HIRSCHMANN
A BELDEN BRAND

White Paper

Cybersicherheit: Das Prinzip Hoffnung hat ausgedient

Prof. Dr. Tobias Heer – Senior Architekt für den Bereich Netzwerksicherheit, Hirschmann Automation and Control GmbH

Lukas Wüsteney – Architekt für den Bereich Industrial Networking, Hirschmann Automation and Control GmbH

Einleitung

Durch die enorme Häufung schwerer Cybersecurity-Vorfälle bei deutschen Leuchtturm-Unternehmen hat der Glauben an die Sicherheit der eigenen Firma und der Sicherheit der Industrie insgesamt einen schweren Knacks bekommen. Wer kann heute noch mit breiter Brust verkünden: „Unsere Firma ist sicher, es wird bei uns niemals einen Cybersicherheits-Vorfall geben!"? Aus dieser Unsicherheit erwächst nun die Frage: Wenn man sich der Sicherheit nicht mehr sicher sein kann, was kann man dann unternehmen, um mit dem unausweichlichen Fall einer erfolgreichen Cyberattacke richtig umzugehen und wie kann man strukturelle Vorkehrungen treffen, welche die Auswirkungen eines solchen Angriffs abfedern? Dieses White Paper beleuchtet das Zusammenspiel aus vorbeugenden Maßnahmen und Reaktionsmöglichkeiten, die in Industrie-Netzwerken getroffen und umgesetzt werden können, um sich nicht weiterhin auf das Prinzip Hoffnung verlassen zu müssen und stattdessen zukünftigen erfolgreichen Cyberangriffen besser gewappnet gegenüberzustehen.

Inhaltsverzeichnis

tripwire

HIRSCHMANN
A BELDEN BRAND

Be certain.
Belden.

Noch vor wenigen Jahren schien das Thema Cybersicherheit beherrschbar und übersichtlich zu sein. Eine Firewall, aktuelle Patches, ein Virenscanner auf den Endsystemen und ein VPN Gateway für die Kommunikation in die Firma hinein. Denn die Fertigung war nicht mit dem Rest der Welt verbunden und sowieso mit allen Werkzeugen der Angreifer technisch inkompatibel – so stellte sich die IT-Sicherheit für viele Unternehmen dar. Heute häufen sich schwerwiegende Sicherheitsvorfälle bei großen namhaften Firmen, und die Schäden gehen teils in den mehrstelligen Millionenbereich. Das Vertrauen in die IT-Sicherheit ist so schwer erschüttert, dass sich kein Verantwortlicher heute mehr traut zu sagen: „Unser Unternehmen ist sicher und kann nicht gehackt werden“. Wenn man allerdings diese Unsicherheit genauer betrachtet, erwächst daraus eine neue Verantwortung: Wenn man davon ausgehen muss, früher oder später gehackt zu werden, stellt sich die Frage, welche Maßnahmen und Mechanismen man eingesetzt hat, um mit dem zu erwartenden Cyberangriff richtig umzugehen. Dieses White Paper unternimmt einen Streifzug durch die moderne Sicherheitslandschaft und geht dabei auf Abwehrmaßnahmen, die Erkennung von Angriffen sowie Reaktionen ein, um ein ganzheitlicheres Bild der Cybersicherheitslandschaft industrieller Anlagen zu zeichnen.

Altbewährtes und Bekanntes

Um auf Angriffe vorbereitet zu sein und das Ausmaß des Schadens bzw. die Reichweite eines Angriffs einzudämmen, sollte mit einem gar nicht so neuen Konzept begonnen werden: mit der Segmentierung und der Verbesserung des Schutzes der Netzwerkinfrastruktur. In vielen der dokumentierten Fälle konnten sich automatisierte Schadsoftware sowie gezielt vorgehende Angreifer aufgrund einer fehlenden Aufteilung und Abschottung der Netzwerke dort ungehindert bewegen und so zahlreiche angreifbare Systeme für weitere Angriffe oder für die Sabotage und Störung der Fertigung nutzen. Sowohl eine gute Trennung von IT- und OT-Netzwerk als auch eine Trennung von funktional unabhängigen Teilen des OT-Netzwerks sollte heute in jedem modernen Industrienetzwerk vorhanden sein. Gerade die letzten katastrophalen Auswirkungen von Ransomware-Infektionen bei großen Industriebetrieben zeigen jedoch, dass diese Segmentierung nicht vorhanden bzw. nicht effektiv war.

Die Segmentierung von Netzwerken wird durch das Prinzip der Zonen und Zonenübergänge erreicht. Hierzu werden funktional unabhängige Zonen im Netzwerk definiert, die überwiegend für sich autark arbeiten können. Zwischen den Zonen werden Paketfilter (z.B. Firewalls oder Gateways) installiert (vgl. Abbildung 1), die den Netzwerkverkehr, der trotzdem über die Zonengrenzen hinaus fließen muss, begrenzen und überwachen. In einem gut segmentierten Industrienetzwerk gibt es also nicht nur eine Firewall zwischen OT-und IT-Netzwerk, sondern zahlreiche Firewalls zwischen den einzelnen Anlagenteilen und Maschinen. Sogenannte Soft Targets (alte netzwerkfähige Geräte, die keine aktuellen Patches mehr erhalten können bzw. nicht über ausreichende Sicherheits-Features verfügen) werden zusätzlich durch Paketfilter wie z.B. kleine Firewalls vom Netzwerk isoliert, um ihre große Angriffsfläche vor einem Angreifer verborgen zu halten.

Eine Unterteilung in Zonen erschwert es einem Angreifer, der bereits erfolgreich ins Netzwerk eingedrungen ist, sich dort ungehindert zu bewegen. Automatisch agierende Malware kann meist die Firewalls an den Zonengrenzen nicht überwinden und ist so auf die Geräte innerhalb der betroffenen Zone begrenzt. Dadurch lässt sich der Schaden im Angriffsfall drastisch reduzieren. Auch für menschliche Angreifer stellt eine Zonenbildung ein großes Hindernis dar, da nur die Geräte, die innerhalb der Zone des Angreifers sind, als weitere Angriffsziele zur Verfügung stehen. In der Regel versucht ein Angreifer jedoch, sich durch das Netzwerk zu bewegen (engl. Lateral Movement), um neue Rechner zu übernehmen. Dafür ist er auf Geräte mit Schwachstellen oder unzureichenden Konfigurationen angewiesen. Die Unterteilung in Zonen

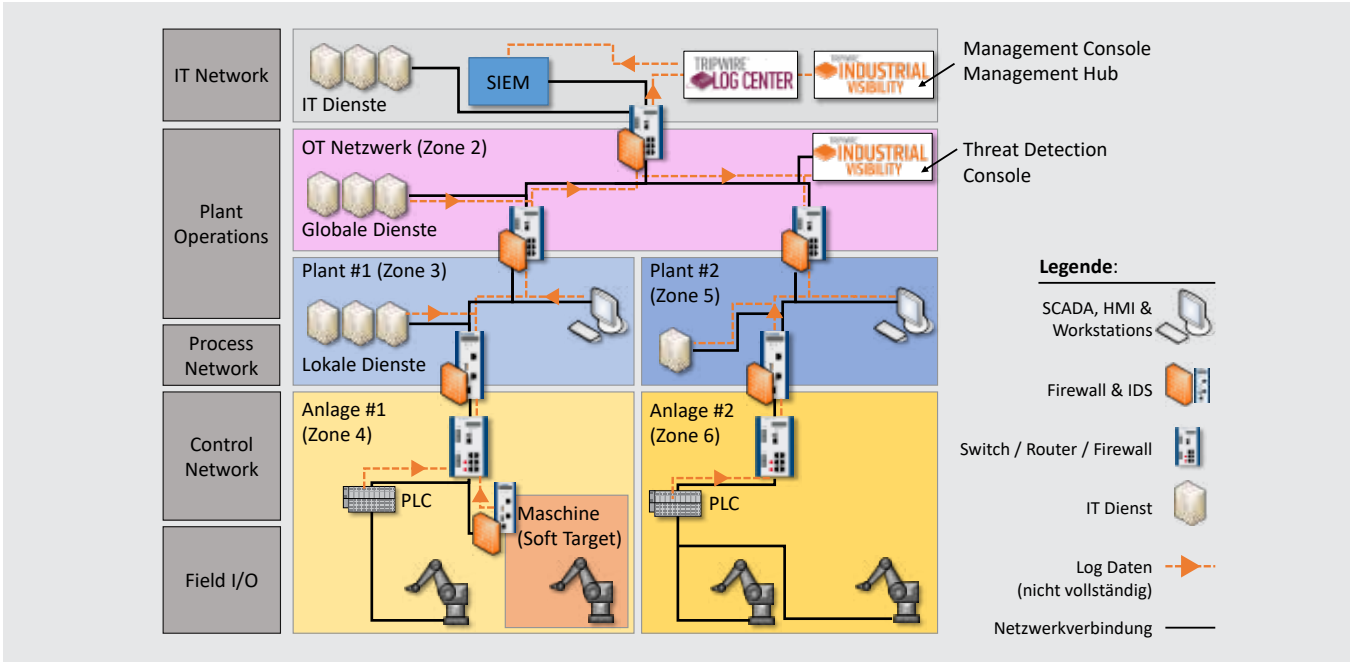

Abb. 1: Netzwerksegmentierung und Überwachungssysteme

EMEA +49 (0) 7127/14-1809 | hirschmann.com ■ US 1-800-BELDEN-1 | belden.com

verringert die Auswahl an verwundbaren Geräten deutlich und schränkt den Angriff damit stark ein. Epidemie-artigen Masseninfektionen kann so vorgebeugt werden. Zusätzlich bleiben große Teile der Anlage nach dem Angriff funktionsbereit, da sie unabhängig von den angegriffenen Systemen sind. So muss nach einem Angriff nicht großflächig auf verzweifelte und veraltete computerlose Maßnahmen wie Laufkarten und Handarbeit zurückgegriffen werden.

Auch die Aufräumarbeiten nach einem Angriff werden durch eine klare und effektive Zonenbildung deutlich vereinfacht. Denn je weniger Systeme ein Angreifer erreichen konnte, desto weniger forensische Aufgaben und Wiederherstellungsarbeiten fallen an. Diese Arbeiten sind äußerst kostenintensiv und langwierig und können ein Industrienetzwerk selbst nach dem Ende des Angriffs wochen- oder gar monatelang lahmlegen. Schließlich handelt es sich um einen Tatort, weshalb zusätzlich sichergestellt werden muss, dass alle Hintertüren und Schadprogramme des Angreifers restlos eliminiert wurden.

Automatisierung und Netzwerkhygiene

Der erste Schritt für einen Angreifer ist in der Regel, Zugriff zu einem System im Netzwerk zu erlangen. Dies kann entweder geschehen, indem er eines seiner eigenen Systeme über einen offenen, ungeschützten Ethernet-Port oder über ein kompromittiertes WLAN in das Netzwerk einschleust (z.B. einen Kleinstcomputer mit Mobilfunkmodem). Der Zugang kann aber auch über ein durch Malware kompromittiertes System, das per Download oder E-Mail infiziert wurde, erfolgen.

Im ersten Fall lässt sich erkennen, dass ein unbekanntes Gerät (das des Angreifers) im Netzwerk vorhanden ist. Deshalb kann ein Alarm ausgelöst werden, der es ermöglicht, schnell auf diese Abweichung von der Norm zu reagieren (vgl. Abbildung 2). Noch besser ist es jedoch, wenn das Gerät gar nicht erst in das Netzwerk gelangt. Hierzu bieten Protokolle wie IEEE 802.1X [1] bei Ethernet und WPA2 Enterprise [2] mit IEEE 802.1X bei WLAN die Möglichkeit, jedem Gerät individuelle Zugangsdaten für das Netzwerk zu geben. Somit muss sich jedes Gerät, das dem Netzwerk beitreten möchte, sich zuerst authentifizieren, bevor es dort kommunizieren kann. Einem Angreifer, der Zugang zum Firmengelände oder der Fertigung erlangt hat, kann so der Zugang zum Netzwerk deutlich erschwert werden.

In der Praxis treten aber immer wieder Fälle auf, in denen Industrie-Equipment die Authentifizierung über 802.1X oder WPA2 Enterprise nicht unterstützt. In solchen Fällen muss bei kabelgebundenen Verbindungen zu einer MAC Bypass genannten Methode gegriffen werden, bei der das Gerät nur anhand seiner (leicht fälschbaren) MAC-Adresse erkannt wird. Im WLAN wird auf das aus den Heimnetzen gut bekannte WPA2 mit Pre-shared Key zurückgegriffen, bei dem sich alle so verbundenen WLAN-Geräte einen einzigen geheimen Schlüssel, das „WLAN Passwort", teilen. In diesen Fällen kann jedoch nicht mehr eindeutig festgestellt werden, welches Gerät sich mit dem Netzwerk verbinden möchte, weshalb zusätzliche Maßnahmen zur Wahrung der Netzwerkhygiene getroffen werden müssen (z.B. Automatismen zur Überprüfung der Identität des Geräts mittels automatisierter Logins durch einen Überwachungsserver). Solche Automatismen sind häufig als „Post Connect"-Phase (vgl. Abbildung 3) in Netzwerk Access Control-Lösungen (NAC) [3] verfügbar. Falls ein Angreifer ein bereits in das Netzwerk integriertes System kompromittiert hat (z.B. durch eine unachtsam geöffnete E-Mail oder durch die Ausnutzung eines schwachstellenbehafteten Netzwerkdienstes), handelt es sich um ein legitimes Netzwerkgerät, sodass Maßnahmen wie IEEE 802.1X und WPA2 Enterprise nicht greifen (das kompromittierte Gerät verfügt ja über gültige Netzwerkschlüssel). Daher müssen zusätzlich Methoden zur Überwachung des Zustands und der Integrität des Geräts getroffen werden. Im Gegensatz zum Schutz vor dem Verbinden eines Geräts mit dem Netzwerk („Pre-Connect"-Check) kann ein automatisches System nach dem Verbinden mit diesem Gerät interagieren („Post-Connect"-Checks). Dies wird entweder erreicht, indem ein sogenannter Agent (kleine Software) auf dem System installiert wird, der sich dann ausweisen kann und wichtige Systemeigenschaften überwacht. Alternativ kann auch eine agentenlose Lösung verwendet werden, bei der sich ein Kontrollsystem auf dem zu überwachenden Gerät anmeldet (z.B. über SSH oder ein ähnliches Remote Management-Protokoll) und dann per Kommandozeilenbefehlen dessen Zustand prüft. Zu den entsprechenden Parametern gehören etwa der Zustand des Antivirussystems (aktiv/abgeschaltet, aktuelle Virendefinitionen/veraltete Virendefinitionen), der Zustand der Geräte-Firewall, gestartete Programme auf dem Gerät, vorhandene oder nicht vorhandene Dateien sowie angemeldete Benutzer. Typische Vorgehensweisen eines Angreifers (z.B. das Abschalten

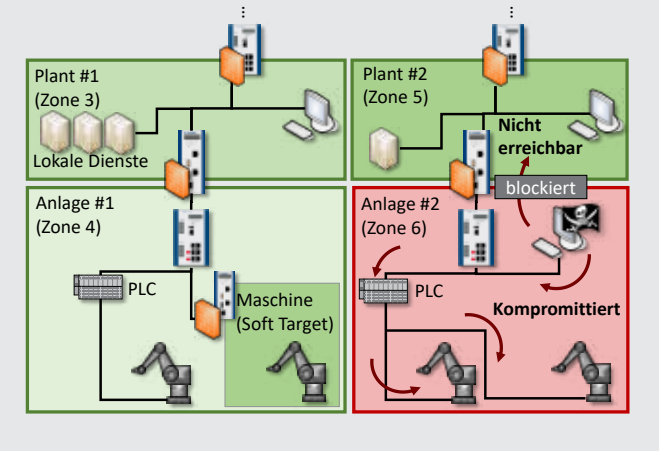

Abb. 2: Der Angreifer wird auf eine einzige Zone eingegrenzt

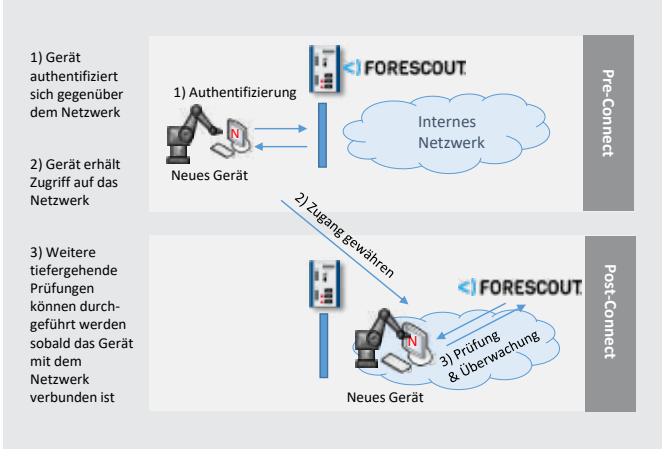

Abb. 3: Prozess der Gerätezulassung zum Netzwerk

des lokalen Anti-Virus-Programms oder das Starten eigener Schadroutinen) können so erkannt werden. Geräte, die als unsicher erkannt werden, lassen sich anschließend automatisch aus dem Netzwerk entfernen. Dies erschwert es einem Angreifer, nach der Übernahme eines Geräts weiter in das Netzwerk vorzudringen und unentdeckt zu bleiben. Auch anfangs erfolgreiche Angriffe können so deutlich schneller erkannt und eingedämmt werden. Eine aktive Überwachung des Zustands der mit dem Netzwerk verbundenen Geräte und eine effektive Netzwerkzugangskontrolle stellen daher einen wichtigen Baustein der Security-Hygiene in industriellen Netzwerken dar.

Zusätzlich kann eine Network Access Control Management-Lösung auch das Asset-Management, also die Erfassung aller vorhandenen Systeme und Geräte, unterstützen. Die Kenntnis aller Geräte (engl. Assets) und deren Funktion ist eine wichtige Grundlage für die Risikobetrachtung vor einem Angriff und die Entscheidung für oder gegen reaktive Maßnahmen (abschalten, isolieren, laufen lassen) im Angriffsfall.

Erkennung von Angriffen und Vorbereitung für den Ernstfall

Das beste Verteidigungskonzept ist sinnlos, wenn es keine Maßnahmen zur Erkennung von erfolgreichen Angriffen enthält. Denn sonst kann ein technisch überlegener Angreifer die Verteidigungsmaßnahmen umgehen und sich im Netzwerk ausbreiten und so maximalen Schaden anrichten. Der Begriff der technischen Überlegenheit hört sich hier ausgefeilter an, als er tatsächlich ist. Die Tatsache, dass im Jahr 2019 immer noch jede vierte Cyberattacke auf die seit 2017 Schaden anrichtende Ransomware „Wannacry“ [4] zurückgeht, spricht Bände. Wannacry nutzt dabei eine Schwachstelle aus, für die es bereits seit 2017 Patches, also effektive Gegenmaßnahmen, gibt. Von High-Tech kann dabei trotz technischer Überlegenheit der Angreifer im Verhältnis zu den Verteidigungsmaßnahmen keine Rede sein. Und modernere Malware legt die Latte für die Verteidigung nochmals deutlich höher. Denn sie verwendet nicht nur technisch effektivere Angriffswege, sondern nutzt zudem auch oft höchst erfolgreiche Social-Engineering-Methoden, also die Ausnutzung menschlicher Schwächen wie Unwissenheit, Angst oder Gier.

Um die Erkennung und Klassifizierung von Cyberangriffen in Protokolldateien zu unterstützen, können sogenannte Security Information and Event Management-Systeme (SIEM) eingesetzt werden. Sie gehören in vielen Office-IT-Umgebungen heute bereits zum Standardrepertoire, sind in vielen industriellen Netzwerken aber noch nicht zu finden. Die Notwendigkeit für den Einsatz in Industrienetzwerken ist jedoch ebenso gegeben wie in IT-Netzwerken, da sich die genutzte Technik sowie die von Angreifern verwendeten Werkzeuge und Methoden oft ähneln oder gar identisch sind.

Bei der Kompromittierung von Geräten hinterlassen Angreifer jedoch unweigerlich Spuren. Es bleiben z. B. verräterische Registry-Einträge, Angriffs-Programme und Dateien zurück, es werden verdächtige Prozesse auf den Systemen gestartet oder es werden Systemkonfigurationen wie etwa die Anti-Virus- und Firewall-Eistellungen verändert. All diese Dinge finden sich in den Ereignisprotokollen der kompromittierten Geräte wieder. Betrachtet man die Protokolle aller Geräte, so ergibt sich ein umfassendes Bild sämtlicher Aktivitäten im industriellen Netzwerk.

Die Ereignisprotokolle und Verkehrsmuster stellen einen unglaublichen Schatz an verwertbaren Security-Informationen dar. Leider wird dieser Schatz oftmals nicht gehoben, da der Umgang mit ihm äußerst schwierig ist. Zum einen ist bereits die zentrale Sammlung der Informationen von Hunderten Geräten ohne ein dafür geeignetes Verwaltungssystem (ein Log-Management-System) nicht leistbar. Zum anderen handelt es sich um Unmengen an kleinteiligen Informationen, aus denen Angriffe nicht einfach zu erkennen sind. Um im Bilde des Schatzes zu bleiben, handelt es sich also um Tonnen von 1-Cent-Münzen, unter denen sich auch noch ein erheblicher Teil an Falschgeld befindet. Das „Falschgeld“ sind in diesem Sinne Informationsfragmente, die zwar nicht zu einem Angriff gehören, jedoch trotzdem als solcher aufgefasst werden können. Normale Wartungsarbeiten an einer Anlage, die etwa das Starten neuer Programme, Software-Aktualisierungen und das Öffnen von Netzwerk-Ports erfordern, sind Beispiele für solche Aktivitäten. Es stellt sich also nicht nur das Problem, Cybersecurity-Bedrohungen in der Unmenge von Protokolleinträgen zu erkennen, sondern auch Falscherkennungen, sogenannte False Positives, zu vermeiden.

Neben der Möglichkeit zur Auswertung großer Log-Datenmengen bieten SIEM-Systeme auch Möglichkeiten zur automatischen Erkennung von Angreifern. Diese Systeme nennen sich dann Intrusion Detection-Systeme (IDS) [3]. Sie analysieren nicht nur Log-Einträge sondern auch Netzwerkverkehr zwischen den Geräten im industriellen Netzwerk.

Weitergedacht kann nach der Erkennung eines Angriffs auch automatisch eine Gegenmaßnahme getroffen werden. Diese sogenannten Intrusion Prevention Systeme (IPS) können viele teilweise erfolgreiche Angriffe unterbrechen und weiteren Schaden verhindern. Sie haben in industriellen Anlagen einen schlechten Ruf, da sie bei unbedachtem Einsatz zu Ausfällen, Standzeiten und schwer zu behebenden Funktionsfehlern führen können – selbst wenn kein Angriff vorliegt sondern nur eine harmlose Aktivität als Angriff fehlerkannt wurde (ein False Positive, also das Falschgeld). Dieser schlechte Ruf rührt davon, dass IPS Systeme in der Vergangenheit oftmals mit zu aggressiven Sperren in einem Angriffsfall reagiert haben. Ganze Netzwerkteile oder Geräte wurden pauschal bei einem (ggf. fehl-)erkannten Angriff zum Schutz vom Netzwerk getrennt. Die Folge sind weitreichende Funktionsausfälle. Heute ist es möglich IDS Systeme zielgenauer zu verwenden. So kann bei auch im Angriffsfall ein Steuerungsgerät seine Steuerungsaufgaben fortsetzen, während die für den Angreifer interessante Konfigurations-Schnittstelle durch das IPS System vom Netzwerk getrennt werden kann. Durch eine solche Teil-Isolation kann auch im Angriffsfall der Betrieb von essentiellen Geräten fortgesetzt werden während die Ausbreitung eines Angriffs trotzdem unterbunden werden kann.

Nach einem Angriff

Schließlich muss bei einem erkannten Vorfall auch schnell und effektiv reagiert werden. Um solch eine Reaktion vorzubereiten, müssen sowohl die für eine Analyse erforderlichen Daten umfassend und aussagekräftig im Log-Management-System vorliegen als auch qualifizierte Mitarbeiter vorhanden sein. Die bereits angesprochenen Log-Management- und SIEM-Systeme leisten hier einen wichtigen Beitrag, da sie die Informationen in leicht und effizient durchsuchbarer Form bereithalten. Da bei einer umfassenden zentralen Protokollierung oft gigabyteweise Log-Daten anfallen,

ist die Erkennung eines Angriffsweges (und damit die Feststellung, welche Systeme vom Angriff betroffen sind) wie die Suche nach der Nadel im Heuhaufen. Außerdem ist das Ganze aufgrund der extremen Datenmengen im höheren Gigabyte-Bereich auch technisch nicht einfach. Wer rechtzeitig ein effektives System für den Ernstfall aufbaut, kann im Falle eines Angriffs schnell reagieren. Ohne Vorsorge drohen im schlimmsten Fall eine langfristige Isolation vieler potenziell betroffener Systeme vom Netzwerk und ein manuelles Kopieren von Log-Dateien mit USB-Sticks zur Analyse. Dies führt zu langen Standzeiten und dementsprechend auch zu Lieferausfällen bzw. Vertragsverletzungen. Unter diesem Gesichtspunkt rentiert sich die Anschaffung eines geeigneten Systems oft schon dann, wenn dadurch nur ein Ransomware-Angriff erfolgreich abgewehrt werden konnte.

Neben den technischen Systemen spielen die Fähigkeiten der Mitarbeiter bei der aktiven Abwehr und Aufarbeitung eines Angriffs eine entscheidende Rolle. Abbildung 4 zeigt ein solches Zusammenspiel verschiedener technischer und personeller Maßnahmen. Sowohl die technische Ausbildung durch geeignete Studiengänge für neue Mitarbeiter und die Fortbildung vorhandener als auch sorgfältig ausgearbeitete und kommunizierte „Incident Response"-Pläne sind wichtige Schritte, um im Ernstfall schnell und effektiv reagieren zu können. Größere Unternehmen bündeln die Security-Kompetenzen in sogenannten Security Operation Centern (SOC). Zusätzlich sollte bereits im Vorfeld Kontakt zu spezialisierten Diensteistern aufgenommen werden, um im Angriffsfall schnell zusätzliche Hilfe mit Expertise im Bereich Incident Response zu bekommen. Auch Übungen für Ernstfallsituationen sind unerlässlich – nur dann kann gewährleistet werden, dass das Abwehrteam dem Angreifer voraus ist. Ein Learning-by-doing ist für den Bereich Incident Response stets die schlechteste Lösung, da sowohl die Verfügbarkeit der Produktion als auch Firmengeheimnisse und nicht zuletzt die persönlichen Daten und ggf. sogar die Unversehrtheit von Mitarbeitern und Kunden auf dem Spiel stehen. Auch die gesetzlichen Anforderungen an die Reaktionszeiten sprechen für den Aufbau eines kompetenten Teams zum Umgang mit Cybervorfällen. Für Zwischenfälle, in denen persönliche Daten von Kunden oder Mitarbeitern betroffen sind, gilt eine Meldezeit von 72 Stunden. Für Betriebe, die als kritische Infrastruktur eingestuft sind, muss eine Meldung an das Bundesamt für Sicherheit (BSI) unverzüglich, also ohne schuldhafte Verzögerung erfolgen. In Anbetracht dieser sehr knappen Fristen und bei Beachtung der Arbeitszeiten der Mitarbeiter (ein Wochenende hat 56 Stunden) bleibt einem Unternehmen keine andere Wahl, als für den Ernstfall vorbereitetes Personal vor Ort zu haben.

Weitere Maßnahmen und Ausblick

Neben den beschriebenen Maßnahmen gibt es natürlich noch weitere Schutzmaßnahmen, die eher präventiv wirken, jedoch die Erfolgschancen eines Angreifers oder einer automatisierten Malware ebenfalls nachhaltig schmälern. Abbildung 4 gibt einen Überblick über sinnvolle Möglichkeiten zur Verbesserung des Schutzes des Unternehmens- und Fertigungsnetzwerks.

Darüber hinaus ist auch eine breite Sensibilisierung und umfassende Ausbildung der gesamten Belegschaft essentiell, um Angriffe, die Social-Engineering-Methoden wie Druck, Täuschung und Verlockung nutzen, zu verhindern. Hier ist es wichtig, auch weniger IT-affine Mitarbeiter aus der Verwaltung und der Produktion zu schulen, falls sie Zugriff auf Computersysteme haben. Denn Angreifer wählen oftmals weniger technisch versierte Mitarbeiter als Ziel einer ersten Attacke aus.

Die oben beschriebenen technischen Lösungen werden von verschiedenen Unternehmen angeboten. Belden [5] ist durch seine industriegerechten Netzwerkgeräte wie die Firewalls, Switches, Router und Access Points von Hirschmann Automation & Control GmbH [6] sowie die Security-Lösungen des Schwesterunternehmens Tripwire, Inc. [7] in der Lage, Netzwerk-, Log-Management- und SIEM-Systeme aus einer Hand bereitzustellen. Über die enge Kooperation mit Forescout Technologies Inc. [8], dem Marktführer bei Network Access Control-Lösungen, kann Belden zudem auch ein mächtiges NAC-System einschließlich umfassender Pre-Connect- und Post-Connect-Checks sowie Asset Management für Industrieanlagen aus einem Guss realisieren.

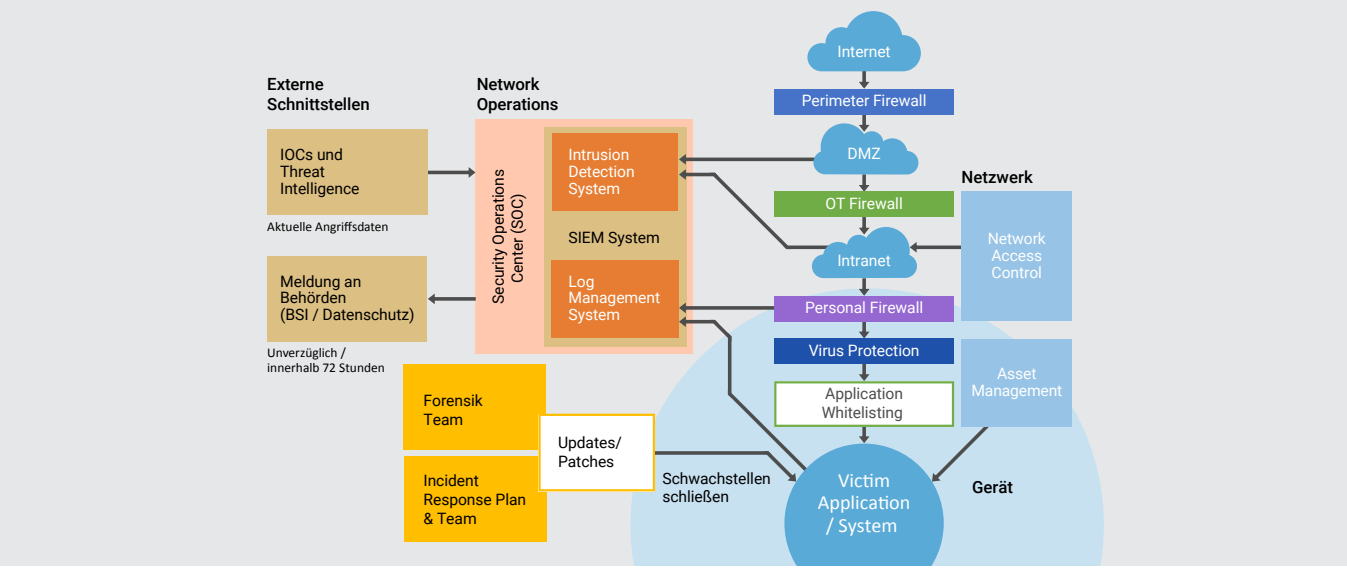

Abb. 4: Zusammenstellung verschiedener Maßnahmen zur Vermeidung, Erkennung und Reaktion auf Cyberangriffe

Referenzen

[1] 802.1X-2010 - IEEE Standard for Local and metropolitan area networks--Port-Based Network Access Control, https://standards.ieee.org/standard/802_1X-2010.html

[2] 802.11i-2004 - IEEE Standard for information technology-Telecommunications and information exchange between systems, https://standards.ieee.org/standard/802_11i-2004.html

[3 Monitoring Industrial Control Systems to Improve Operations and Security, https://www.forescout.com/company/resources/monitoring-industrial-control-systems-to-improve-operations-and-security/

[4] Ransomware reloaded: Wannacry verursacht immer noch Schäden in Milliardenhöhe, https://t3n.de/news/ransomware-reloaded-wannacry-1240246/

[5] Belden, Inc. Website, https://www.belden.com/

[6] Hirschmann Automation & Control GmbH Website, https://hirschmann.com/

[7] Tripwire, Inc. Website, https://www.tripwire.com/

[8] Forescout Technologies, Inc. Website, https://www.forescout.com/

Immer auf dem neuesten Stand mit Belden

In einem stark wettbewerbsgeprägten Umfeld sind zuverlässige Partner, die Ihrem Unternehmen einen Mehrwert liefern können, unverzichtbar. Im Bereich Signalübertragung ist Belden der Lösungsanbieter erster Wahl. Wir verstehen Ihr Geschäft und möchten Ihre speziellen Herausforderungen und Ziele besser kennenlernen, um zu erfahren, wie effektive Signalübertragungslösungen Ihnen einen Wettbewerbsvorteil verschaffen können.

Durch Kombination der Stärken unserer führenden Marken Belden, GarrettCom, Hirschmann, Lumberg Automation, Tofino Security und Tripwire sind wir in der Lage, Ihnen die Lösung anzubieten, die Sie brauchen. Heute kann dies ein einzelnes Kabel, ein Switch oder ein Steckverbinder zur Behebung eines speziellen Problems sein; morgen ein kompletter Satz an integrierten Anwendungen, Systemen und Lösungen. Da das Industrial Internet of Things (IIoT) immer mehr intelligente, vernetzte Geräte mit sich bringt, können wir gemeinsam sicherstellen, dass Ihre Infrastruktur die Datenmengen bewältigen und nutzen kann. Stellen Sie Ihre Prozesse jetzt auf einen sofortigen Zugriff auf Informationen um und verwirklichen Sie Ihre Vision. Weitere Informationen unter info.belden.com/iiot.

Über Belden

Belden Inc., einer der Weltmarktführer von Komplettlösungen für die Signalübertragung, bietet ein umfassendes Produktportfolio, das auf die Anforderungen unternehmenskritischer Netzwerkinfrastrukturen in den Branchen Industrie- und Gebäudeautomation sowie Rundfunk zugeschnitten ist. Das Unternehmen mit Hauptsitz in St. Louis, USA, wurde 1902 gegründet und betreibt Fertigungsstätten in Nord- und Südamerika, Europa und Asien.

Über ForeScout

Die Lösungen zur Netzwerkzugangskontrolle von ForeScout ermöglichen mehr als 2.900 Unternehmen in über 80 Ländern eine intelligente, kostengünstige Überwachung des Netzwerkzugriffs, die sowohl den höchsten Standards für Sicherheit und der Einhaltung gesetzlicher Vorschriften entspricht als auch eine komfortable Bedienung und eine einfachen Einsatz bietet.

Die ForeScout Plattform ist entweder als virtuelle oder als physikalische Appliance erhältlich, die innerhalb Ihrer vorhandenen Infrastruktur eingesetzt wird, und erfordert normalerweise keine Änderungen an Ihrer Netzwerkkonfiguration. Sie wird Out-of-Band installiert, was Latenzen oder Probleme im Zusammenhang mit Netzwerkausfällen vermeidet, und kann bis zu zwei Millionen Endpunkte von einer Enterprise Manager Konsole aus zentral und dynamisch verwalten.

Für weitere Informationen besuchen Sie uns unter www.belden.com und folgen Sie uns auf **Linkedin** und **Facebook**.