 Critical Security Controls 20

Customer Case study 25

5 Vorgehensweise und Empfehlungen aus der Praxis 28

6 Zusammenfassung und Empfehlungen 36

Fazit 40

Kontakt 41

Quellenverweise 42

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.