HOCHSCHULE
MITTWEIDA
UNIVERSITY OF
APPLIED SCIENCES

DIPLOMARBEIT

Herr
Mathias Ogrzey

Optimierung der Cyber-Security in Produktionsnetzwerken mittels Verhaltensanalyse

Einsatz und Validierung in einem automatisierten Produktionsnetzwerk der August Storck KG

2021

Fakultät **CB**

DIPLOMARBEIT

Optimierung der Cyber-Security in Produktionsnetzwerken mittels Verhaltensanalyse

Einsatz und Validierung in einem automatisierten Produktionsnetzwerk der August Storck KG

Autor:
Mathias Ogrzey

Studiengang:
Technische Informatik

Seminargruppe:
TI17W1-F

Erstprüfer:
Prof. Dr.-Ing. habil. Matthias Vodel

Zweitprüfer:
Dipl.-Ing. Alois Ahlrichs

Mittweida, 07 2021

Bibliografische Angaben

Ogrzey, Mathias: Optimierung der Cyber-Security in Produktionsnetzwerken mittels Verhaltensanalyse, Einsatz und Validierung in einem automatisierten Produktionsnetzwerk der August Storck KG, 71 Seiten, 29 Abbildungen, Hochschule Mittweida, University of Applied Sciences, Fakultät CB

Diplomarbeit, 2021

Satz: LaTeX

Referat

Diese Diplomarbeit zeigt zu Beginn die Risiken, die moderne Angriffe auf ein Produktionsnetzwerk darstellen, in mehreren Facetten auf. Um diesen möglichen Schaden für Unternehmen abzuwenden, wird eine mögliche Lösung vorgestellt, die diese Angriffe, die trotz bereits vorhandener Sicherheitsmaßnahmen erfolgreich sein können, erkennen kann. Diese Lösung wird planmäßig durch die Einbindung in die Infrastruktur eines Produktionsnetzwerkes umgesetzt. Um die volle Funktionalität sicherstellen zu können, wird die Lösung auch in einem separatem Testnetzwerk durch Powershell-Scripte und Pentesting-Tools, die in Kali Linux gebündelt sind, überprüft. Dies soll dem Schutz der vorhandenen, teils überholten Infrastruktur in der Produktion dienen, die durch ihr teilweise hohes Alter durch dieses Pentesting ausfallen könnten. Abschließend werden die ermittelten Ergebnisse bewertet. Ein Fazit über die Möglichkeiten der Optimierung sowie ein Ausblick in eine mögliche Zukunft runden diese Diplomarbeit ab.

Sehr hilfreich dazu waren diverse Online-Tutorials, Wikis zu Projekten mit Powershell bei github sowie die Lektüre von Michael Kofler und die Bachelorarbeit von Brigitte Fischer vom BSI.

I. Inhaltsverzeichnis

II. Abbildungsverzeichnis

III. Abkürzungsverzeichnis

AD ..... Active Directory, Seite 28

ADS ..... Alternate Data Streams, Seite 50

API ..... Application Programming Interface, Seite 51

APT ..... Advanced Persistent Threats, Seite 18

ARP ..... Address Resolution Protocol, Seite 36

BSI ..... Bundesamt für Sicherheit in der Informationstechnik, Seite 1

C&C ..... Command & Control, Seite 25

CIP ..... Common Industrial Protocol, Seite 10

CISO ..... Chief Information Security Officer, Seite 59

CMS ..... Content Management System, Seite 54

CP ..... Communication Processor, Seite 35

CVE ..... Common Vulnerabilities and Exposures, Seite 42

DGA ..... Domain Generation Algorythmus, Seite 25

DMZ ..... Demilitarisierte Zone, Seite 9

DNS ..... Domain Name Service, Seite 37

DSGVO ..... Datenschutz-Grundverordnung, Seite 30

EDR ..... Endpoint Detection and Response, Seite 26

ETO ..... Elektrotechnik Ohrdruf, Seite 1

FTP ..... File Transfer Protocol, Seite 40

GVM ..... Greenbone Vulnerability Management, Seite 36

HIPS ..... Host-based Intrusion Prevention System, Seite 13

IDS ..... Intrusion Detection System, Seite 25

IEEE ..... Institute of Electrical and Electronics Engineers, Seite 10

IIS ..... Internet Information Server, Seite 52

IoC ..... Indicator of Compromise, Seite 25

IP ..... Internet Protocol, Seite 48

IPC ..... Industrie-PC, Seite 35

IPS ..... Intrusion Prevention System, Seite 56

IRT ..... Isochronous Real-Time, Seite 11

IT ..... Informationstechnologie, Seite 1

ITZ ..... Informationstechnikzentrum, Seite 16

KI ..... Künstliche Intelligenz, Seite 13

LAN ..... Local Area Network, Seite 48

LKA ..... Landeskriminalamt, Seite 22

M2M ..... Machine to Machine, Seite 8

MAC ..... Media Access Control, Seite 48

MitM ..... Man in the Middle, Seite 36

NBAD ..... Network Behavior Anomaly Detection, Seite 4

NGFW ..... Next Generation Firewall, Seite 38

NTFS ..... New Technology File System, Seite 50

NTP ..... Network Time Protocol, Seite 7

OSI ..... Open Systems Interconnection, Seite 4

OT ..... Operational Technology, Seite 2

PCS ..... Process Control System, Seite 19

RaaS ..... Ransomware as a Service, Seite 16

RDP ..... Remote Desktop Protocol, Seite 40

RfC ..... Request for Comments, Seite 11

SAM ..... Security Account Manager, Seite 20

SCADA ..... Supervisory Control and Data Acquisition, Seite 18

SERCOS ..... Serial Realtime Communication System, Seite 11

SIEM ..... Security Information and Event Management, Seite 30

SIL ..... Sicherheits-Integritätslevel, Seite 11

SMART ..... Self-Monitoring, Analysis and Reporting Technology, Seite 5

SMB ..... Server Message Block, Seite 4

SNMP ..... Simple Network Management Protocol, Seite 4

SOAR ..... Security Orchestration, Automation and Response, Seite 26

SPAN ..... Switched Port Analyzer, Seite 57

SPS ..... Speicherprogrammierbare Steuerung, Seite 5

TAP ..... Test Access Point, Seite 57

TCP ..... Transmission Control Protocol, Seite 7

TIA ..... Totally Integrated Automation, Seite 44

UDP ..... User Datagram Protocol, Seite 7

URL ..... Uniform Resource Locator, Seite 25

VNC ..... Virtual Network Computing, Seite 9

VPN ..... Virtual Private Network, Seite 9

WinCC ..... Windows Command and Control, Seite 35

IV. Vorwort

Da mich die IT schon seit vielen Jahren interessiert, war die Vertiefung in diese Richtung schon lange ein großer Wunsch. Das Studium zum Diplom-Ingenieur an der Hochschule Mittweida hat mir, auch durch die vielen tollen Menschen, die ich kennenlernen durfte, sehr viel Spaß gemacht und diesen Wunsch nun erfüllt. Ich glaube fest daran, dass die IT in der Zukunft immer wichtiger wird.

Bei Stefan Ripperger bedanke ich mich für die Unterstützung meines Studiums und das in mich gesetzte Vertrauen. Ebenfalls bedanken möchte ich mich bei Saskia Mühlhausen für ihre zahl- und hilfreiche Kritik an meiner Arbeit. Das Feedback hat eindeutig zu einer Verbesserung geführt.

Ein besonderer Dank gilt Dr. Sven Sander, der mir in vielen Stunden als äußert kompetenter Helfer bei allen fachlichen Fragen zur Seite stand. Ihm war dabei keine Zeit zu spät und in unseren Gesprächen darf ich ihn mittlerweile als meinen Freund bezeichnen.

Ebenfalls danken möchte ich Prof. Dr.-Ing. habil. Matthias Vodel für die Zusage zu meiner Abschlussarbeit und den damit verbundenen Mühen. Er hat mir immer mit einem lockeren Wort und viel Aufmunterung zur Seite gestanden.

Ohne die unerschöpfliche Unterstützung durch Alois Ahlrichs wäre diese Diplomarbeit nicht vorstellbar. Er trägt den neben dem Autor den größten Anteil am Thema, dem Inhalt sowie der Gestaltung. Er hat für den Autor auch nie mit kritischen Worten gespart - DANKE Alois.

Meinen Eltern danke ich besonders für das Vertrauen und die jahrelange Unterstützung seit frühen Kindheitstagen. Sie ließen mich meinen Weg gehen, unterstützten mich in allen wichtigen Situationen und haben mir immer Mut zugesprochen.

Mein größter Dank gilt meiner großen Liebe Liane, die mir seit über sieben Jahren den Rücken frei gehalten hat. So konnte ich all meine Kraft und Zeit in das Studium stecken. Nicht zuletzt hat sie die zahlreichen Einschränkungen mit mir gemeinsam durchgemacht. Auch dafür liebe ich dich!

„Tomorrow belongs to those who can hear IT coming“ [54]
David Bowie † 10.01.2016

1 Einleitung

1.1 Motivation

Laut BSI[1] sind deutsche Unternehmen ständig den Gefahren durch die seit Jahren steigende Anzahl an Angriffen aus dem Internet ausgesetzt. Viele Firmen mussten in der Vergangenheit bereits schmerzhafte Erfahrung machen, die nicht nur finanziellen Schaden, sondern auch einen Verlust der Reputation in der öffentlichen Wahrnehmung nach sich gezogen haben. Fast täglich sind diesbezüglich neue Meldungen zu lesen. Nach mehreren Ausfällen des Automatisierungsnetzwerkes am Standort Ohrdruf wurde 2019 in der Fachabteilung ETO[2] beschlossen, ein Netzwerkmonitoringsystem aufzubauen. Dieses soll in Zukunft die Verfügbarkeit des Netzwerkes überwachen und dabei Probleme mit Clients sowie den Ausfall eines Netzwerkteilnehmers erkennen. Das Netzwerkmonitoring überwacht dabei aber nur die reine Infrastruktur und bringt keine Verbesserung bei der Cyber-Security im Netzwerk oder auf den Clients. Ebenso wird auch ungewöhnliches Verhalten kaum oder nur spät erkannt und dann auch nur als Auswirkung der eigentlichen Ursache.

Somit ist sicher, das trotz Überwachung im Netzwerk sowie auf den Clients weiterhin Netzwerke attackiert werden und auch ausfallen können. Die Gefahr durch die erwähnten Angriffe kann dabei nicht nur von außen erfolgen, sondern ist auch durch Innentäter, die eigene Mitarbeiter oder Servicedienstleister sein können, realistisch.

1.2 Zielsetzung

Ziel dieser Arbeit ist es aufzuzeigen, wo die Grenzen des geplanten Monitoringsystems sowie den bereits bei der August Storck KG umgesetzten Bausteine aus dem BSI IT[3]-Grundschutz-Kompendium liegen und warum es sinnvoll ist, zusätzlich zu den bisher getroffenen IT-Sicherheitsmaßnahmen eine Verhaltensanalyse für die umfassende Überwachung des Netzwerkverkehrs auf Anomalien zu installieren. [11]

Als Grundlage für die Diplomarbeit dient die Belegarbeit zum Modul „Praxisprojekt II“, in der Anforderungen an Systeme für Anomalieerkennung herausgearbeitet und eine Auswahl der Hersteller mit Kriterien in einer Übersicht zusammengestellt wurden. Auf dieser Grundlage soll die Möglichkeiten zur Verbesserung der Cyber-Security mit Hilfe

[1] Bundesamt für Sicherheit in der Informationstechnik
[2] Elektrotechnik Ohrdruf
[3] Informationstechnologie

einer Anomalieerkennung praktisch umgesetzt werden. Dazu wird in folgenden Kapiteln ein Weg zur Implementierung beschrieben und der erfolgreiche Einsatz mit selbst gestellten Testszenarien unter Beweis gestellt.

So soll diese Arbeit das Potenzial einer Netzwerkverhaltensanalyse in Produktionsnetzwerken wissenschaftlich bewerten und als Grundlage für die weitere Optimierung der IT-Sicherheit in Produktionsnetzwerken bei der August Storck KG dienen. Sie soll im idealen Fall die IT-Sicherheit in der Produktion in eine sicherere Zukunft führen. [8]

1.3 Gliederung

Die Arbeit ist wie folgt gegliedert: Kapitel 2 behandelt die Möglichkeiten und Grenzen von Netzwerküberwachung. Die Besonderheiten, die es in der OT[4] zu beachten gilt, werden im Kapitel 3 beschrieben und in Kapitel 4 um das Thema Endpoint Protection in Automatisierungsnetzwerken ergänzt. Anschließend werden im Kapitel 5 die aktuell größten Cyber-Bedrohungen für produzierende Unternehmen beschrieben, die dem Leser eine Einschätzung der realen Gefahren für die Unternehmen erlaubt. Mit der im Kapitel 6 beschriebenen Anomalieerkennung wird dem Leser die Netzwerkanomalieerkennung als mögliche Optimierungsmaßnahme näher gebracht. Darauf folgend werden im Kapitel 7 die Testmethoden für die Verhaltensanalyse beschrieben, die der Validierung der erwählten Lösung dienen sollen. Abschließend erfolgt eine Auswertung der erzielten Ergebnisse sowie ein Fazit der Arbeit.

[4] Operational Technology

2 Warum Überwachung in Netzwerken wichtig ist

Wie wichtig Überwachung und Sicherheit in der IT ist, hat die jüngste Vergangenheit gezeigt, in der vor allem Unternehmen durch Cyber-Angriffe empfindlich getroffen wurden. Allerdings sind nicht nur Unternehmen, sondern auch öffentliche Einrichtungen Opfer von Angriffen geworden. So geschehen mit der Infektion des Kammergerichts in Berlin. Dabei war der Schaden besonders groß und die Auswirkungen mit einem eingeschränkten Betrieb waren seit Oktober 2019 noch weit bis in das Jahr 2020 zu spüren. [44] Ebenfalls einen Totalausfall musste die Stadtverwaltung Neustadt nach einem Angriff durch Emotet vermelden. Die ganze Verwaltung konnte nur noch telefonisch agieren und selbstverständliche Vorgänge wie die Zulassung von Kraftfahrzeugen oder die Ausstellung von Dokumenten wie Personalausweis oder Reisepass war bis zu den erfolgreichen Reparaturarbeiten nicht möglich. [57]

Das es dabei auch große Unternehmen treffen kann, zeigen die Beispiele von ThyssenKrupp aus dem Jahr 2016 [63], KraussMaffei im Jahr 2018 [12] oder Norsk Hydro aus dem März 2019. Der Angriff gegen Norsk Hydro, einem in 50 Ländern agierendem Aluminiumhersteller, hatte große Auswirkungen auf die gesamten IT-Systeme des Unternehmens, inklusive der in Europa und den USA verteilten Produktionsanlagen. Aufgrund dieses Angriffs waren viele der Maschinen nur noch per Handbetrieb bedienbar und der Gewinn brach um mehr als 80 % ein. Dies hatte einen Schaden von knapp 70 Millionen Dollar zur Folge und der Preis für eine Tonne stieg auf ein Kurshoch. [15] & [3]

Die Cyber-Terroristen machen dabei auch vor Krankenhäusern nicht halt. Die IT des Krankenhauses in Fürstenfeldbruck war durch den Angriff so schwer getroffen, dass nur eine Notversorgung der Patienten möglich war. Das Krankenhaus musste sich auch von der zentralen Rettungsleitstelle des Landes Bayern abmelden und war erst nach einer Woche wieder einsatzbereit. [19]

2.1 Möglichkeiten und Grenzen des Monitoring

Bei vielen erfolgreichen Angriffen werden Zugangsdaten ermittelt und damit die Infrastruktur auf weitere Schwachstellen untersucht. Dabei helfen keine Virenscanner, da die Schadprogramme durch kleine Veränderungen im Programmcode meist nicht von den gängigen Scannern erkannt werden. Die Schadsoftware verteilt sich über gängi-

ge Netzwerkprotokolle wie SMB[5] weiter im Unternehmensnetzwerk - dieses Verhalten wird auch als Lateral Movement bezeichnet. Da dies weder von einem Monitoringsystem erkannt noch von den internen Firewalls als verdächtig eingestuft wird, bleibt diese Ausbreitung ohne eine NBAD[6], also Netzwerkverhaltensanalyse, meist unentdeckt.

Monitoring, oder besser auch Netzwerküberwachung, würde demnach nicht helfen, einen Angriff frühzeitig zu erkennen. Manche Monitoringsysteme können mit Erweiterungen zwar die Logs von Assets wie Clients, Firewalls, Switches und Virenscannern auswerten, aber erst mit dem Protokollieren und Analysieren der im Netz auftretenden Pakete und Datenströme, wie es eine NBAD macht, lässt sich ein Angriff frühzeitig und nahezu in Echtzeit erkennen.

Monitoring dient daher im Wesentlichen zur Erkennung von Auffälligkeiten in der Netzwerkinfrastruktur, die Einfluss auf technische und wirtschaftliche Belange nehmen können. Monitoring ist dabei ein Oberbegriff für alle Arten der unmittelbaren systematischen Erfassung, Beobachtung oder Überwachung eines Vorgangs oder Prozesses mittels technischer Hilfsmittel oder anderer Beobachtungssysteme. Nachfolgend deshalb die Erläuterung der drei Stufen des Monitorings.

2.2 Netzwerk-Monitoring

Im Netzwerk-Monitoring wird die Infrastruktur und Verfügbarkeit des Netzwerkes und seiner Teilnehmer überwacht. Es läuft im OSI[7]-Modell Layer 3 per SNMP[8] und überwacht die elektrische Verbindung sowie die grundsätzliche Erreichbarkeit der Teilnehmer.

2.3 Performance-Monitoring

Beim Performancemonitoring wird das Medium Netzwerk benutzt, um den Status der einzelnen Netzwerkverteiler zu überwachen. Sollte hier ein Teilnehmer ungewöhnliche Werte annehmen, wird eine Nachricht per SNMP abgesetzt. Dies betrifft oftmals Netzwerkteilnehmer wie Switches (Load Limits) oder Firewalls, wenn Ports wegen Überlastung abgeschaltet werden.

[5] Server Message Block
[6] Network Behavior Anomaly Detection
[7] Open Systems Interconnection
[8] Simple Network Management Protocol

2.4 System-Monitoring

Beim System Monitoring werden die Systemeigenschaften auf einzelnen Hosts im Netzwerk überwacht. Dies können Server, Clients oder auch Steuerungen, wie SPS[9] sein. Diese bringen die SNMP-Funktionen durch betriebssystemeigene Dienste standardisiert mit, haben einen separaten Daemon installiert oder bieten in ihrer Firmware die Möglichkeit, die erfassten Daten per SNMP zu übertragen. So ist es beispielsweise per SMART[10] möglich, den Zustand von Datenträgern auszulesen und proaktiv einen sich anbahnenden Ausfall zu verhindern.

Typische Parameter sind:

- CPU-Auslastung
- Zustand von Datenträgern
- Auslastung Arbeitsspeicher
- Zustand einer SPS (RUN/STOPP)
- Überwachung einzelner Programme (Datenbanken)

2.5 Fazit Monitoring

Alle Monitoringlösungen verfolgen den Ansatz des Schutzes der Infrastruktur. Der Netzwerkverkehr wird dabei nicht aktiv auf Gefahren überwacht. Somit sind Anomalien nur anhand ihrer Auswirkungen, die sehr massiv ausfallen können, zu erkennen und damit häufig zu spät. Viele Unternehmen haben sich in der Vergangenheit auf das Monitoring verlassen und sind dann durch Infektionen mit Emotet überrascht worden. Spätestens mit einer solchen Infektion sind dem Monitoring Grenzen gesteckt. Hier setzt die Verhaltenserkennung von Netzwerkverkehr und deren Teilnehmern an. [61]

[9] Speicherprogrammierbare Steuerung
[10] Self-Monitoring, Analysis and Reporting Technology

3 Besonderheiten eines Netzwerkes in der OT

Ohne eine weitreichende Vernetzung der eingesetzten Steuerungskomponenten wäre die größtenteils automatisierte Produktion, wie sie bei der August Storck KG zu finden ist, nicht mehr möglich. Viele der verbauten Komponenten verwenden mittlerweile die gleiche Technik, die sich bereits im Umfeld von Office Arbeitsplätzen bewährt haben. Allerdings ist es in der OT, im Gegensatz zur IT der Officeumgebung, nicht möglich, einfach einen anderen Computer zu verwenden, wenn der eigene mal nicht funktioniert. Die Produktion ist direkt und unmittelbar an die Verfügbarkeit der verbauten Sensoren, Steuerungs- und Netzwerkkomponenten gebunden. Ohne die störungsfreie Funktion all dieser Bauteile stehen die Maschinen, sei es bei der Herstellung der Schokoladenmassen, der Verarbeitung zur Schokoladentafel oder der Einlagerung in das Logistikzentrum, still.

3.1 Unterschiede der OT zur IT

Oft werden IT und OT als gemeinsame Technologie betrachtet und die Begriff deshalb synonym verwendet. Dies kommt vor allem daher, dass die aus der IT bekannten Techniken Einzug in die OT gehalten haben. Dadurch wurden etablierten Techniken kostengünstig in die industrielle Welt übernommen, sodass im Jahr 2020 sogar Netzteile einen Netzwerkanschluss besitzen.

Wenn man sich genauer mit der OT beschäftigt, sind wichtige Unterschiede gegenüber der IT zu erkennen, die im Folgenden näher erläutern werden. Grundlegend beruhen beide auf den gleichen Technologien, wie z. B. Ethernet, die aber in ihrem jeweiligem Einsatzgebiet weiterentwickelt wurden. So ist eine der wichtigsten Anforderungen in der OT die Echtzeitverarbeitung. Ebenso wird die zwingende Verwendung von TCP[11] bei der Übertragung von Sensor- und Steuersignalen vorausgesetzt. Das UDP[12] spielt in der OT eine ergänzende Rolle, meist durch bekannte Protokolle aus der IT. Dies kommt beispielsweise beim NTP[13] zum Synchronisieren aller Zeiten zum Einsatz.

Wie im Bild 3.1 ersichtlich, verschmelzen beide Techniken in den Unternehmensnetzwerken und oftmals verschwimmen die Grenzen, wenn es keine deutliche Trennung der beiden Netzwerke gibt. Bei der August Storck KG werden diese Grenzen durch Firewalls

[11] Transmission Control Protocol
[12] User Datagram Protocol
[13] Network Time Protocol

auf Layer sieben in den jeweiligen Produktionsgebäuden realisiert, die den Übergang der Daten zwischen beiden Netzwerken kontrollieren. Eine Übersicht aus dem Produktionsgebäude C ist als Anhang A.1 zu finden.

Abbildung 3.1: IT/OT Pyramide [21]

3.1.1 Datenfluss

Im Gegensatz zur IT, die vorrangig in Büroumgebungen mit nicht zeitkritischen Anwendungen eingesetzt wird, stehen für die Automatisierung die «M2M[14]-Kommunikation» und die jeweilige spezielle Applikation im Fokus. Alle beteiligten Endgeräte benötigen dabei einen stetigen Datenaustausch. Schon bei minimal zeitlich verzögerter Zustellung oder gar einem Verlust einzelner Daten kann es zum Stillstand der Anlage kommen, was einen direkten Einfluss auf das Geschäftsergebnis hat. Im Gegensatz zur IT muss in industriellen Kommunikationsnetzwerken die Signalübertragung deshalb innerhalb einer definierten Antwortzeit durchgeführt und abgeschlossen sein. Somit ist diese deterministische Auslegung der Kommunikation einer der wesentlichen Unterschiede zwischen Automatisierungsnetzwerken und Standard-IT und die Voraussetzung für die «M2M-Kommunikation». [47]

3.1.2 Security

Während in der IT die verschlüsselte Übertragung von Daten längst Standart ist, findet die Kommunikation in Automatisierungsnetzwerken nahezu unverschlüsselt statt. So gehört die unsichere Kommunikation innerhalb der Feldbusprotokolle zu den größten Risiken in einem Automatisierungsnetzwerk. Bei fast allen Protokollen in einem OT werden Informationen und Steuerbefehle ungeschützt im Klartext übertragen.

[14] Machine to Machine

Damit ist das Mitlesen oder Manipulieren von Informationen, wie leicht in der Abbildung 3.2 zu erkennen ist, und damit das Einspeisen eigener Steuerbefehle mit geringem Aufwand möglich. [47]

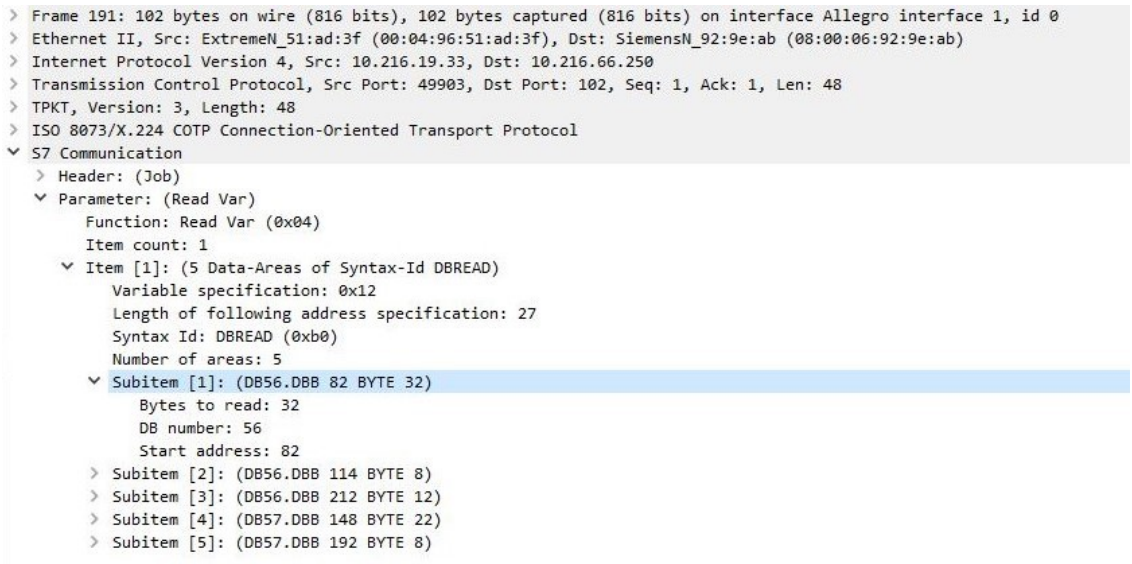

Abbildung 3.2: Wireshark - S7Comm DB Werte mitlesen

Die Siemens AG hat dieses Sicherheitslücke erkannt und bietet unter dem Motto „Defense in Deep“ nun eine Reihe von Sicherheitsmaßnahmen in der OT an, die bereits aus der IT bekannt sind. Dazu werden spezielle Geräte wie Switche oder Router mit Techniken wie DMZ[15] oder VPN[16] kombiniert. Damit ist es zum einen möglich, exponierte Dienste anzubieten und dabei den Rest der OT abzusichern. Zum Anderen findet bei entsprechender Konfiguration die Kommunikation zwischen einzelnen Netzwerksegmenten nun verschlüsselt statt. Dabei werden die Kommunikationsteilnehmer sicher authentifiziert.

3.2 Eingesetzte Protokolle

In einem Automatisierungsnetzwerk findet überwiegend Netzwerkverkehr mit spezialisierten Protokollen für die Automatisierungstechnik wie S7Comm, Profinet oder SERCOS statt. Allerdings werden auch aus der IT bekannte Protokolle wie NTP oder VNC[17] verwendet. Daran ist ebenfalls ersichtlich, wie beide Welten weiter verschmelzen.

[15] Demilitarisierte Zone
[16] Virtual Private Network
[17] Virtual Network Computing

3.2.1 Ethernet

EtherNet umfasst eine Gruppe von Netzwerktechnologien für viele Arten von Netzwerken. Es wurde 1980 kommerziell eingeführt und 1985 als IEEE[18] 802.3 standardisiert. Dieser Standard umfasst Festlegungen für mehrere Typen von Kabeln und Steckern sowie Signalprotokolle der OSI-Modelle und bildet, beschränkt auf Layer 1 und 2, die Grundlage für viele weitere Protokolle in beiden Welten. [30]

3.2.2 Industrial Ethernet

Industrial Ethernet ist eine Weiterentwicklung des Ethernetstandards. Hierbei geht es um die Möglichkeit, auch Geräte, die mit der industriellen Fertigung und Kontrolle beschäftigt sind, an ein Netzwerk unter industriellen Voraussetzungen anzubinden. Unter dem Dach Industrial Ethernet gibt es ungefähr 20 verschiedene Protokolle, die sich an der Norm IEEE 802.3 orientieren. Hierüber sind auch die verwendeten Stecker- und Kabeltypen definiert.

Vorteile liegen in der Durchgängigkeit der Kommunikationssysteme, sowie in der direkten Übernahme der Anwendungsschicht des Feldbus, der einfachen Portierbarkeit sowie der Eigenschaft zur Echtzeitverarbeitung. Nachteil ist der relativ große Overhead bei der Benutzung des TCP-Protokolls, der bei Echtzeitanwendungen unpraktisch ist. Daraus haben sich im Zuge der fortwährenden Entwicklung weitere Protokolle, spezialisiert auf die jeweiligen Anwendungsfälle, entwickelt.

Das für die industriellen Anwendungen entscheidende Protokoll ist das CIP[19]. Dieses arbeitet in der Transportschicht und ermöglicht den zyklischen und zeitkritischen Datenverkehr der Automatisierungstechnik. CIP-Netzwerke sind interoperabel konzipiert. Das bedeutet, dass ihre Kommunikation untereinander standardisiert ist und ermöglicht beispielsweise, dass ein DeviceNet mit einem EtherNet/IP-Gerät arbeiten kann. [31]

3.2.3 Profinet

Profinet ist die Abkürzung für Process Field Network und ist der offene, herstellerübergreifende Industrial Ethernet Standard für die Automatisierungsindustrie. Profinet ist auf die Kommunikation zwischen einer Steuerung und den dezentralen Feldgeräten zugeschnitten. Der aktuelle Standard heißt Profinet-IO und hat sich kurz nach der Entwicklung als eines der führenden Industrial-Ethernet Protokolle etabliert.

[18] Institute of Electrical and Electronics Engineers
[19] Common Industrial Protocol

Neben dem zyklischen Nutzdatenaustausch bietet Profinet zusätzliche Funktionen für die Übertragung von Diagnosen, Parametrierungen und Alarmen.

Innerhalb von Profinet-IO werden Prozessdaten und Alarme immer taktsynchron in Echtzeit (IRT[20]) übertragen. Diese Echtzeitdaten werden gegenüber dem TCP/IP-Daten hoch-prioritär behandelt. Mit dieser Art des Datenaustauschs sind Buszykluszeiten im Bereich von wenigen Millisekunden erreichbar. [18], [17], [24] & [32]

3.2.4 S7 Comm

Das S7 Protokoll RfC[21] 1006) dient zur Verbindung von S7 Automatisierungsgeräten mit beliebigen Kommunikationspartnern. Es ermöglicht den direkten Zugriff auf die Speicherbereiche einer SPS, ohne dass Änderungen in der Benutzeranwendung selbst durchgeführt werden.

Das S7 Comm ermöglicht die Adressierung aller internen SPS-seitigen Daten, das bedeutet, es gibt keine Einschränkung bei den Datenbausteinen (DB). Je nach SPS müssen nur kleine oder gar keine Konfigurationsänderungen zur Unterstützung des S7-Protokolls vorgenommen werden. [25]

3.2.5 SERCOS[22]

Das SERCOS Protokoll dient zur Übertragung von Daten in Echtzeit. Durch diese Priorität ermöglicht es höchste Präzision für die Positionierung von Motorachsen, auch bei hohen Geschwindigkeiten.

Als physikalisches Medium wurde bis zur Version zwei noch ein Lichtwellenleiter verwendet, seit Version drei aus dem Jahr 2005 wird aber auch hier auf das in der Industrie mittlerweile übliche Ethernet gesetzt. [45]

3.2.6 SafetyNET

Ziel der Entwicklung von SafetyNET war es, die Feldbus-Kommunikation über Ethernet in Echtzeit und gleichzeitig für die Kommunikation von Daten im Sinne der Maschinensicherheit zu ermöglichen. Es kann entsprechend der Safety Network International in Sicherheitskreisen bis einschließlich der Kategorie SIL-3[23] eingesetzt werden.

[20] Isochronous Real-Time
[21] Request for Comments
[22] Serial Realtime Communication System
[23] Sicherheits-Integritätslevel

SafetyNET kann überall dort zum Einsatz kommen, wo die zeitliche und inhaltliche Konsistenz von kommunizierten Daten zur Absicherung von Gefahren erforderlich ist. Durch die Spezialisierung sind hier Zykluszeiten von 62,5 µs möglich. Es kann sich bei den Gefahren um die Gefährdung von Leib und Leben handeln, aber auch um die Absicherung von Wirtschaftsgütern. [42] & [33]

4 Endpoint Protection

Eine neue Herangehensweise beim Schutz der Assets in der OT ist eine umfassende Endpoint Protection. Denn wenn sich Infektionen in vernetzten Systemen ausbreiten können, sind Endpoints in den meisten Fällen der Ursprung. Dies kann durch unachtsame Mitarbeiter oder auch durch Infektionen durch den Besuch eines Servicetechnikers entstehen, wie in einem späteren Kapitel näher erläutert wird.

4.1 Virenscanner

Virenscanner galten lange als das Mittel der Wahl für umfassende Sicherheit. Allerdings hatten Virenscanner schon immer das Problem mit der Performance sowie der Einschränkung, dass ihre Erkennung mit Hilfe von Mustern arbeitet. Somit haben die Virenscanner immer einen prinzipbedingten Nachteil, sobald sich der Code der Schadsoftware ändert. Bei Tests der Firma Rack911 hat man Virenscanner sogar dazu gebracht, wichtige Systemdateien oder auch Komponenten der eigenen AV-Software selbst zu löschen. Natürlich werden die Signaturupdates jeden Tag länger, was ebenfalls zu einem Verlust in der Performance führen muss, da jede Datei mit den Mustern in der Signaturdatenbank verglichen werden muss. Deshalb führt der Einsatz von Virenscannern heute oftmals nur zu einer gefühlten Sicherheit. [2] & [59]

4.2 Moderne Endpoint Protection

Viele Jahre lang haben renommierte Hersteller ihre AntiViren Software jedes Jahr neu veröffentlicht und in regelmäßigen Abständen mit neuen Virendefinitionen versorgt. In den letzten Jahren hat hier aber ein technologischer Fortschritt stattgefunden, der vor allem durch neue Firmen, die in den Markt eingetreten sind, getrieben wurde. Dieser Fortschritt hat auch die etablierten Hersteller zur Implementierung neuer Techniken wie KI[24], Integration der Cloud oder maschinellem Lernen gezwungen, um die Kunden noch von Ihren Produkten zu überzeugen. Mittlerweile ist der Funktionsumfang auch um einfache Firewallfunktionen oder den Schutz von Schnittstellen, wie beispielsweise USB, erweitert worden.

Angefangen hat dies mit sogenannten HIPS[25]. Hierbei wurden Regeln definiert, das ein Browser keine anderen beliebigen Programme starten darf. Er sollte auch nur auf

[24] Künstliche Intelligenz
[25] Host-based Intrusion Prevention System

bestimmte Bereiche der Registry zugreifen dürfen. So kann ein HIPS verhindern, dass eine Malware größeren Schaden auf einem Endpoint anrichtet oder sich im Netzwerk weiter verbreiten kann. Die benötigten Regeln müssen aber genau auf die verwendeten Programme angepasst werden. Dafür ist eine Anpassung an neue Malware nicht mehr notwendig. Der damit erreichbare Schutz ist durchaus hoch - zumindest solange die Malware als ausführbares Programm programmiert wurde oder diese Form nachgeladen wird.

Die Weiterentwicklung ist die Überwachung von Prozessen auf den Endgeräten. Bei diesen überwacht ein lokaler Agent jede laufende Aktivität inklusive der gesamten Kommunikation sowie den Zugriffen auf Ressourcen eines laufenden Prozesses. Im Gegensatz zu einem HIPS werden diese Aktivitäten jedoch nicht anhand einzelner Policies erlaubt oder blockiert, sondern das Verhalten wird im gesamten Verlauf analysiert, um bei der Ausführung bösartiges Verhalten zu entdecken und entsprechend darauf reagieren zu können.

Dabei geht es nicht um das Verhalten einzelner, angemeldeter Benutzer, sondern einzig um das der jeweiligen Prozesse. Die Bewertung der Verhaltensmuster wird dann oftmals mit der herstellereigenen Cloud abgeglichen und per KI-Unterstützung bewertet. [50]

4.3 Einsatz von Yara

Falls trotz aller Sicherheitsmaßnahmen doch Malware ins Unternehmen gekommen ist, lässt sich diese auch im Nachhinein noch untersuchen. Dabei werden dann oft sehr wichtige Informationen gewonnen, die weitere Entscheidungen maßgeblich bestimmen können. So ist es für eine Säuberung nach einer Infektion unabdingbar, möglichst viel über die Malware und deren Wirkungsweise in Erfahrung zu bringen. Ein sehr nützliches Tool dafür ist Yara. Damit lassen sich erkannte Strings in allen möglichen Dateien sowie in laufenden Prozessen ermitteln. Damit ist es dann möglich, schnell eine Übersicht über die Assets zu erlangen und eine Entscheidung über die Neuinstallation zu treffen.

5 Übersicht über Bedrohungen

Im folgenden Kapitel werden mögliche Bedrohungen, die für ein Produktionsnetzwerk relevant sind, beschrieben. Durch die Verbindung der OT mit Netzwerken der IT gelten die Gefahren gemein hin auch für diese - erst Recht, da IT-Netzwerke meist einen direkten Internetzugriff besitzen. In etlichen Studien, die unter anderem das BSI als Lagebericht zur IT-Sicherheit in Deutschland veröffentlicht hat, wurden Vorfälle mit Infektionen betroffener Unternehmen untersucht und dabei die am häufigsten verwendeten Einfallsvektoren ermittelt. In den Jahren 2019 und 2020 waren sehr viele Attacken mit Emotet erfolgreich, in der häufig massenhaft versendete E-Mails als Einfallsvektor benutzt wurden. Dies lässt sich aber aus Sicht der Angreifer immer schwerer umsetzen, da die E-Mail Gateways die Technik hinter diesen Angriffen aufgrund der stetigen Anpassungen durch Updates der Hersteller sowie Optimierungen durch Security Spezialisten besser erkennen können. Somit sind sie zur Spezialisierung ihrer Angriffe gezwungen oder konzentrieren sich gezielt auf finanziell aussichtsreichere Ziele. Damit werden die Angriffe nicht mehr ziellos durch die Massen-E-Mails geführt sondern mit Unterstützung durch Social Engineering und anderen Techniken an die auserwählten Opfer angepasst und sind dadurch erfolgversprechender. [10]

5.1 Bedrohungen von Außen

Täglich werden tausende Unternehmen über ihre Peripherie oder von außerhalb erreichbare Server angegriffen. Nur ein kleiner Teil davon ist bei guter IT-Security Ausstattung erfolgreich.

Dazu kommen bisher unbekannte Sicherheitslücken in den eingesetzten Produkten als Gefahrenquelle, die in der Informationstechnik als Zero-Day Lücken bezeichnet werden. Werden diese mit einem funktionierenden Exploit aktiv ausgenutzt, ist das Gefahrenpotential als sehr hoch einzustufen, da wie im Kapitel 4 beschrieben, die meisten Sicherheitsmechanismen in diesem Fall machtlos sind.

So erst jüngst geschehen mit der vom BSI als extrem kritisch eingestuften Sicherheitslücke im Groupware Dienst Exchange von Microsoft. Hierbei haben Angreifer allein in Deutschland potenziell zehntausende Server als Ziele, die wahrscheinlich schon kurz nach Bekanntwerden der Lücke infiziert wurden. Zum Zeitpunkt der Veröffentlichung wurden bereits Angriffe auf Server beobachtet. [9]

Kritisch dabei ist die Anbindung der Exchange Server. Sie kommunizieren oftmals direkt mit dem Internet und halten kontinuierlich die Verbindung zu den vielen Clients im Intra-

net. Der Weg von einem kompromittierten Groupware-Server bis in die tiefer liegende IT-Infrastruktur mit vielen anderen Servern und die unterlagerte OT ist oftmals nur durch wenige Hürden, beispielsweise eine interne Firewall, gesichert. Hier kann eine einzige fehlerhafte Regel oder ein fehlendes Sicherheitsupdate die gesamte IT inklusive der OT kompromittieren.

In einem anderen Fall wurde der Angriff auf die IT der Unternehmen über deren eingesetzte Software umgesetzt. Die Angreifer haben Schadcode in Updates für SolarWinds Produkte (z. B. Orion) integriert. Dadurch hatten Sie bis zur Entdeckung durch die Firma FireEye, die diesen aufwändigen Hack erst durch einen Angriff auf die eigene Infrastruktur bemerkt und veröffentlicht hat, bei vielen Unternehmen Zugriff auf die interne Infrastruktur. Das hat auch Branchengrößen wie Microsoft, Intel, VISA, Mastercard, Siemens oder Lufthansa getroffen. Das Ausmaß wurde nur langsam ersichtlich und erstreckt sich in bisher ungeahnte Dimensionen. Insgesamt muss von einem Zugriff auf bis zu 18.000 Unternehmen, die Software von SolarWinds einsetzen, ausgegangen werden und damit als potenzielle Opfer gelten. Wie so oft in solchen Fällen ist der Angriff bei Solarwinds dem betroffenem Unternehmen nicht selbst aufgefallen, sondern durch Externe eher zufällig entdeckt worden.

Der FDP-Bundestagsabgeordnete Manuel Höferlin (FDP) hat im Dezember 2020 eine schriftliche Anfrage an die Bundesregierung gestellt, ob SolarWinds-Produkte auch auf Bundesebene eingesetzt wurden. Die Antwort dazu lautet: Allein 16 Bundesbehörden und Ministerien gehören zu den Kunden, darunter das Bundeskriminalamt, das Kraftfahrt-Bundesamt, die Physikalisch-Technische Bundesanstalt, das Robert Koch-Institut und der zentrale IT-Dienstleister des Bundes, ITZ[26] Bund. Allerdings haben nicht alle die unsichere Orion-Software eingesetzt. Die Bundesregierung hat auf Höferlins Anfrage geantwortet, es habe keine unberechtigten Zugriffe auf Systeme der Bundesverwaltung gegeben. [4], [28], [35], [49], [56] & [58]

Da die Angreifer sich allerdings auch ständig weiterentwickeln, entstehen auch hier immer wieder neue Technologien. Relativ neu ist das RaaS[27]. Dadurch können selbst unbedarfte Hacker ihre Angriffssoftware wie in einem WebShop zusammenstellen und bekommen dabei ein Komplettpaket, dass sogar die Zahlungsabwicklung, also die erfolgreiche Erpressung der Opfer, übernimmt. Damit hat sich die Bedrohungslage weiter verschärft.

[26] Informationstechnikzentrum
[27] Ransomware as a Service

5.2 Bedrohungen von Innen

Bedrohungen von Innen entstehen immer wieder und können grundsätzlich in Vorsatz oder Fahrlässigkeit unterschieden werden. So können Bedrohungen durch Mitarbeiter, die andere Interessen verfolgen oder auch eine Kündigung erfahren haben, erfolgen. Da sich die Art von Täter oftmals sehr gut im Unternehmen auskennen, werden diese Vorfälle meist nicht oder nicht rechtzeitig entdeckt und der Schaden kann erhebliche Ausmaße annehmen. In anderen Fällen wurden präparierte USB-Sticks ausgelegt und von unachtsamen Mitarbeitern unerlaubt mit den Computern im Unternehmensnetzwerk verbunden.

5.2.1 Innentäter - vorsätzliches Fehlverhalten

Ein Beispiel für einen frustrierten Mitarbeiter, das besonderes Aufsehen erregt hat, ist die Verhaftung eines langjährigen und pflichtbewussten IT-Technikers der NATO[28], der eigentlich nur auf die vorgefundenen Missstände in der IT und den sehr offenen Umgang mit vertraulichen und geheimen Dokumenten aufmerksam machen wollte.

Manfred K. wies seine Vorgesetzten wiederholt auf diverse Sicherheitslücken hin, erst vorsichtig, dann in immer schärfer werdendem Ton. Er mochte sich mit den erhaltenen Antworten nicht abfinden, denn er wusste, dass er Recht hatte. Also schrieb er Beschwerden nach Brüssel, wollte auch einen Beitrag in der Mitarbeiterzeitschrift veröffentlichen, schaltete schlussendlich sogar den Generalsekretär ein. Doch die NATO ließ ihn auflaufen. So stieg der Frust über seine Vorgesetzten immer weiter und brachte Manfred K. zu einer folgenschweren Entscheidung. Dermaßen frustriert nutzte er mehrere der angeprangerten Sicherheitslücken und stahl sensible Daten aus dem inneren Kreis der NATO. Er wurde nach seiner Verhaftung angeklagt und muss sich nun zum Vorwurf des Landesverrat verantworten. [13]

5.2.2 Innentäter - fahrlässiges Fehlverhalten

Ein anderer möglicher Fall ist die Fahrlässigkeit von Angestellten. Dabei unterlaufen Mitarbeitern ohne offensichtliche Absicht teils folgenschwere Fehler, die zu einer großen Bedrohung führen können. Im Fall, den das BSI beschrieben hat, kam ein Servicetechniker bei Routinearbeiten mit einem infizierten USB-Stick zum Einsatz und infizierte damit etliche Server. Aufgrund von Echtzeitanforderungen und regulatorischen Vorgaben konnte auf den Systemen keine Antiviren Software betrieben werden. Als er dann zur Vorbereitung seiner Wartungsarbeiten den verwendeten USB-Stick an einem Entwicklungsrechner einsteckte, löste die dort installierte Antiviren-Software Alarm aus.

[28] North Atlantic Treaty Organization

Im weiteren Verlauf wurde entschieden, einen Virenscanner ohne Installation zu nutzen und so einen möglichst geringen Eingriff in den Systemen zu verursachen. Bei der weitergehenden Analyse ergab sich, dass der Betreiber eine der wichtigsten Sicherheitsmaßnahmen umgesetzt hatte: Aus der Leitstelle heraus war keine Kommunikation mit dem Internet möglich. Dies führte vermutlich dazu, dass die Schadsoftware keinen Kontakt zu einem Command & Control Server aufnehmen konnte, um an diesen Daten abfließen zu lassen und weitere Anweisungen oder Schadcode entgegenzunehmen. [6]

5.3 Bedrohungen durch APT[29]

Eine der aktuell größten Bedrohungen stellen mit Abstand die APT dar. Dabei handelt es sich um „fortgeschrittene, andauernde Bedrohungen“, in denen die Angriffe mit viel Aufwand langfristig geplant und gezielt auf das Ziel zugeschnitten werden. Oftmals werden bei APT angriffen Zero-Day Lücken verwendet, womit sie nur sehr schwer zu verhindern sind.

Während andere Angreifer mit ihren Aktionen möglichst viel Aufmerksamkeit erlangen wollen, indem sie prominent Zahlungsaufforderung auf den Bildschirmen mit entsprechenden Bezahlmodalitäten präsentieren, zielen APT auf eine möglichst lange Verschleierung ab, um so ungehindert an möglichst viele Daten zu gelangen.

Fortgeschritten sind die Angriffe deshalb, weil den Angreifern große Mengen an Zeit und Geld sowie meist enorme Entwicklungskapazitäten zur Verfügung stehen. Für die Opfer ist der Angriff auf ihre IT-Infrastruktur kaum nachvollziehbar und mit herkömmlicher IT-Security nur schwer aufzudecken. So können sich die Eindringlinge meist unerkannt über mehrere Wochen oder sogar Monate hinweg im internen Netz bewegen.

5.3.1 Stuxnet

Einer aufgrund seiner Komplexität einzigartiger APT-Angriff ist der Hack der iranischen Urananreicherungsanlage in Natanz im Jahr 2010 mit dem Schadprogramm Stuxnet. Es wurde speziell zum Angriff auf das SCADA[30]-System des Herstellers Siemens entwickelt, um die Steuerung von Frequenzumrichtern zu manipulieren.

Dabei wurde das automatische Update der Prozessabbilder deaktiviert und von Stuxnet kontrolliert, welche Signalzustände der legitime Code erhält und welche Aktionen überhaupt an die Aktoren weitergeleitet werden. Der Schadcode zeichnete zunächst für

[29] Advanced Persistent Threats
[30] Supervisory Control and Data Acquisition

21 Sekunden die Sensorsignale auf und speicherte sie in einem dynamisch angelegten Datenbaustein. Diese gespeicherten Daten wurden dann in einer Endlosschleife in das Prozessabbild kopiert, um den legitimen Steuerungscode und mit ihm letztendlich auch die Bediener im Leitstand zu täuschen.

Aufgrund der Komplexität von Stuxnet wird ein außerordentlich hoher Entwicklungsaufwand vermutet, bei dem der Zeitaufwand auf mindestens sechs Monate und der Personalaufwand auf bis zu zehn Hauptentwickler geschätzt wurde. Neben dem Know-How für die Entwicklung mussten Kenntnisse über unbekannte Sicherheitslücken und Zugang zu geheimen Signaturen zweier Unternehmen vorhanden sein. So wird vermutet, dass die Stuxnet-Entwicklung insgesamt rund 50 Millionen US Dollar gekostet hat. [36] & [62]

Die Einzigartigkeit von Stuxnet zum Zeitpunkt seiner Entdeckung zeigt sich insbesondere in der Art seiner Verbreitung durch:

- Ausnutzung von Zero-Day Lücken in Microsoft Windows & Windows Server
- Installation eines Rootkits mit Hilfe gestohlener, vertrauenswürdiger Signaturen
- genaue Kenntnisse des Prozessvisualisierungssystems WinCC
- Installation eines weiteren Rootkits in der Steuerung einer PCS-7[31]-Anlage

5.3.2 Die fünf Stufen eines APT Angriffes

Im Gegensatz zu gewöhnlichen Attacken mit Spam-Mails, bei denen Hacker eine große Anzahl E-Mails versenden, um zufällige Opfer zu treffen, sucht eine APT-Gruppierung vorsätzlich nach einem ausgewählten Ziel. Dabei gehen die Angreifer nach einem klassischen Muster vor, das sich in fünf Stufen unterteilen lässt. Diese Einstufung lässt sich natürlich weiter auflösen.

1. Erkunden und Recherchieren (Initial access)

Ist ein Ziel ausgewählt, geht es in dieser ersten Phase des Angriffs darum, möglichst viele Informationen über das Unternehmen oder die Organisation zu sammeln. Hierbei greifen die Hacker besonders auf Unternehmenswebsites, Social Media und andere öffentliche zugängliche Quellen zu, um Einstiegsmöglichkeiten in die Systeme des Ziels zu finden. Hier kann eine unüberlegte Bemerkung über Interna dramatische Folgen haben.

[31] Process Control System

2. Einfall in das System

Hat der Angreifer eine gute Vorstellung über die Struktur seines Angriffsziels gewonnen und in Erfahrung gebracht, welche IP-Adressen, Domains und Systeme in welcher Art miteinander verbunden sind, kann er detailliert nach Schwachstellen suchen. Um letztendlich Zugriff zu den Systemen des Ziels zu erhalten, bedienen sich die Hacker verschiedener Methoden wie Social Engineering, CEO-Fraud, Phishing sowie Ransomware. So geht es beim Thema Cyber-Security nicht nur um verwundbare Computersysteme und angeschlossene Netzwerke. Häufig nutzen die professionellen Angreifer den Faktor Mensch als Schwachstelle gezielt aus, indem Hilfsbereitschaft und Vertrauen ausgenutzt werden.

3. Ausspähen und Ausbreiten (Credential access and lateral movement)

Sobald die Angreifer Zugriff auf die internen Systeme haben, operieren sie üblicherweise möglichst vorsichtig, um ihre Entdeckung möglichst lange zu verhindern. Die Sicherheitsvorkehrungen und eingesetzte Software des Unternehmens werden in dieser Zeit identifiziert, um weitere Sicherheitslücken zur Ausweitung des Zugriffs zu ermitteln. Mithilfe der gefundenen Daten wird beispielsweise versucht, Passwörter aus den ermittelten Hashes zu ermitteln und so Zugänge zu weiteren Datensätzen und Systemen herzustellen. Auch das Übertragen gekaperter SAM[32]-Dateien auf andere Systeme kann je nach Schwachstellenlage und bereits erlangten Zugriffsrechten erfolgreich sein.

4. Ausführung des Angriffs (Command & control and exfiltration)

In dieser Phase wird auf die nun ungeschützten Systeme zugegriffen und beispielsweise sensible Unternehmensdaten über einen längeren Zeitraum hinweg kopiert. Dabei wird meist parallel versucht, über die entdeckten Sicherheitslücken weitere Malware in den IT-Systemen zu installieren, damit bei einer Entdeckung eine bis dahin unentdeckte Hintertür verfügbar bleibt. Aber auch das Stilllegen von Systemen ist eine Option, um den Opfern nachhaltig zu schaden.

5. Analyse der Daten & Spuren verwischen

Die erhobenen Daten und Informationen werden an einen zentralen Server der Angreifer übermittelt und dort analysiert. Hierbei werden dann die Informationen zur weiteren Nutzung aufbereitet. Wie üblich bei APT-Angriffen werden die Daten meist sehr behutsam übertragen, um keine auffälligen Datenströme zu erzeugen. So ist es verständlich, dass das Abgreifen der Daten teilweise über Monate fortdauert. Neuerdings werden

[32] Security Account Manager

zur Beschleunigung des Datentransfers auch Cloudanbieter wie Dropbox in die Angriffe eingebunden, um die Übertragungen im gesamten Netzwerkverkehr zu „verstecken“.

Je nach Intention bestimmen dann finanzielle Aspekte oder die politischen Ziele das weitere Vorgehen. Wenn die Angreifer erfolgreich sind, ist es der letzte Schritt, die eigenen Spuren so gut wie möglich zu verwischen. Dies betrifft vor allem den eingesetzten Code inklusive der nachgeladenen Malware sowie das Manipulieren von Log-Dateien. Natürlich ist dies nicht restlos möglich, da ab einem gewissen Zeitpunkt durch das rekursive Verhalten der Zugriff stark eingeschränkt ist. [16] & [29]

5.3.3 Verwendete Techniken während eines APT-Angriffs

APT-Angriffe mit ihren vielen einzelnen Schritten und beteiligten Personen erfordern einen enormen Koordinationsaufwand sowie den gezielten Einsatz bewährter Angriffstechniken im Bezug auf Menschen und IT-Systeme. Bei den bisher bekannten APT-Angriffen wurden die verwendeten Taktiken der Angreifer analysiert. Dabei wurden verschiedene davon wiederholt beobachtet.

Social Engineering

Die älteste und zugleich erfolgreichste aller Methoden zur Infiltration ist klassisches Social Engineering. Es ist viel einfacher, jemanden zu überzeugen, den benötigten Zugang zu verschaffen als ihn selbst zu stehlen oder zu entwickeln. Die meisten APT-Angriffe haben eine Social-Engineering-Komponente, die entweder am Anfang während der Zielerforschungsphase oder gegen Ende, um die Spuren zu verwischen, eingesetzt wird.

Spear Phishing

Spear Phishing beschreibt einen gezielten Versuch, einer bestimmten Person die Zugangsdaten zu entwenden. Das Zielobjekt wird typischerweise während der Zielforschung ausgekundschaftet und als möglicher Türöffner für die Infiltration identifiziert. Wie bei normalen, weit gestreuten Phishing Angriffen verwenden Spear-Phishing Angriffe Malware, Keylogger oder E-Mails, um den Einzelnen dazu zu bringen, die Anmeldeinformationen weiterzugeben.

Rootkits

Rootkits beziehen sich auf den englischen Begriff Wurzel und verweisen dabei auf den innersten Kern eines IT-Systems. Somit sind sie tief im System verankert und auch deshalb schwer zu erkennen, da sie einen regulären Zugang zum infizierten System

gewähren können. Einmal installiert können Angreifer über das Rootkit auf infizierte Infrastruktur des Zielunternehmen zugreifen und sich per Lateral Movement weiter im Unternehmensnetzwerk ausbreiten. Sollte sich das Rootkit im BIOS befinden, hilft nur der komplette Austausch der Hardware, da sich das Rootkit bei jedem Neustart wieder installieren würde. Eine Säuberung oder der Tausch der Festplatten wäre nutzlos. [43]

Exploits

Ein Exploit beschreibt die aktive Ausnutzung einer Schwachstelle zum Ziele eines Angriffs auf IT-Systeme. Zero-Day Exploits sind die gefährlichere Variante, da es für die bisher unbekannte Sicherheitslücke noch keinen Patch zur Abhilfe gibt. Natürlich kann ein nicht gepatchtes System mit einer bereits bekannten Sicherheitslücke zu einem Problem werden, wie der APT-Angriff bei Equifax, der mehrere Monate unentdeckt stattfand, bewiesen hat. [48]

Manche Angreifergruppen verwenden mittlerweile Cloud-Dienste wie Dropbox, um ihre Exploits zu verteilen. Dabei „verstecken“ sie den schädlichen Download in dem normalen Traffic des Unternehmens. Gerade in Zeiten, wo die Nutzung von Cloud Diensten en-vouge ist, fällt dies den meisten Administratoren durch die Nutzung legitimer Infrastrukturen wahrscheinlich nicht auf. [60]

5.3.4 Beispiel für einen APT-Angriff auf ein Unternehmen in Deutschland

Viel Glück hatte im Mai 2020 die Firma Schmersal in Wuppertal. Das LKA[33] Nordrhein-Westfalen informierte die dortige IT-Abteilung über einen bevorstehenden oder bereits aktiven Angriff auf das Unternehmen. Nach der Verifikation des Anrufes wurde in nur knapp 10 Minuten die komplette Internetverbindung getrennt, danach das gesamte Intranet heruntergefahren. Weltweit waren danach alle Standorte nach nur 90 Minuten offline. Somit war das Unternehmen komplett von außen abgeschottet und hat den Angreifer dem Zugang abgeschnitten - damit wurde Schmersal allerdings auch für die vielen Kunden nicht mehr erreichbar. Alle Systeme zur Kommunikation waren offline.

Wie die beauftragten Forensiker feststellten, war dies die einzig richtige Entscheidung, den die Schadsoftware ließ sich damit isolieren und identifizieren. Glücklicherweise befand sich der Angriff noch in der Vorbereitungsphase. Es wurde dokumentiert, dass die Schadsoftware gezielt auf Schmersal zugeschnitten wurde und deshalb von keinem bisher eingesetztem Schutzsystem erkannt werden konnte.

[33] Landeskriminalamt

Nach knapp einer Woche intensiver Arbeit konnte das Intranet reaktiviert werden und die Firma war damit vom Lager aus wieder lieferfähig. Nach insgesamt 14 Tagen konnte die Produktion in Deutschland wieder in den regulären Betrieb übergehen. Laut Philip Schmersal hatte dieser Angriff neben den Neuanschaffungen in der IT deshalb auch einen hohen wirtschaftlichen Schaden für Schmersal. [34]

Vor allem bei solch individualisierten und ausgefeilten Vorgehensweisen ist offensichtlich, dass sich gezielte Angriffe auf die IT eines Unternehmens über Dauer vermutlich nicht verhindern lassen. So sollte der Fokus der IT-Sicherheit im Unternehmen auf der gezielten Detektion sowie unmittelbaren Reaktion liegen. Die vergangenen Kapitel haben deutlich gezeigt, dass es genügend Sicherheitslücken in der eigenen Infrastruktur geben kann, für die man selbst keine Verantwortung tragen muss oder Menschen fahrlässig handeln. In solchen Fällen kann eine NBAD die Reaktionszeit nach einer Infektion enorm verkürzen. Sollte hier also ein Asset ungewöhnlichen Netzwerkverkehr erzeugen, wird dies mit hoher Wahrscheinlichkeit durch eine NBAD aufgedeckt.

6 Einsatz einer Netzwerkverhaltensanalyse

Systeme für eine Netzwerkverhaltensanalyse, oder auch kurz NBAD-Systeme, erfassen den Verkehrsfluss an mehreren Punkten eines Netzwerkes und erstellen während einer Trainingsphase nach der Erst-Inbetriebnahme den Ist-Zustand in einem Verkehrsprofil. Dieses Profil bildet eine der Grundlagen für die spätere Erkennung von Anomalien, wobei der Ist-Zustand in der operativen Phase in nahezu Echtzeit mit den erlernten Verkehrsprofil abgeglichen wird.

Grundsätzlich werten NBAD-Systeme dafür nur die Metadaten der Pakete aus, das sich Aufgrund der Menge an Paketen auch nicht anders realisieren lässt. Die Systeme analysieren den Verkehrsfluss und erzeugen bei Bedarf Alarme, so genannte Detections. Das geschieht bei fast allen Anbietern mit Unterstützung von künstlicher Intelligenz, die entweder On-Premise oder in der Cloud vorgehalten wird. Damit haben die Hersteller einen zentralen Punkt, um neu erkannte Methoden der Angreifer per Verhaltensmuster in die eigenen Erkennungsmechanismen zu integrieren und es ihren Kunden zur Verfügung zu stellen.

Bei NBAD-Systemen wird vor allem mit den MITRE-Indikatoren analysiert und bei eindeutigen Anomalien auch mit Verwendung von Multiplikatoren ein entsprechend hoher IoC[34] gebildet. Der große Vorteil dabei ist, dass ein kompromittierter Host, anders als bei IDS[35], diese Erkennung nicht durch eine bereits erfolgte Infektion mit Schadsoftware manipulieren kann, da NBAD-Systeme autark laufen.

Mit Unterstützung des MITRE ATT&CK® Enterprise Framework bekommen Sicherheitsanalysten einen Leitfaden an die Hand, mit deren Hilfe ungewöhnliches Verhalten erkannt und bewertet werden kann. Deutliche Indikatoren sind unter Anderem das Lateral Movement, der Versuch der Rechteausweitung, die Kontaktaufnahme zu C&C-Servern oder das Aufrufen ungewöhnlicher URLs[36], die auch mit einem DGA[37] erzeugt sein können. Die Übersicht über das Framework ist im Anhang A.2 zu finden. [51]

[34] Indicator of Compromise
[35] Intrusion Detection System
[36] Uniform Resource Locator
[37] Domain Generation Algorythmus

6.1 Vorteile einer NBAD

Viele Angriffe, die nach einem APT-Muster vorgehen, lassen sich nur durch ihre Verhaltensmuster erkennen. Aber auch das ist ziemlich schwierig, da eines der wichtigsten Ziele darin beseht, möglichst lange unentdeckt zu bleiben und das befallene Unternehmen möglichst lange zu infiltrieren. Dabei wird oft auch ein großer Aufwand seitens der Angreifer betrieben, die sich sehr genau mit ihrem Ziel auseinander setzen und oftmals spezielle Schadsoftware, zugeschnitten auf die Infrastruktur des Zielunternehmens, programmieren und einsetzen.

Kaum ein Betreiber einer Infrastruktur kann die Firmware selbstständig pflegen und ist bei einer Sicherheitslücke abhängig vom Patchmanagement des Herstellers. Hier sind NBAD Systeme eine Möglichkeit, diese veränderten Verhaltensmuster im Netzwerk zu entdecken und entsprechende Maßnahmen zu veranlassen.

Das die Gefahr real ist und sich der Einsatz einer NBAD rentieren kann, beweisen die immer wieder bekannt werdenden Entdeckungen von Zero-Day Lücken. Nur in den wenigsten Fällen kann man solche Sicherheitslücken mit dem Einsatz einer modernen Firewall kompensieren. Für eine möglichst frühe Veröffentlichung solcher Sicherheitslücken hat Trendmicro die Zero-Day Initiative ins Leben gerufen. Hier werden während einer Pwn2own genannten Veranstaltung Programmierer für das Entdecken und Belegen von bisher unbekannten Sicherheitslücken mit hohen Preisgeldern belohnt. [53]

NBAD-Systeme sind im Allgemeinen am Nützlichsten, wenn sie in Verbindung mit anderen Sicherheitswerkzeugen und Monitoringtools in ein SOAR[38] integriert werden. Eine andere Möglichkeit besteht darin, vorhandene EDR[39] in die NBAD zu integrieren. Eine NBAD ist daher eine gute Möglichkeit, schwer zu entdeckende mögliche Sicherheitsbedrohungen zu finden, die mit herkömmlichen Sicherheitstools nicht ermittelt werden können. Falls andere Schutzmechanismen bereits versagt haben und sich eine Schadsoftware bereits im Netzwerk befindet, ist ein NBAD-System meist die einzige Möglichkeit, den Befall trotzdem frühzeitig zu erkennen.

NBAD-Systeme können mit automatisierten Schutzmechanismen ausgestattet sein, die bei der Erkennung von Anomalien aktiv werden. Sie können dann andere, kompatible Netzwerkkomponenten steuern und beispielsweise gezielt Ports deaktivieren oder per EDR-Lösung den Client isolieren. Damit kann die Verbindungen auffälliger Clients gezielt unterbrochen und das Lateral Movement frühzeitig gebremst werden. Allerdings ist hier auch immer eine genaue Bewertung der Auswirkungen von möglichen „false positive“ notwendig. Aufgrund möglicher Folgen nutzen deshalb nicht alle Kunden den automatischen Eingriff. [26]

[38] Security Orchestration, Automation and Response
[39] Endpoint Detection and Response

6.2 Vectra Cognito Detect

Vectra Networks bietet mit der Cognito Plattform ein System, dass mit der Fähigkeit zur Echtzeiterkennung von Bedrohungen und Analyse auch APT-Angriffe aus Kapitel 5.3 erkennen kann. Die kontinuierliche Analyse des Netzwerkverkehrs ermöglicht dabei die automatische Erkennung aller Phasen eines unbefugten Zugriffs beim Versuch der Spionage, des Diebstahls sowie bei der Ausbreitung eines Angreifers im Netzwerk per Lateral Movement. Cognito Detect analysiert die übertragenen Datenpakete dabei einzig anhand der Metadaten (Header).

Vectra unterteilt die erkannten Hosts anhand ihrer Detections in vier ineinander übergehende Quadranten - siehe Bild 6.1. Dabei wird mit der Ordinatenachse die Bedrohung und mit der Abszisse die Wahrscheinlichkeit der Erkennung abgebildet. Diese verändern sich dynamisch mit dem Verhalten der einzelnen Assets über die Zeit.

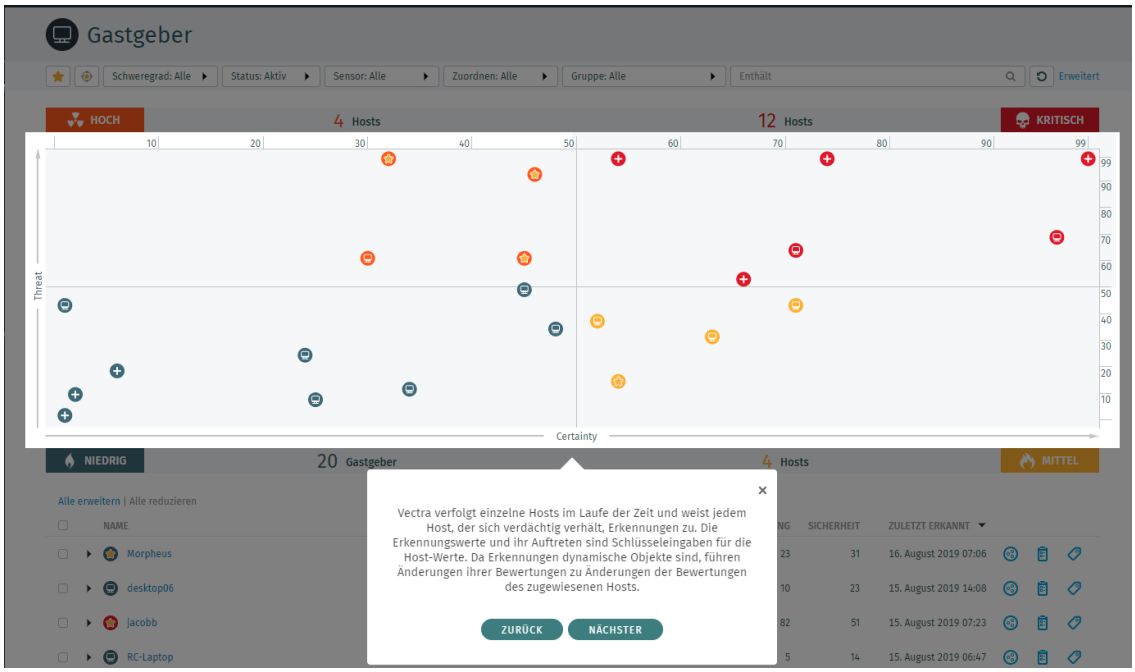

Abbildung 6.1: Vectra AI - DashBoard - Threat & Certainty

Cognito Detect speichert die gesammelten Metadaten nur für eine kurze Zeit und erzeugt daraus, wie in Abbildung 6.2 zu sehen, die Detections für einzelne Hosts. Die Metadaten werden in Absprache mit dem Betriebsrat und nach geltenden Datenschutzrichtlinien behandelt und nach der Verarbeitungszeit verworfen. [22]

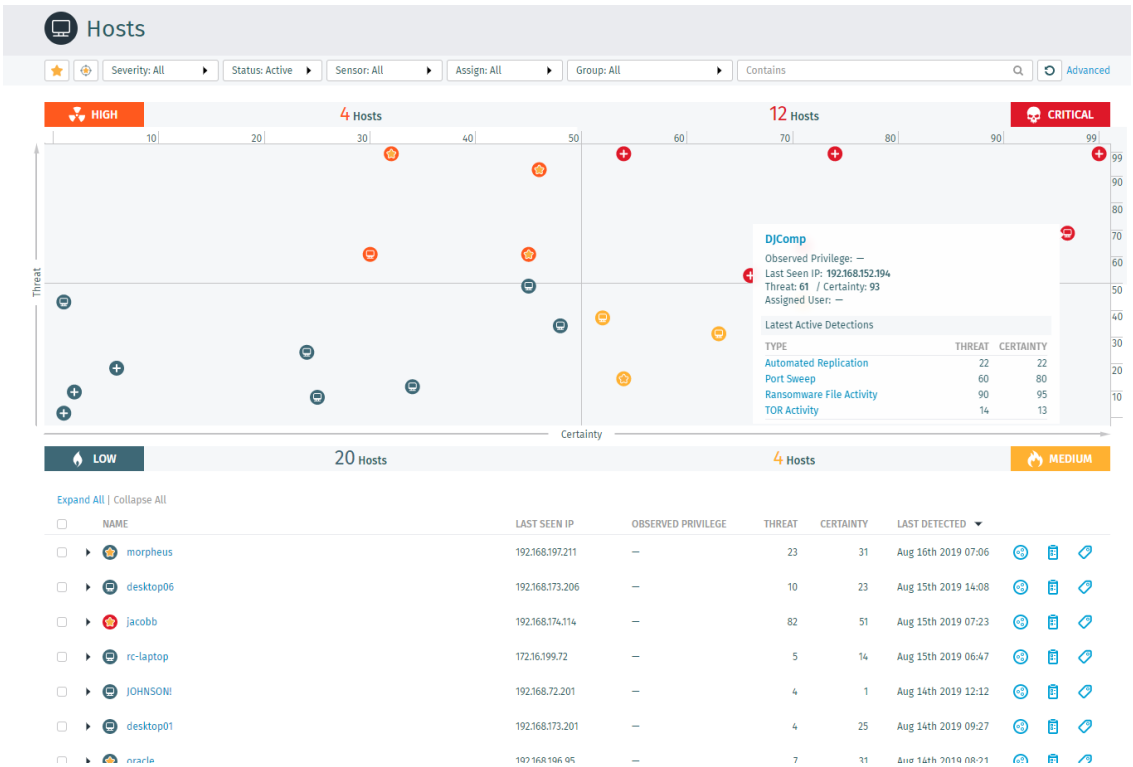

Abbildung 6.2: Vectra AI - DashBoard - Hostübersicht

Die einzelnen Detections werden pro Host aufgelistet und aufsteigend sortiert. Diese Übersicht ist in Abbildung 6.2 zu sehen und zeigt dabei die letzten fünf Ereignisse, die dem einzelnen Host und auch Accounts zugeordnet werden konnten. Dies wird über die Anbindung externer Connectoren, beispielsweise ein AD[40]-Server oder vSphere, wie im Bild 6.4 zu sehen, ermöglicht. Damit werden die Detections unabhängig von den eingesetzten Clients oder verwendeten IP-Adressen.

In den Hostdetails aus Abbildung 6.3 ist genau zu sehen, welche Verhaltensmuster Vectra dem einzelnen Host zuschreibt und welche Wertung für die Bedrohung (Threat) und Gewissheit (Certainty) vorgenommen wurden. Dadurch ist schnell zu erkennen, ob es sich um potenziell gefährliche Verhaltensmuster handelt und mit welcher Sicherheit einer Bedrohung Vectra dies bewertet hat. Diese Bewertung ist an das MITRE ATT&CK Framework angelehnt, dass im Anhang A.2 zu finden ist. Dadurch wird die Arbeit der Sicherheitsanalysten deutlich erleichtert. [52].

[40] Active Directory

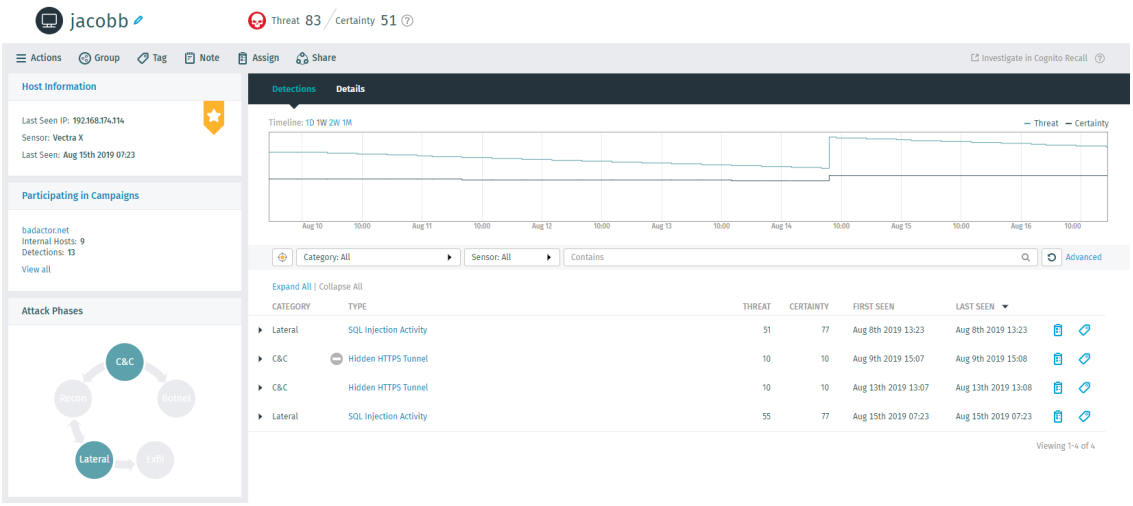

Abbildung 6.3: Vectra AI - DashBoard - Details zum Host

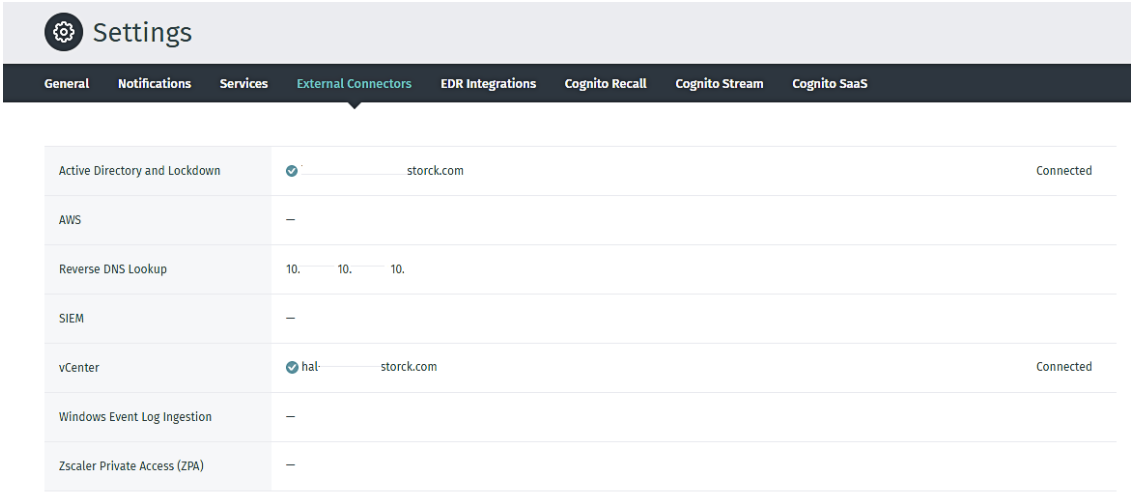

Abbildung 6.4: Vectra AI - Externe Connectoren

6.2.1 Vectra Cognito Recall

Cognito Recall kann als Ergänzungsmodul erworben werden und analysiert, in Verbindung mit Cognito Detect, die große Menge an gespeicherten Metadaten. Dabei hilft es Sicherheitsanalysten bei der Suche nach Sicherheitsvorfällen mit Hilfe von künstlicher Intelligenz aus der Cloud von Vectra. Diese wird dabei ständig durch die anonymisierten Erfahrungen anderer Kunden erweitert.

Damit ist Cognito Recall in der Lage, eine Kette an forensischen Beweisen zu jeder Detection zu liefern. Alle in Cognito Recall gespeicherten Metadaten sind mit Geräten und Hostnamen verknüpft, nicht nur mit IP-Adressen. Die dazu notwendigen Informationen bezieht Cognito Recall ebenfalls aus der Anbindung eines AD-Servers, die in Abbildung

6.4 bereits zu sehen ist. Dies ermöglicht eine intelligente Untersuchung der Aktivitäten jedes Geräts im Laufe der Zeit, unabhängig von Entitätswechseln der Nutzer. [55]

6.2.2 Vectra Cognito Stream

Cognito Detect kann auch mit dem Modul Cognito Stream erweitert werden. Im Unterschied zu Recall werden bei Stream die gesammelten Daten nicht in die Cloud, sondern an ein On-Premise betriebenes SIEM[41] wie Splunk oder SolarWinds weitergereicht. Die Auswertung findet dadurch nur lokal statt und das SIEM muss von den Sicherheitsanalysten selbst eingerichtet werden. Dies kann bei besonders strengen DSGVO[42] notwendig sein. Allerdings muss dabei auf die künstliche Intelligenz aus der Cloud und den Erfahrungen anderer Kunden verzichtet werden.

6.3 Bedienung Vectra AI

Da Vectra sehr mächtig ist und bei entsprechendem Netzwerkverkehr viele Erkennungen liefert, ist es notwendig/möglich, diese entsprechend zu filtern. Dazu bietet Vectra, wie im Bild 6.5 zu sehen, sogenannte Triage Filter, die zum Ausschluss bekannter und akzeptabler Detections genutzt werden können.

[41] Security Information and Event Management
[42] Datenschutz-Grundverordnung

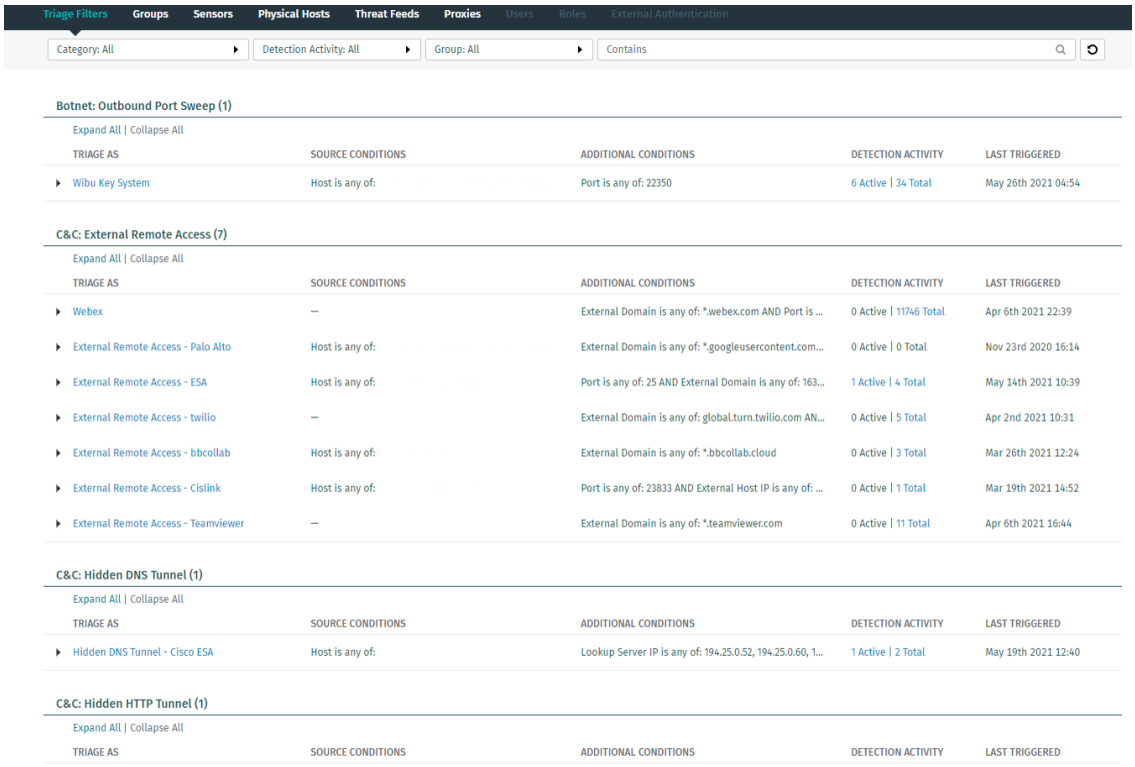

Abbildung 6.5: Vectra AI - Triage Filter

Dies dient der Übersichtlichkeit im Dashboard und entlastet Sicherheitsanalysten bei der täglichen Arbeit mit vielen Clients. Diese Filter können vorteilhafterweise direkt aus einer Detection heraus erstellt werden. Hierbei sollte sich der Nutzer allerdings sicher sein, da alle weiteren Ereignisse, die die Kriterien dieses Filters erfüllen, ausgeblendet werden.

7 Testumgebung für die Netzwerkverhaltensanalyse

Um die Netzwerkverhaltensanalyse in ihrer Funktionsweise zu validieren, ist es notwendig, diese auch zu testen. Dazu wurde der Vectra S2 Sensor zuerst in ein Produktionsnetzwerk integriert, um seine grundsätzliche Funktionsweise in diesem neuen Umfeld zu analysieren und zu verstehen. Anschließend wurde ein kleines, separates Testnetzwerk mit in der OT üblichen Komponenten aufgebaut, um dem Sensor in einer realistischen Umgebung auffälligen Netzwerkverkehr zu präsentieren. Verständlicherweise ist es in einem Produktionsnetzwerk nicht wünschenswert und mit zu viel Risiko behaftet, einen realen Trojaner oder andere Schadsoftware zu Testzwecken einzusetzen.

Neben den vielen Tools, die unter Kali Linux bereitgestellt werden, war PowerShell wegen seiner hervorragenden Eignung die verwendete Scriptsprache. Diese ist in aktuellen Windowsversionen sehr tief im System verankert und erlaubt dadurch einen hohen Grad der Steuerung. Gerade deshalb ist PowerShell bei vielen Administratoren beliebt, da es eine enorme Arbeitserleichterung ermöglicht. Allerdings ergibt sich daraus auch ein hohes Risiko, falls schädlicher Code ausgeführt werden sollte. Angreifer verfolgen damit meist die Ausweitung der beschränkten Rechte als erstes Ziel (privilege escalation). Die die Fähigkeit von Powershell, auch dateiloses Code auszuführen, kann leicht einen installierten Virenscanner oder ein Whitelisting von Applikationen umgehen.

In der Testumgebung ist es allerdings nicht das vorrangige Ziel, lokale Rechte mit einem eingeschränkten Benutzer auf einem Windowssystem auszuweiten, auch wenn das mit den verwendeten Betriebssystemen wie Windows Server 2003 problemlos möglich wäre. Vielmehr soll die Kompromittierung der Windowssysteme und deren Dienste über das Netzwerk realisiert und deren gesteuertes Netzwerkverhalten mit Vectra beobachtet werden.

Vor der Planung der Testszenarien wurde bekannte Schadsoftware in ihrer grundsätzlichen Funktionsweise, auch mit Hilfe der sogenannten Cyber-Kill-Chain betrachtet. Mit Hilfe der Scripte und Tools soll dann das Verhaltensmuster von Schadsoftware nachgeahmt werden, ohne dabei den schädlichen Code auszuführen. [20]

7.1 Einrichtung/Erstbetrieb der Netzwerkverhaltensanalyse

Es wurde beschlossen, den S2 Sensor von Vectra im modernen Produktionsnetzwerk des Produktionsgebäudes C einzusetzen. Hier soll die Lösung Verständnis schaffen, wie sich dieser Sensor in einer bekannten Umgebung verhält. Mit diesem Einsatz und den Erkenntnissen soll eine neue Sichtweise auf ein bekanntes Netzwerk geschaffen und ein besseres Verständnis für die Lösung entwickeln werden.

Mit dem zweiten Eingang am Sensor wurde das Testnetzwerk verbunden. In diesem wurden ausgemusterte Assets per Switch verbunden. In diesem separatem Netzwerk kann die Netzwerkverhaltensanalyse gefahrlos auf ihre Erkennungsleistung hin überprüft werden. Das kommt dem Einsatzgebiet im Produktionsnetzwerk mit einer realen Infektion mit Schadsoftware zwar nicht vollständig gleich, da es Grenzen bei der Komplexität der Tests gibt. Trotzdem ist mit den Komponenten eine realistische Bewertung über die Fähigkeiten der Netzwerkverhaltensanalyse in OT-Netzwerken möglich.

7.1.1 Konfiguration der Switches

An den beiden Switches **SW128008** und **SW128009**, die die Uplinks zur den Firewalls **fw-ohr-pc-prd1-1** und **fw-ohr-pc-prd1-2** bereitstellen, wurden Spiegelports konfiguriert. Die notwendigen Einstellungen sind in Abbildung 7.1 ersichtlich.

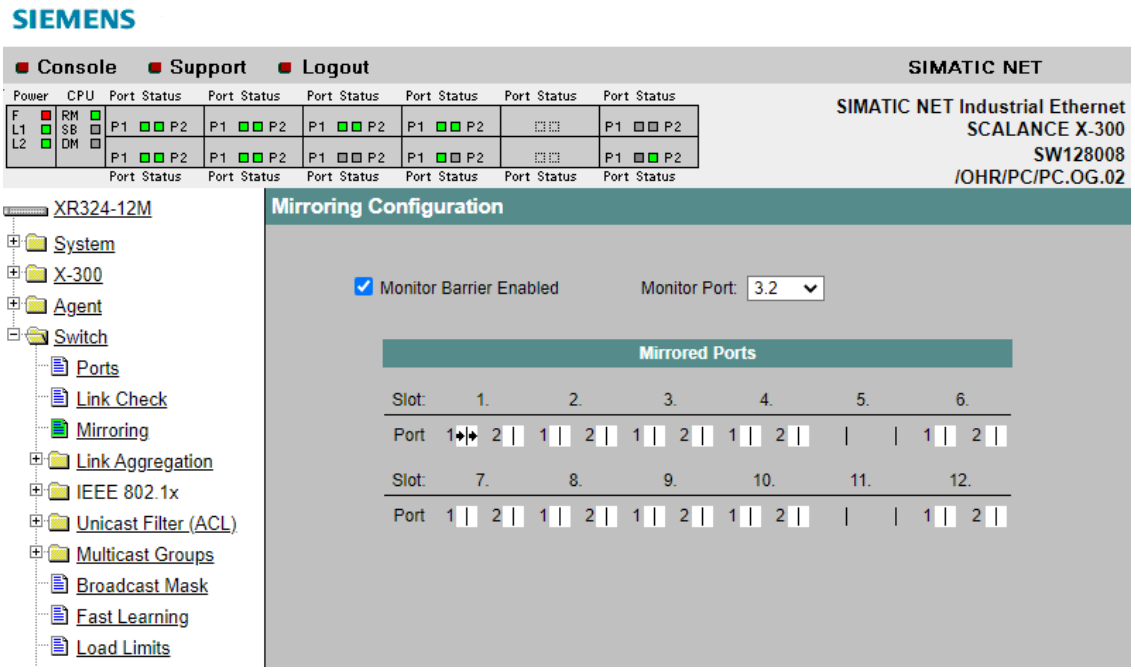

Abbildung 7.1: Siemens XR324 (SW128008) - Konfiguration Spiegelport

Dazu wurde das Mirroring vom jeweiligen Uplink 1.1 auf den Port 3.2 eingestellt, um damit den Netzwerkverkehr rückwirkungsfrei beobachten zu können. Ein dritter Port für das Management des Vectra S2 Sensors wurde im Office Netz am Switch **sw-ohr-pc-og02-cl1-slot1** konfiguriert. Die komplette Übersicht dazu ist im Anhang A.1.

7.2 Beschreibung Testaufbau

Wie in Abbildung 7.2 zu sehen, wurde im Testnetzwerk eine SPS S7-416 mit CP443-2[43] verwendet, die zusammen mit den IPCs[44] bis vor kurzen in der Produktion im Einsatz war. Dieser Aufbau bildet den notwendigen Kommunikationspartner für das verwendete WinCC[45] Projekt auf den beiden IPC, die als Bedienpanels für Anlagenfahrer fungierten. Der IPC PC35537 kommuniziert per Industrial Ethernet mit dem CP der SPS und lädt die entsprechenden Zustände der Variablen aus deren Datenspeicher. Zusätzlich läuft ein SQL Server als Datenbasis für das WinCC Projekt. Der zweite IPC PC35536 öffnet das Projekt inklusive aller Daten vom PC35537 und stellt es in einer lokalen Runtime dar. So können beide IPC die gleichen Zustände auf verschiedenen Bildern der Bedienoberfläche visualisieren und Zustandsänderungen an die SPS übermitteln. Diese Kommunikation ist, wie bereits in Kapitel 3.1.2 beschrieben, unverschlüsselt und kann mit einfachen Mitteln manipuliert werden. Auch die verwendeten Login-Daten für die Verbindung zu einem SQL Server sind damit leicht nachvollziehbar. Als Ergänzung wurde noch eine virtuelle Maschine mit Windows 7 für die Verwendung der Powershell Scripte eingesetzt.

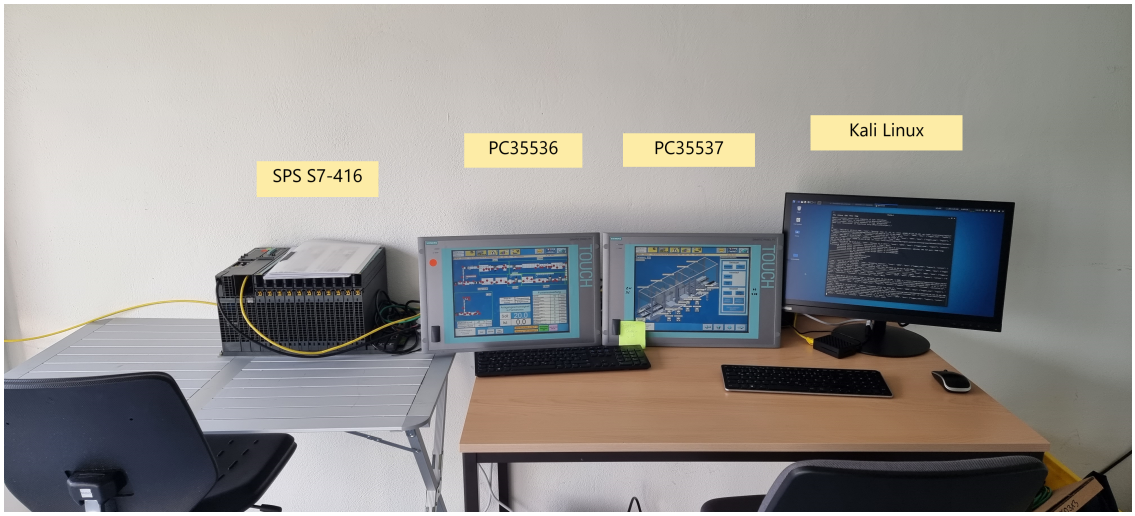

Abbildung 7.2: Testaufbau mit SPS, IPCs & Kali Linux

[43] Communication Processor
[44] Industrie-PC
[45] Windows Command and Control

7.3 Beschreibung der Testszenarien

Die Testszenarien sind an die Cyber-Kill-Chain angelehnt, die ein Konzept für Cyberangriffe in insgesamt sieben Ebenen aufteilt, die ein Angreifer für die Umsetzung seines Vorhabens sukzessive erreichen muss. Diese reichen von der Identifizierung, der Vorbereitung, den ersten Ausführungen, einem Schwachstellenscan sowie der Installation einer Backdoor. Damit kann das angegriffene System dann ferngesteuert werden und das Ziel ist erreicht. Umgekehrt ist es auf der Verteidigungsebene möglich, den gesamten Angriff des Cyberkriminellen durch Unterbrechung auf einer Stufe zu blockieren. Die von Lockheed Martin erdachte Cyber-Kill-Chain ist im Anhang A.3 zu finden. [20]

Angelehnt an diese Vorgehensweise wurde als geeignete Anforderungen zu Beginn das Aufrufen einer Internetadresse verbunden mit dem Versuch, etwas herunterzuladen, ausgewählt. Dies ahmt das Nachladen von Schadcode nach. Danach folgt ein Netzwerk-Scan, bei dem aktive Hosts als mögliche Ziele ermittelt werden. Weiter wird ein PortScan gegen aktive Hosts gestartet, der schon deutlichen Verkehr im Netzwerk erzeugt. Dabei wird auch mit Hilfe von NMAP gezielt nach den eingesetzten Versionen der offenen Dienste gesucht. Dies dient der Informationsbeschaffung und der Auswahl lohnender Ziele. Weiter geht es mit einem Angriff auf gefundene Windows Ordner-Freigaben, die Angreifern eindeutig dem Erlangen von weiteren Informationen dienen.

Mit dem GVM[46] von Greenbone wird ein Schwachstellenscanner auf das Testnetzwerk angesetzt. Hiermit soll die offene Bedrohungslage für mögliche Angriffsvektoren dargelegt werden. Denn oftmals können in der OT die eingesetzten Assets nicht aktuell gehalten werden. In den meisten Fällen verhindert der Einsatz proprietärer Software die Verwendung aktueller Systeme und bekannte Schwachstellen müssen auf anderem Wege abgesichert werden. Dies würde dem Schritt vier der Cyber-Kill-Chain entsprechen.

Zusätzlich zur Cyber-Kill-Chain soll ein lokaler ARP[47]-Spoofing Angriff einen MitM[48]-Angriff simulieren. Damit könnte ein Angreifer den Datenaustausch zwischen PC35537 und der SPS manipulieren. Dieses Szenario ist ein Angriff auf das Netzwerk, bei dem die Erkennung durch Vectra erwartet werden kann.

[46] Greenbone Vulnerability Management
[47] Address Resolution Protocol
[48] Man in the Middle

7.3.1 Verbindung ins Internet

Eine gewöhnliche Anfrage ins Internet stellt in einem Netzwerk keinen ungewöhnlichen Verkehr dar. Dies passiert in Netzwerken mit vielen IT-Assets eigentlich ständig. Allerdings sollte es auffallen, wenn ein OT-Assets plötzlich gehäuft versucht, Verbindungen ins Internet aufzubauen. Sind die angefragten Adressen auch noch auf einer Liste mit bekannten C&C-Servern, ist ein hoher IoC eine logische Folge. Moderne Firewalls blockieren solche Anfragen mit ihren aktuellen Filterlisten und Vectra würde wie in Abbildung 7.3 ersichtlich einen Threat Intelligence Match generieren.

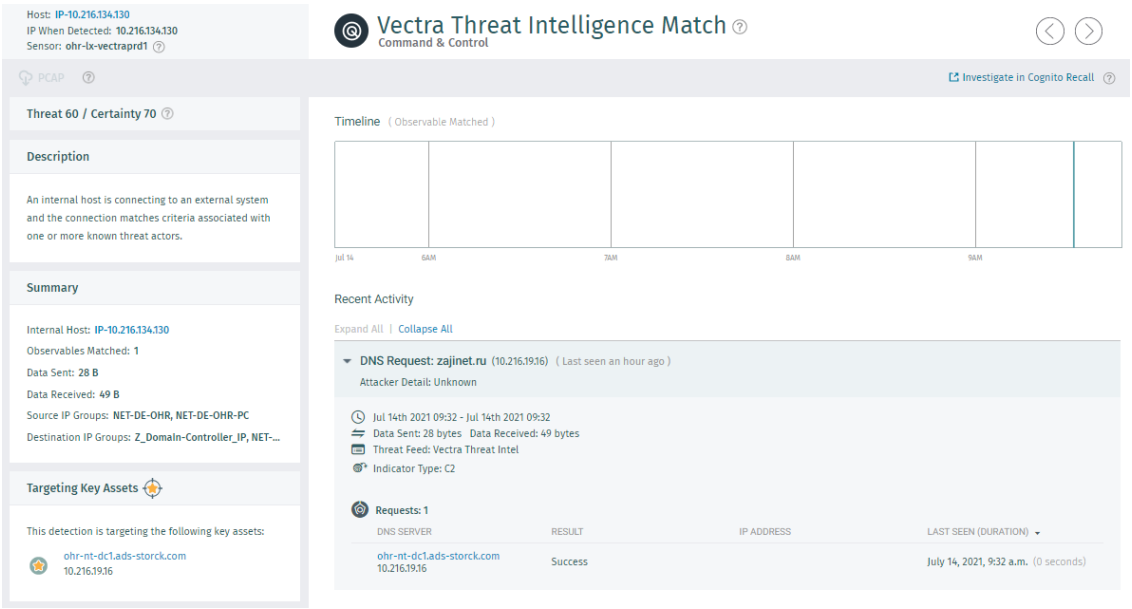

Abbildung 7.3: Vectra AI - Erkennung von verdächtigen Domains

Deshalb haben Angreifer einen Domain Generation Algorithmus (DGA) für gewöhnliche DNS[49]-Anfragen in ihre Malware integriert, um diese einfache Blockade zu umgehen und auch bei Ausfall einzelner Server die Verbindung zwischen einem infizierten Host und der eigenen Infrastruktur nicht zu verlieren. Mit dem Einsatz von per DGA generierten Domains lassen sich die ausgefallenen Server ziemlich leicht ersetzen. Beide Seiten erzeugen mit identischen Parametern neue, bisher unbekannte Domains, deren Aufrufen bei einfach gesicherten Netzwerken keinen Verdacht erzeugen soll.

[49] Domain Name Service

Die Erkennung von per DGA generierten Domains funktioniert ähnlich eines Wörterbuches. Die NBAD untersucht mit Unterstützung von KI, wie sich die Buchstabenkombinationen der Hostnamen zusammen setzen. Sollte es eine ungewöhnliche Konstellation geben, also eine stark zufällige Folge von Buchstaben, die einer natürlichen Formulierung durch einen Menschen widerspricht, wird das von der NBAD erkannt und daraus eine Detection generiert. Mit dieser Zufälligkeit wird die Shannon-Entropie berechnet. [27]

Als Beispiel dient hier der sehr interessante Artikel von Johannes Bader, der in einem Blogeintrag den DGA in der Malware „BazarLoader“ untersucht hat. Beispiele für per DGA generierte Domains siehe Listing 7.1. [1]

```
1 ecfgjkehhgjm.bazar
2 afhhjkakjhjm.bazar
3 beggklbjigkn.bazar
4 cfhhjkckjhjm.bazar
5 bdehklbighkn.bazar
6 dcegjldhggjn.bazar
```

Listing 7.1: Beispiele für per DGA generierte Domains

Auswertung - Verbindung ins Internet

Ein Versuch, eine schädliche Domain zu erreichen und dort Schadsoftware herunterzuladen, wird von Vectra AI erkannt und zusätzlich über die bei der August Storck KG bereits vorhandenen Sicherheitsvorkehrungen blockiert. Die Anfrage dazu wird zwar vom DNS-Server verarbeitet, die gelieferte Antwort führt aber anhand der Sicherheitsmaßnahmen zu einem Sinkhole-Server. Die eingesetzten NGFW's[50] verhindern die Verbindung, da sie eine klare Trennung zwischen der IT und OT realisieren und keine Verbindung von Assets aus der OT ins Internet zulassen. Zusätzlich filtern sie den Netzwerkverkehr mit einer ständig erweiterten URL-Blacklist.

[50] Next Generation Firewall

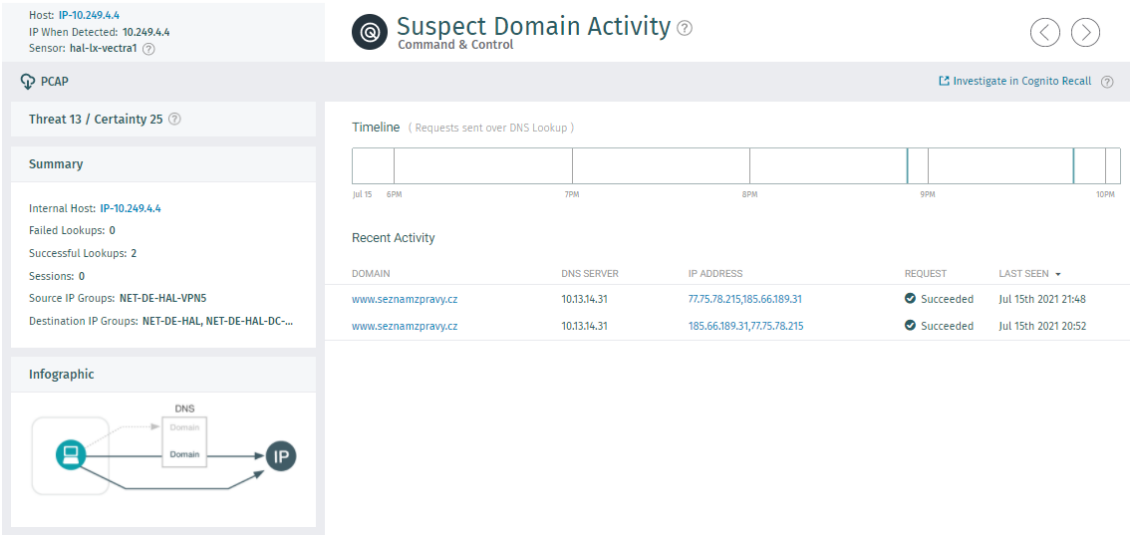

Abbildung 7.4: Vectra AI - Suspect Domain Activity

Wie in Abbildung 7.4 zu sehen, wurde die Anfrage von Vectra AI als Suspect Domain Activity erkannt, in die Phase C&C eingeordnet und mit einer Bedrohung (Threat) von 12 und einer Gewissheit (Certainty) von 25 bewertet. Dies ist gut nachvollziehbar, da es sich ja auch, wie in diesem Fall, um eine reguläre Domain aus Tschechien handeln kann. Ohne weitere Detections bliebe der Aufruf somit ohne Konsequenzen. Der Aufruf für die Detection wurde im Office-Netz durchgeführt, da es dafür im Produktionsnetz keine Freigabe gab. Da alle Sensoren von der gleichen, zentralen Appliance verwaltet werden, würde der Aufruf im Produktionsnetz mit der gleichen Detection erkannt werden.

7.3.2 Netzwerk Scan

Ein Netzwerk Scan beschreibt die aktive Suche nach vorhandenen Hosts. Damit kann sich ein Angreifer einen grundsätzlichen Überblick über die Struktur der Hosts im angebundenen Netzwerk verschaffen. Dabei werden verständlicherweise nur aktive Hosts erkannt, weshalb dieser Scan regelmäßig wiederholt werden muss. Der Netzwerk Scan gehört zur Recon-Phase, also der Informationsbeschaffung.

Auswertung - Netzwerk Scan

Wie in Abbildung 7.5 gut zu sehen wurde dieser Scan erfolgreich erkannt. Vectra hat dies mit einer Bedrohung (Threat) von 37 und Gewissheit (Certainty) von 32 bewertet. Damit gehört es noch zum Bereich Medium und zu den ungefährlicheren Szenarien. Da dieser Scan auch nach nicht aktiven IP-Adressen gesucht hat, wird er auch als Darknet-Scan bezeichnet und von Vectra als solcher erkannt.

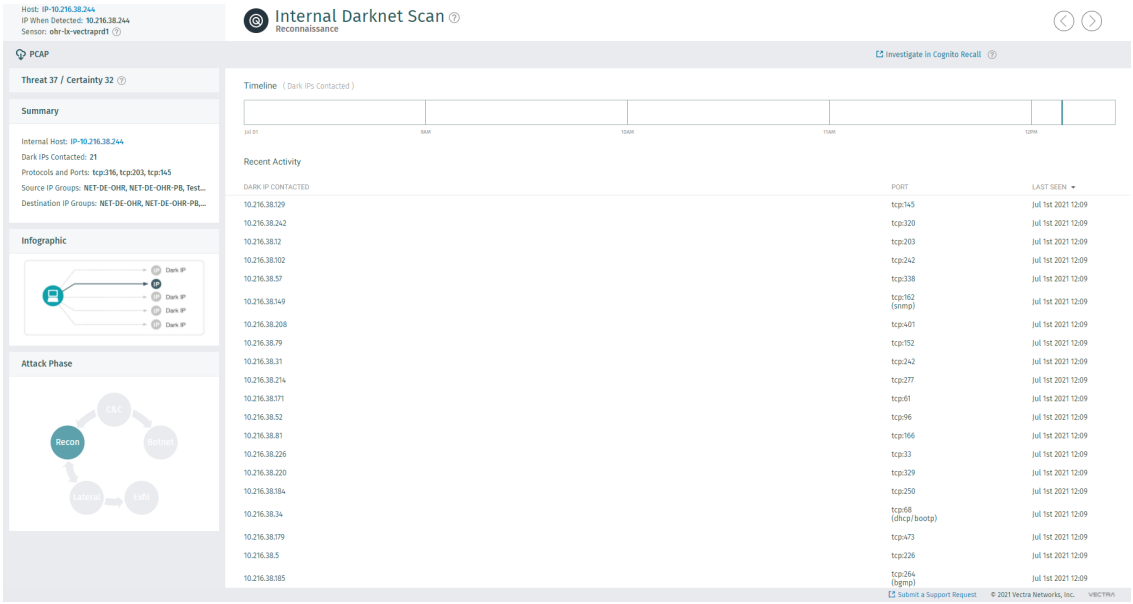

Abbildung 7.5: Vectra AI - Darknet Scan

7.3.3 Portscan

Ein Portscan ist in einem Netzwerk normalerweise nicht ungewöhnlich. Damit wird durch Administratoren schnell eine Übersicht über die offenen Diensten von einzelnen Clients erstellt. Dies ist, wie in Listing 7.2 zu sehen, mit drei Zeilen Powershell möglich und kann beliebig um die gewünschten Ports ergänzt werden. Gleichzeitig ist das Ergebnis eines Portscans aber auch eine gute Informationsquelle für mögliche Angreifer. Denn immer wieder werden regulär genutzte Dienste durch vorhandene Schwachstellen zum Einfallstor für Schadsoftware. Dabei sind etliche Dienste so gesprächig, dass man auch Informationen zu den eingesetzten Versionen geliefert bekommt - siehe Abbildung 7.6. Das umfasst die eingesetzte Version des Betriebssystems, einem FTP[51]-, SQL-Server oder einem per RDP[52] erreichbaren Server.

[51] File Transfer Protocol
[52] Remote Desktop Protocol

```
$ports = "21 22 23 25 53 80 88 111 139 389 443 445 873 901 902 903
    904 1099 1433 1521 1723 2049 2100 2121 3299 3306 3389 3632 4369
    5038 5060 5432 5900 5985 6379 6667 8000 8080 8443 9200 27017"
$ip = "10.216.38.201"
$ports.split(" ") | % {echo ((new-object Net.Sockets.TcpClient).
    Connect($ip,$_)) "Port $_ is open on $ip"} 2>$null
```

Listing 7.2: Portscan des PC35537 [23]

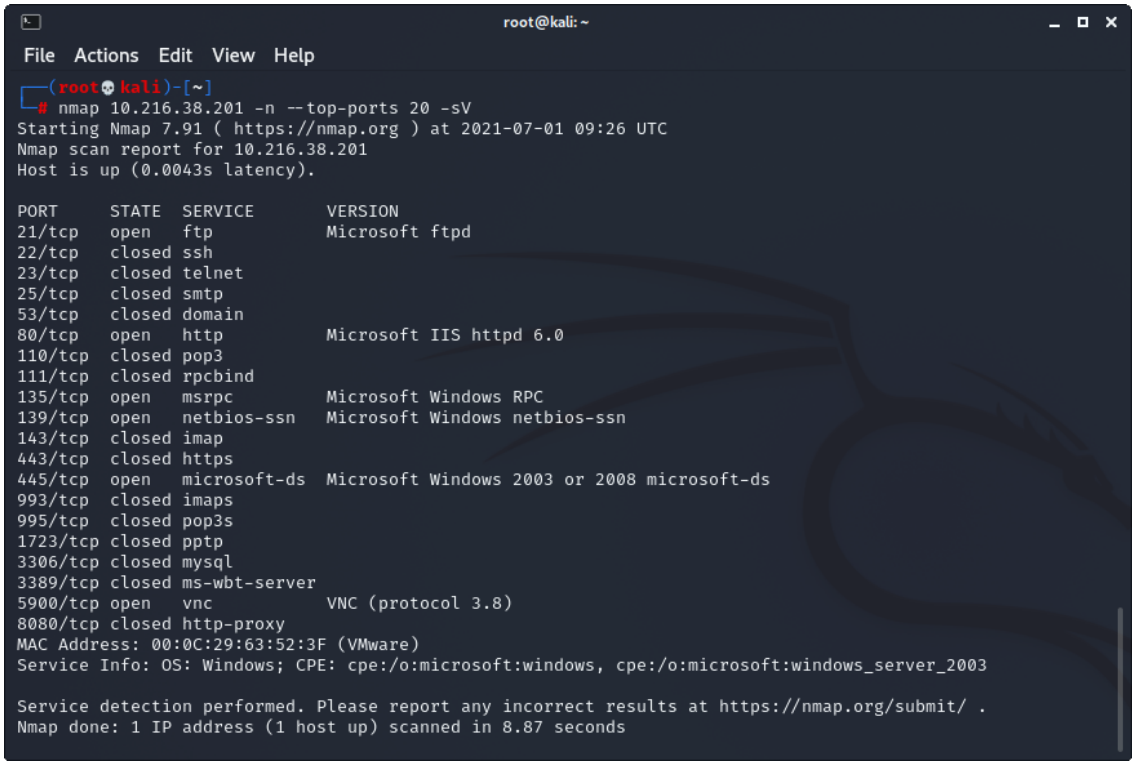

Abbildung 7.6: Kali Linux - nmap mit Versionsermittlung

Wie in Abbildung 7.6 zu sehen, gibt **nmap** detaillierte Ergebnisse zu den erreichbaren Diensten zurück, die entsprechend interpretiert werden müssen. Es ist leicht erkennbar, ob der Port auf dem Host gesperrt ist, eine Firewall den Netzwerkverkehr filtert oder ob der Port offen ist - das potenziell gefährlichste Ergebnis. Der TCP-SYN-Scan als Standardeinstellung ist relativ unauffällig, da er TCP-Verbindungen nicht abschließt. Er erlaubt eine klare, zuverlässige Unterscheidung zwischen den Zuständen offen, geschlossen und gefiltert. Sollte es keine klaren Ergebnisse geben, können andere Techniken wie beispielsweise segmentierte Paket eingesetzt werden.

offen

Ein Programm ist bereit, TCP- oder UDP-Verbindungen auf diesem Port anzunehmen. Dies bietet eine mögliche Angriffsfläche eines verwundbaren Dienstes.

geschlossen

Ein geschlossener Port ist erreichbar und beantwortet die Anfragen des Scanners. Allerdings gibt es kein aktuelles Programm, das ihn abhört. Man kann mit Ports in diesem Status das eingesetzte Betriebssystem ermitteln. Deshalb sollten Administratoren solche Ports mit einer Firewall filtern.

gefiltert

Man kann mit diesem Ergebnis nicht feststellen, ob der Port bei einem spezifischen Host offen ist. Wahrscheinlich wurde eine Paketfilterung eingerichtet, die verhindert, dass Testpakete den Port am Host erreichen. Das entspricht bei modernen Firewalls der Option **DROP**, bei der keine Benachrichtigung an den Absender übermittelt wird und das Paket von der Firewall verworfen wird.

NMAP kann mit viele Optionen an die entsprechenden Verhältnisse angepasst werden. Weitere Informationen zu den zu setzenden Flags auf der Homepage von NMAP `https://nmap.org/man/de/`. [39] & [40]

Auswertung - Portscan

Wie in Abbildung 7.7 gut zu sehen, wurden die Portscans gegen die ermittelten Windows Hosts erfolgreich detektiert. Vectra hat dies mit einer Bedrohung (Threat) von 60 und einer Gewissheit (Certainty) von 80 bewertet. Die Detection wurde der Phase **Recon**, also der Aufklärung zugeordnet. Das ist absolut nachvollziehbar, da in dieser Phase weitere Informationen zum Netzwerk ermittelt wurden.

Die hohe Bewertung lässt sich damit erklären, das ein möglicher Angreifer mit einem Portscan wichtige Informationen zu erreichbaren Teilnehmern und deren offenen Diensten ermitteln könnte. Sollte es in der CVE[53]-Datenbank eine passende Schwachstelle zu eingesetzten Applikationen geben, ist die Gefahr ziemlich groß, dass diese auch ausgenutzt wird. Meist ist dabei das Ziel, den jeweiligen Dienst zu übernehmen und damit höhere Rechte zu erlangen.

[53] Common Vulnerabilities and Exposures

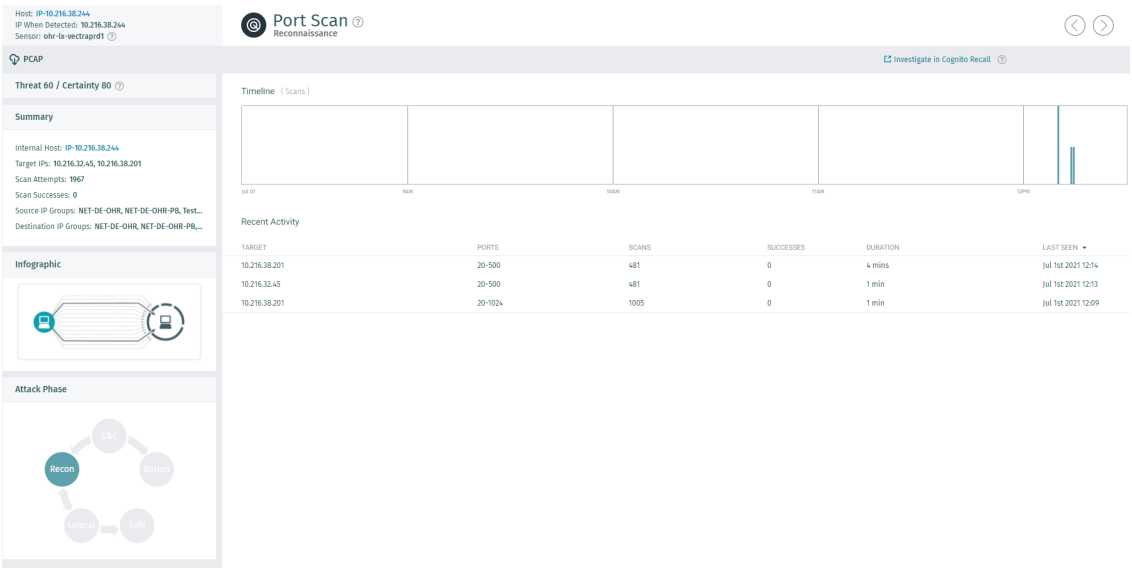

Abbildung 7.7: Vectra AI - Detection des Port Scan

7.3.4 Port Sweeping

Dieses Szenario beschreibt den Einsatz eines Port Sweepings, bei dem viele Hosts, auch über Subnetzgrenzen hinweg, nach einzelnen, bestimmten Diensten abgesucht werden. Wie im Listing 7.3 zu sehen, ist der Scan nach SMB-Freigaben per PowerShell mit einem Dreizeiler zu lösen.

Dabei wird gezielt nach dem Port **445** über das Subnetz **10.216.38.0** gescannt. Denn auch in der OT mit einem hohen Automatisierungsgrad aufgrund der vielen Steuerungskomponenten sind die eingesetzten Windows Assets meistens das größte Einfallstor.

```
1 $port = 445
2 $net = "10.216.38."
3 0..255 | foreach { echo ((new-object Net.Sockets.TcpClient).Connect
    ($net+$_,$port)) "Port $port is open on $net$_"} 2>$null
```

Listing 7.3: PowerShell - PortSweep des Subnetzes 10.216.38.0 [23]

Auswertung - Port Sweep

Wie in Abbildung 7.8 zu erkennen hat Vectra bereits im Netzwerk des Produktionsgebäudes C ein Port Sweeping erkannt. Dabei konnte anhand der verwendeten IP-Adressen leicht nachgewiesen werden, dass es sich hier um geplante Arbeiten von beauftragten Programmierern gehandelt hat. Diese haben mit der Projektierungssoftware TIA[54]-Portal von Siemens im Netzwerk nach der richtigen Steuerung gesucht. Dies ist ein bekanntes Verhalten des TIA-Portals und damit nicht ungewöhnlich oder unerwartet.

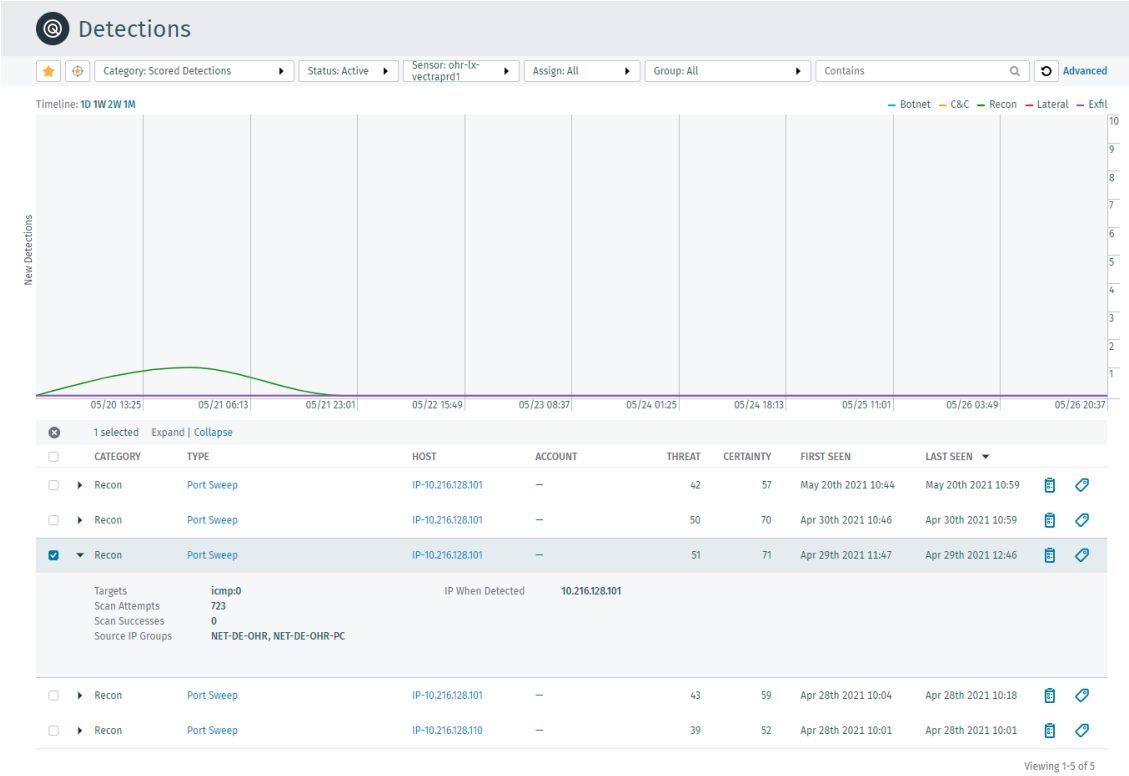

Abbildung 7.8: Vectra AI - Detection Port Sweep

[54] Totally Integrated Automation

7.3.5 Samba Shares attackieren

Server Message Block (SMB) wurde ursprünglich über NetBIOS unter Verwendung von Port 139 realisiert. Die Verwendung von Port 445 deutet auf die aktuellere Version von SMB hin, die ab Windows 2000 Verwendung findet. Damit wurden Windows Freigaben auch über das Internet erreichbar. Die Idee von Microsoft, Dateien per Freigabe leichter auszutauschen, hat sich mittlerweile als Sicherheitsrisiko herausgestellt.

Mit **smbmap** unter Kali Linux können SMB-Freigaben in einem Netzwerk schnell ermittelt werden. Dabei lassen sich Freigabelaufwerke, Laufwerksberechtigungen und Freigabeinhalte auflisten. SMBmap kann die Suche nach potenziell sensiblen Daten in großen Netzwerken vereinfachen und es können mit passenden Parameter Dateien übertragen oder sogar Remotebefehle ausgeführt werden. Im Listing 7.4 wurde der Parameter **-H** für die IP-Adresse des PC 35537 und **-L** für die Auflistung der Freigaben mit entsprechenden Berechtigungen verwendet. [46]

```
1 sudo smbmap -H 10.216.38.201 -L
```

Listing 7.4: smbmap - Gast-Zugriff auf PC35537

Mit den ermittelten Informationen kann im weiteren Verlauf unter Verwendung von **hydra** ein Brute-Force Angriff gestartet werden, der dann ziemlich auffällig ist. Hydra wurde dazu mit dem bekannten Benutzer **Bediener** und einem Wörterbuch als Parameter gestartet.

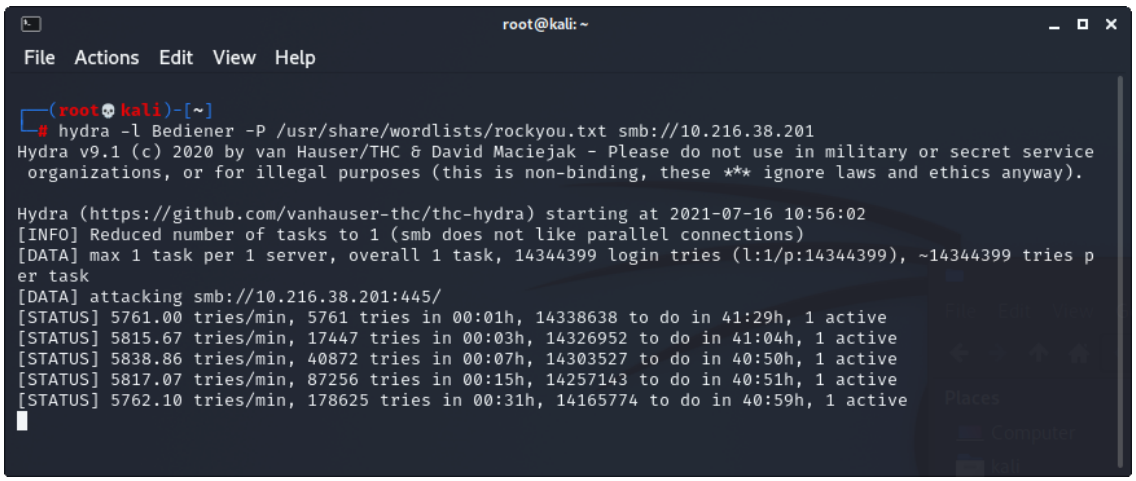

Abbildung 7.9: Vectra AI - Brute-Force Angriff auf SMB mit hydra

Für Angreifer stellen Ordnerfreigaben ein lohnendes Ziel dar, da sie über die abgelegten Dateien leicht an weitere Informationen zum Unternehmen gelangen. So erfahren sie immer mehr über ihr Opfer und dringen dadurch immer tiefer in die Systeme ein.

Wie im Listing 7.5 zu sehen, war es nach dem Ermitteln von relevanten User Credentials leicht, an sensible Informationen einer kompletten Gießanlage zu kommen. Diese lagen im gleichen Ordner wir das WinCC Projekt, dass für den zweiten IPC per SMB-Share zur Verfügung gestellt wird.

```
sudo smbmap -H 10.216.38.201 -s Projekt -u Bediener -p be5000 --
    download Storck_EA23_WinCC_Projektmappe.xls
```

Listing 7.5: smbmap - Download von Projektinformationen

Auswertung - Samba Shares attackieren

Mit der Detection **File Share Enumeration** aus Abbildung 7.10 hat Vectra erkannt, dass ein Host ungewöhnlich oft auf Dateifreigaben zugegriffen hat. Dies ist so, gerade in dieser Häufigkeit, bisher nicht vorgekommen. Dabei ist die Bedrohungsbewertung proportional zur Anzahl der Freigaben.

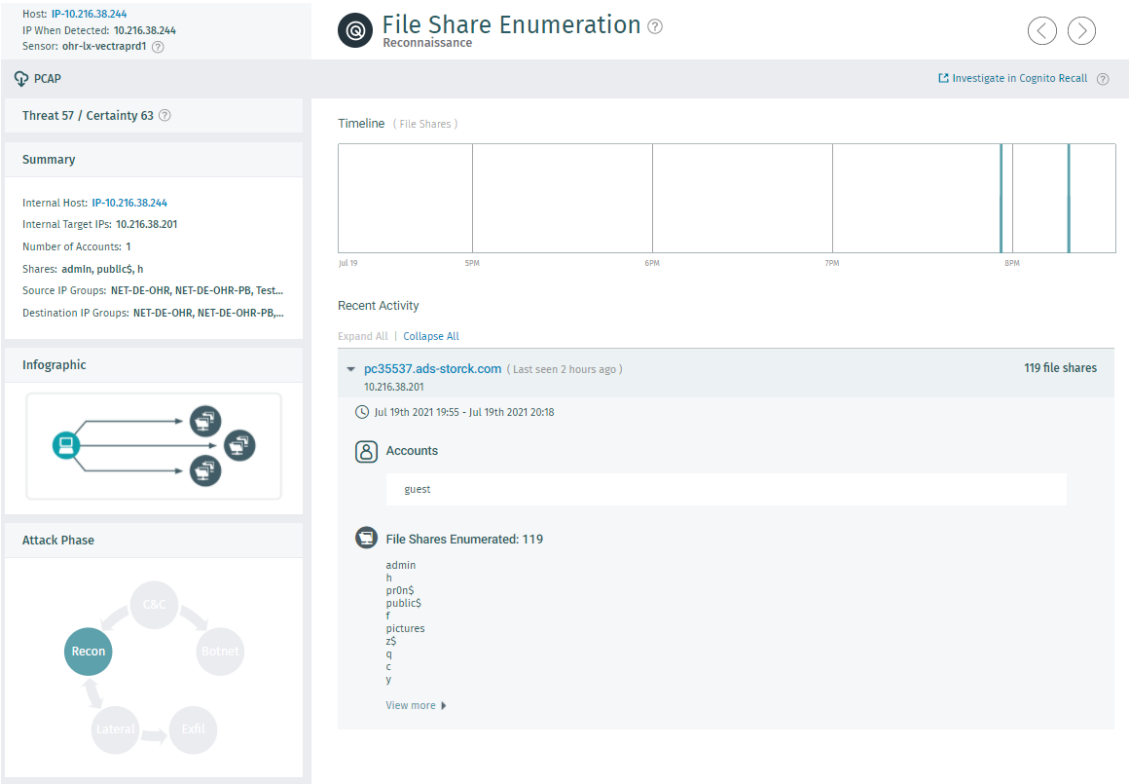

Abbildung 7.10: Vectra AI - Aufzählung der Dateifreigaben

In Abbildung 7.11 ist ersichtlich, das Vectra den Brute-Force Angriff per SMB unter Verwendung von hydra als SMB-Brute Force detektiert hat. Dabei hat Vectra erkannt, dass ein Host viele Anmeldeversuche mit demselben Konten durchgeführt hat. Der Brute-Force Angriff wurde erkannt, da viele dieser Authentifizierungen fehl geschlagen sind. Die Bedrohungsbewertung (Threat) wurde mit 70 festgelegt und wurde durch die Anzahl der Anmeldeversuche bestimmt. Die Sicherheitsbewertung (Certainty) wurde mit 95 bestimmt und wird durch die Gesamtzahl der Anmeldeversuche beeinflusst.

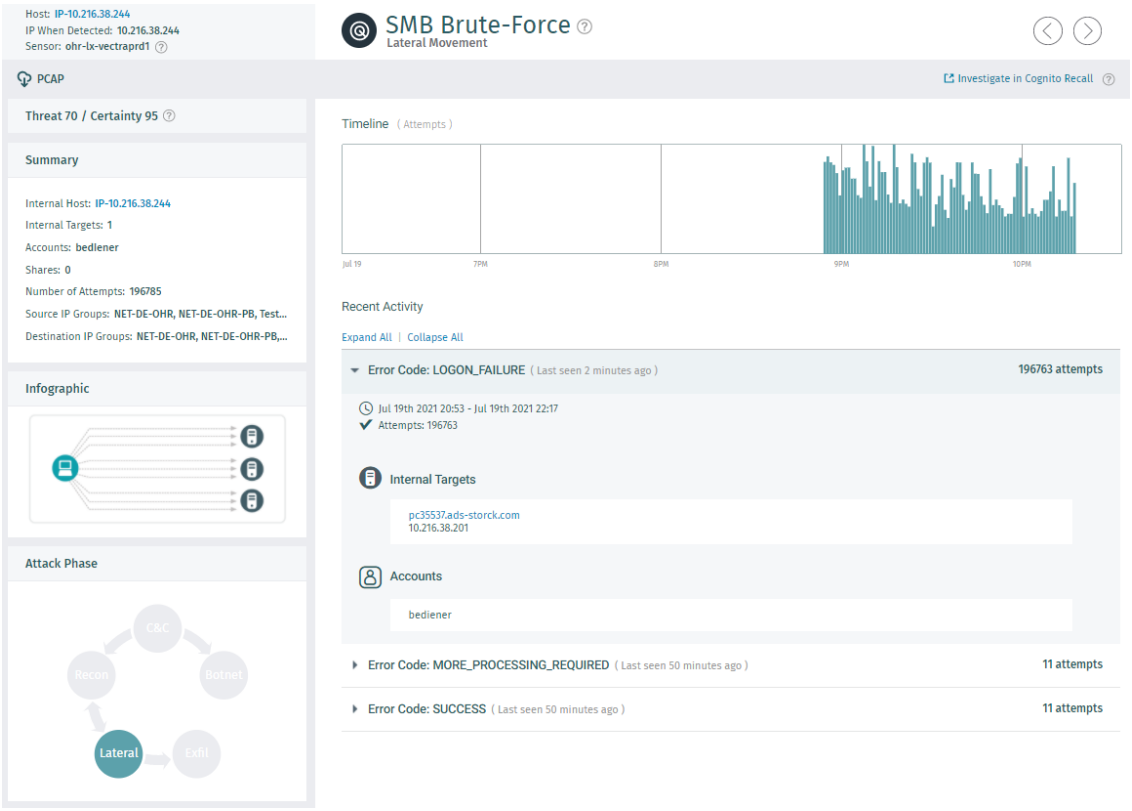

Abbildung 7.11: Vectra AI - Erkennung des SMB Brute-Force-Angriffs mit hydra

Die Brute-Force Attacke wurde mit einer Bedrohung (Threat) von 70 und einer Gewissheit (Certainty) von 95 besonders hoch bewertet. Dabei wird die Bedrohung durch die Anzahl der Anmeldeversuche und die Sicherheitsbewertung durch die Gesamtzahl der Anmeldungen bestimmt. Zusätzlich liefert Vectra tiefe Details über den Angriffe auf die SMB-Freigaben. Es sind deutlich die IP des Angreifers, das Ziel sowie der verwendeten User-Login erkennbar. So lassen sich gut Rückschlüsse auf einen vermeintlichen vorherigen Angriff für das Ermitteln des Benutzernamens ziehen. Bei solchen Fakten sollte unmittelbar das Kennwort des betroffenen Accounts geändert werden.

7.3.6 ARP Spoofing

In jedem LAN[55] dient das Address Resolution Protocol (ARP) dem Auflösen bekannter IP-[56] zu notwendigen MAC[57]-Adressen. Dies ist nach dem OSI-Modell notwendig, um die Kommunikation mit der benachbarten Schicht zu ermöglichen.

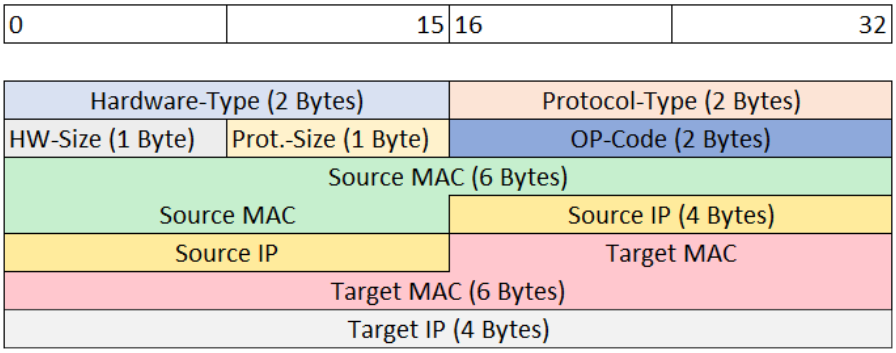

Abbildung 7.12: Struktur eines ARP Paketes

Dazu sendet der anfragende Client, falls nach der Kontrolle seines eigenen ARP-Caches die IP-Adresse nicht aufgelöst werden kann, einen ARP-Request per Broadcast an alle erreichbaren Teilnehmer. In Abbildung 7.12 wird dazu zum besseren Verständnis die Struktur eines ARP-Paketes dargestellt. Der Teilnehmer, der die angefragte IP-Adresse als seine eigene erkennt, antwortet mit einem ARP-Reply und der eigenen MAC-Adresse im TARGET-Bereich des ARP-Paketes. Er ändert dazu den OP-Code von 1 auf 2, was dann der Antwort entspricht. Danach trägt der anfragende Client diese Kombination aus MAC- und IP-Adresse im eigenen ARP-Cache ein und führt diesen bis zur Aktualisierung weiter fort.

Genau hier setzt das ARP-Spoofing an. Dabei leitet der Angreifer, wie in Abbildung 7.13 schematisch dargestellt, den regulären Verkehr (gelbe Verbindung) zwischen WinCC Server und der SPS auf sich selbst um (rote Verbindungen) und kann damit alle Pakete mitlesen und auch manipulieren.

In der OT sind aufgrund von proprietärer Software häufig neben aktuellen Assets auch ältere Betriebssysteme im Einsatz. Bei diesen ist es nicht ungewöhnlich, dass diese nicht prüfen, ob ein ARP-Reply tatsächlich auf einen kürzlich versendeten ARP-Request selbst zurückzuführen ist. Deshalb übernehmen sie, falls keine statischen ARP-Einträge konfiguriert sind, die neuen Informationen in den eigenen ARP-Cache ohne weitere Prüfung. Diese ungefragten Pakete stellen oftmals den Anfang eines MitM-Angriffes dar und sollten demzufolge einen hohen IoC generieren. [37]

[55] Local Area Network
[56] Internet Protocol
[57] Media Access Control

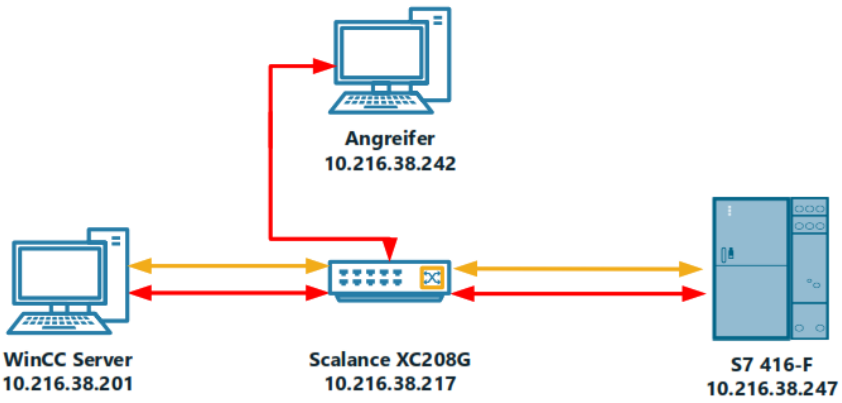

Abbildung 7.13: ARP-Spoofing in schematischer Darstellung

Der Angriff erfolgt gegen beide Hosts, deren ARP-Cache durch gefälschte ARP-Replys manipuliert werden muss. Das ist unter Kali-Linux mit zwei Konsolen und jeweils einer Befehlszeile mit root-Rechten zu realisieren. Angegeben werden muss lediglich die IP des Ziels sowie die Adresse des Gateways oder des anderen Ziels.

```
#Konsole 1
arpspoof -i eth0 -t 10.216.38.201 10.216.38.247
#Konsole 2
arpspoof -i eth0 -t 10.216.38.247 10.216.38.201
```

Listing 7.6: arpspoof mit Parametern für SPS und PC35537

Auswertung - ARP Spoofing

Wie in Abbildung 7.14 ersichtlich ist, war der ARP-Spoofing Angriff für die Verbindung zwischen WinCC Server und SPS erfolgreich. Dies lässt sich leicht daran erkennen, dass sich die MAC-Adresse für die SPS (**08-00-06-94-a9-4c**) mit der IP **10.216.38.247** vom ersten Aufruf mit **arp -a** gegenüber dem zweiten Aufruf während des laufenden Angriffes auf die MAC-Adresse des RaspberryPi (Angreifer (**e4-5f-01-0b-da-ec**)) verändert hat. Damit werden alle weiteren Pakete, die für die SPS bestimmt sind, an den Angreifer gesendet. Nach dem Ende des ARP-Spoofing erfolgt automatisch ein Re-ARP-Spoofing mit der Wiederherstellung des vorhergehenden Zustandes. Diesen Zustand zeigt der dritte Aufruf des ARP-Cache.

Vectra hat diesen vermeintlich einfachen Angriff nicht erkannt. Dies ist anders als erwartet und laut Hersteller mit einem nicht vorhandenen Detection Modell zu erklären. Es ist also gar nicht als Angriffsvektor definiert. Die Analyse des Verkehrs geht nach eigenen Angaben nicht in diese Tiefe, sondern sucht mehr nach den Auffälligkeiten, die aus einer erfolgreichen Infektion heraus entstehen und mit anderen Aktionen in Verbindung gebracht werden können. Somit ist das ARP-Spoofing als atomarer Angriff zu

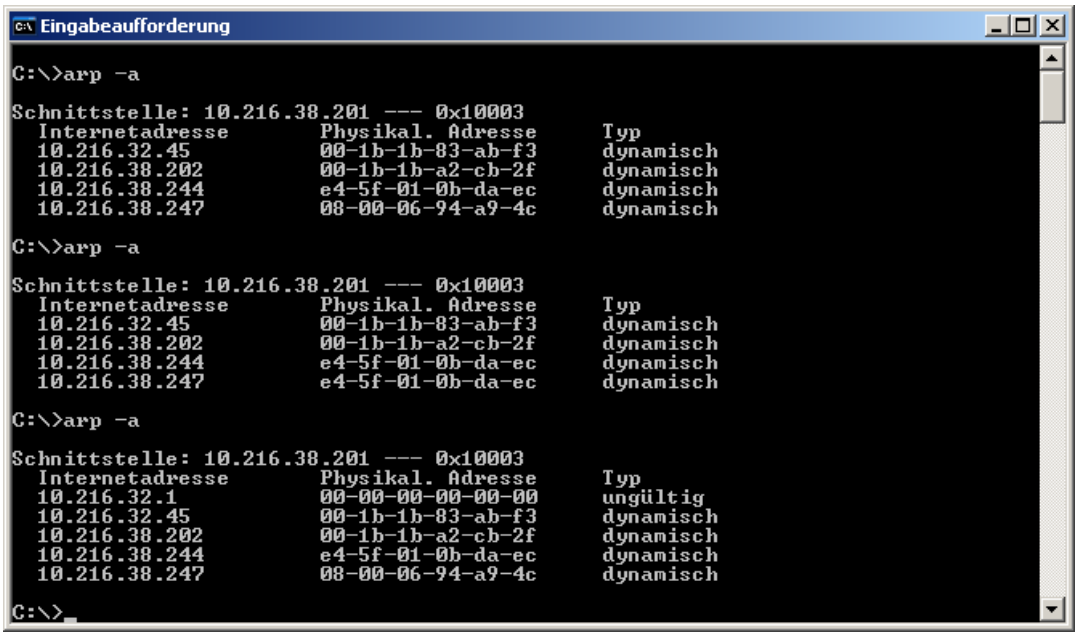

Abbildung 7.14: PC35537 - Resultat eines erfolgreichen ARP-Spoofing Angriffes

klassifizieren.

Mit dieser Erkenntnis würde eine Manipulation der Verbindung zwischen IPC und SPS durch eine Anomalieerkennung nicht entdeckt. Vectra sowie ein vorhandenes Monitoring System würden den neuen Host allerdings erkennen und das Asset Management im Monitoring würde eine Meldung generieren. Das sind allerdings Details, nach denen man gezielt suchen muss, da für die neue Anmeldung eines Hosts normalerweise keine Detection ausgelöst wird.

7.3.7 Alternativer Datenstrom auf NTFS Laufwerken

Das Windows Standart Dateisystem NTFS[58] ermöglicht sogenannte Alternative Datenströme, kurz ADS[59]. Damit ist es möglich, zusätzliche Daten an eine beliebige Datei anzuhängen. Das sind gewöhnlicherweise Vorschaubilder, sogenannte Thumbnails, die dem Nutzer vorab eine bessere Übersicht geben sollen oder das Ordnersysmbol im Explorer ersetzen. Da es eine Funktion der neueren Versionen von Windows ist, funktioniert es nur, solange sich die Dateien auf NTFS formatierten Laufwerken befindet.

Diese Eigenschaft von NTFS ist nicht allseits bekannt und wird durch vorhandene Virenscanner eventuell übersehen. Diese Eigenschaft von NTFS kann ausgenutzt werden, um schädlichen Code an die Datei anzuhängen, der beim Aufrufen zusätzlich zum

[58] New Technology File System
[59] Alternate Data Streams

Öffnen des Bildes ausgeführt wird.

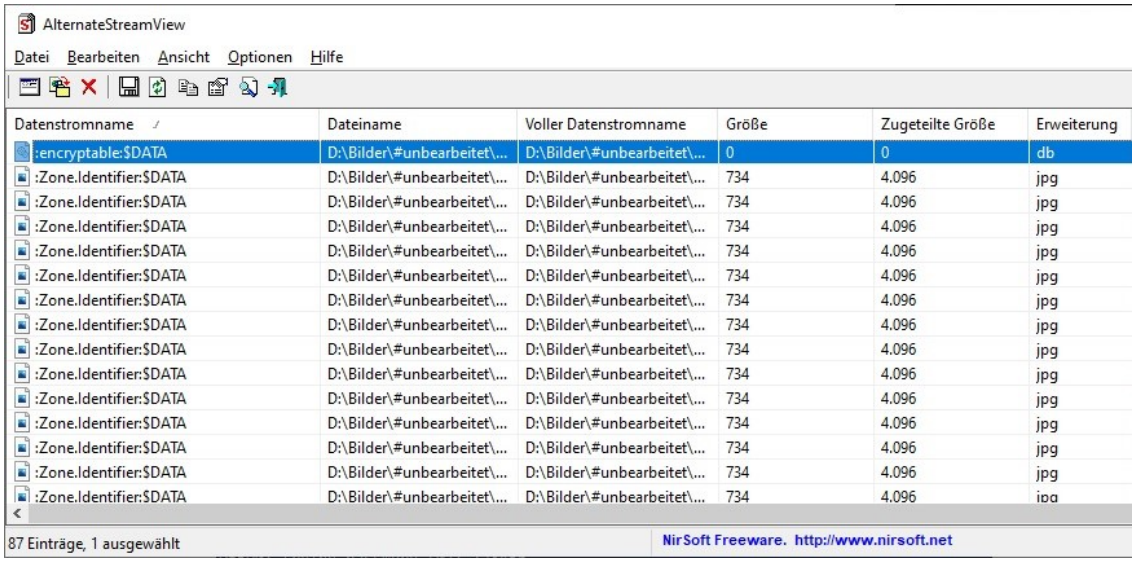

Abbildung 7.15: Darstellung von alternativen Datenströmen per AlternateStreamView

Auswertung - Alternativer Datenstrom auf NTFS Laufwerken

Da diese Form des Angriffes rein auf Dateiebene realisiert wird, ist es für ein NBAD technisch nicht möglich, diese Form zu erkennen. Vectra analysiert, wie im Kapitel 6 beschrieben, nur die Metadaten der einzelnen Netzwerkpakete und kann somit keine modifizierten Dateien im Payload erkennen. Anders ausgedrückt bietet Vectra eine reine Betrachtung, Wer wann mit Wem wie kommuniziert hat. Dafür schlägt in einem solche Fall eine gute EndPoint Protection an. Diese kann per API[60], wie in Abbildung 6.4 im Menüpunkt EDR, in das vorhandene Vectra System eingebunden werden, sodass mehr Daten korreliert werden können und damit eine bessere Erkennungsleistung erzielt werden kann.

7.3.8 Schwachstellenanalyse

Ein erfolgreicher Angreifer, der sich einmal Zugang zu einem Netzwerk verschafft hat, versucht im weiteren Verlauf oft an mehr Informationen zu gelangen. Dieses Verhalten wurde bereits im Kapitel 5.3 beschrieben und meint das „Lateral Movement“. Eine mögliche Methode ist dabei die gezielte Suche nach Schwachstellen. Das Ziel ist dann die Rechteausweitung mit der Erlangung weiterer User Credentials. Die Schwachstellenanalyse entspricht in der Cyber-Kill-Chain dem Schritt vier.

[60] Application Programming Interface

Solche mittlerweile automatisierten Scanner integrieren komplette CVE-Datenbanken mit weit über 150.000 Einträgen, um die Assets nach Schwachstellen zu untersuchen. Diese Datenbanken lassen sich gezielt nach Anwendungen durchsuchen und die gefundenen Schwachstellen lassen sich dann anhand der ausführlichen Anleitungen mit Codebeispielen, verfügbar auf beispielsweise `https://www.exploit-db.com`, leicht nachvollziehen und gezielt ausnutzen.

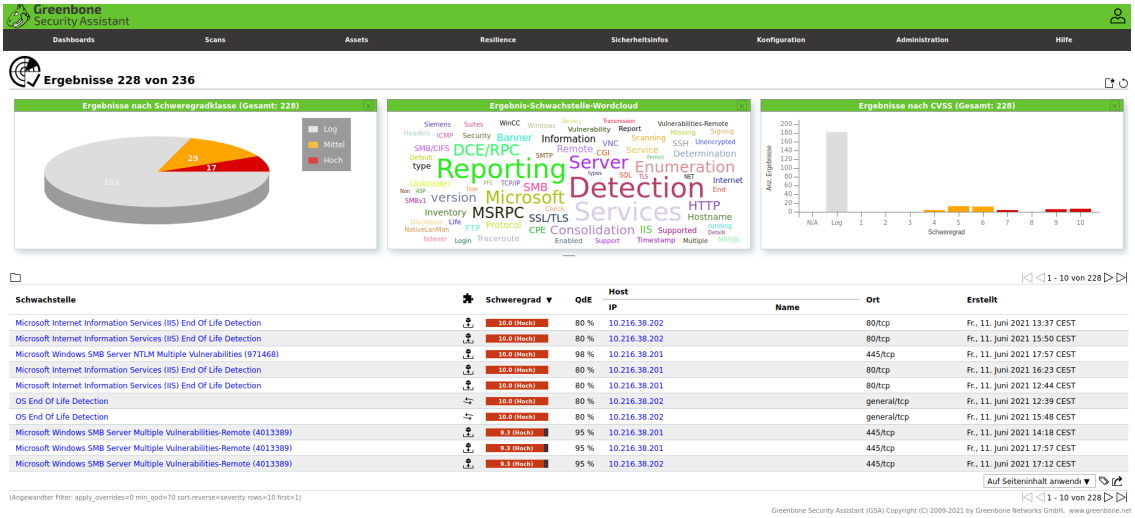

Abbildung 7.16: GVM - Scan des Testnetzwerkes auf bekannte Schwachstellen

Wie in Abbildung 7.16 zu sehen, wurde im Testnetzwerk das GVM von Greenbone zur Schwachstellensuche eingesetzt. Es ist gut zu erkennen, dass die bis vor kurzem in der Produktion eingesetzten Komponenten kritische Sicherheitslücken aufweisen. Die erkannten Sicherheitslücken ließen sich zum Teil mit einem Patch vom Hersteller beheben. Dies ist, wie bereits in 7.3 beschrieben, in der OT nicht ohne weiteres möglich. Alternativ sollte zwingend geprüft werden, ob der verwundbare Dienst, wie beispielsweise der eingesetzte IIS[61] wirklich benötigt wird oder zur Optimierung der IT-Sicherheit deaktiviert werden kann.

[61] Internet Information Server

Auswertung - Scan nach Schwachstellen

Die Schwachstellenanalyse im Netzwerk ist, falls es keine geplante Aufgabe der firmeninternen IT-Abteilung war, ein deutliches Zeichen eines Angriffes, da es sonst keine logische Erklärung für diese Netzwerkaktivität gibt.

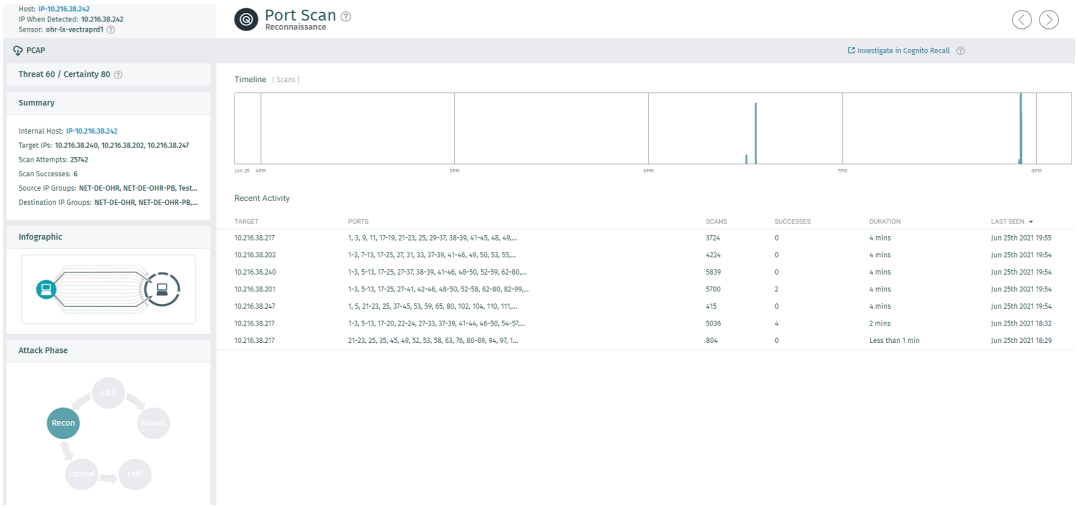

Abbildung 7.17: Vectra AI - Erkennung eines Schwachstellenscans

Wie in den Abbildungen 7.17 und 7.18 zu sehen, wurde der Schwachstellenscan über mehrere MITRE ATT&CK® Muster erkannt und mit einer Bedrohung (Threat) von 60/68 und Gewissheit (Certainty) von 80/83 bewertet. Dabei ist die SQL-Injection das deutlichste Indiz für eine Anomalie.

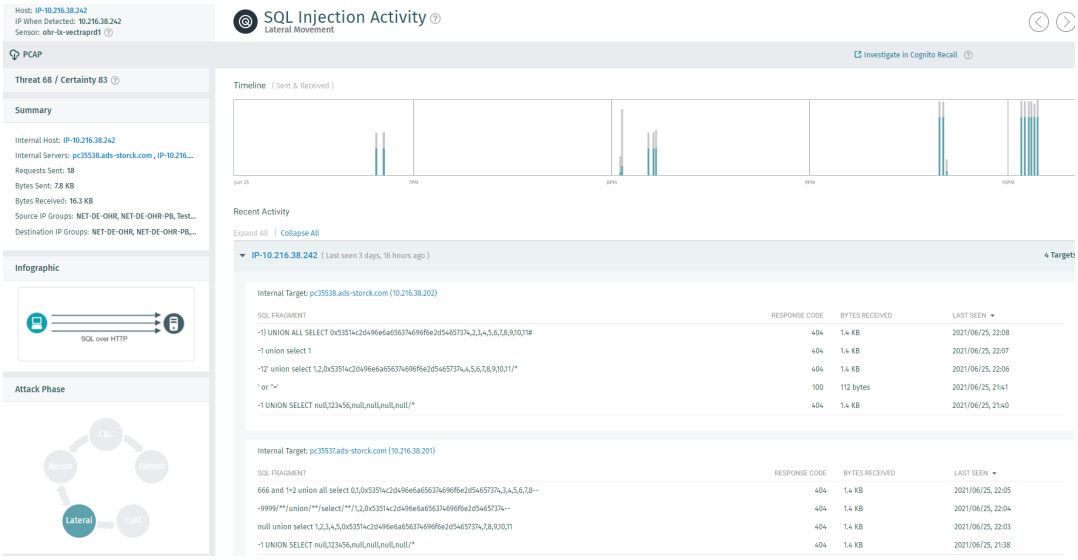

Abbildung 7.18: Vectra AI - Erkennung eines Schwachstellenscans

Gerade bei Abbildung 7.18 ist gut ersichtlich, wie ein Schwachstellenscanner intern vorgeht. In dem ersten Teil der Informationsbeschaffung wurde der Portscan durchgeführt, bei dem ein aktiver HTTP und ein SQL Server ermittelt wurden. Nun versucht GVM mit bekannten Schwachstellen aus weit verbreiteten CMS[62] wie joomla oder Wordpress eine SQL-Injection. Dabei soll über bekannte URLs schädlicher SQL Code an das vermutete CMS übergeben werden. Ist dies erfolgreich, ist der Server angreifbar. Diese Vorgehensweise erzeugt allerdings auffälligen Netzwerkverkehr.

[62] Content Management System

8 Fazit & Ausblick

8.1 Testbetrieb im Produktionsgebäude C

Der Sensor zur Anomalieerkennung wurde in die vorhandene Infrastruktur des Produktionsgebäudes C eingebunden und lieferte schnell erste Daten. Es gab während den fünf Wochen im Testbetrieb einige Erkennungen mit nur geringer Kritikalität. Somit verlief die Integration des Vectra S2 in ein OT-Netzwerk ohne Probleme und kann als erfolgreich abgeschlossen werden. Details zur Installation sind dem Anhang A.1 zu entnehmen.

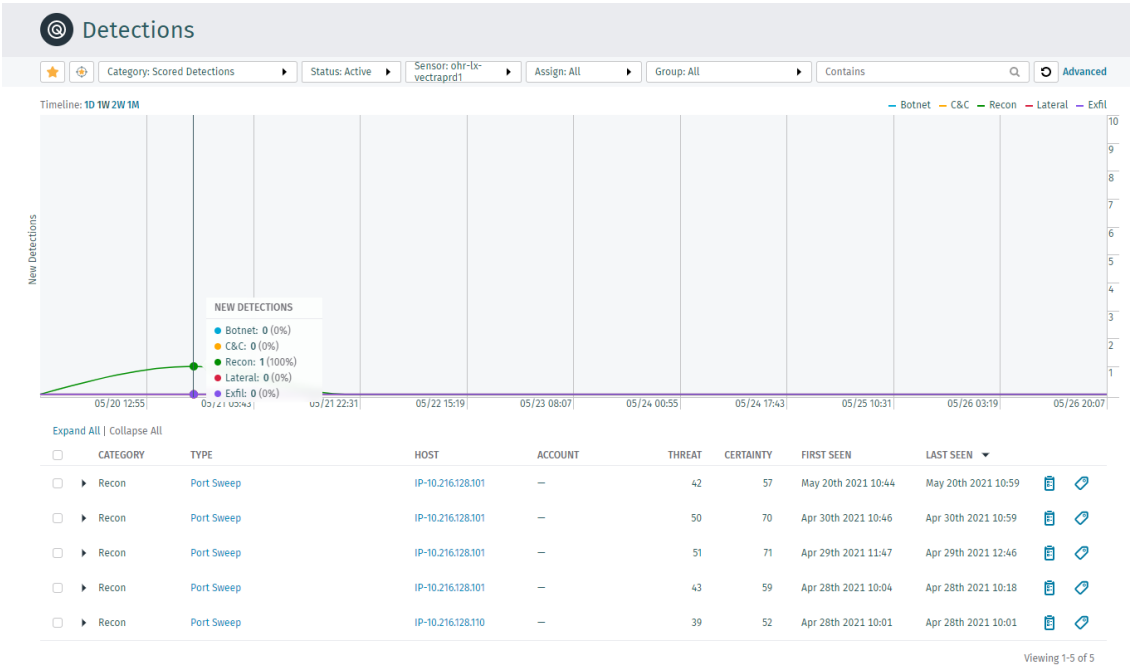

Abbildung 8.1: Vectra AI - Detections im Produktionsnetzwerk Gebäude C

In der Abbildung 8.1 ist zu sehen, welche Detections im Testzeitraum im Produktionsnetzwerk des Gebäudes C erkannt wurden. So ist nur das Port Sweeping als Detection in der Kategorie Recon aufgetreten. Recon steht hier für die Aufklärung im verbundenen Netzwerk und das Port Sweeping für eine gezielte Suche nach bestimmten Diensten über viele Hosts hinweg.

In den vorliegenden Detections ist sehr gut zu erkennen, wie das Programmieren einer Siemens S7-Steuerung begonnen hat. Die Detections für das Port Sweeping entstehen durch den Scan des Siemens TIA-Portals nach kompatiblen Steuerungen in den erreichbaren Subnetzen. Die auffälligen IP-Adressen kommen aus einem reservierten

Pool für firmenfremde Programmierer und konnten somit eindeutig dem Einsatz von Fremdfirmen zugeordnet werden.

Somit ist dies ein typischer Fall für den bereits im Kapitel 6.3 erwähnten und in Abbildung 6.5 ersichtlichen Triage-Filter, um damit False-Positive Detections aus dem Dashboard auszublenden und die Übersichtlichkeit zu gewährleisten.

8.2 Fazit

Bisher war in vielen Unternehmen der Einsatz von Firewalls und Virenscannern gesetzt. Allerdings reicht dies in den Zeiten, in denen täglich über neue Cyber-Angriffe berichtet wird, längst nicht mehr aus. Da eine Firewall mit einer IDS[63] oder IPS[64] Erweiterung wie auch ein Virenscanner nur mit Pattern arbeitet, fehlt hier die wichtige Komponente der künstlichen Intelligenz und die Erkennung von bisher unbekannten, aber ungewöhnlichen Verhaltensmustern. Der Hersteller müsste erfolgreiche Angriffe unter dem Einsatz seiner Produkte zusammen mit den betroffenen Kunden rückwirkend sehr genau analysieren und dann entsprechende Updates programmieren. Nur dann wären andere Kunden bei erneuten Angriffen nach dem gleichen Muster abgesichert. Dies dürfte, gerade bei einem Angriff nach APT Muster, sehr schwierig werden. Neben einer notwendigen, modernen EndPoint Protection kann eine Ergänzung mit einer Netzwerkanomalieerkennung (NBAD), wie Vectra AI sie bietet, das bereits vorhandene IT-Sicherheitskonzept sinnvoll ergänzen und optimieren.

Wichtig zu wissen ist, dass die Infektion mit Schadsoftware meist an den Endpoints geschieht und deshalb eine gute EndPoint Protection als Baustein im Sicherheitskonzept wichtig ist. Sollte dieser erste Baustein im Sicherheitskonzept überwunden sein, ist das frühzeitige Erkennen einer Infektion mit Schadsoftware das wichtigste Ziel. So kann eine Netzwerkanomalieerkennung Angreifer anhand ihres typischen Verhaltens erkennen und eine frühe Reaktion des IT-Sicherheitspersonals ermöglichen.

Auch wenn der Angreifer die ersten Schritte der sogenannten „Cyber Kill Chain“ erfolgreich abgeschlossen hat, kann man durch richtiges Protokollieren und Überwachen der verdächtigen Aktivitäten möglicherweise eine weitere Phase verhindern – beispielsweise das Abfließen sensibler Daten oder der Zugriff auf Ordnerfreigaben mit anschließender Verschlüsselung. Die ganze Cyber-Kill-Chain ist im Anhang A.3 zu sehen. [38] & [41]

Eine in das eigene Sicherheitskonzept integrierte NBAD selbst arbeitet als passiver Teilnehmer und kann somit keinen Einfluss auf das angeschlossene Netzwerk ausüben.

[63] Intrusion Detection System
[64] Intrusion Prevention System

Dies ist bei veralteten Clients, die in OT-Netzwerken immer noch eingesetzt werden, ein wichtiger Punkt. Manchmal reicht bei solchen Assets schon eine SNMP Anfrage, damit es zu einer Fehlfunktion kommt. Auch durch den Scan eines Angreifers bliebe eine NBAD vom Typ Vectra AI anonym, da sie an den Schnittstellen für das zu überwachende Netzwerk keine IP-Adressen verwendet und keinerlei Pakete versendet. Der Sensor liefert die ermittelten Daten über einen unabhängigen Port an eine eigene zentrale Appliance. So ist das System weitestgehend vor Angriffen geschützt und es sind kaum Manipulationen möglich.

Ebenfalls wichtig ist, dass die Einbindung in vorhandene Netzwerke eine wichtige Rolle für die mögliche Erkennungsleistung sowie den Erfolg einer NBAD spielt. Dies stellt auch eine große Herausforderung zwischen einer tiefen Erkennung von Anomalien in jedem Subnetz und einer sinnvollen Kostengestaltung dar. Eine Netzwerkanomalieerkennung kann verständlicherweise nur den Netzwerkverkehr beobachten, der an diesem System vorbei geleitet wird. Dies kann, je nach Möglichkeiten der eingesetzten Netzwerkkomponenten, durch einen Spiegelport (SPAN[65]) oder einem entsprechenden TAP[66] realisiert werden.

Anhand der Ergebnisse der einzelnen Tests aus Kapitel 7.3 ist gut zu erkennen, dass ohne eine Netzwerkverhaltensanalyse wie Vectra AI ungewöhnlicher Netzwerkverkehr in der OT unentdeckt geblieben wäre. Dies betrifft beispielsweise den Portscan, den ungewollten Zugriff auf SMB-Shares oder die Schwachstellenanalyse. Keine der bisher bei der August Storck KG eingesetzten Techniken in der OT würde solchen Netzwerkverkehr als auffällig einstufen. Somit bietet der Einsatz einer verhaltensbasierten Anomalieerkennung einen Gewinn bei der IT-Sicherheit in Produktionsnetzwerken.

Mit der steigenden Anzahl von IPC's und Servern mit Windows als Betriebssystem in Produktionsnetzwerken wird der Einsatz einer NBAD immer sinnvoller. Denn oftmals stellen sie, auch aufgrund Ihrer Verbreitung in der IT, den größten Angriffsvektor dar und sind in den Studien des BSI zur IT-Sicherheit von deutschen Unternehmen als größtes Einfallstor benannt. [5] & [7]

8.2.1 Fazit der Testbedingungen

Vectra hat einige der Tests ohne Detections oder mit geringem IoC[67] bewertet. Dies lässt sich zum einen mit der Lernphase erklären, die bei jedem neuen Einsatz ca. 14 Tage dauert. Zum Anderen mit dem Einsatz der künstlichen Intelligenz, die zum Geschäftsgeheimnis von Vectra AI gehört. Die genaue Ursache bleibt den Kunden damit verschlossen. Weiterhin ist es die Philosophie von Vectra AI möglichst wenige, dafür

[65] Switched Port Analyzer
[66] Test Access Point
[67] Indicator of Compromise

aber sichere Detections zu erzeugen. Vectra AI geht es bei der verhaltensbasierten Anomalieerkennung vielmehr um das Zusammenspiel von Verhaltensmustern, die sich gut an der Cyber-Kill-Chain ablesen lassen und an das MITRE ATT&CK® Enterprise Framework angelehnt sind.

Sollten sich also zwei Verhaltensmuster beim gleichen Host ergänzen, wird der Host automatisch mit einer höheren Bedrohung eingestuft, auch wenn einzelne Muster keinen hohen IoC erreicht haben. Damit sind diese dann deutlich im Dashboard, siehe Abbildung 6.2, in den entsprechenden Quadranten eingestuft und durch das IT-Sicherheitspersonal mit akzeptablem Aufwand zu bearbeiten. So lässt sich auch ein großes Netzwerk mit angemessenem Personaleinsatz gut auf Anomalien überwachen.

8.3 Ausblick

In der nahen Zukunft werden sich immer mehr der IT-Technologien in der OT wiederfinden. Wie bereits erwähnt kommt es zu einer immer stärkeren Verschmelzung der früher getrennten Welten. Der Einzug der weitreichenden Vernetzung in der OT bis in die Sensorebene baut dabei die Brücke. Dadurch wird allerdings auch die gestiegene Bedrohungslage der IT unfreiwillig in die OT transferiert. So ist es offensichtlich, dass zwingend auch die IT-Sicherheit in OT-Netzwerken Beachtung finden muss. [14]

Der Prozess der Verschmelzung wird mit der voranschreitenden Einführung der Industrie 4.0 noch weiter beschleunigt. Die Einbindung von smarten Sensoren und die Anbindung an die Cloud kann bei einer Sicherheitslücke weitreichende Folgen für ein Unternehmen haben. Somit ist klar, dass sich die Unternehmen diesen neuen Herausforderungen stellen und die bisherigen IT-Sicherheitskonzepte auf ihre Standfestigkeit prüfen müssen. Dabei sollte die Frage beantwortet werden, ob das bisherige Sicherheitskonzept den veränderten Herausforderungen gewachsen ist oder angepasst werden muss.

Ein weiterer wichtiger Punkt ist die Integration von Clouddiensten. Immer mehr Unternehmen und auch kleine Firmen stellen sich die Frage, ob eine Installation der benötigten Software vor Ort oder die Nutzung der Cloud für die Zukunft das Richtige ist. Dabei stehen die meisten davon vor großen Herausforderungen. Bisher musste, gerade bei kleinen Unternehmen, relativ wenig Personal die IT betreuen. Hier wird es sehr darauf ankommen, die richtigen Entscheidungen für die Zukunft zu treffen. Der Trend in die Cloud ist vermutlich nicht mehr aufzuhalten, da selbst das neue Windows 11 in Form von Windows 365 nun aus der Cloud kommt. Office 365 oder auch die Clouddienste von Google werden in den meisten Technologieunternehmen heutzutage schon großflächig eingesetzt.

Auf der anderen Seite möchte man als Produktionsleiter einen stetigen Überblick über die wichtigen Kennzahlen aus der OT besitzen. So verschmelzen also die klassische IT mit der Einbindung von Clouddiensten und die Produktionsnetzwerke immer weiter. Hierdurch wird es umso wichtiger eine gute IT-Sicherheitsrichtlinie zu planen und umzusetzen, um nicht durch einen erfolgreichen Angriff die Zukunft des Unternehmens zu riskieren. Das man in beiden Fällen keine absolute Sicherheit erreichen kann, muss den Entscheidungsträgern bewusst sein. Beide Möglichkeiten haben Vor- sowie Nachteile, die man im Einzelfall abwägen muss. Mit Vectra Cognito ist es auch möglich, ausgelagerte Dienste wie das AD oder E-Mail aus der Cloud zu überwachen.

Eine Netzwerkverhaltensanalyse wie Vectra AI kann in beiden Varianten zur Optimierung der IT-Sicherheit in Unternehmens- wie auch Produktionsnetzwerken beigetragen. Somit bleibt es am Ende dem Informationssicherheitsbeauftragten (CISO[68]) in Verhandlungen mit der Geschäftsführung überlassen, den weiteren Einsatz einer Verhaltensanalyse in den eigenen Produktionsnetzwerken gegenüber der Gefahr eines möglichen Angriffs und der damit verbundenen Kosten zu befürworten. Ein möglicher Schaden kann, wie im Kapitel 2 bereits beschrieben, für ein Unternehmen schnell in die Millionen Euro gehen.

Wenn sich ein Unternehmen entscheidet, die IT in die Cloud zu verlegen, müssen frühzeitig zwingend passende Sicherheitsstrategien festgelegt werden. Die akute Bedrohungslage lässt das spätere Festlegen im Sinne der IT-Sicherheit nicht zu.

Eine verhaltensbasierte Netzwerkanomalieerkennung (NBAD) stellt eine sinnvolle Ergänzung in einer ganzheitlichen IT-Sicherheitsstrategie eines Unternehmens, bestehend aus technischen und organisatorischen Maßnahmen, dar. Eine NBAD darf dabei aber nur ein Baustein in dieser Strategie sein. Ein weiterer Ausbau der verhaltensbasierten Netzwerkanomalieerkennung über die Testinstallation im Produktiosnetzwerk des Gebäudes C hinaus sollte mit einer Gegenüberstellung der Kosten gegen den Gewinn der Sicherheit bewertet werden. Sicherlich fällt es hier nicht leicht, die hohen Kosten dieser Technologie für weitere Sensoren mit einem nicht offensichtlich messbaren Gewinn an Cyber-Security zu bewerten. Aufgrund der aktuellen Gefahrenlage wird der weitere Ausbau in anderen Produktionsgebäuden aber ausdrücklich empfohlen.

[68] Chief Information Security Officer

Anhang A: Anlagen

A.1 Netzwerkstruktur Produktionsgebäude C

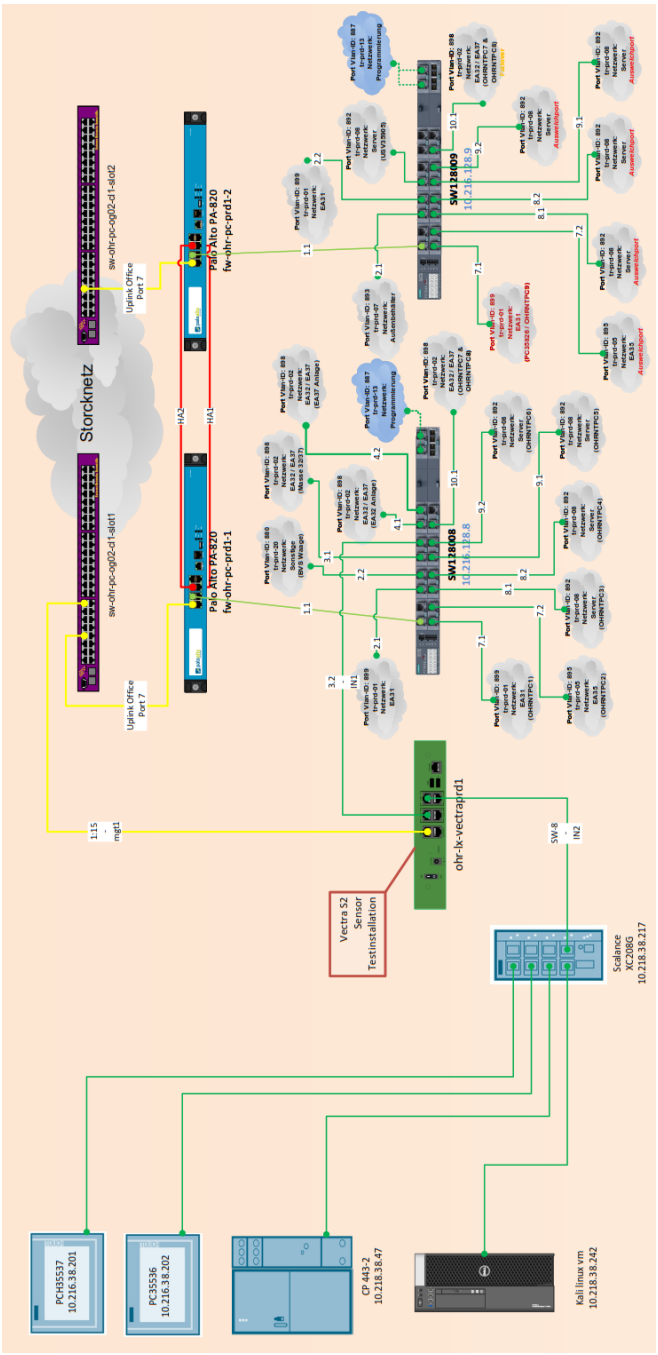

Abbildung A.1: Netzwerkstruktur im Produktionsgebäude C (Auszug)

A.2 MITRE ATT&CK® Enterprise Framework

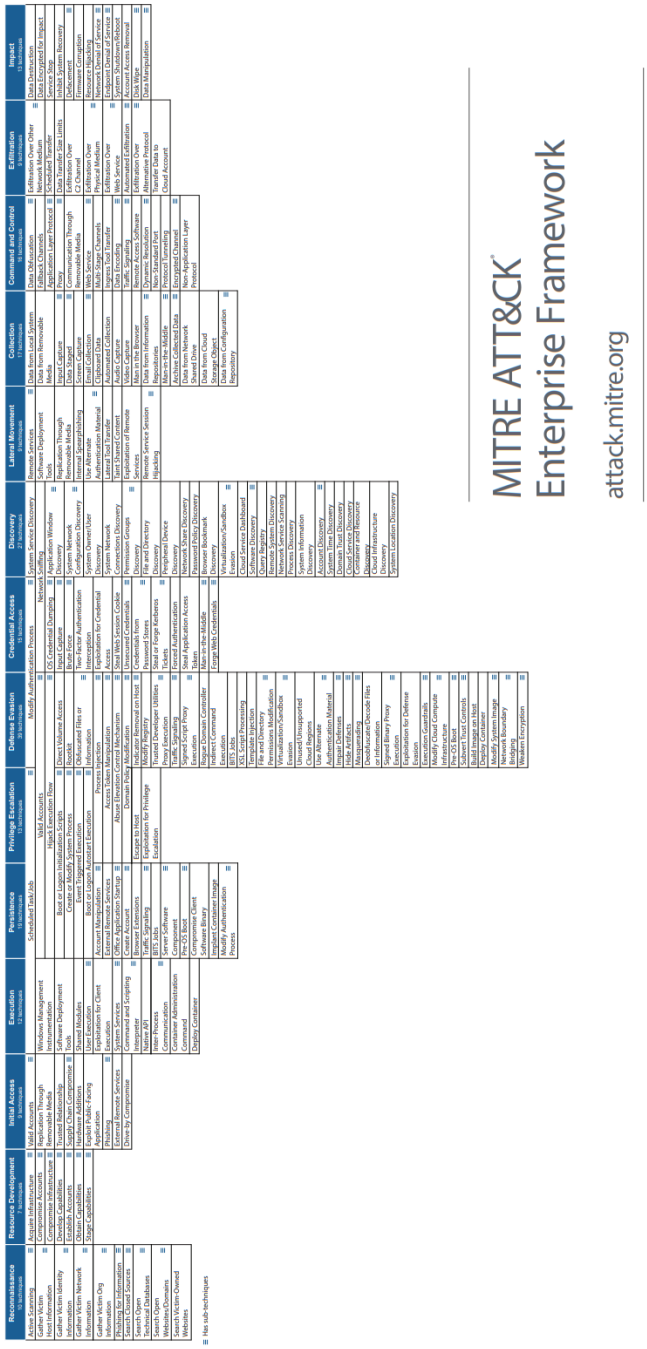

Abbildung A.2: MITRE ATT&CK® Enterprise Framework [52]

A.3 Lockheed Martin Cyber Kill Chain

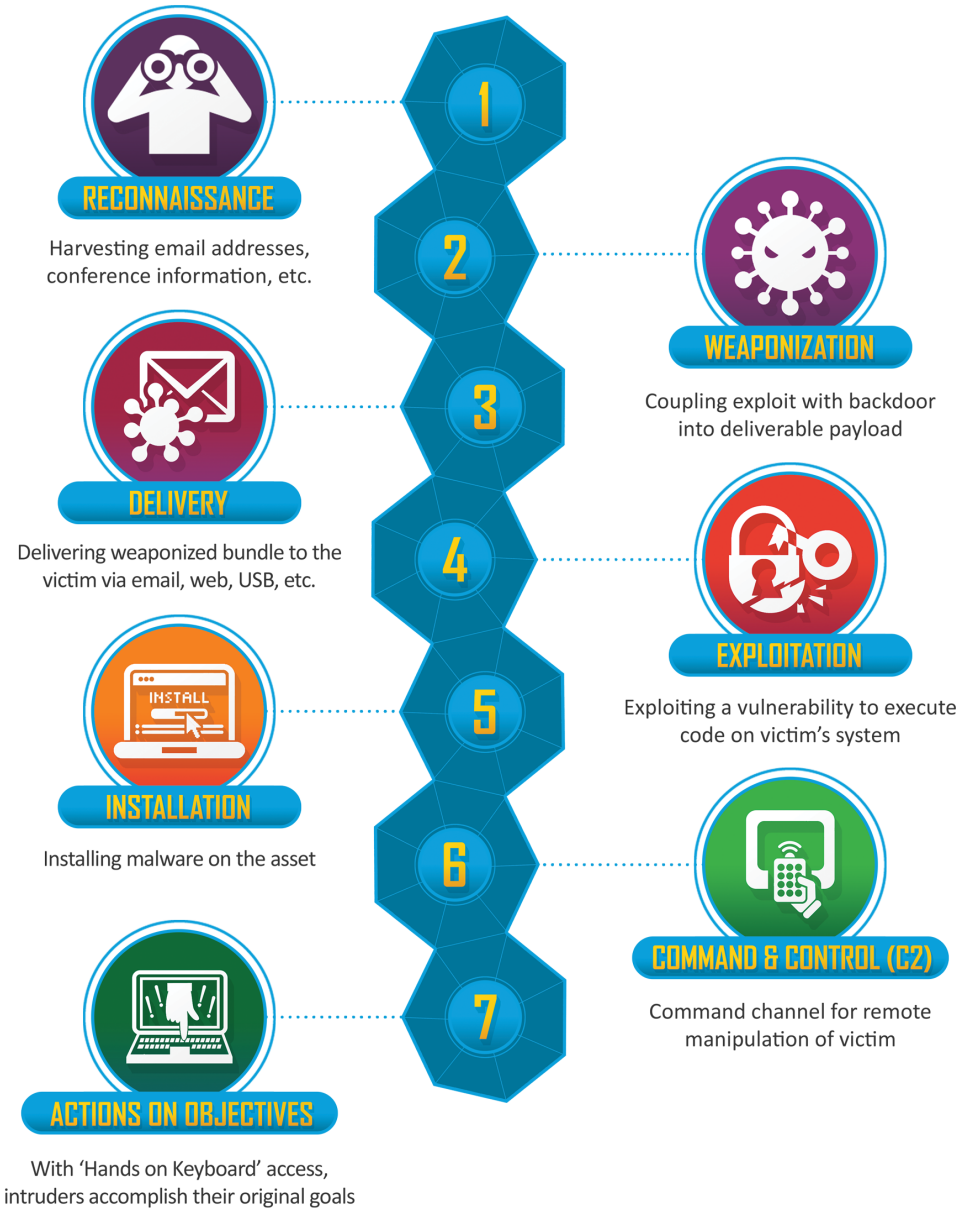

Abbildung A.3: Lockheed Martin Cyber Kill Chain [38]

Literaturverzeichnis

[1] BADER, J. : *The Domain Generation Algorithm of BazarLoader*. https://johannesbader.ch/blog/the-dga-of-bazarbackdoor/. Version: Jul. 2020

[2] BEIERSMANN, S. : *Antiviruslösungen im Performancetest*. online. https://tinyurl.com/y45476yl. Version: Okt. 2017

[3] BÖHM, M. : *Computerattacke auf Norsk Hydro - Angreifer legten Alu-Konzern mit Erpressersoftware lahm*. https://www.spiegel.de/netzwelt/netzpolitik/norsk-hydro-hackerangriff-war-eine-lockergoga-ransomware-attacke-a-1258627.html. Version: März 2019

[4] BORN, G. : *Trojaner in SolarWinds-Updates ermöglicht Cyberangriffe*. https://heise.de/-4989903. Version: Dez. 2020

[5] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: *Industrielle Steuerungs- und Automatisierungssysteme (ICS) Security Kompendium*. Version: 1, Nov. 2013. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Industrielle-Steuerungs-und-Automatisierungssysteme/industrielle-steuerungs-automatisierungssysteme_node.html

[6] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: *Fallbeispiel Servicetechniker: Der Virus kommt zu Fuß*. https://www.bsi.bund.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_095c.html?nn=128704. Version: 2, 2018

[7] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: *Industrial Control System Security: Top 10 Bedrohungen und Gegenmaßnahmen*. https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_005.html. Version: 1.3, Febr. 2019

[8] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: *Die Lage der IT-Sicherheit in Deutschland 2019*. Bonn : Bundesamt für Sicherheit in der Informationstechnik, 2019

[9] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: *Kritische Schwachstellen in Exchange-Servern*. https://www.bsi.bund.de/DE/Themen/

Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Server/Microsoft-Exchange_Schwachstelle/schwachstelle_exchange_server_node.html. Version: März 2021

[10] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: *Die Lage der IT-Sicherheit in Deutschland*. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Lageberichte/Jahreslageberichte/jahreslageberichte_node.html. Version: 2021

[11] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: *BSI-Standards*. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/bsi-standards_node.html. Version: Nov. 2017

[12] BÜNTE, O. : *KraussMaffei von Hackern erpresst*. https://heise.de/-4244880.html

[13] DIEHL, J. : *Diebstahl geheimer Daten bei der Nato*. https://www.spiegel.de/politik/deutschland/prozess-gegen-it-experten-datendiebstahl-bei-der-nato-a-911646.html. Version: Jul. 2019

[14] DOLL, N. : *Zahl der Cyberattacken auf Unternehmen so hoch wie nie zuvor*. https://www.welt.de/politik/deutschland/article232275409/Cyberattacken-auf-Unternehmen-Zahl-so-hoch-wie-nie-zuvor.html. Version: Jul. 2021

[15] DPA: *Werke auf manuellem Betrieb: Cyberangriff auf Aluminiumkonzern Norsk Hydro*. https://heise.de/-4339886. Version: März 2019

[16] EHRLICH, T. : *Advanced Persistent Threats (APTs) erklärt*. https://www.computerwoche.de/a/advanced-persistent-threats-apts-erklaert,3545302. Version: Okt. 2019

[17] HENNING, C. : *ProfiNet for Network Geeks*. https://us.profinet.com/profinet-network-geeks-want/. Version: Jan. 2014

[18] HMS INDUSTRIAL NETWORKS GMBH: *ProfiNet*. https://www.feldbusse.de/profinet/profinet.shtml

[19] HOLLAND, M. : *Malware legt IT im Klinikum komplett lahm*. https://heise.de/-4223573. Version: Nov. 2018

[20] HORNETSECURITY: *Die Cyber Kill Chain im Detail*. https://www.hornetsecurity.com/de/wissensdatenbank/cyber-kill-chain/. – Schritt für Schritt die IT-Sicherheit im Unternehmen stärken

[21] HUBER, W. : *IT-OT Pyramide*. https://images.channelpartner.de/bdb/3274342/890x.webp

[22] INFOGUARD AG: *VECTRA NETWORKS –AI-Basierte Breach Detection Platform*. https://www.infoguard.ch/de-ch/partner/vectra-networks-breach-detection

[23] INFOSECMATTERS.COM: *PowerShell Commands for Pentesters*. https://www.infosecmatter.com/powershell-commands-for-pentesters/. Version: Okt. 2020

[24] IPCOMM GMBH ; IPCOMM GMBH (Hrsg.): *Profi-Net*. https://www.ipcomm.de/protocol/Profinet/de/sheet.html. Version: 2020

[25] IPCOMM GMBH ; IPCOMM GMBH (Hrsg.): *S7 Protokoll (RFC1006)*. https://www.ipcomm.de/protocol/S7ISOTCP/de/sheet.html. Version: 2020

[26] ITWISSEN.INFO: *NBAD (network behavior anomaly detection) :: ITWissen.info*. https://www.itwissen.info/NBAD-network-behavior-anomaly-detection.html. Version: 4.3.2020

[27] KOVAR, R. : *Random Words on Entropy and DNS*. https://www.splunk.com/en_us/blog/security/random-words-on-entropy-and-dns.html. Version: Okt. 2015

[28] KREMPÖ, S. : *Massiver Hackerangriff geht weit über SolarWinds hinaus*. https://heise.de/-5041427. Version: Jan. 2021

[29] KREYENBURG, H. : *APT - die unsichtbare Bedrohung*. https://www.hornetsecurity.com/de/security-informationen/advanced-persistent-threats/. Version: Okt. 2018

[30] KUNBUS GMBH: *EtherNet Grundlagen*. https://www.kunbus.de/ethernet-ip-grundlagen.html

[31] KUNBUS GMBH: *Industrial Ethernet*. https://www.kunbus.de/industrial-ethernet-warum-i.html

[32] KUNBUS GMBH: *Profi-Net Grundlagen*. https://www.kunbus.de/profinet-grundlagen.html

[33] KUNBUS GMBH: *SafetyNet*. https://www.kunbus.de/safetynet.html

[34] KUNZE, S. : *Gehackt: Schmersal erholt sich von Cyberangriff*. https://www.elektrotechnik.vogel.de/gehackt-schmersal-erholt-sich-von-cyberangriff-a-940770/. Version: Jun. 2020

[35] KÜHL, E. : *Ein Hackerangriff, der um die Welt geht*. https://www.spektrum.de/news/solarwinds-ein-hackerangriff-der-um-die-welt-geht/1819187. Version: Jan. 2021

[36] LANGNER, R. : *Stuxnet und die Folgen*. https://www.langner.com/wp-content/uploads/2017/08/Stuxnet-und-die-Folgen.pdf. Version: Aug. 2017

[37] LEITNER, T. D. . A.: *Angriffstechnik im lokalen Netz: ARP-Spoofing und -Poisoning*. https://www.linux-magazin.de/ausgaben/2004/06/interner-zugriff/. Version: Jun. 2004

[38] LOCKHEED MARTIN CORPORATION: *Cyber Kill Chain®*. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

[39] LYON, G. : *Grundlagen von Port-Scans*. https://nmap.org/man/de/man-port-scanning-basics.html. Version: März 2021

[40] LYON, G. : *Port-Scanning-Methoden*. https://nmap.org/man/de/man-port-scanning-techniques.html. Version: März 2021

[41] MURER, F. : *Netzwerksicherheit im Active Directory: So enttarnen Sie Angreifer durch Logs*. https://heise.de/-6141370. Version: Jul. 2021

[42] PILZ GMBH & CO. KG: *Systemkomponenten SafetyNET p*. https://www.pilz.com/de-DE/eshop/00103002137081/Systemkomponenten-SafetyNET-p. Version: März 2021

[43] SCHERSCHEL, F. A.: *BIOS-Rootkit LightEater: In den dunklen Ecken abseits des Betriebssystems*. https://heise.de/-2582782. Version: März 2015

[44] SCHMIDT, J. : *IT-Totalschaden beim Kammergericht Berlin*. https://heise.de/-4646568

[45] SERCOS INTERNATIONAL E.V.: *SERCOS 3*. https://www.sercos.de/technologie/sercos-iii/

[46] SHAWNDEVANS: *smbmap*. https://tools.kali.org/information-gathering/smbmap

[47] SIEMENS AG, ÖSTERREICH: *Der grosse Unterschied*. https://www.hitech.at/industrie/der-grosse-unterschied/. Version: Okt. 2018

[48] SOKOLOV, D. A.: *Megahack Equifax' war „absolut vermeidbar"*. https://heise.de/-4259677. Version: Dez. 2018

[49] SOKOLOV, D. A.: *Hackern pluendern FireEye Arsenal*. https://heise.de/-4980417. Version: Dez. 2020

[50] STROBEL, S. : *Neue Techniken der Endpoint-Security*. https://www.heise.de/select/ix/2019/12/1922715312549153160. Version: Dez. 2019

[51] THE MITRE CORPORATION: *ATT&CK® for Industrial Control Systems*. https://collaborate.mitre.org/attackics/index.php/Main_Page

[52] THE MITRE CORPORATION: *MITRE ATT&CK® Matrix for Enterprise*. https://attack.mitre.org/versions/v9/matrices/enterprise/

[53] TRENDMICRO: *Pwn2own 2021 - Schedule and Live Results*. https://www.zerodayinitiative.com/blog/2021/4/2/pwn2own-2021-schedule-and-live-results. Version: Apr. 2021

[54] UNIVERSITY OF BATH: *Tomorrow belongs to those who can hear it coming*. https://blogs.bath.ac.uk/iprblog/2016/01/14/tomorrow-belongs-to-those-who-can-hear-it-coming/. Version: Jan. 2016

[55] VECTRA AI: *Vectra Cognito Recall*. https://tinyurl.com/y4j3gb9z. Version: Mai 2018

[56] WELCHERING, P. : *IT-Sicherheit in Deutschland desaströs*. https://www.zdf.de/nachrichten/politik/it-sicherheit-deutschland-100.html. Version: März 2021

[57] WESTERNHAGEN, O. von: *Trojaner-Befall: Neue Emotet-Welle legt Neustädter Stadtverwaltung lahm*. https://heise.de/-4518819. Version: Sept. 2019

[58] WESTERNHAGEN, O. von: *Cyberangriffe via SolarWinds-Software – neue Entwicklungen im überblick*. https://heise.de/-4991255. Version: Dez. 2020

[59] WESTERNHAGEN, O. von: *Schwachstellen in 28 AV-Programmen*. https://heise.de/-4710337. Version: Apr. 2020

[60] WESTERNHAGEN, O. von: *Turla und Co. tarnen Angriffe durch scheinbar harmlose Aktivitäten*. https://heise.de/-4978541. Version: Dez. 2020

[61] WIKIPEDIA.ORG: *Monitoring*. https://de.wikipedia.org/wiki/Monitoring. Version: 19.12.2019

[62] WIKIPEDIA.ORG: *Stuxnet*. https://de.wikipedia.org/wiki/Stuxnet. Version: März 2021

[63] WILKENS, A. : *Hacker-Angrif auf ThyssenKrupp*. https://heise.de/-3565857.html

Erklärung

Hiermit erkläre ich, dass ich meine Arbeit selbstständig verfasst, keine anderen als die angegebenen Quellen und Hilfsmittel benutzt und die Arbeit noch nicht anderweitig für Prüfungszwecke vorgelegt habe.

Stellen, die wörtlich oder sinngemäß aus Quellen entnommen wurden, sind als solche kenntlich gemacht.

Mittweida, 24. 07 2021