MASTERARBEIT

TECHNISCHE ASPEKTE ZUR ABSICHERUNG VON UNTERNEHMENSNETZWERKEN

Ausgeführt am

Studiengang
Informationstechnologien und Wirtschaftsinformatik

Jakob Glanzer MA, BSc
Personenkennzeichen: 2010320024

Graz, am 6. Juli 2022 .....

Unterschrift

EHRENWÖRTLICHE ERKLÄRUNG

Ich erkläre ehrenwörtlich, dass ich die vorliegende Arbeit selbstständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen nicht benützt und die benutzten Quellen wörtlich zitiert sowie inhaltlich entnommene Stellen als solche kenntlich gemacht habe.

.....

Unterschrift

DANKSAGUNG

An dieser Stelle möchte ich mich bei all denjenigen bedanken, die mich während der Anfertigung dieser Masterarbeit und während des Studiums unterstützt und motiviert haben.

Zuerst gebührt mein Dank Herrn DI (FH) Günther Zwetti, der meine Masterarbeit betreut und begutachtet hat. Für die hilfreichen Anregungen, konstruktive Kritik und vor allem die zeitnahen Feedbacks bei der Erstellung dieser Arbeit möchte ich mich herzlich bedanken.

Ebenfalls möchte ich meinem Arbeitgeber, der GAW Beteiligungs GmbH, meinem Vorgesetzten Herrn Ing. Ingomar Gaksch und meinen Arbeitskollegen für die Ermöglichung dieses Studiums und ihren unermüdlichen Einsatz während meiner durchaus flexiblen Arbeitszeiten im Zuge der Erstellung dieser Arbeit bedanken.

Ein besonderer Dank gilt den Experten für die Interviews, ohne die diese Arbeit nicht hätte entstehen können.

Abschließend möchte ich mich bei meinen Eltern bedanken, die mir bereits in meinen jungen Jahren einen gesunden Ehrgeiz beigebracht haben, der mich durch die schwierigen Zeiten dieses Studiums trug.

Jakob Glanzer

KURZFASSUNG

Die IT ist aus modernen Unternehmen nicht mehr wegzudenken. Sämtliche elektronische Kommunikation ist ohne die entsprechende Infrastruktur unmöglich und für Unternehmen essenziell. Doch diese Unternehmensnetzwerke werden immer öfter durch Cyber-Attacken gefährdet.

Aus diesem Grund wird von Unternehmen eine Vielzahl an Sicherheitsmaßnahmen eingesetzt, um die IT-Infrastruktur zu schützen. Um das System vor Gefahren von außen und innen optimal abzusichern, schränken diese Maßnahmen die Möglichkeiten der Endanwender ein, da der User eine der größten Sicherheitslücken darstellt.

Das Ziel dieser Arbeit ist die Ausarbeitung der aktuell angewandten Sicherheitsmaßnahmen in Unternehmensnetzwerken, deren Möglichkeiten das System zu schützen und auf deren Einfluss auf die Endanwender einzugehen. Dazu wird folgende Forschungsfrage gestellt: „Welche technischen Maßnahmen mit vertretbaren Einschränkungen für den operativen Betrieb schützen Firmennetzwerke effektiv vor Angriffen?“

Um die Forschungsfrage und Hypothesen dieser Masterarbeit beantworten zu können, wurde zunächst eine Literaturrecherche durchgeführt, um einen Überblick über die derzeitigen Sicherheitsstandards zu gewinnen. Im Anschluss wurden qualitative Experteninterviews geführt, um die quantitativen Ergebnisse zu analysieren, priorisieren und zukünftige Möglichkeiten aufzuzeigen.

Sowohl Literaturrecherche als auch Experteninterviews zeigen auf, dass die behandelten Sicherheitsmaßnahmen für die User in einer homogenen IT-Infrastruktur, in der auf Usability-Anforderungen im Sicherheitskonzept geachtet und sicherheitstechnisch ein Kompromiss eingegangen wurde, mit vertretbaren Einschränkungen verbunden sind.

Die Untersuchung von zukünftigen Sicherheitskonzepten wie Zero Trust oder der Einsatz von künstlicher Intelligenz in diesem Kontext bieten ein breites Spektrum für weitere Forschung.

ABSTRACT

Since its invention information technologies have become one of the most important enablers in companies. Most of the processes would be unthinkable without the help of IT infrastructure. But especially nowadays the company networks are under the attack of cyber-criminals. Companies must use an abundance of security measures to defend and secure their networks, which in turn also influences the users.

The objective of this thesis is the evaluation of current security measures and their influence on the users in the network. For this purpose, the following research question is: "Which technical measures with justifiable restrictions for operations effectively protect company networks from attacks?"

To answer the research question and hypotheses of this master's thesis, literature research was first carried out to gain an overview of the current security standards. Qualitative expert interviews were then conducted to analyze and prioritize the quantitative results and to identify future opportunities.

The literature research as well as expert interviews show that the discussed security measures have justifiable and reasonable restrictions on the users. It is important to note that a security concept which pays attention to usability requirements, a homogenous IT-infrastructure, and a compromise in terms of security are necessary.

The investigation of future security concepts such as Zero-Trust or artificial intelligence in IT-security offers a broad spectrum for further research.

INHALTSVERZEICHNIS

1 EINLEITUNG

"Security is always excessive until it's not enough."

- Robbie Sinclair

Der Einsatz unterschiedlichster Informationstechnologien wird weltweit in sämtlichen Bereichen immer wichtiger.

Viele Geschäftsprozesse werden heute mit der Hilfe von IT-Systemen umgesetzt und optimiert. Dadurch entsteht allerdings eine große Abhängigkeit von diesen Programmen. Viele Geschäftsprozesse werden direkt an ein IT-System angebunden und können bei einem Ausfall dieses Systems nicht mehr durchgeführt werden.

Aus diesem Grund ist es für Unternehmen essenziell IT-Sicherheitslücken zu schließen und Cyber-Attacken abwehren zu können. Auch im Falle eines erfolgreichen Angriffes sollte das System so konzipiert sein, dass der Schaden gering und die Downtime betroffener Prozesse möglichst gering sind.

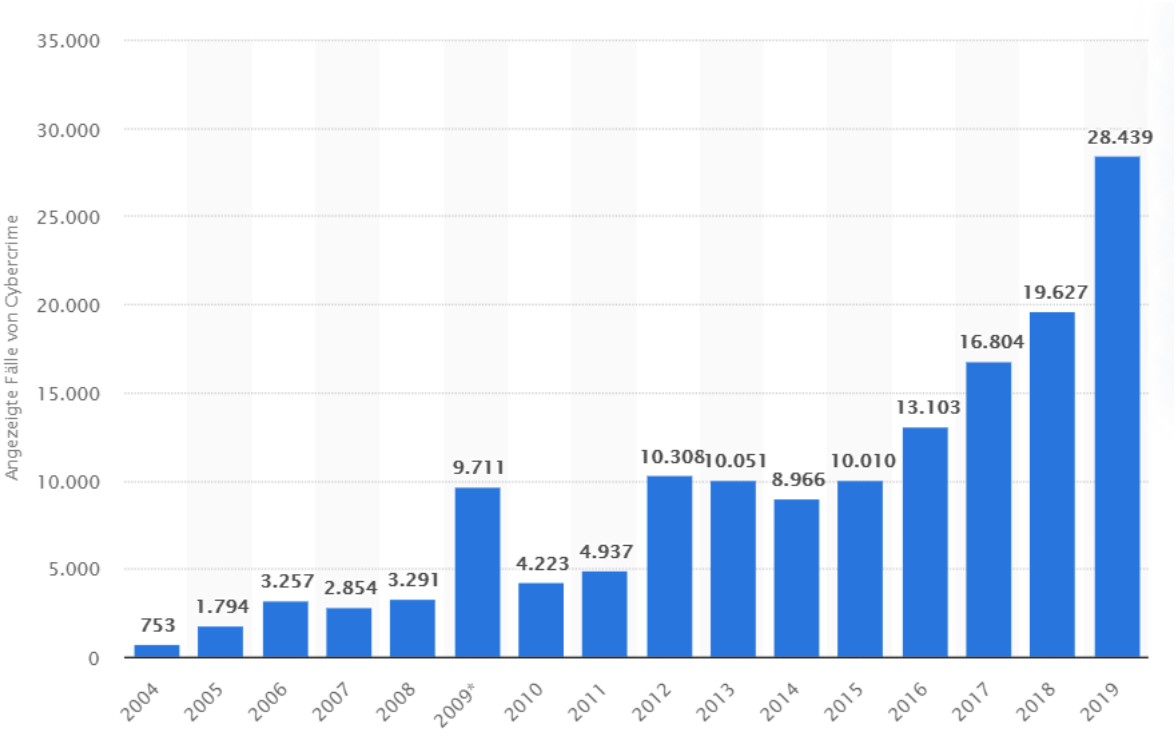

Abbildung 1: Angezeigte Fälle von Cybercrime (gesamt) in Österreich von 2004 bis 2019 (shorturl.at/duwG3)

Wie in Abbildung 1 zu sehen ist, kann ein eindeutig steigender Trend bezüglich Cyber-Attacken in Österreich wahrgenommen werden. Um die Sicherheit von Unternehmensnetzwerken zu gewährleisten, müssen immer komplexere Sicherheitsmaßnahmen getroffen werden.

1.1 Zielsetzung

Ziel dieser Arbeit ist die Analyse von neuesten IT-Sicherheitsstandards und deren teilweise Implementierung in einem Unternehmensnetzwerk.

Das Hauptaugenmerk soll dabei auf den technischen Aspekten dieser Standards und Maßnahmen liegen.

Hierzu wird ein expliziter Cyber-Angriff aus jüngster Vergangenheit analysiert, um eine aktuelle Verbreitungs- und Angriffsmethodik von Malware aufzuzeigen. Zusätzlich wird das von diesem Angriff betroffene Unternehmensnetzwerk analysiert. Mögliche Sicherheitsmaßnahmen werden aufgezeigt und teilweise implementiert.

Im Zuge dieser Arbeit sollen folgende Fragen beantwortet werden:

- Was sind die aktuellen Sicherheitsstandards für Netzwerke aus technischer Perspektive?
- Mit welchen technischen Maßnahmen kann der Schaden durch Cyber-Attacken minimiert werden?

Ein Nicht-Ziel dieser Arbeit ist die Ausarbeitung eines Sicherheitskonzeptes in Bezug auf Social-Engineering.

1.2 Hypothesen und Forschungsfrage

Im Rahmen der Masterarbeit soll folgende Forschungsfrage beantwortet werden:

- Welche technischen Maßnahmen mit vertretbaren Einschränkungen für den operativen Betrieb schützen Firmennetzwerke effektiv vor Angriffen?

Folgende Hypothesen sollen behandelt werden.

Hypothese 1:

- H0: Mehrere kleine, durch eine Firewall getrennte Subnetzwerke sind sicherer als ein großes Netz.
- H1: Viele kleine, durch eine Firewall getrennte Subnetzwerke bieten keinen messbaren Sicherheitsvorteil gegenüber einem einzelnen großen Netzwerk.

Hypothese 2:

- H0: Ein technisch laut neuesten Sicherheitsanforderungen gut geschütztes Netz kann auch durch Anwendungsfehler und bewusste Manipulation von berechtigten Usern nicht gefährdet werden.
- H1: Selbst laut neuesten Sicherheitsanforderungen gut geschützte Netze können durch Anwendungsfehler und bewusste Manipulation von berechtigten Usern gefährdet werden.

1.3 Methodik

Um die Forschungsfrage und Hypothesen dieser Masterarbeit beantworten zu können, wird ein quantitativer als auch qualitativer Forschungsansatz gewählt.

Zunächst wird eine ausführliche quantitative Literaturrecherche durchgeführt, um einen Überblick über die derzeitigen Sicherheitsstandards zu gewinnen.

Im Anschluss werden qualitative Experteninterviews geführt, um die Ergebnisse aus der Literaturrecherche zu analysieren, teilweise zu priorisieren und zukünftige Möglichkeiten aufzuzeigen.

Die Experteninterviews wurden aufgenommen und transkribiert, damit die daraus gewonnenen Erkenntnisse nachvollziehbar sind. Da Netzwerksicherheit unterschiedlichste Ausprägungen haben kann, ist es in dieser Arbeit notwendig, sich auf Experteninterviews zu beziehen, damit auf derzeitige Praxisstandards Bezug genommen werden kann.

Abschließend wird die Implementierung einer Auswahl der erarbeiteten Sicherheitsmaßnahmen anhand eines Fallbeispiels aufgezeigt und Hypothesen sowie Forschungsfrage entsprechend beantwortet.

2 GRUNDLAGEN DER NETZWERKSICHERHEIT UND SCHADENSPRÄVENTION

Der Einsatz von IT-Infrastrukturen wird für Unternehmen in der heutigen Zeit immer wichtiger und ist in den meisten Bereichen aus den Kernprozessen nicht mehr wegzudenken. Durch den stetig steigenden Wert an Daten wird der Diebstahl als auch die Verschlüsselung von diesen lukrativer, was zu einer Erhöhung von Cyber-Attacken führt. In den ersten drei Quartalen von 2020 wurden weltweit über 36 Milliarden Datensätze durch Datenlecks (Data Breaches) veröffentlicht und allein in den USA ist die Anzahl der Datenlecks von 1.108 (2020) auf 1.291 (2021) um 17 % gestiegen. Die Kosten für ein Datenleck belaufen sich laut IBM im Jahr 2020 im Schnitt auf 3,86 Millionen Dollar. (Miloslavskaya, 2021) (Fortinet, 2021) (IBM, 2020) (Singleton, 2021)

Durch diese Zahlen wird klar, dass die Informationssicherheit in Unternehmen nicht zu unterschätzen ist, insbesondere da Angriffe, wenn der derzeitige Trend fortgesetzt wird, über die nächsten Jahre immer häufiger werden.

Um die Informationssicherheit von Unternehmensnetzwerken zu gewährleisten, werden in diesem Kapitel die bekanntesten Malware- und Ransomware-Attacken der letzten Jahre kurz vorgestellt und danach auf technische Möglichkeiten zur Absicherung von Netzwerken eingegangen. Diese werden sich nicht nur auf die Abwehr von etwaigen Angriffen fokussieren, sondern auch auf Aspekte der Schadenbegrenzung.

2.1 Cyber-Attacken

Damit Ransomware- und Malware-Attacken in Systemen effektiv werden und Schaden anrichten können, müssen diese zunächst über eine Schwachstelle eindringen. Diese Schwachstellen können durch fehlerhafte Netzwerkkonfigurationen, ungewartete Server oder auch durch fehlerhaftes Verhalten der User entstehen.

2.1.1 Initiale Zugriffsarten

Die drei beliebtesten Arten zur Verschaffung von illegalem Zugriff auf ein Unternehmensnetzwerk waren im Jahr 2020 „Scan and Exploit“ mit 35 % aller Angriffe, „Phishing“ mit 33 % aller Angriffe und Zugangsdatendiebstahl mit 18 % aller Angriffe. Insgesamt wurden 86 % aller IBM gemeldeten Zwischenfälle durch diese drei Arten ausgelöst. (Singleton, 2021, S. 7)

Da „Phishing“ und Zugangsdatendiebstahl bekannt bzw. selbsterklärend sind, wird hier nicht weiter darauf eingegangen.

Bei „Scan and Exploit“ werden die im Internet offenen Zugänge, wie z. B. ungesicherte Remote-Zugänge, gescannt und durch ungepatchte Sicherheitsupdates ausgenutzt. Um dies zu vermeiden, sollten gerade die nach außen exponierten Services so aktuell wie möglich gehalten werden. Allerdings kommt es immer wieder vor, dass es sogenannte „Zero-Day-Exploits“ gibt.

Bei diesen Attacken werden Schwachstellen ausgenützt, die bis zur aktuellen Verwendung sogar den Entwicklern der Programme und Services unbekannt waren. Eine der größten Schwachstellen in diesem Bereich war zum Beispiel die Citrix-Schwachstelle „CVE-2019-19781“, welche im ersten Halbjahr 2020 für 15 % der Zwischenfälle gesorgt hat. (Singleton, 2021, S. 11)

2.1.2 Angriffsarten

Die drei beliebtesten Angriffsarten im Jahr 2020 waren Ransomware, Datendiebstahl und Serverzugriff.

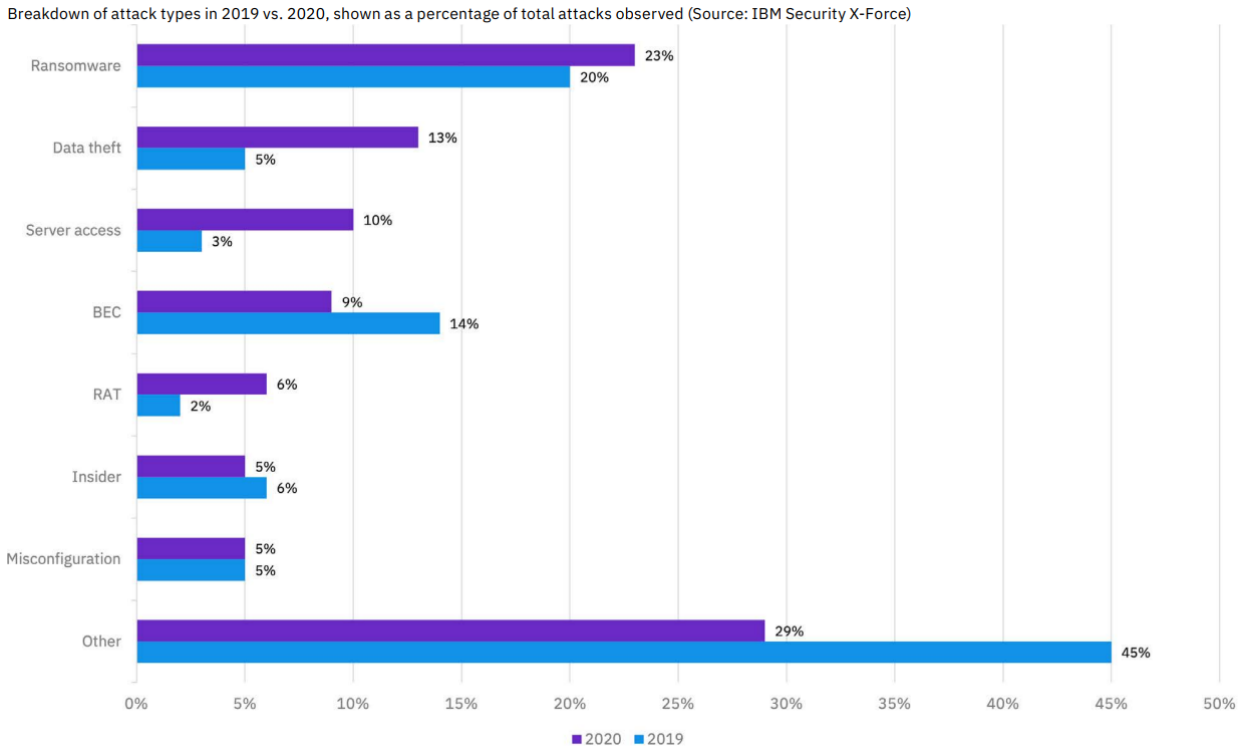

Abbildung 2: Angriffsarten 2020 vs. 2019 (t.ly/1Hxi)

Ransomware ist eine die beliebteste Art des Cyberangriffes. Bei diesen Angriffen wird durch Malware die gesamte IT-Infrastruktur verschlüsselt. In der Regel bekommen die Unternehmen in Textdateien auf Servern bzw. durch Popups eine Benachrichtigung, wohin über Kryptowährungen wie viel Geld zu überweisen ist, damit das System wieder entschlüsselt wird. Um mehr Druck ausüben zu können, werden essenzielle und sensitive Unternehmensdaten vor der Verschlüsselung bereits gestohlen und angedroht diese Daten bei Zahlungsunwilligkeit zu veröffentlichen oder zu verkaufen. Insgesamt waren, wie in Abbildung 2 zu sehen ist, 23 % aller Attacken im Jahr 2020 Ransomware-Angriffe. (Singleton, 2021, S. 9) (Department of Homeland Security CISA, 2020) (Mohurle & Patil, 2017)

2.1.2.1 Problematiken

Im Falle einer erfolgreichen Ransomware-Attacke gibt es mehrere Szenarien, die in einem Unternehmen geschehen können. Bei keiner dieser Strategien gibt es keine Nachteile für die Unternehmen.

Bei angebrachten Sicherheitsmaßnahmen kann so ein Angriff allerdings wesentlich harmloser ablaufen als bei einer unvorbereiteten IT-Infrastruktur. Das Worst-Case-Szenario wäre in diesem Fall überhaupt keine Vorbereitung und würde bedeuten, dass die gesamte digitale Infrastruktur verschlüsselt ist und keine Sicherungen vorhanden sind. Dann bleibt dem Unternehmen nichts Anderes übrig, als entweder das Lösegeld zu bezahlen oder alles von Anfang an neu aufzubauen. Je nach Unternehmensgröße kann es zu mehrwöchigen Stillständen kommen. Das Problem dabei ist, dass selbst eine getätigte Bezahlung keine Garantie dafür ist, dass das System wieder entschlüsselt wird. Zusätzlich kommt meistens die „Double Extortion Strategy“ zum Einsatz. Das Unternehmen soll nämlich nicht nur für die Entschlüsselung des Systems zahlen, sondern auch für die Löschung der im Vorhinein gestohlenen Daten. Diese sensitiven Daten könnten selbst bei Bezahlung weiterverkauft bzw. veröffentlicht werden. (Mohurle & Patil, 2017) (Tuttle, 2021)

Bei einer IT-Infrastruktur, die auf Cyber-Angriffe vorbereitet ist, würde die Attacke für Unternehmen wesentlich glimpflicher ausfallen. Bei entsprechenden Netzwerksegmentierungen könnten nur bestimmte Teile des Systems betroffen sein, welche durch eine Sicherung zeitnah zurückgesetzt werden können. Auch die Dauer bis zur Entdeckung der Ransomware kann je nach vorhandenen Schutzmaßnahmen variieren und im besten Fall die Software blockieren, bevor etwas geschieht. Allerdings gilt zu beachten, dass bei einer erfolgreichen Ransomware-Attacke, selbst bei geringem Schaden im System, immer die Möglichkeit besteht, dass bereits sensitive Daten gestohlen wurden. So kann selbst ein harmloser Befall schnell zu einem kostenintensiven Problem werden. (Gazet, 2008)

2.1.2.2 Sodinokibi

Obwohl viele unterschiedliche Arten und Abwandlungen von Ransomware im Umlauf sind, gibt es eine Software, die im Jahr 2020 für einen Großteil der Ransomware-Attacken verantwortlich war.

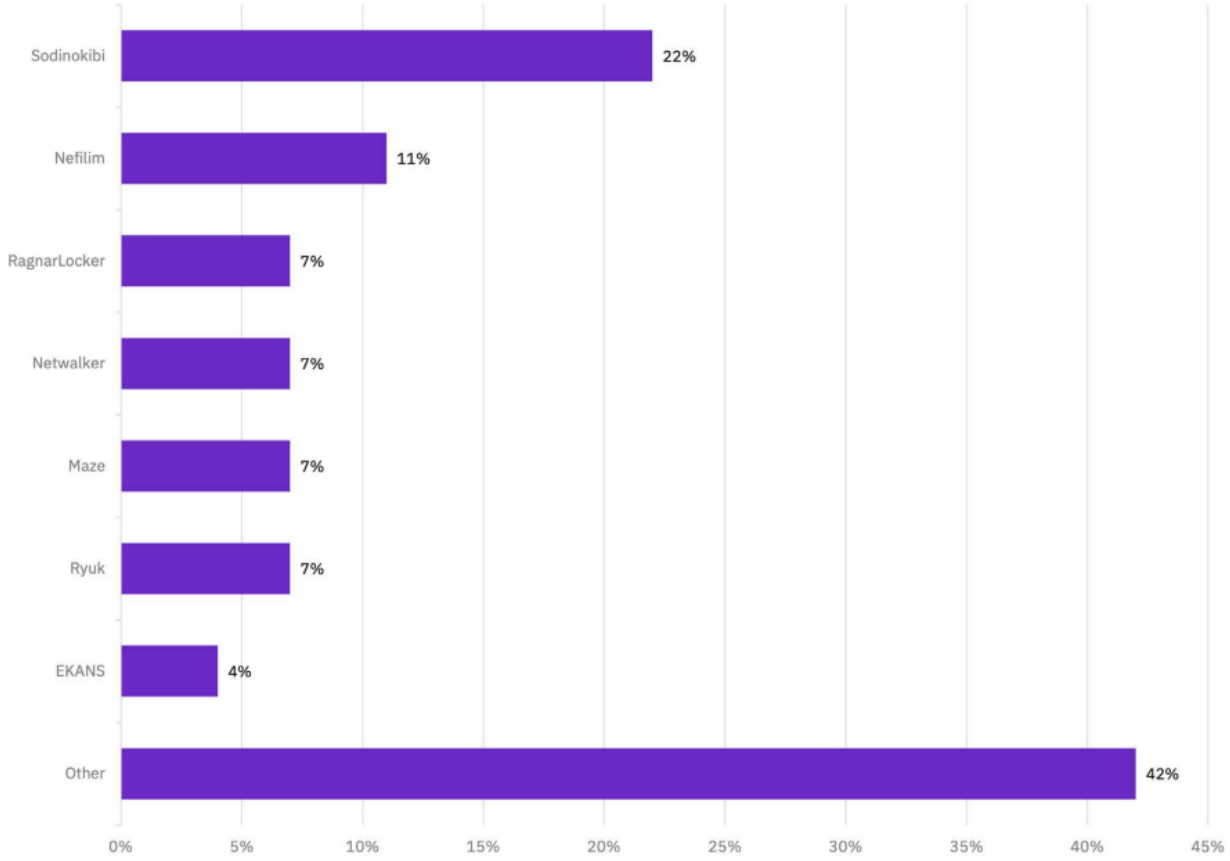

Abbildung 3: Beliebteste Ransomware-Software 2020 (t.ly/8irH)

Sodinokibi bzw. REvil wurde in diesem Jahr für über 22 % aller Ransomware-Angriffe eingesetzt und ist somit für einen großen Teil der Angriffe mitverantwortlich. (Singleton, 2021, S. 9)

Die weite Verbreitung von Sodinokibi lässt sich unter anderem auf das „Ransomware as a Service“ (RaaS)-Geschäftsmodell zurückführen. In diesem Modell wird die Software gegen einen Initialpreis bereits auf das angedachte Opfer, wie zum Beispiel das Netzwerk einer Firma, zugeschnitten. Der Auftraggeber benötigt nur minimale Programmierfähigkeiten, um die Ransomware einzusetzen. Sollte der Angriff erfolgreich sein und mit einer Lösegeldbezahlung enden, erhalten die Entwickler zusätzlich einen 20-30%igen Anteil des bezahlten Betrages. Dadurch entstehen Vorteile für sowohl die Entwickler als auch die Auftraggeber. Die Entwickler erhalten unabhängig von dem Erfolg des Angriffes immer eine Abfindung. Zusätzlich steht der Auftraggeber oft in engerer Verbindung mit dem angedachten Opfer, wodurch dieser Insiderinformationen liefern kann, was die Wahrscheinlichkeit für den Erfolg der Attacke steigert und wiederum zur Lösegeldprovision der Entwickler führt. Der Vorteil für den Auftraggeber liegt vor allem darin, dass kaum Programmierfähigkeiten notwendig sind. Des Weiteren ist die

Software durch die mögliche Lösegeldprovision leistbarer und die Wahrscheinlichkeit eines erfolgreichen Angriffs steigt durch die erfahrenen und routinierten Entwickler weiter an. Insgesamt ist RaaS für Entwickler als auch Auftraggeber eine Win-Win-Situation. (Meland, Fahmy Bayoumy, & Sindre, 2020)

Ein weiterer Grund für die hohe Beliebtheit von Sodinokibi ist unter anderem die Verwendung bzw. schnelle Adaptierung von Zero-Day-Exploits. Beispielsweise konnte im Falle einer Oracle-Sicherheitslücke im April 2019 nachgewiesen werden, dass Sodinokibi eine Sicherheitslücke in der „Oracle WebLogic" bereits am 17. April für illegale Zugriffe und Verschlüsselungen verwendete. Das Notfall-Patch seitens Oracle wurde erst am 26. April zur Verfügung gestellt. Dadurch waren sämtliche Systeme mit „Oracle WebLogic" für zumindest neun Tage höchst gefährdet. (Cadieux, Grady, Schultz, & Valites, 2019)

Es wird davon ausgegangen, dass im Jahr 2020 allein durch Sodinokibi über 123 Millionen US-Dollar „erwirtschaftet" und über 21,6 Terabyte an Daten gestohlen wurden. Es ist für viele Angreifer ein sehr rentables Geschäft, da gerade bei unvorbereiteten Unternehmensnetzwerken die Lösegeldzahlung oft der einzig realistische Ausweg für Firmen ist. Die Entdeckung und Ausnutzung von Zero-Day-Exploits ermöglichen es, dass sogar gut gewartete und abgesicherte Systeme Opfer von Ransomware-Attacken werden, obwohl diese verhältnismäßig selten stattfinden. Zero-Day-Exploits könnten auch als ein goldener Schlüssel zu einem System bezeichnet werden, wobei diese gerade in der heutigen Zeit immer seltener auftreten. Wesentlich häufiger ist eine vermeidbare Sicherheitslücke an einem erfolgreichen Ransomware-Angriff schuld, weswegen im nachfolgenden Kapitel genau auf aktuelle sicherheitstechnische "Best Practices" und Standards eingegangen wird. (Singleton, 2021, S. 8-9)

2.1.3 Allgemeiner Angriffsprozess

In den folgenden Kapiteln wird auf mehrere Schutzmaßnahmen gegen einen Cyber-Angriff eingegangen, wobei es im Sinne der Prävention bzw. Schadensminimierung relevant ist, darauf zu fokussieren, zu welchem Zeitpunkt einer Cyber-Attacke die einzelnen Maßnahmen Wirkung zeigen.

Abbildung 4: Ransomware-Prozess (shorturl.at/djvMZ)

Als Beispiel für einen Cyberangriff wird, wie in Abbildung 4 zu sehen, ist auf einen Ransomware-Angriffsprozess eingegangen. Dieser Prozess ist auch zum Großteil bei anderweitigen Angriffen wiederzufinden, da in den meisten Fällen nur das Endergebnis unterschiedlich ist. Sowohl im Falle eines Datendiebstahls als auch bei einem Ransomware-Angriff probieren die Angreifer

zunächst Zugriff auf das System zu bekommen, auch wenn das Ziel unterschiedlich ist. (Thomas & Galligher, 2018)

Ein Ransomware-Angriff kann in 5 Phasen unterteilt werden. Diese sind die Infizierungsphase („Infection“), die Zustellungsphase („Delivery“), die Backup-Angriffsphase („Backup Attack“), die Verschlüsselungsphase („Encryption“) und die Benachrichtigungsphase („User Notification“).

Infizierungsphase

Zu Beginn jeder Cyber-Attacke ist es notwendig, dass auf dem Zielgerät eine „bösartige“ Datei ausgeführt wird, damit weitere Schadsoftware in das System gelangen kann. Dies kann durch Phishing-Mails, wo ein User auf einen falschen Link klickt oder auch über ein „Exploit-Kit“, welches Schwachstellen im System ausnützt, geschehen.

Zustellungsphase

In diesem Prozessabschnitt wird die eigentliche Ransomware durch die in der ersten Phase entstandene Lücke in das System geschleust. Zusätzlich werden erste Prozesse angestoßen, um gegen etwaiges Handeln von Usern oder anderen Programmen vorzugehen. Dadurch wird z. B. ermöglicht, dass die Ransomware auch nach einem Neustart der Hardware weiterarbeitet.

Backup-Angriffsphase

In dieser Phase greift die Ransomware alle aufgefundenen Backups des Systems an. Dies dient dazu, dass das betroffene System nicht einfach zurückgeholt werden kann und so die Lösegeld-Zahlung als einziges Mittel zur Systemwiederherstellung bleibt.

Verschlüsselungsphase

Nach der Entfernung aller Backups beginnt die Malware das gesamte System zu verschlüsseln. Dies geschieht mit Hilfe von komplexen Verschlüsselungs-Verfahren wie z. B. dem „Advanced Encryption Standard“ (AES). Im Falle von AES wird entweder ein 128- oder 256-Bit-Schlüssel verwendet, die das „Erraten“ des Schlüssels nach heutigen Leistungsstandards absolut unmöglich macht. Sogar bei Einsatz eines der leistungsstärksten Netzwerke der Welt, dem Bitcoin-Netzwerk, würde die Brute-Force-Entschlüsselung 70 Quadrillionen Jahre bei einem AES-128-Schlüssel benötigen. (Tobias, 2012)

Benachrichtigungsphase

Nachdem das gesamte System verschlüsselt und die Backups gelöscht worden sind, werden am Gerät noch Anweisungen bezüglich der Lösegeld-Zahlung hinterlassen. Diese Nachricht kann leicht unterschiedlich aussehen, aber legt dem User bzw. den Administratoren nahe eine Internetseite mit weiteren Instruktionen aufzusuchen. Zuletzt löscht sich die Malware selbst vom System, damit gegen diese im Rahmen einer forensischen Untersuchung schlechter Schutzmaßnahmen gefunden werden können. (Brewer, 2016)

2.2 Maßnahmen zur Prävention

Um IT-Systeme vor Malware zu bewahren, müssen Netzwerke einerseits vor dem Eindringen der Schadsoftware geschützt und Sicherheitslücken geschlossen werden und andererseits der mögliche Schaden minimiert werden. In diesem Kapitel werden Präventionsmaßnahmen behandelt.

2.2.1 Updates

Eine der wichtigsten Maßnahmen zur Prävention von erfolgreichen Cyber-Attacken ist, das System am neuesten Stand zu halten. Dies betrifft in Unternehmensnetzwerken nicht nur Clients, sondern auch Server und Netzwerkinfrastrukturen. Besonders bei bekanntgewordenen Zero-Day-Exploits sind Updates, sofern diese bereits verfügbar sind, eine der wenigen Maßnahmen, um die ausgenutzten Sicherheitslücken zu schließen. (Bilge & Dumitras, 2012)

Gerade bei Clients und Servern, die als Betriebssystem Windows verwenden, sind regelmäßige Updates notwendig und meistens mit geringem Aufwand verbunden. Wie viele Softwaregroßanbieter bietet auch Microsoft einen transparenten Updateplan, sodass sich deren Kunden darauf einstellen und vorbereiten können.

Diese Updates sind in unterschiedliche Kategorien teilbar. Meistens gibt es ein regelmäßiges Hauptupdate, auf das eine gewisse Anzahl an Kleinupdates folgt. In diesem Hauptupdate werden unter anderem Funktionsupdates sowie wichtige Sicherheitsupdates, die eine gewisse Eskalationsstufe nicht überschreiten, ausgerollt. Die Kleinupdates dienen zur Mängelbehebung von etwaigen Problemen, die vom Hauptupdate ausgelöst worden sind und können auch Funktionsvorschauen des nächsten Hauptupdates enthalten. Ursprünglich wurden diese Updates direkt nach der Fertigstellung und Testung ausgerollt, wodurch bei IT-Administratoren immer wieder vermeidbare Stresssituationen aufgetreten sind. Bei Microsoft gibt es seit Oktober 2003 den Patch Tuesday, an welchem immer zum gleichen Zeitpunkt das Update bereitgestellt wird. Dies hat für die Anwender den Vorteil, dass es zu keinen Überraschungen kommt, und für die Entwickler, dass ein klarer Terminplan mit einer definierten Planung möglich ist. (Wilcox & Poulson, 2021)

Für schwerwiegende Sicherheitsmängel wird immer die Option eines Notfallupdates offengehalten. Diese Updates sind ausschließlich für Sicherheitslücken vorgesehen, deren Ausnutzung folgenschwere Konsequenzen nach sich ziehen können.

Im Falle von Windows gibt es z. B. einmal im Monat, normalerweise am zweiten Dienstag eines jeden Monats, das Hauptupdate. Dieser Dienstag ist unter anderem auch als „Patch Tuesday“ bekannt und wird von Microsoft intern als „B“ Update bezeichnet. Des Weiteren gibt es noch „C“ und „D“ Updates, welche allerdings nur zum Testen von zukünftigen Funktionalitäten angedacht sind und keine Sicherheitsupdates beinhalten. Zusätzlich zu diesen drei Update-Typen gibt es ein „Out of band release“, das für die vorhin beschriebenen essenziellen Sicherheitsupdates verwendet wird. (Morrisey, 2021) (Microsoft, 2021)

Die Veröffentlichung dieser Notfall-Patches wird softwareanbieterseitig genauestens auf deren Notwendigkeit analysiert und kann unter anderem folgende Überlegungen beinhalten:

- Ist das vorzeitige Release außerhalb des Updatezyklus auf Grund der weitreichenden und schwerwiegenden Folgen gerechtfertigt?
- Wie weit ist die Sicherheitslücke verbreitet? Wie groß ist die Anzahl der Anwender, die mit Schäden rechnen müssen?
- Wann wurde die Sicherheitslücke entdeckt? Zu welchem Zeitpunkt ist das Patch einsatzbereit und wie weit wäre ein reguläres Release im normalen Updatezyklus entfernt?
- Welche Risiken birgt das vorzeitige Release des Sicherheitsupdates? Könnten dadurch anderweitige größere Schwachstellen auftreten?

Diese Fragen werden unter anderem bei der Entscheidung über die Ausrollung des Sicherheitsupdates mit einbezogen. Wie bereits aus den Fragen entnommen werden kann, handelt es sich bei einem „Out of band release“ um eine Notfallsituation gravierenden Ausmaßes. Die Ausrollung dieser Updates kann durch Zero-Day-Exploits und besonders gefährliche Viren, Trojaner oder andere Malware gerechtfertigt sein. Ohne diese Updates würden Systeme bis zum nächsten Hauptupdate ungeschützt sein, insofern diese auch regelmäßig installiert werden. Sollten diese Hauptupdates oder Sicherheitsupdates außer Acht gelassen werden, kann es zu folgenschweren Zwischenfällen kommen, welche durch verhältnismäßig einfache Maßnahmen verhindert werden hätten können. (ComputerWeekly, 2016)

2.2.2 Firewall-Konfiguration

Firewalls sind Netzwerkkomponenten, die sämtliche eingehende und ausgehende Datenpakete nach definierten Regeln behandeln. Sofern diese Regeln nicht korrekt konfiguriert sind, kann es zu gefährlichen Sicherheitslücken kommen. Genau deswegen sollte auf die Firewall als Kernstück einer jeden IT-Infrastruktur ein genaues Augenmerk gelegt werden. (Voronkov, Iwaya, Martucci, & Lindskog, 2017)

Zusätzlich zum Einsatz der Firewall als Trennwand zwischen Internet und internem Netzwerk dient sie als Einschränkungsmittel in verwalteten Netzwerken. So kann auch über die Firewall der Zugriff auf sensitivere Netzwerkteile, wie in einem Unternehmen z. B. die Personalverwaltung oder die Buchhaltung, eingeschränkt werden. Durch den Einsatz der Firewall zur Regelung eines Unternehmensnetzwerkes kann auch der ungewollte Zugriff auf Systeme und Ressourcen verhindert werden. Des Weiteren bieten moderne Firewalls praktische Sicherheitsfunktionalitäten an, um Netzwerke noch besser abzusichern. (Scarfone & Hoffman, 2009, S. 11-12)

2.2.2.1 Technologien/Funktionalitäten:

Die ursprüngliche Funktionalität von Firewalls nennt sich „Packet-Filtering“. Beim Packet-Filtering werden Datenpakete auf Herkunfts- oder Zieladresse überprüft und je nach eingesetzten Regeln

durchgelassen oder blockiert. Wichtig ist, dass diese Funktionalität nur das einzelne Datenpaket untersucht und mehrere Pakete nicht in Zusammenhang bringt. Geräte, die nur Packet-Filtering unterstützen, werden auch „Stateless-Inspection-Firewalls“ genannt. Dies ist darauf zurückzuführen, dass diese Firewalls den Verbindungstatus der Netzwerksitzung, aus der das Datenpaket kommt, ignorieren. (Bellovin & Cheswick, 2014)

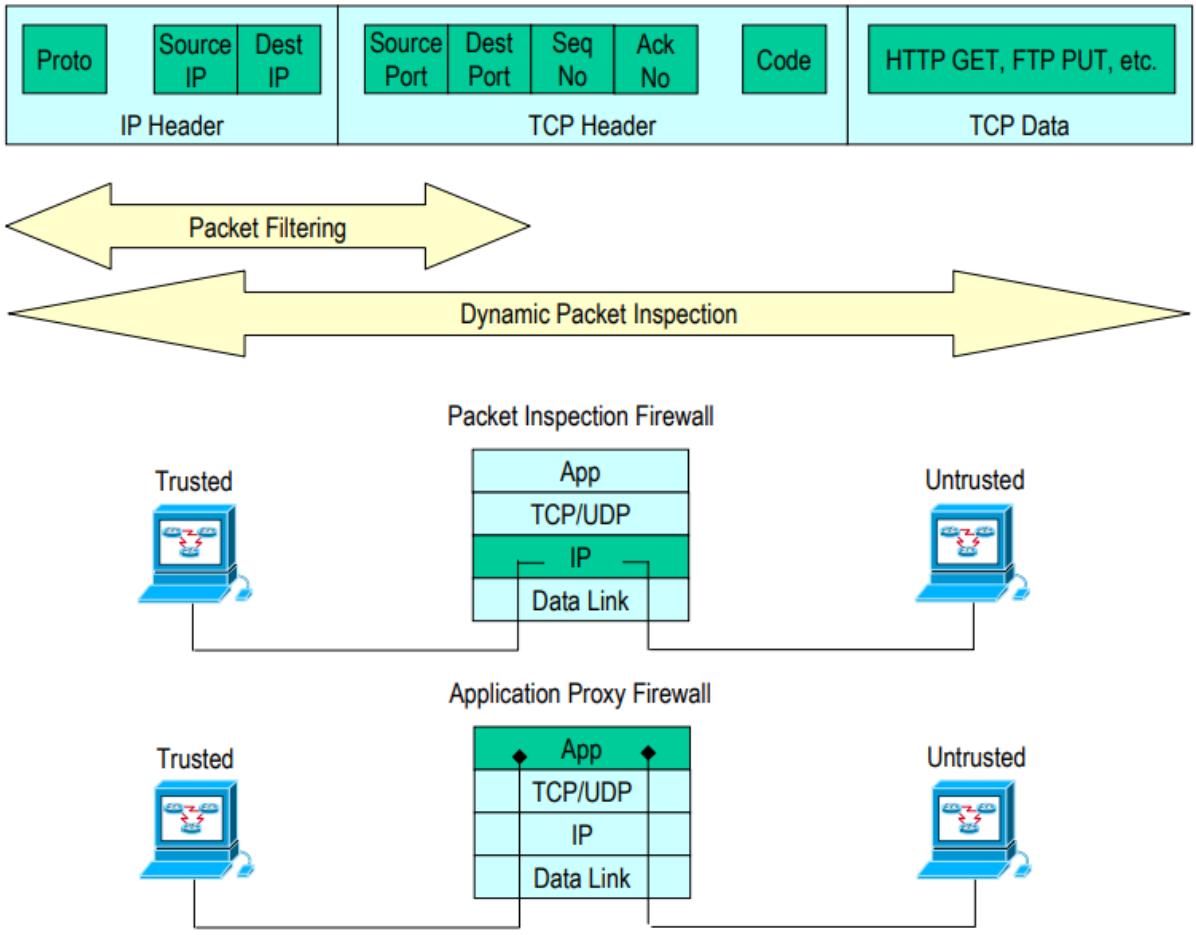

Abbildung 5: Firewall-Arten (t.ly/2q3P)

Eine Erweiterungsstufe der Packet-Filtering Firewall ist die „Stateful-Inspection-Firewall“, bei dieser werden, wie in Abbildung 4 ersichtlich, zusätzlich zu der Herkunfts- und Zieladresse die Verbindungsdaten (z. B. TCP-Sequenznummer) untersucht. Sitzungen (Sessions), die keiner Firewall-Regel entsprechen, werden einfach abgelehnt. Dadurch kann sichergestellt werden, dass nicht ein jedes Programm Daten senden kann. Zuerst muss sich der User bzw. das Programm authentifizieren, wobei untersucht wird, ob korrekte Daten wie z. B. „http“ auf Port 80 gesendet werden. Durch diese Funktion entstehen Kontroll- und Regelmöglichkeiten, die mit einer einfachen Packet-Filtering Firewall nicht umsetzbar wären, und es können z. B. URLs gefiltert und mit Blacklists abgeglichen werden. (Roeckl, 2014)

Die Weiterentwicklung von Stateful-Inspection-Firewalls sind „Application-Firewalls“. Diese überprüfen zusätzlich zu den Elementen der Stateful-Inspection-Firewall auch noch die Aktivitäten innerhalb einer Sitzung. Dadurch kann sichergestellt werden, dass das Verhalten von Programmen wie angedacht ist. So entstehen neue Möglichkeiten zur Regelung von erlaubten

Übertragungen. So kann beispielsweise ein lesender FTP-Zugriff auf einem Server innerhalb der Firewall erlaubt, aber ein schreibender Zugriff verboten sein. (Byrne, 2006)

Eine weitere wichtige Funktionalität von Firewalls ist die Überprüfung von Endgeräten, die sich in das interne Netz verbinden wollen. Diese Überprüfung wird auch „Network-Access-Control" (NAC) genannt und benötigt am Endgerät eine Software, welche mit der Firewall kommuniziert. Mögliche Punkte zur Überprüfung der Endgeräte sind:

- Update-Stand und Konfiguration von Antivirensoftware
- Vergangene Zeit seit letzter Systemüberprüfung
- Version des Betriebssystems
- Sicherheitskonfiguration des Betriebssystems

Nur wenn der den von der Firewall definierten Regeln entsprechende Status vorhanden ist, wird dem Gerät erlaubt mit dem geschützten Netz zu kommunizieren bzw. mit internen Berechtigungen zu agieren. (Serrao, 2010)

Neuere Firewalls setzen zur Sicherung des Netzwerkes nicht nur auf herkömmliche Firewall-Funktionalitäten, sondern auch auf weitere nicht nur Firewall-zugeschriebene Besonderheiten. Dazu zählen beispielsweise Inhaltsfilterung, Spamfilterung, „Intrusion-Detection"-Systeme, Datendiebstahlprävention und Antivirus-Tätigkeiten. Die Vereinigung dieser Eigenschaften wird unter „Unified-Threat-Management" (UTM) zusammengefasst und bietet einige Vorteile als auch ein paar Nachteile. Der größte Vorteil ist das vereinfachte Handling, da sämtliche Systeme auf einer einzelnen Oberfläche zu pflegen sind. Dadurch wird auch die allgemeine Komplexität der Grundinstallation solcher Funktionalitäten verringert, da die einzelnen Setups bereits aufeinander abgestimmt sind. Ein Nachteil bei diesen UTM-Systemen ist, dass wenn möglich alle benötigten Sicherheitseigenschaften von diesem Gerät zur Verfügung gestellt werden sollten, da die Nacheinbindung in eine UTM-Infrastruktur nur schwer möglich ist. Des Weiteren benötigen sämtliche Funktionalitäten die dementsprechenden Ressourcen, welche nicht von einer jeden beliebigen Infrastruktur zur Verfügung gestellt werden können. (Agham, 2016)

Eine immer öfters zum Einsatz kommende Firewall-Variante ist die „Web-Application-Firewall" (WAF). Diese Firewall dient, wie der Name bereits impliziert, dazu, Online-Programme zu schützen. Gerade in der heutigen Zeit von mobilem Webbanking, Trading-Plattformen und immer mächtigeren und komplexeren Online-Applikationen ist es essenziell diese zu schützen. Durch eine WAF kann der gesamte Datenverkehr zu diesem Online-Dienst kontrolliert und geregelt werden, wodurch auch etwaige Programmschwächen umgangen werden können. Herkömmliche Cyber-Attacken wie z. B. SQL-Injektionen, Cookie-Diebstahl, Cross-Site-Scripting und Session-Hijacking können dadurch abgewehrt werden. Das Regelmodell einer WAF wird meistens nach einem von zwei Security-Modellen aufgebaut. Es gibt den positiven Ansatz, bei welchem nur Datenpakete durchgelassen werden, die den definierten Regeln entsprechen, und den negativen Ansatz, wo nur Datenverkehr, der den Regeln entspricht, geblockt wird. Vom Prinzip her ist dies ident mit Whitelisting (positiver Ansatz) und Blacklisting (negativer Ansatz) in anderen IT-Sicherheitskontexten. (Clincy & Shahriar, 2018)

2.2.2.2 Netzwerkarchitekturen

Die Firewall stellt in einem jeden Netzwerk ein absolutes Kernstück der Infrastruktur dar. Auch wenn durch die oben erwähnten Funktionalitäten der Leistungsumfang einer Firewall die ursprünglichen Anforderungen weit überschreitet, erfüllt sie noch immer ihren eigentlichen Zweck, nämlich unerlaubte Zugriffe in das interne Netz zu verhindern.

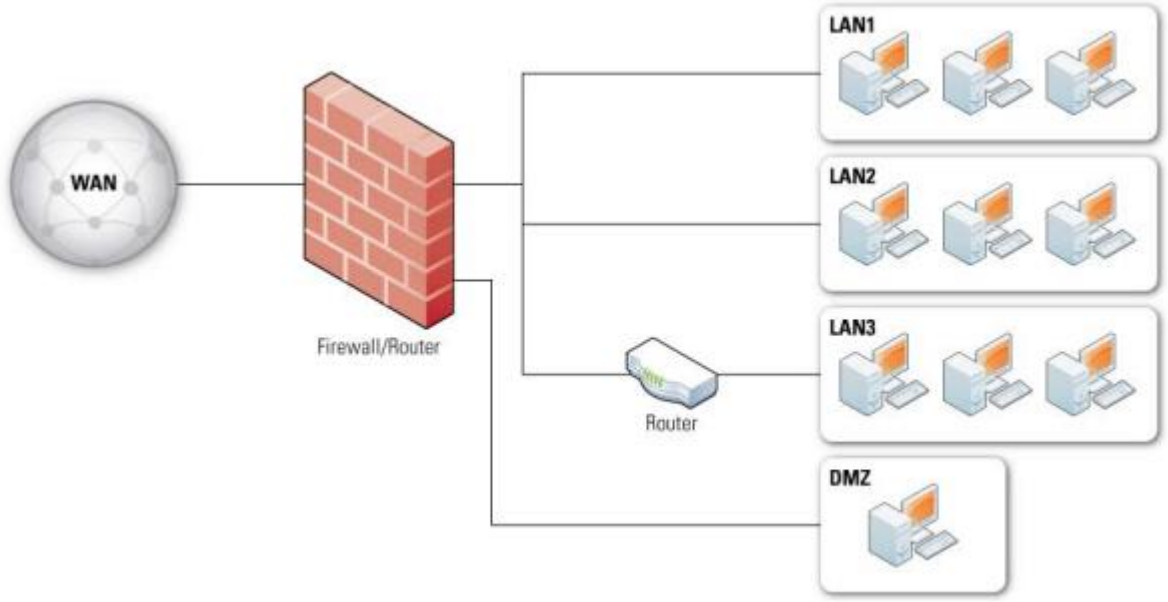

Abbildung 6: Visualisierung einer möglichen Netzwerkinfrastruktur (t.ly/U4LD)

Genau aus diesem Grund wird die Firewall, wie in Abbildung 5 ersichtlich, als Schnittstelle zwischen internem und externem Netz eingesetzt. (Hunt, 1998)

Zusätzlich kommt bei diesem beispielhaften Netzwerk eine DMZ zum Einsatz. DMZ steht für „Demilitarized-Zone“ und bietet den IT-Infrastrukturen Möglichkeiten anspruchsvollere Netzwerkszenarien, unter Bedacht vom Sicherheitsgedanken, abzubilden. Geräte oder Server in einer DMZ unterliegen anderen Firewall-Regeln als die netzwerkinternen Geräte. Gerade die Services, die in einer DMZ angesiedelt sind, sollen von außen leichter erreichbar sein und können notwendige Daten vom internen Netz anfordern. Mögliche Dienste einer DMZ sind:

- DNS Server
- FTP Server
- Mail Server
- Proxy Server
- Web Server

Zu beachten ist, dass im Vergleich zu einer rein netzinternen Kommunikation der gesamte Datenverkehr über die Firewall geht und bei Rückfragen ins interne Netz wieder gefiltert und kontrolliert wird. Je nach Netzwerkkomplexität können auch mehrere Firewalls vorhanden sein, wobei diese meistens eine Verbindung in das äußere Netz und mehrere in unterschiedliche interne Netzwerke haben. (Iskandar, Virma, & Saleh Ahmar, 2018)

In den meisten Hochverfügbarkeits-Netzwerken kommen auch „High-Availability“ (HA) Firewalls zum Einsatz. Dies bedeutet, dass am gleichen Netzwerkknotenpunkt zwei idente miteinander synchronisierte Firewalls im Einsatz sind.

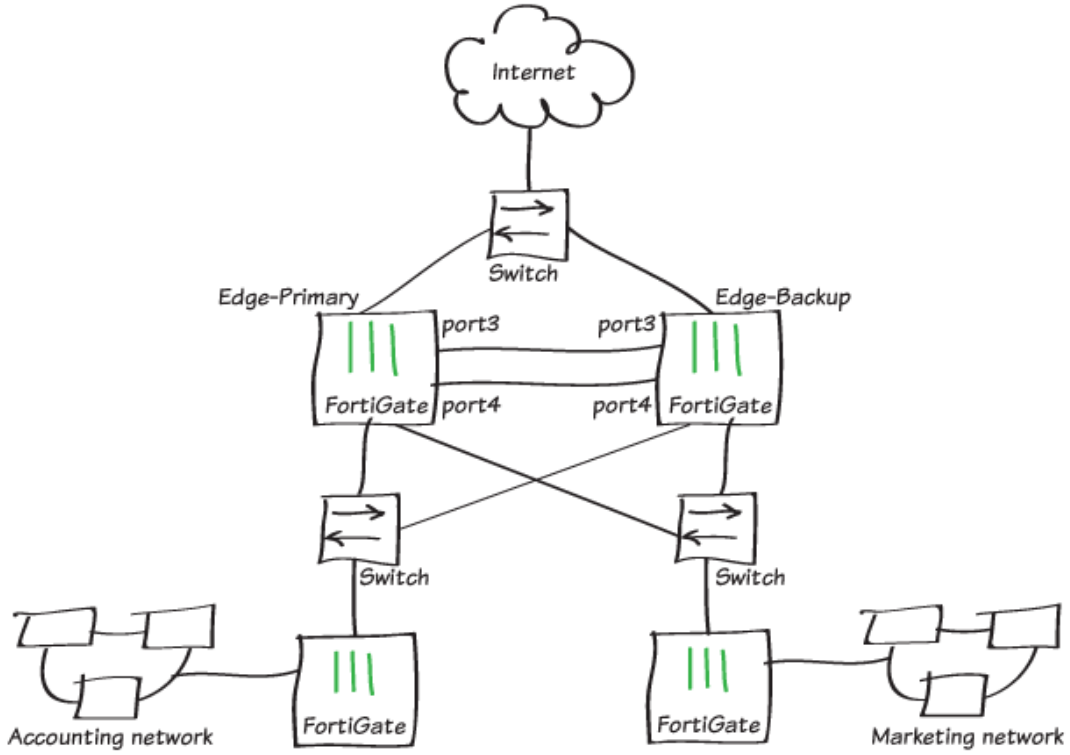

Abbildung 7: Beispiel eines HA Firewall Setups (t.ly/s8QX)

Die Kommunikation zwischen den zwei Firewalls findet auf dafür speziell konfigurierten Ports statt, wodurch beim Ausfall einer Firewall der gesamte Datenverkehr über die Backup Firewall geleitet wird. Im besten Fall bekommen die User außer einer minimalen Verbindungsunterbrechung nicht einmal mit, dass eine der wichtigsten Netzwerkkomponenten einen Totalausfall hat. Je nach angebotenen Diensten bzw. Tätigkeiten im Netzwerk kann es Sinn machen ein Hochverfügbarkeitsnetz aufzubauen. Eine Bank wird zum Beispiel eher dazu tendieren eine Hochverfügbarkeitsarchitektur einzusetzen als eine Marketingfirma. (Cisco, 2021)

2.2.2.3 Policies

Die Firewall-Regeln/Policies definieren, wie Daten, die zur Firewall kommen, behandelt werden. Wie im Unterkapitel Technologien/Funktionalitäten beschrieben, kann eine Firewall weitaus komplexere Regeln durchsetzen als Vorgaben, die nur Herkunfts- und Zieladressen beachten. Filterungseigenschaften von Firewalls sind unter anderem:

- IP-Adressen (Herkunfts- und Zieladresse)
- Ganze Adressbereiche (bei Zieladressen)
- Protokolle (HTTP, HTTPS, FTP usw.)

- Applikationen
- Inhaltarten (aktiver Inhalt, statischer Inhalt)

Um die korrekten Regeln einzuführen, sollte zunächst eine allgemeine Umstands- und Risikoanalyse stattfinden. Nur so kann sichergestellt werden, dass die Regeln so einschränkend wie möglich und so offen wie notwendig sind. Im Allgemeinen ist ein positiver Regelansatz, sofern technisch sinnvoll und möglich, empfehlenswert. Dies würde bedeuten, dass z. B. zu einer gewissen IP-Adresse sämtlicher Datenverkehr, außer für die definierten Ausnahmen, blockiert wird. (Cheng, Wang, Wang, & Wang, 2011)

2.2.2.4 Planung und Implementierung

Die Einführung bzw. Planung einer Firewall kann je nach Unternehmensumständen eine durchaus komplexe und herausfordernde Aufgabe sein. Seitens des „National Institute of Standards and Technology“ (NIST) gibt es eine phasenbezogene Step-by-Step-Anleitung zur erfolgreichen Implementierung einer Firewall in ein Unternehmensnetzwerk.

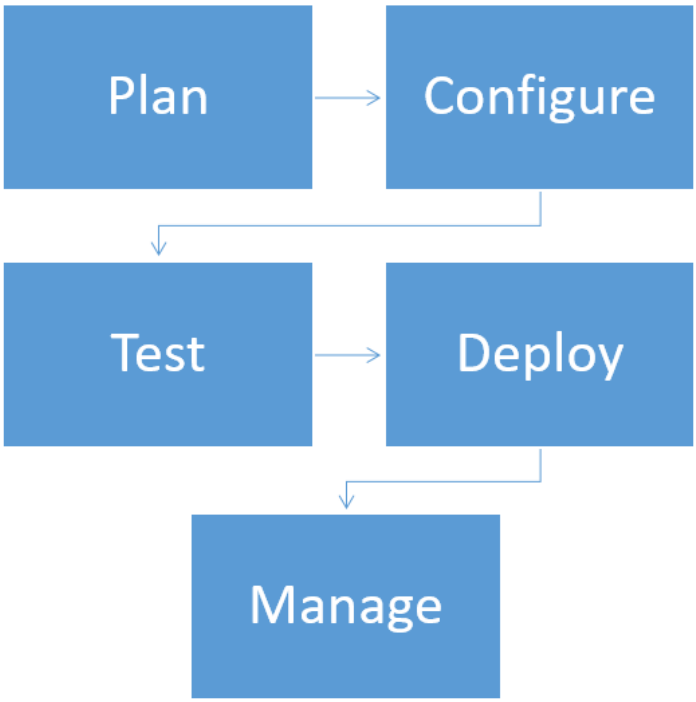

Abbildung 8: NIST Firewall-Implementierungsprozess

Wie in Abbildung 8 zu sehen ist, wird die Einführung einer Firewall laut NIST in die fünf Phasen „Plan“, „Configure“, „Test“, „Deploy“ und „Manage“ unterteilt.

Die Planungsphase besteht, wie oben bereits kurz beschrieben, initial zunächst aus einer Risikoanalyse. In dieser sollten nicht nur die Gefahren für das System und die Schwachstellen im derzeitigen System analysiert, sondern auch der mögliche Schaden, der durch einen Systemausfall zustande kommen kann, miteinbezogen werden. Zusätzlich sind die zukünftig angedachten und gewünschten Kontrollmöglichkeiten zu beachten.

In der Konfigurationsphase wird sowohl die Hardware als auch die Software installiert und konfiguriert. Darunter fällt nicht nur die Basiskonfiguration der Firewall, denn es wird bereits in diesem Schritt das gesamte Regelkonzept als auch Logging- und Alarm-Funktionalitäten implementiert.

In der Testphase wird die Firewall-Konfiguration überprüft. Dazu sollte eine möglichst realistische Testumgebung zum Einsatz kommen, die sofern möglich dem Produktivnetz gleicht oder zumindest ähnelt. Auch die Simulation eines realistischen Datenflusses ist empfehlenswert, um etwaige Ressourcenengpässe zu identifizieren.

In der Phase der Ausrollung wird die Firewall in das produktive Netzwerk integriert, wobei im Vorhinein der organisatorische Ablauf für möglicherweise auftretende Probleme definiert wird und die User darüber in Kenntnis gesetzt werden. Die Implementierung der Firewall umfasst zusätzlich sämtliche Konfigurationen bei anderweitigen Netzwerkkomponenten, wie z. B. der exponierten Dienste in einer DMZ.

Die Managementphase betrifft sämtliche Tätigkeiten während des Firewall-Betriebs im Produktivsystem. Dazu zählen unter anderem Firewall-Updates, die Erweiterung des Netzwerkes um weitere Dienste, interne Netzwerkänderungen und Policy-Anpassungen. (Scarfone & Hoffman, 2009, S. 32-39)

2.2.3 E-Mail-Absicherung

Durch die vorhin angeführten Sicherheitsmaßnahmen kann bereits ein Großteil der sogenannten „Scan and Exploit"-Attacken abgewehrt werden, allerdings gibt es noch weitere Methoden, um Zugriff in IT-Netzwerke zu bekommen. Wenn alle bekannten Sicherheitslücken gesperrt und der ungewünschte Zugriff von extern nicht möglich sind, besteht für Angreifer immer noch die Möglichkeit sich „einladen zu lassen". Damit sind unter anderem Phishing-Attacken und -Strategien gemeint. Bei Phishing wird versucht über Userfehler Zugriff in das System zu bekommen bzw. die User zu kostspieligen Fehlern zu bewegen. Dies kann von der Veröffentlichung des eigenen Passwortes bis hin zu einer getätigten Überweisung auf Grund einer gefälschten E-Mail gehen. Es könnte auch versucht werden den User dazu zu bewegen auf einen „gefährlichen" Link zu klicken, wodurch Trojaner oder andere Schadsoftware auf das System heruntergeladen und eingeschleust werden. Die Hoffnung der Angreifer hierbei ist, dass der Server bzw. der Client des Users auf einem schlechteren Sicherheitsstandard ist als die nach außen exponierten IT-Infrastrukturkomponenten. (Dhamija, Tygar, & Hearst, 2006) (Chandrasekaran, Narayanan, & Upadhyaya, 2006)

Eine der beliebtesten und gleichzeitig je nach Kanälen der Unternehmenskommunikation gefährlichsten Methoden ist Phishing über E-Mail. Allerdings können nicht nur Phishing-Attacken über E-Mail in das Netzwerk kommen, sondern auch Viren, Trojaner und andere Malware. Aus diesem Grund ist auch die Absicherung von E-Mails für die Sicherheit der allgemeinen IT-Infrastruktur essenziell. (Ayodele, Henrydoss, Schrier, & Boult, 2011)

Gerade für Unternehmen ist es wichtig den E-Mail-Kanal möglichst gut abzuschirmen, da dieser eine der größten Schnittstellen zur ungesicherten Außenwelt darstellt. Mittlerweile gibt es eine

Vielzahl an sogenannten E-Mail-Sicherheitsprodukten, die Unternehmen genau bei dieser Problematik unterstützen sollen. (Porter, 2012, S. 38-50)

Die Funktionalitäten dieser Produkte gehen mittlerweile weit über die herkömmlichen Spam- und Malware-Erkennungen hinaus und umfassen unter anderem:

- Sandbox-Umgebungen zur Überprüfung von verdächtigen E-Mails
- Algorithmen zur Erkennung von Spear-Phishing bzw. Whaling-Attacken
- Ausgehende E-Mail-Überprüfungen
- URL-Überprüfungen

(TitanHQ, 2022)

Bei Spear-Phishing als auch Whaling handelt es sich um eine spezielle Art des Phishings. Bei normalen Phishing-Attacken werden E-Mails mit gefährlichen Links oder Anhängen millionenfach ausgesendet. Für die Angreifer besteht zumindest zu Beginn die Hoffnung, dass diese E-Mails durch die E-Mail-Filter durchkommen. Dann muss ein User nur noch das Pech bzw. fehlende Feingefühl haben und die Links aus dieser E-Mail öffnen und schon könnte es je nach dahinterliegendem Sicherheitskonzept für die Angreifer spannend werden.

Beim Spear-Phishing wiederum werden seitens der Angreifer nicht auf gut Glück irgendwelche E-Mails ausgeschickt, sondern diese gezielt auf Unternehmen bzw. Personen angepasst. Whaling ist noch etwas spezifizierter und fokussiert sich auf hochrangige Mitarbeiter bzw. Manager in Unternehmen. (Caputo, Pfleeger, Freeman, & Johnson, 2014)

Sandbox-Umgebungen sind physische oder virtuelle Umgebungen, in denen fragwürdige Softwarekomponenten bzw. E-Mail-Anhänge geöffnet und analysiert werden können. Fortgeschrittene Malware kann erst nach einer bestimmten Zeit oder durch gewisse Tätigkeiten des Users aktiviert werden. Dadurch besteht die Gefahr, dass diese Malware bei initialen Scans von Virenschutzprogrammen oder E-Mail-Schutzprogrammen unerkannt bleibt. In Sandboxen werden alle möglichen Interaktionen mit der E-Mail oder dem Programm simuliert und analysiert, ob die Komponenten als Schadsoftware einzuschätzen sind. Sollte das E-Mail tatsächlich schädlich sein und z. B. das gesamte Netzwerk bedrohen, so ist dies durch die Sandbox komplett abgekapselt und es kommt zu keinem Schaden. (Hudson, 2014)

Eine weitere wichtige Funktionalität von E-Mail-Sicherheitsprodukten ist die URL-Überprüfung. Durch die ständige Weiterentwicklung von Virenentdeckungssystemen für E-Mails ist eine weitere beliebte Strategie bei Phishing-Angriffen, in E-Mails nur die Links zu verpacken, die zum Download von Malware oder zu Fake-Seiten führen. Bei der URL-Überprüfung werden genau diese in der E-Mail eingebundenen URLs überprüft und gegebenenfalls blockiert. (Kim, Kim, & Kang, 2018, S. 790-806)

Ein weiterer Aspekt der E-Mail-Sicherheit, den es zu beachten gilt, ist, dass nicht nur die eingehenden E-Mails gescannt, sondern auch die ausgehenden E-Mails überprüft werden sollten. Der Mehrwert dieser Maßnahme kristallisiert sich vor allem bei mit Malware infizierten Systemen heraus. Die Konsequenzen von Malware sind schwer vorherzusagen und oft nicht bemerkbar. So

könnte zum Beispiel ein Bot anfangen im Namen des Unternehmens E-Mails aussenden, wodurch folgende Problematiken auftreten könnten:

- Aussendungen von Malware an bekannte Partnerunternehmen (Spear-Phishing)
- Aussendungen von gefälschten Anweisungen an derzeitige Projektpartner z. B. neues Bankkonto für die Projektfinanzierung (Spear-Phishing)
- Allgemeine Aussendung von Spam-Nachrichten (Phishing)
- Aussendung von Malware an tausende E-Mailadressen (Phishing)

Durch die Spear-Phishing-Methoden kann es zu erheblichen Schäden bei direkten Geschäftspartnern kommen, wodurch auch die Beziehung zwischen den Unternehmen geschädigt werden kann. Die Phishing-Attacken können dazu führen, dass die Unternehmensdomäne auf einer E-Mail-Blacklist landet. Dadurch würde der Großteil des Mailverkehrs blockiert werden, was wiederum zu weiteren Unannehmlichkeiten führt. (Pandove, Jindal, & Kumar, 2010) (Foster, et al., 2015)

Gegen die immer fortschrittlicher werdenden Phishing- und Malware-Attacken über E-Mails kann ein herkömmliches System kaum mehr ankommen. Gerade bei immer realistischer werdenden Spam-Mails können Mitarbeiter immer schwerer unterscheiden, ob es sich bei einem E-Mail um eine harmlose Nachricht oder um einen gefährlichen Angriff handelt. Der Einsatz von spezifischen E-Mail-Sicherheitsprodukten ab einer gewissen Unternehmensgröße ist empfehlenswert.

2.2.4 WLAN-Absicherung

Eine aus einem modernen Netz nicht mehr wegzudenkende Funktionalität ist das WLAN. Eine undurchdachte Konfiguration von WLANs kann aber schwerwiegende Sicherheitsproblematiken hervorrufen. Beim Einsatz von drahtlosen Netzwerken ist es sinnvoll zu bedenken, welche Möglichkeiten dem User zur Verfügung stehen sollten und wie diese mit dem allgemeinen Sicherheitsstandard im Unternehmen vereinbar sind. So wäre zum Beispiel ein offenes Wifi, von dem beliebige User auf interne Dienste und Server zugreifen können, eine fatale Sicherheitslücke. (Min-kyu, Rosslin, Chang-hwa, & Tai-hoon, 2008)

Ein möglicher Ansatz zur Lösung solcher Problematiken ist die Ausrollung mehrerer drahtloser Netzwerke, wobei von einem komplett offenen WLAN so gut wie immer abzuraten ist. So könnte z. B. für externe User ein eigenes „Gast“-WLAN mit minimalen Sicherheitsberechtigungen verwendet werden. Dieses Netz wird nur für reinen Internetzugang konfiguriert und hat keinerlei Berührungspunkte mit anderen internen Netzwerkdiensten. (Souppaya & Scarfone, 2012)

Mitarbeitern mit Firmengeräten steht wiederum ein anderes WLAN zur Verfügung. Eine elegante Art, um dies umzusetzen, ist der Einsatz vom „Remote Authentication Dial-In User Service“, besser unter der Abkürzung RADIUS bekannt. Bei RADIUS handelt es sich um ein „AAA“-Protokoll. Die Buchstaben stehen für Authentifizierung, Autorisierung und Accounting, dies beschreibt auch die Funktionen des RADIUS-Protokolls. (Nakhjiri & Nakhjiri, 2005)

Bei der Authentifizierung wird festgestellt, wer sich überhaupt anmelden will. Dies wird klassisch über Benutzername und Passwort oder auch über Security-Token stattfinden. Sofern der User erfolgreich identifiziert wurde, erfolgt die Autorisierung des Users. Bei der Autorisierung werden dem User die zugeteilten Berechtigungen gegeben, was in einfachster Ausführung z. B. den Zugriff auf Fileserververzeichnisse oder andere interne Dienste gewährleistet. Unter Accounting wird bei Radius eine gewisse Nachverfolgbarkeit des Users verstanden wie beispielsweise das übertragene Datenvolumen oder Zugriffshäufigkeiten. (Luber & Schmitz, 2017)

2.2.5 Endgerät-Absicherung

Die Absicherung von Endgeräten kann je nach Sicherheitsrichtlinien in Unternehmen eine anspruchsvolle Herausforderung sein. Insofern nur firmeneigene Geräte im Netzwerk erlaubt sind, können diese Geräte wie zum Beispiel in Kapitel 2.2.2.1 beschrieben über die „Network-Access-Control“ oder Antivirus-Software überprüft und gesichert werden. (Perakovic, Husnjak, & Remenar, 2012)

Problematischer wird die Absicherung des Systems allerdings bei sogenannten „Bring Your Own Device“ (BYOD)-Geräten. Diese werden von Usern selbst an den Arbeitsplatz mitgebracht und auch für Tätigkeiten in Unternehmen verwendet. Dazu zählen beispielsweise Privattelefone mit Dual-SIM-Karte oder auch private Laptops und Tablets. Diese Geräte besitzen meistens nur werkseitig vorkonfigurierte Sicherheitsprogramme, die nicht den Sicherheitsstandards in Unternehmen entsprechen. (Armando, Costa, & Merlo, 2013)

BYOD-Geräte können für Unternehmen in unterschiedlichen Kontexten gefährlich werden. Einerseits könnten die Geräte mit Malware infiziert sein, die beim Verbindungsaufbau mit dem internen Netzwerk auf die IT-Infrastruktur übertragen wird. Andererseits stellen die Geräte selbst auch ein attraktives Ziel für Angreifer dar. Gerade bei modernen Smartphones und Tablets können durch Synchronisierungen auch sensitive Daten übertragen werden. Bei Mitarbeitern, die externe Tätigkeiten, wie beispielsweise Montageabreiten, für das Unternehmen durchführen, können auf Laptops Pläne oder interne Betriebsdaten liegen.

Eine der großen Herausforderungen bei BOYD-Endgeräten ergibt sich aus der Tatsache, dass diese von den Usern sowohl im Privatbereich als auch Unternehmenskontext genutzt werden. Dadurch besteht nicht die Möglichkeit Sicherheitseinschränkungen im vollen Umfang umzusetzen, da z. B. ein Verbot zur Installation von zusätzlichen Applikationen am Privatgerät der User kaum umsetzbar ist. (Garba, Armarego, & Murray, 2015)

Es gibt mehrere Lösungsansätze für diese Problematik, wobei es keine Pauschallösung gibt. Da die Lösung dieser Thematik unternehmensabhängig ist, kommt meistens eine Mischung der Lösungsansätze auf die Sicherheitsanforderungen der Unternehmen zum Einsatz.

Eine beispielhafte Strategie für mobile Endgeräte wäre der Einsatz von „Mobile Device Management“ (MDM)-Systemen. MDM-Lösungen sind Softwarepakete, die auf Smartphones installiert werden und Sicherheitsrichtlinien durchsetzen. Dies ist für User, welche nur die Standardfunktionalitäten des Telefons benötigen, eine legitime Lösung. Für User, die allerdings

auch privat aktiv auf ihrem Smartphone tätig sind und zusätzliche Applikationen installieren wollen, wird es zu Komplikationen kommen.

Ein vielversprechender Ansatz sowohl für Laptops als auch Smartphones ist die Verwendung von virtuellen Maschinen (VMs). Der große Vorteil bei virtuellen Maschinen ist, dass diese den Firmenkontext vom Privatkontext trennen können. Im Privatgebrauch verwendet der User ausschließlich die „normale“ Oberfläche seiner Geräte und im Firmengebrauch wird ausschließlich in der virtuellen Maschine gearbeitet. Dadurch kommt es zu einer Abtrennung der zwei Systeme, was aber wieder gewisse Nachteile hat. Einer der Grundgedanken beim Einsatz von BYOD-Geräten für Mitarbeiter ist, dass die Informationen bewusst teilweise zusammengeführt werden. So ist z. B. ein Kalender am Smartphone mit sämtlichen Terminen aus dem Privatbereich und der Firma für viele User ein großer Pluspunkt, der bei einer ganz sauberen Trennung durch VMs wieder wegfallen würde.

Wie oben bereits geschrieben, gibt es keine Pauschallösung für diese Thematik, wobei es bei Rücksichtnahme auf unternehmensspezifische Sicherheitsfaktoren zu annehmbaren Kompromisslösungen kommen kann. (Yong, Jinpeng, & Vangury, 2014)

3 MAßNAHMEN ZUR SCHADENSBEGRENZUNG

Wie im vorherigen Kapitel beschrieben, gibt es viele Möglichkeiten, um Netzwerke abzusichern. Allerdings werden Cyber-Attacken immer kreativer und können auch bei einem gut abgesicherten Netzwerk Schäden verursachen. Dies könnte aus technischer Sicht zum Beispiel durch einen Zero-Day-Exploit geschehen oder eben auch durch menschliche Fehler. Aus diesem Grund ist es notwendig und wichtig im Rahmen einer technischen Sicherheitsanalyse nicht nur die Maßnahmen zur Prävention von Schäden zu beachten, sondern auch die Möglichkeiten zur Schadensbegrenzung bei Eintritt eines Sicherheitsvorfalls, welche in diesem Kapitel behandelt werden.

3.1 Sicherung

Wie in Kapitel 2.1.3 aufgezeigt wird, ist der Angriff auf Backups ein essenzieller Bestandteil sämtlicher Ransomware-Angriffe. Backups dienen dazu, ein zerstörtes System mit Hilfe von Sicherungen wieder möglichst schnell funktionsfähig zu machen. Im einfachsten Sinne gelingt dies dadurch, dass zum Beispiel ein mit Malware infizierter und verschlüsselter Server einfach gelöscht und eine Sicherung von einem vorherigen Stand zurückgeholt werden kann. Dies kann in modernen IT-Infrastrukturen innerhalb von wenigen Minuten geschehen. Da dies allerdings mit einem Verlust der Deltadaten seit dem letzten Backup einhergeht, sind Sicherungsrhythmen und Sicherungsarten im Rahmen von Backup Management von großer Bedeutung. (Alani, 2014)

3.1.1 Backup-Strategie

Um den Datenverlust möglichst gering zu halten, ist ein definierter Backup-Prozess von Vorteil. Dabei ist nicht nur die Menge der potenziell gefährdeten Daten, sondern auch die Systemkapazitäten und die Datenpriorität sind auschlaggebend. Eine Backup-Strategie kann je nach Unternehmen und gesicherten Daten variieren. Eine Bäckerei wird zum Beispiel die Daten anders sichern als eine Bank. Genauso werden die Backups für Maschinenpläne bei einem Rüstungsunternehmen einem anderen Sicherheitsstandard unterliegen als sekundäre Userdaten in einem Unternehmensnetzwerk.

Grund dafür sind einerseits der Zeitaufwand, der für ein Backup benötigt wird, als auch die Kosten für die notwendige Infrastruktur. Je nach Sicherheitsanforderungen verändert sich die Backup-Strategie, wobei grundsätzlich zwischen inkrementellen und kompletten Backups unterschieden wird. (Ruofan, Xiaoyan, Javier, Fumio, & Kishor, 2014)

Ein komplettes Backup spiegelt einfach eine vollständige Kopie des gegenwärtigen Standes des Systems wider und bietet für alle weiteren Backup-Varianten die Basis. Das inkrementelle Backup nimmt nur veränderte Daten in das Backup auf. Beide Varianten bieten sowohl Vorteile als auch Nachteile, wobei im realen Umfeld fast immer auf eine Mischform der zwei Varianten gesetzt wird. Bei einem kompletten Backup werden alle Daten gesichert, was je nach Datenmenge ein

zeitaufwendiger und ressourcenintensiver Vorgang sein kann. Dies bietet allerdings den Vorteil, dass die gesamte Datenmenge auf einer einzelnen Sicherheitskopie liegt und so auch dementsprechend einfach zurückgeholt werden kann. Bei einem inkrementellen Backup wird im Falle von einem täglichen Backup auch jeden Tag ein neues Image angelegt. Sollte nun ein Systemausfall vorliegen, muss die Sicherung aus diesen unterschiedlichen Kopien vereint werden. Ein Standardsicherungsrhythmus für Unternehmen ohne besondere Anforderungen, aber durchaus größeren Datenmengen, wäre zum Beispiel ein Komplett-Backup am Wochenende, wo die notwendigen Systemressourcen frei sind, und inkrementelle Backups in den Nächten unter der Woche, um potenziellem Datenverlust vorzubeugen. (Nelson, 2011, S. 2-7)

Je nach Backup-Strategie können dann die Daten der vorherigen Woche beibehalten, gelöscht oder ausgelagert werden. Ein realistisches Szenario dabei ist, dass zumindest in den ersten zwei Wochen die inkrementellen Backups beibehalten und erst nach einer gewissen Zeit gelöscht werden. Die Stände der kompletten Backups werden in der Regel etwas länger beibehalten, wobei auch hier mit der Zeit auf immer größere Abstände übergegangen wird. Die ersten drei Monate gibt es so zum Beispiel die wöchentlichen Backups, danach nur noch 14-tägige Sicherungen und nach 6 Monaten nur ein monatliches Backup. Das Ziel dabei ist vor allem eine Balance zwischen Speicherplatzverbrauch und Datensicherheit zu finden. (Nakamura, Nakayama, & Nakagawa, 2009)

3.1.2 Backup-Sicherheit

Ein weiterer wichtiger Aspekt bei der Sicherung ist die Sicherheit der Backups selbst. Wie in Kapitel 2.1.3 beschrieben, wird bei Ransomware-Attacken explizit darauf abgezielt die vorhandenen Backups zu zerstören. So soll eine Wiederherstellung der Daten erschwert und ohne Lösegeldzahlung quasi unmöglich gemacht werden. Aus diesem Grund ist es bei Backups absolut essenziell auch auf die Sicherheit dieser zu achten. (Wu & Li, 2014)

3.1.2.1 Lokales Backup

Unter einem lokalen Backup sind alle Sicherungsvarianten zu verstehen, welche im eigenen lokalen Netzwerk gespeichert werden. Hierzu zählen sowohl reguläre Sicherungsserver als auch explizite Offline-Backup-Varianten.

Zu den Vorteilen von lokalen Backups zählen:

- Basis-Sicherheit: Die Daten liegen im eigenen internen Netz, das bereits durch eine Firewall und weitere Sicherheitsmaßnahmen geschützt ist.
- Lokale Verfügbarkeit: Die Daten stehen jederzeit zur Verfügung und sind nicht von externen Faktoren abhängig, wie etwa einem Internetzugang.
- Zeitnahe Daten-Rückholung: Da die Daten lokal gespeichert sind, können die Daten mit vollen lokalen Netzwerkkapazitäten zurückgeholt werden.

Zu den Nachteilen zählen unter anderem die erhöhten Anschaffungskosten, erhöhte Aufwände bei der lokalen IT-Abteilung und eine erhöhte Anfälligkeit gegenüber Ransomware-Attacken im Vergleich zu Cloud-Backups. (Nath, 2022)

3.1.2.2 Cloud-Backup

Cloud-Backups sind Backups, die, wie der Name bereits impliziert, online bei einem Serviceanbieter gelagert werden. Online-Backups bieten sämtliche Standardvorteile der Cloud wie zum Beispiel flexible Ressourcenerweiterung und niedrige Anschaffungskosten. (Marks & Lozano, 2010)

Zusätzliche Vorteile von Cloud-Backups sind:

- Erhöhte Sicherheit des Speichermediums: Die Daten sind auf mehreren High-End-Speichersystemen gesichert und stehen immer online zur Verfügung.
- Ressourceneffizienz: Das Unternehmen muss nur für die gemieteten Ressourcen zahlen und nicht für in etwa einen ganzen Server.
- Erhöhte Datensicherheit: Die Cloud-Anbieter sind für einen adäquaten Sicherheits- und Patch-Standard der Server verantwortlich. Zusätzlich sind bei einer großen Serverfarm auch die dementsprechenden Ressourcen bezüglich der Serversicherheit abgestellt, sodass aktuelle Sicherheitsprotokolle umgesetzt werden. Dazu zählen unter anderem die „End-to-End“-Verschlüsselung, die permanente Verschlüsselung von ruhenden Daten und komplexe Zugriffsmechanismen.

Zu den Nachteilen bei dieser Art des Backups zählen unter anderem Bandbreiten-Beschränkungen, die zu langsamen Backups- und Wiederherstellungsvorgängen führen können, die Internetabhängigkeit und die eingeschränkte Kontrolle über die Daten. (Obrutsky, 2016) (Kulkarni, Sutar, & Gambhir, 2012) (Nath, 2022)

3.2 Netzwerksegmentierung

Um Angriffe möglichst früh zu entdecken beziehungsweise aufhalten zu können, ist eine durchdachte Netzwerkarchitektur notwendig. Durch eine wohlüberlegte Netzwerksegmentierung können Angriffe in einem Subnetz gehalten und bestenfalls sogar entdeckt werden, bevor größerer Schaden entsteht. Die Hauptbegrifflichkeiten und Vorteile eines aufgesplitteten Netzes werden in diesem Unterkapitel erklärt und hervorgehoben.

3.2.1 Defense in Depth

Unter Netzwerksegmentierung wird die Aufsplittung eines großen internen Netzwerks in mehrere kleine Netzwerke verstanden. In unsegmentierten Netzwerken kontrollieren Firewalls nur den Datenverkehr, der von extern zu den Clients kommt. Dies führt dazu, dass im Falle einer erfolgreichen Malware-Attacke das gesamte Netzwerk angreifbar ist. In herkömmlichen Netzen

sind Subnetzunterteilungen meistens durch die Notwendigkeit für gewisse Dienste entstanden, ohne dass dabei ein Sicherheitsgedanke zu Grunde gelegen ist. Oftmals ist die Netzunterteilung schon deswegen notwendig, damit ältere Hardware, die im Netzwerk liegt, nur unter einer bestimmten Konfiguration überhaupt funktionsfähig ist. So können Programme spezielle Ports zur Kommunikation nach außen oder auch spezifische Berechtigungen im internen Netz benötigen. (Wagner, Şahin, Pena, Riordan, & Neumayer, 2017)

Die Netzwerksegmentierung ist Teil der „Defense in Depth"-Strategie. Das Ziel von Defense in Depth ist, dass, auch wenn die erste Sicherheitsbarriere von Angreifern überwunden wurde, noch weitere Sicherheitsmechanismen existieren. In der Fachliteratur wird dabei auch von „Layered Protection" gesprochen. Durch diese zusätzlichen Barrieren soll für Systemadministratoren genügend Zeit gewonnen werden, um etwas gegen die Malware zu unternehmen. Zusätzlich wird das Schadensausmaß durch die erschwerte Verteilung der Malware geringgehalten. (Department of Homeland Security, 2016)

In vielen Teilbereichen von Unternehmensnetzwerken kommt die Netzwerksegmentierung bereits seit Jahren zum Einsatz, nur dass diese anders benannt wird. So ist der Begriff „Demilitarized Zone" (DMZ) jedem IT-Fachpersonal bekannt und stellt ein Anfangsszenario eines segmentierten Netzwerkes dar. Eine DMZ ist ein spezielles Subnetz, das zwischen internem und externem Netzwerk liegt. In diesem Subnetz liegen Server und Dienste, auf welche typischerweise von extern und intern zugegriffen wird. Dies betrifft zum Beispiel den Mailserver oder Webserver. Der Hauptunterschied zwischen der DMZ und dem internen Netz ist, dass der Datenverkehr aus der DMZ bei der Weiterleitung in das interne Netz noch einmal von einer Firewall durchleuchtet wird, da dort problematische Inhalte wahrscheinlicher sind. Bei Defence in Depth geht der Sicherheitsgedanke allerdings noch ein paar Schritte weiter und so wird das interne Netz nochmals aufgesplittet und eine Firewall zwischengeschaltet. (Mhaskara, Alabbadab, & Khedri, 2021)

3.2.2 Implementierungsstrategie

Die Festlegung der Implementierungsarchitektur einer Netzwerksegmentierung ist in kleinen Netzwerken ohne größeren Aufwand möglich. Dabei festzuhalten ist allerdings, dass die Einführung der Netzwerksegmentierung einen kompletten Netzwerkumbau bedeutet, was zu einer Ressourcenbelastung führt.

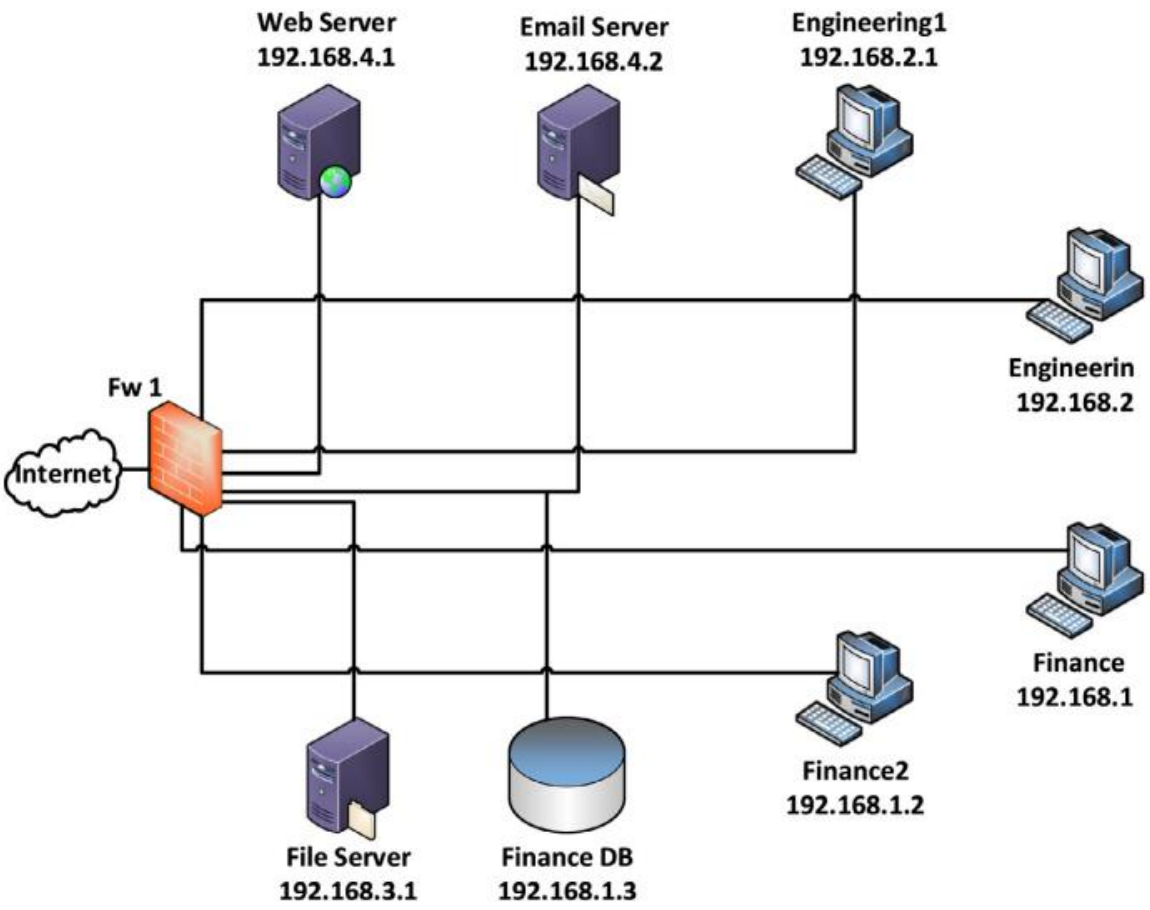

Abbildung 9: Beispielhaftes segmentiertes Netz (t.ly/mu50)

Wie in Abbildung 9 zu sehen ist, kann ein Netzwerk auch mit nur einer einzelnen Firewall durchaus unterteilt werden. Diese Art der Unterteilung hat allerdings konzeptionelle Nachteile und kritische Sicherheitslücken. Grundsätzlich könnte eine einzelne Firewall für ein Unternehmensnetzwerk genügen. Bei dem in Abbildung 9 dargestellten Fall kann es aber zu Sicherheitsproblematiken kommen, da die Firewall für die E-Mail-Server-Funktionalitäten den Zugriff von außen gewährleisten muss. Dadurch könnten je nach Konfiguration der Firewall interne Ressourcen gefährdet sein. So würde es bei einer Standardkonfiguration in diesem Beispiel Sinn machen die Finanzrechner auf die Server, die Finanzdatenbank und den Fileserver zugreifen zu lassen. Dies würde allerdings bei einem erfolgreichen Malware-Befall ermöglichen, dass diese ganzen Systeme lahmgelegt werden. Dabei spielt die sogenannte laterale Verbreitung des Virus eine wichtige Rolle, da es bei dieser Architektur und dieser Konfiguration kaum Schutz durch Angriffe von innen gibt. (Wagner, et al., 2016) (Mhaskara, Alabbadab, & Khedri, 2021)

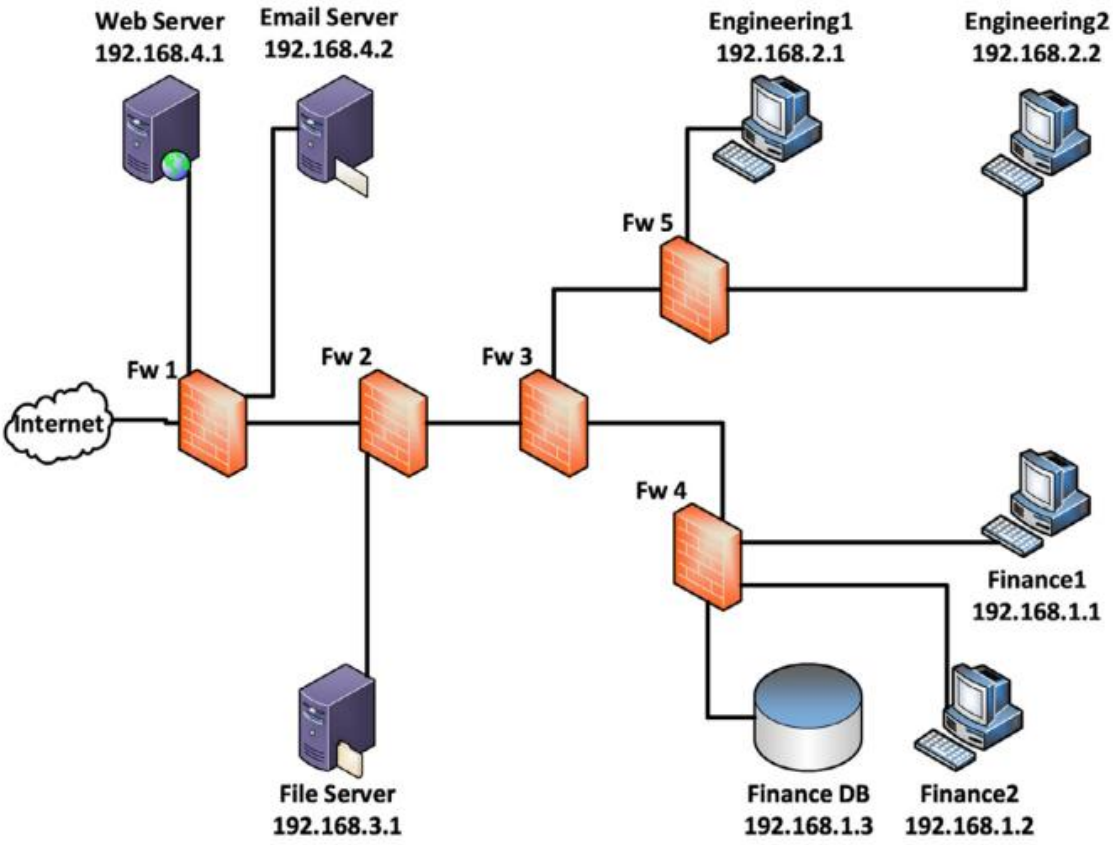

Abbildung 10: Vollständig segmentiertes Netzwerk (t.ly/OCvm)

Ein vollständig segmentiertes Netzwerk kann auch aus einem kleinen unkomplizierten Netz eine komplexe Netzwerkarchitektur entstehen lassen. Wie in Abbildung 10 zu sehen ist, sind nun sämtliche Subnetze durch eine eigene Firewall getrennt. Anhand dieses Beispiels kann auch gut erkannt werden, warum die Begriffe „Defense in Depth“ und „Layered Protection“ verwendet werden. Selbst wenn der Angreifer es schafft, den Web- und E-Mail-Server zu infizieren, sind die kritischen Finanzdaten noch hinter weiteren Firewalls geschützt. Auch bietet diese Architektur einen guten Schutz gegen Angriffe von innen, da die Subnetze durch Firewalls voneinander getrennt sind. In einem Unternehmensnetzwerk würde sich noch ein weiteres Subnetz bezüglich den Backup Servern anbieten, so dass bei einem Ausfall bzw. einem Angriff die Daten schnell wiederhergestellt werden können. (Mhaskara, Alabbadab, & Khedri, 2021)

3.2.3 Software Defined Networks

Wie im vorherigen Kapitel beschrieben, steuert eine gut strukturierte Netzwerkarchitektur einen essenziellen Bestandteil zur Netzwerksicherheit bei. Beim Vergleich von Abbildung 9 zu Abbildung 10 wird allerdings auch klar, dass durch eine Netzwerksegmentierung die Komplexität des Netzwerks zunimmt. Diese ist in kleinen Netzwerken noch überschaubar, aber stellt bei größeren Infrastrukturen eine schwierige Herausforderung dar. Zur Lösung dieser Thematik kommen immer öfters „Software Defined Networks“ (SDNs) zum Einsatz.

Software Defined Networks ermöglichen das gesamte Netzwerk zentral zu konfigurieren und zu überwachen. Dies wird über eine Trennung der Datenebene („Data Plane“) von der Kontrollebene („Control Plane“) bewerkstelligt. Zusätzlich gibt es ident wie bei einem traditionellen Netzwerk noch die Applikationsebene („Applikation Plane“), welche unter anderem die Steuerung der Netzwerkregeln initiiert. (Masoudi & Ghaffari, 2016)

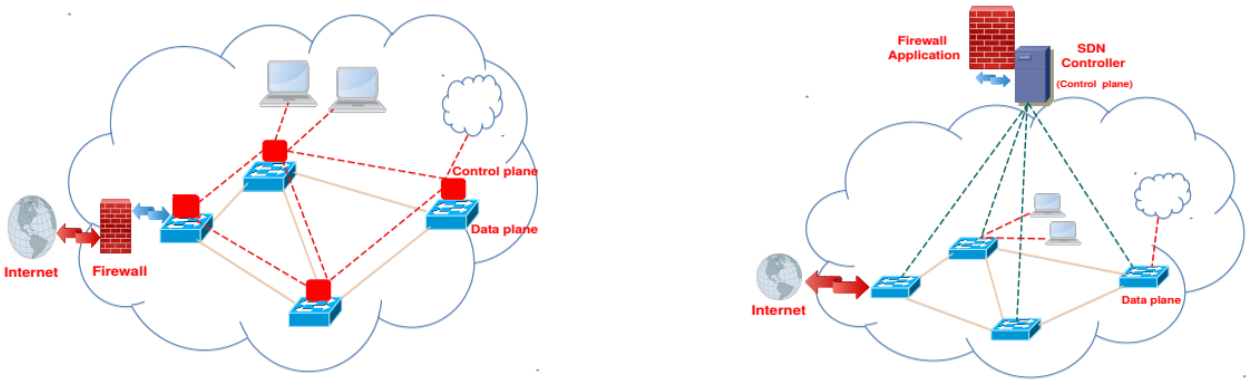

Abbildung 11: Traditionelles Netzwerk vs. SDN (t.ly/A2Pz)

Durch die Aufteilung von Kontroll- und Daten-Ebene wird, wie in Abbildung 11 zu sehen ist, nur noch eine einzelne Kontrollinstanz benötigt. Sämtliche Netzwerk-Konfigurationen können zentral verwaltet und eingesehen werden. Wichtig dabei ist, dass die Firewall bei einem SDN in der Kontroll-Ebene liegt und gegebenenfalls vom SDN-Controller abgetrennt ist. Im Vergleich zu Firewalls in traditionellen Netzen untersucht die Firewall in einem SDN nicht mehr sämtliche Datenpakete, sondern nur das erste Paket eines Datenflusses. Basierend auf dem ersten Datenpaket werden die dementsprechenden Regeln auf den Switches im SDN eingerichtet. Zusätzlich kann dieser zentrale Controller von Usern, Administratoren und Applikationen über APIs angesprochen werden, was zu vielseitigen Programmiermöglichkeiten führt. Die Hauptvorteile von SDNs sind ein zentrales Regelmanagement, ein zentrales Datenflusstracking, Konfliktlösungskonzepte, automatische Prioritätsvergaben und optimierte Skalierungsmöglichkeiten. (Dixit, et al., 2018)

Zentrales Regelmanagement

Das zentrale Regelmanagement bietet die Möglichkeit sämtliche Netzwerk-Richtlinien zentral zu verwalten. Diese Regeln können im Controller von groben Grundregeln bis hin zu fein granulierten Bestimmungen festgelegt und dann auf das Netzwerk verteilt werden.

Zentrales Datenflusstracking

Die korrekte Anwendung der Regeln wird vom Controller über ein Datenflusstracking ermittelt. Um etwaige Netzwerkkonflikte zu erkennen, ist es dabei wichtig, dass der gesamte Datenfluss überwacht und nicht nur das Ankommen des Pakets selbst überprüft wird.

Konfliktlösungskonzepte

Durch die mehrfachen Updatequellen ist es wichtig Regelkonflikten vorzubeugen. Je nach SDN-Anbieter überprüft der Controller die Updateregeln und versucht bei Konflikten alternative Lösungen zu finden.

Automatische Prioritätsvergaben

Wenn es bei einem Regelupdate zu einem unumgänglichen Konflikt kommt, kann eine SDN-Firewall je nach Quelle durch eine manuelle Vorgabe oder eben automatisch die „wichtigeren" Regeln definieren und diese durchsetzen.

Skalierung

In großen Netzwerken besteht die Möglichkeit, dass durch Administratoren oder Applikationen an unterschiedlichen Firewalls Regelkonflikte entstehen. Da die Firewalls nacheinander upgedatet werden, kann es bis zur Problemfindung und Behebung zu Wartezeiten kommen. Auch bei Erweiterung des Netzwerks müssen neue Switches konfiguriert und angepasst werden. Bei einem SDN wird der neue Switch einfach mit den vorhandenen Regeln bespielt und ist sofort einsatzfähig. (Dixit, et al., 2018)

Das SDN bietet aber nicht nur Vorteile, sondern auch neue Herausforderungen bezüglich der Absicherung des Netzes.

Applikationsebene

Die Applikationsebene ist ein essenzieller Bestandteil der SDNs. Sie steuert die Konfigurationen, die in der Kontrollebene vergeben werden. Dadurch gibt es allerdings auch gewisse Sicherheitslücken, die bedacht werden müssen. Die Programme in der Applikationsebene übernehmen indirekt die Berechtigungen aus der Kontrollebene, wodurch diese einen weiteren Angriffspunkt bieten. Ist eine Applikation kompromittiert, gefährdet sie das gesamte Netz. Des Weiteren ist zu beachten, dass an diese Applikationen, die direkt mit dem SDN über APIs kommunizieren, noch weitere Programme angeschlossen sein könnten, welche wiederum ein erneutes Sicherheitsrisiko darstellen. (Kreutz, Ramos, & Verissimo, 2013)

Kontrollebene

Die Kontrollebene und damit der Controller bilden das zentrale Element in einem jeden SDN. Deswegen ist es notwendig diesen besonders zu schützen. Die Applikationsebene stellt wie zuvor beschrieben einen gewissen Risikofaktor dar. Zusätzlich ist der Controller für sämtliche Datenflussentscheidungen verantwortlich. Dies führt normalerweise zu keinen Problemen, weil bei jedem neuen Datenfluss nur das erste Paket aktiv überprüft und an die richtige Stelle weitergeleitet wird. Alle weiteren Datenpakete in diesem Fluss werden dann nach dem gleichen Schema weitergeleitet. Gerade bei dieser initialen Zuteilung kann es zu Engpässen kommen, womit der Controller für „Distributed Denial of Service" (DDOS)-Attacken anfällig ist. Bei einem DDOS-Angriff werden sehr viele neue Datenflüsse generiert, die der Controller nacheinander abarbeiten muss, wodurch es zu Netzwerkstörungen kommen kann. (Naous, Erickson, Covington, Appenzeller, & McKeown, 2008) (Jarschel, et al., 2011)

Datenebene

Die Datenebene selbst fungiert nur als das „dumme" Basisnetz. Dadurch findet auch keine Evaluierung der verteilten Regeln mehr statt, wodurch diese unabhängig von deren Funktionalität zum Einsatz kommen. Eine weitere Angriffsstelle in der Datenebene sind die Switches selbst. Diese können nur eine begrenzte Anzahl an Regeln speichern und verarbeiten, was bei einem

Angriff ausgenutzt werden kann. Die Switches werden durch eine Vielzahl an Regeln überlastet und können diese auch nicht priorisieren, wodurch es zu Komplikationen kommen kann. Zusätzlich ist der Controller die einzige Instanz, welche Regeln für neu eingetroffene Datenpakete vergibt. Dies bedeutet, dass der Switch bis zum Eintreffen der Regel für den neuen Datenfluss sämtliche Daten zwischenspeichern muss, was wiederum zu einer Überlastung des Pufferspeichers führen kann. (Ahmad, Namal, Ylianttila, & Gurtov, 2015)

Insgesamt bieten SDNs eine Vielzahl an Vorteilen, welche gerade in modernen und dynamischen Infrastrukturen gefragt sind. Nichtsdestotrotz ist es bei einer Einführung absolut essenziell, Sicherheitsrisiken zu beachten und etwaige Schritte zur Minimierung dieser zu setzen.

3.2.4 Zero Trust

Zero Trust ist eine neuartige Netzwerk-Architektur, welche die bisherigen Herangehensweisen bezüglich Netzwerkzugriff komplett ändert. Bisher hatten Geräte und User in einem Netzwerk immer eine gewisse Vertrauensstellung. So wurde z. B. allen Usern aus einem internen Netz vertraut und dementsprechend Ressourcen zur Verfügung gestellt. Geräten aus einem externen Netz wurde nicht vertraut und dementsprechend auf nur unkritische Services Zugriff gewährt. Durch diesen Ansatz gibt es allerdings massive Sicherheitsprobleme, sofern ein infiziertes Gerät ins Netz gelangt. Gerade in der heutigen Zeit mit immer mehr mitgebrachten Geräten aus der Home-Office-Umgebung und „Bring your own Device“ Policies kann nicht mehr davon ausgegangen werden, dass sämtliche Geräte im Netzwerk sicher sind. (Chen, Hu, & Cheng, 2019) (Mcginthy & Michaels, 2019)

Das Ziel von Zero Trust ist genau die oben genannten Thematiken zu behandeln und zu lösen. Damit dies möglich ist, gibt es bei Zero Trust einfach keine vertrauten Zonen mehr. Es wird das Prinzip von „Never trust, always verify“ angewandt. Sämtlicher Datenverkehr wird als nicht „vertraut“ eingestuft und muss dementsprechend behandelt werden. (Samaniego & Deters, 2018)

Laut dem NIST gibt es sieben Grundsätze, die bei Zero Trust zu tragen kommen:

1. **Alle Datenquellen und Computerdienste werden als Ressourcen betrachtet.**
2. **Sämtliche Übertragungen sind verschlüsselt unabhängig von Standort des Geräts.** Der Gerätestandort bzw. der Zugriffspunkt macht in Bezug auf die Vertrauensstellung des Geräts keinen Unterschied. Ein Zugriff aus dem lokalen Netzwerk wird gleichbehandelt wie ein Zugriff aus einem fremden Netz. Es werden keine Vertrauensstellungen automatisch vergeben und sämtlicher Datenverkehr soll intern wie extern gleichbehandelt werden. Dies bedeutet, dass auch interne Anfragen durchaus verschlüsselt sind.
3. **Der Zugriff auf individuelle Firmenressourcen (Fileserver usw.) wird pro Sitzung gewährt.** Die Vertrauensstellung des Geräts wird erst bei der Anfrage auf den benötigten Dienst überprüft und bis zum Ablauf der Sitzung freigegeben. Dies gilt nur für den einen individuellen Service, wird ein Zugriff auf eine weitere Ressource benötigt, kommt es wieder zu einer Überprüfung.

4. **Der Zugriff auf die Ressourcen wird durch eine dynamische Richtlinie geregelt. Diese beinhaltet unter anderem die Überwachung des Geräts/des Users in Bezug auf das Verhalten und weitere Faktoren.** Dies bedeutet, dass bei einem Zugriff auf die gewünschte Ressource nicht nur überprüft wird, ob dieses Endgerät mit diesem User auf die Ressource zugreifen darf, sondern auch wie sich der User verhält und ob das Gerät den Sicherheitsstandards entspricht. Wenn ein User z. B. innerhalb von ein paar Sekunden Anfragen auf sämtliche Ressourcen stellt, könnte die Sitzung als mögliche Malware-Attacke gewertet und so der Zugriff verwehrt werden. Es kann auch im Unternehmen speziell schutzwürdige Bereiche, wie etwa die Finanzbuchhaltung, geben. Dort könnte eingestellt sein, dass nur Geräte mit dementsprechendem Updatestand und Schutzsoftware zugreifen dürfen.
5. **Das Unternehmen überwacht und misst die Integrität und den Sicherheitsstatus aller Geräte.** Sämtliche Ressourcen werden durchgehend auf Sicherheitsstandards überprüft und auf Verhaltensauffälligkeiten überwacht. So kann ein unternehmenseigenes Notebook mit Endpoint-Security-Software auf mehr Ressourcen zugreifen als ein mitgebrachtes Gerät.
6. **Alle Authentifizierungen und Autorisierungen sind dynamisch und werden strikt durchgesetzt, bevor der Zugriff erlaubt wird.** Dabei handelt es sich um einen konstanten Kreislauf aus Zugriffsvergabe, Bedrohungen erkennen und einschätzen und die permanente Evaluierung von bestehenden Kommunikationskanälen. Sämtliche User werden überwacht und je nach Richtlinie zu einer erneuten Authentifizierung aufgefordert.
7. **Das Unternehmen sammelt so viele Informationen wie möglich über die Ressourcen, Netzwerkinfrastrukturen und die laufende Kommunikation und nutzt sie zur Verbesserung der Sicherheit.**

(Rose, Borchert, Mitchel, & Conelly, 2020)

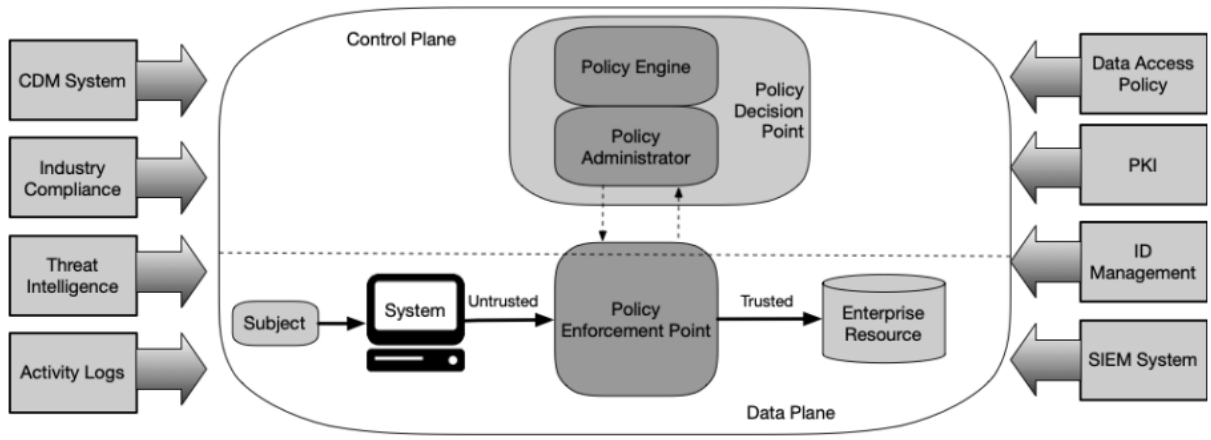

Abbildung 12: Zero-Trust-Netzwerk mit Logikkomponenten (t.ly/-jaB)

Die sieben Grundsätze bieten eine gute Basis für den Aufbau einer Zero-Trust-Architektur. Wie in Abbildung 12 zu sehen ist, geht es im Kern darum, dass niemand ohne Authentifizierung und dementsprechende Autorisierung auf Unternehmensressourcen zugreifen kann. Der User muss

sich am „Policy Enforcement Point“ (PEP) authentifizieren. Der PEP kommuniziert darauf mit dem „Policy Decision Point“ (PDP), wo entschieden wird, ob ein Zugriff auf die Ressource erlaubt wird. Die seitlichen Komponenten in der Grafik stellen unterstützende Systeme dar. Das CDM-System ist z. B. das „Continuous Diagniostics and Mitigation“-System, welches in Punkt 5 der Grundsätze zur kontinuierlichen Überwachung zum Einsatz kommt. (Rose, Borchert, Mitchel, & Conelly, 2020) (Kindervag, Balaouras, & Coit, 2012)

Wie in Abbildung 12 zu sehen ist, wird das Netzwerk auch in eine Kontroll- und Datenebene unterteilt. Da in einer Zero-Trust-Umgebung vom PDP hochkomplexe dynamische Entscheidungen getroffen werden und diese Entscheidungen über das Netzwerkrouting dieser expliziten Sitzung bestimmen, wäre es undenkbar, ein Zero-Trust-Netzwerk ohne ein Software Defined Network aufzubauen. (Dukinfield & Richardson, 2019)

Insgesamt stellt Zero Trust ein vielversprechendes Sicherheitskonzept dar, welches allerdings in der Praxis noch etwas mehr Erfahrungswerte benötigt. Auch die Fachliteratur ist bezüglich dieses Themas noch eher in der konzeptionellen als analytischen Phase. Testkonzepte wurden großteils nur in kleinen Test-Umgebungen umgesetzt. Zukünftig könnte die Zero-Trust-Netzwerk-Architektur durchaus wegweisend sein. (Buck, Olenberger, Schweizer, Völter, & Eymann, 2021)

3.3 Antivirus Suite

Eines der bekanntesten Mittel zur Malware-Eindämmung bzw. -Bekämpfung sind Antivirus-Softwares. Große Anbieter wie Kaspersky, Avast, Avira oder Malwarebytes sind auch für Laien im IT-Fachgebiet keine Fremdbegriffe, wobei deren Funktionsweise, Eigenschaften und Einschränkungen durchaus komplexer sein können, weswegen diese Punkte in diesem Sub-Kapitel genauer beschrieben werden.

3.3.1 Funktionsweise

Die Basis-Funktionalität von Antiviren-Softwares ist das Scannen, Finden und Löschen von Viren am System. Um die Malware erkennen zu können, analysiert der Antiviren-Scan einerseits die Signaturen und andererseits das allgemeine Verhalten der Datei, wenn diese ausgeführt wird.

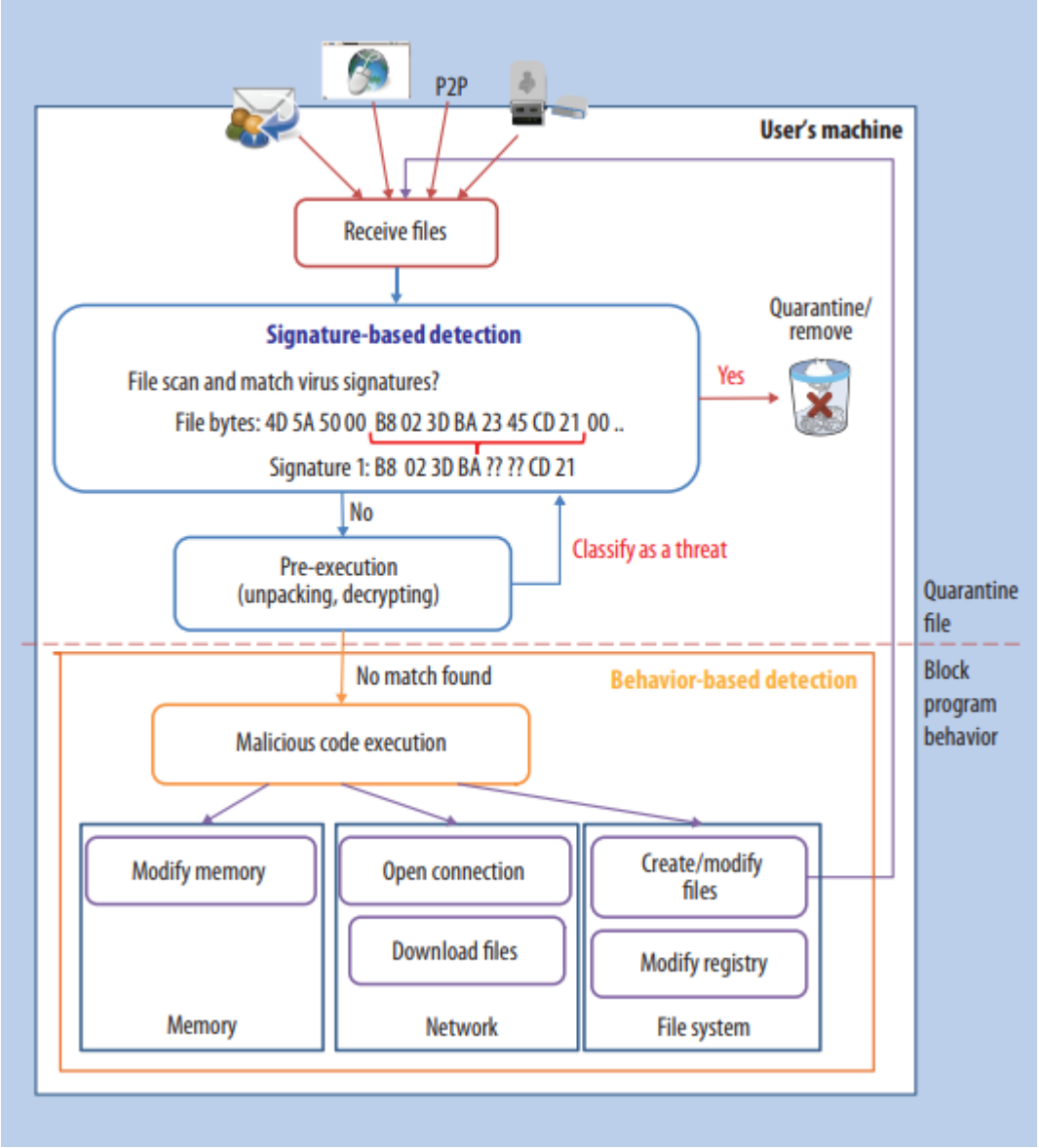

Abbildung 13: Malware-Erkennung und -Behandlung einer Antiviren-Software (t.ly/l8MB)

Wie in Abbildung 12 zu erkennen ist, arbeiten Antiviren-Softwares nach zwei unterschiedlichen Erkennungsmustern. Es gibt die Signatur-Erkennung und die Verhaltensmuster-Erkennung. (Sukwong, Kim, & Hoe, 2011)

3.3.1.1 Signatur-Erkennung

Die Erkennung eines Virus über die Datenmuster-Erkennung (auch Signatur genannt) erfolgt über eine Signaturdatenbank. Dies bedeutet, dass eine neue auf dem Computer angekommene Datei zuerst von der Software gescannt wird. Die Software gleicht das Datenmuster mit allen bekannten Virenmustern in der Datenbank ab und verschiebt die Datei bei einer Übereinstimmung in die Quarantäne, worauf der User entscheiden kann, ob die Datei gelöscht werden soll oder nicht. Dies ist auch von den Einstellungen der Antiviren-Software abhängig. Gerade in kritischen Unternehmensinfrastrukturen wird die sichere Variante gewählt und die Datei direkt gelöscht. (Al-Asli & Ghaleb, 2019)

Wenn die Datei eine Archivdatei („.zip“, „.rar“ usw.) ist, wird die Datei vor der Freigabe von der Software „vorentpackt“ und überprüft. (Sukwong, Kim, & Hoe, 2011)

Gerade über die letzten Jahre kam es immer wieder zu Diskussionen über die Effizienz dieses Ansatzes, da die Malware-Vielfalt immer weiter zunimmt und hochentwickelte Viren zum Teil sogar Virenpermutationen von selbst erstellen, die von Antiviren-Software oft nicht gleich erkannt wird. Die Idee einer zentralen allumfassenden Virendatenbank ist zwar sehr elegant, wird aber realistisch betrachtet zumindest in nächster Zeit nicht umsetzbar sein. Dies bedeutet allerdings nicht, dass die Antiviren-Softwares das bereits vorhandene Wissen ignorieren sollten, wodurch die Signatur-Erkennung auch weiterhin ein essenzieller Bestandteil von Antiviren-Softwares bleiben wird. (Hatem, Wafy, & El-Khouly, 2014)

3.3.1.2 Verhaltensmuster-Erkennung

Die Verhaltensmuster-Erkennung analysiert das Verhalten des Programmes während der Ausführung. Die Virensoftware stuft dann das Programm als harmlos oder schadhaft ein und geht dementsprechend vor. Wenn das Verhalten der Software als schadhaft eingestuft wird, betrachtet die Antiviren-Software das Programm als Malware. Die Ausführung des Programmes wird dann unverzüglich gestoppt und die Programmdatei in die Quarantäne verschoben. Diese Art der Erkennung bietet einen schnellen Schutz gegen eine ausbrechende Malwareinfektion, da bereits im Vorhinein definiert werden kann, welches Verhalten seitens vorhandener Software akzeptabel bzw. inakzeptabel ist.

Dabei gilt auch zu beachten, dass es durch eine zu strenge Konfiguration zu „False-Positive“-Fällen kommen kann, was gerade bei Unternehmen, die im Softwareentwicklungsbereich tätig sind, im Rahmen von Prototypprogrammierungen regelmäßig möglich ist. Im Regelfall lernt die Antiviren-Software die Standardabläufe der unterschiedlichen Programme, wodurch Anomalien schnell auffallen, wenn allerdings neue Software zum Einsatz kommt, gibt es diese angelernten Verhaltensmuster noch nicht und die Antiviren-Software kann nur auf voreingestellte unerlaubte Muster reagieren. (Sukwong, Kim, & Hoe, 2011)

3.3.2 Features

Die Basis-Funktion einer Antiviren-Software besteht aus der Scanfunktion, welche einerseits vom User manuell angestoßen werden kann beziehungsweise in Echtzeit automatisch geschieht.

Die Scansoftware kann auch “Integrity checkers“ einsetzen, die für sämtliche Programme einen Überprüfungscode mit einer Prüfsumme generiert. Wenn die Malware das Programm verändert, ändert sich auch die Prüfsumme, was wiederum zu einer erneuten Überprüfung des Programms führt.

Eine erweiterte Funktion der Scansoftware ist die Emulation einer Systemumgebung, um unsichere Dateien entpacken, ausführen und analysieren zu können. Moderne Malware wird immer mehr durchdacht und passt sich an das Verhalten von Schutzsoftwares an. So schlägt ein jeder Antivirus bei einer heruntergeladenen Datei, welche sofort beginnt, weitere Datenpakete

herunterzuladen, an. Wenn diese Datei allerdings zunächst unauffällig ist, kann sie übersehen werden und über die Zeit Schaden anrichten. Manche Malware überprüft außerdem das System und fängt nur in der passenden Umgebung an zu arbeiten. Um dies simulieren zu können, stellen Antiviren-Softwares Emulationsumgebungen zur Verfügung, in denen unterschiedliche Systeme simuliert und das Softwareverhalten analysiert wird. (Chamorro, Han, & Beheshti, 2012)

Eine weitere Eigenschaft von Antiviren-Softwares ist, dass sie einen Selbstschutz integriert haben. Dies dient dazu, dass ausgeführte Malware auch andere Prozesse beeinträchtigen oder beenden könnte. Damit die Malware nicht einfach den Antivirus-Prozess beendet, werden seitens der Antiviren-Software Schutzmechanismen angewendet. So wird zum Beispiel systemweit der direkte Aufruf von den geöffneten Prozessen in Bezug auf die Antiviren-Software blockiert, damit diese nicht angegriffen werden können. Dabei gilt zu beachten, dass gerade bei unausgereiften Produkten diese Sonderregeln zu großen Sicherheitslücken führen können. (Koret & Bachaalany, 2015, S. 11-13)

Die Notwendigkeit von Antiviren-Softwares ist auch durch andere Sicherheitsmaßnahmen gegeben. So sind im Internet fast alle Übertragungen verschlüsselt, was einerseits sicherheitstechnisch wichtig ist, dass niemand Daten auslesen kann, aber andererseits die Datenüberprüfung seitens der Firewall erschwert. Auch die Firewall hat keine Möglichkeit in verschlüsselte Inhalte hineinzusehen. So kommt das Datenpaket, sofern es von einer genehmigten Quelle kommt, direkt in das System, wo ohne Antiviren-Software die etwaige Malware ausgeführt wird. Weiters noch anzumerken ist, dass Windows bereits eine integrierte Antivirus-Software namens „Windows-Defender“ besitzt, welche zumindest eine Basissicherheit gibt. (McCormack, 2019)

3.3.3 Cloud-Antivirus

Das Scannen und Analysieren von Daten können seitens der Antiviren-Software zu Belastungen führen. Im Falle eines Privatrechners ist dies bei Neugeräten kaum zu spüren, da diese genügend Ressourcen haben. In Firmennetzwerken ist dies aber selten der Fall, gerade essenzielle Server sind in der Regel bereits gut ausgelastet und können durch die Zusatzbelastung der Antiviren-Software an die Grenzen gebracht werden. Aus diesem Grund bieten immer mehr Produkte die Option einer Cloud-basierten Virenüberprüfung an. Die lokale Softwarekomponente stuft die Dateien nur noch rudimentär ein und schickt diese zur Überprüfung in die Cloud. (Oberheide, Cooke, & Jahanian, 2007)

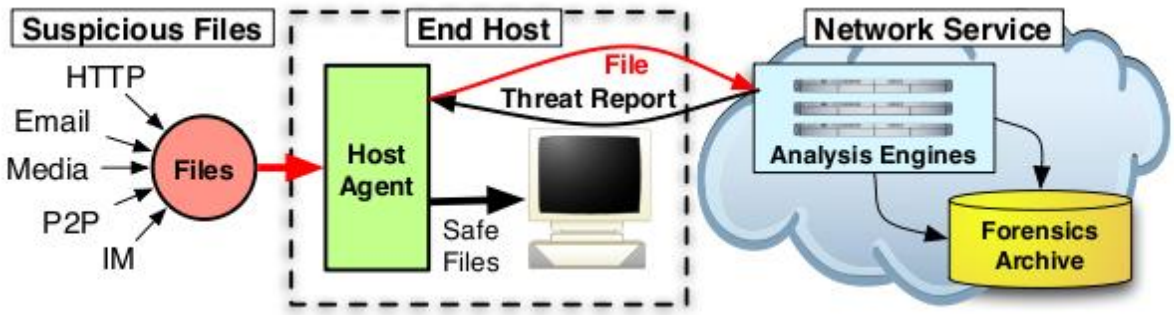

Abbildung 14: Prozess einer Cloud-Antiviren-Software (t.ly/flJc)

Wie in Abbildung 13 zu erkennen ist, wird die Datei, sofern sie als bedenklich eingestuft wird, in die Cloud-Umgebung übertragen und dort untersucht. Dadurch können die klassischen Cloud-Vorteile auch bei der Virenanalyse angewendet werden. Die Ressourcenknappheit kann so umgangen werden und auch bei der Analyse können flexiblere Verfahren angewendet werden. Im besten Fall wird die Datei von einer Vielzahl an Antiviren-Engines durchleuchtet, um so das gesamte Wissen der unterschiedlichen Softwares verwenden zu können.

Wenn solche Viren erkannt werden und noch nicht im Vorhinein bekannt waren, werden bestimmte Erkennungsmarker der Malware in ein forensisches Archiv abgelegt, das zukünftig herangezogen wird. Die Cloud meldet dann an das Endgerät eine Rückmeldung, ob die Datei „OK“ oder eben eine Malware ist, worauf diese gegebenenfalls in die Quarantäne geschoben wird. (Oberheide, Cooke, & Jahanian, 2008)

Zu den genannten Vorteilen gibt es bei Cloud-Systemen auch ein paar Nachteile. Eine lokale Antivirus-Version kann so zum Beispiel wesentlich genauer auf die tatsächliche Systemumgebung eingehen. Die Cloud-Version kann nur mit den mitgelieferten Metadaten arbeiten, welche nicht das lokale System widerspiegeln können.

Ein weiterer Punkt, den es zu beachten gilt, ist, dass der Cloud-Service natürlich von einer funktionierenden Internetanbindung abhängig ist. Sollte diese beeinträchtigt sein, bietet die lokale Komponente der Antiviren-Software keinerlei Schutz.

Zusätzlich erhöht sich die Anzahl der „False-Positive“-Erkennungen, da es bei der Vielzahl an verwendeten Engines in der Cloud zu Fehleinstufungen kommen kann. Durch die erhöhte Entdeckungsrate von Malware erhöht sich auch die „False-Positive“-Rate, was zu Redundanzen und einem größeren Overhead führt.

Insgesamt ist die Cloud-Antiviren-Variante ein gutes Zusatztool zu herkömmlichen Antiviren-Softwares und kann einige Probleme von klassischen Antiviren-Systemen wie die lokale Ressourcen-Belastung beheben. (Agrawal & Wahie, 1016)

3.4 Der menschliche Faktor

Wie in der Einleitung beschrieben, liegt der Schwerpunkt dieser Arbeit auf den technischen Aspekten der Informationssicherheit, weswegen auf den menschlichen Faktor nur in groben Zügen eingegangen wird. Es ist allerdings essenziell zu erwähnen, dass der Mensch in der heutigen Zeit als die größte Sicherheitslücke in einer IT-Infrastruktur angesehen wird. Bereits im Jahr 2000 gibt es Publikationen, die IT-Sicherheit als zusammenhängende Kette aus Verschlüsselungen, Hardware, Software, Netzwerken und Usern betrachten. Und eine Kette ist wie aus dem Sprichwort bekannt nur so stark wie das schwächste Glied. (Schneier, 2000)

Bereits im Jahr 2014 stellte IBM im jährlichen „Cyber Security Intelligence Index“ fest, dass 95 % aller IT-Sicherheitszwischenfälle den menschlichen Faktor als mitwirkendes Element hatten. Hierbei sollte allerdings festgehalten werden, dass es sich nicht nur um User handelt, die auf einen falschen Link in einem Phishing-E-Mail geklickt haben, sondern auch um schlechte Systemkonfigurationen, schwaches Update-Management oder missachtete Userrichtlinien wie z.

B. das Nicht-Abändern des Standardpasswortes bei neuen Usern. Diese Schwachstellen sind unter anderem auch auf fehlenden Support und fehlende Ressourcen seitens der Unternehmen zurückzuführen. Die größte Gefahr beim menschlichen Faktor war trotzdem das „Doppelklicken" auf einen unsicheren Link oder Anhang in einem E-Mail. (IBM Global Technology Services, 2014, S. 3)

Die Hauptgründe für das „Klicken" eines bösartigen E-Mails sind laut einer Umfrage von Tessian folgende:

- Der User war abgelenkt (45 %)
- Die E-Mail hat legitim gewirkt (43 %)
- Die E-Mail kam angeblich von einem hochrangigen Mitarbeiter im Unternehmen (41 %)
- Die E-Mail kam angeblich von einem respektierten Unternehmen (40 %)
- Der User war müde (37 %)

Hierbei gilt auch zu beachten, dass 57 % der befragten User angegeben haben, dass der Arbeitsplatz im Homeoffice größere Ablenkungsfaktoren bietet. Dies dürfte mit ein Grund sein, warum die Ablenkung der User den größten Prozentsatz ausmacht. (Hancock & Tessian, 2022)

Die Möglichkeiten, um das Unternehmen vor etwaigen Userfehlern zu schützen, sind zahlreich, wobei das Security-Awareness-Training als einfache, dafür effektive Maßnahme hervorsticht. Dabei ist es empfehlenswert, dass das Training in regelmäßigen Abständen wiederholt bzw. vertieft wird. Zusätzlich gibt es technische Maßnahmen, die menschliches Fehlverhalten verhindern oder unterbinden können. Diese wären beispielsweise sichere Passwortrichtlinien, verpflichtende Multi-Faktor-Authentifizierung, gut durchdachte Berechtigungskonzepte und Erkennungssysteme für Systemanomalien. Diese Maßnahmen sollen dazu dienen, dass die Wahrscheinlichkeit für menschliches Fehlverhalten sinkt und bei Eintreten dieses Falls der Schaden möglichst geringgehalten wird. (Sarkar, 2012) (Parsons, McCormac, Butavicius, & Ferguson, 2010)

Die Sicherheit ist in der heutigen Zeit ein Grundgedanke in sämtlichen IT-Systemen und kann durch technische Maßnahmen verbessert werden. Die in den vorhergehenden Kapiteln beschriebenen Maßnahmen verhindern nicht nur Angriffe auf die IT-Infrastruktur, sondern schützen auch die User. Ein E-Mail-Sandboxsystem bietet dem System direkt keinen wirklichen Schutz, da ein unbehandeltes E-Mail keinen Schaden anrichten kann. Erst wenn der User das Mail öffnet und dann auf einen gefährlichen Link oder Anhang klickt, startet die Malware-Attacke. Aus diesem Grund ist es unter anderem essenziell die User beim Agieren im System durch technische Maßnahmen zu schützen, wobei diese je nach Wissensstand der User nur eine unterstützende Funktion einnehmen sollten. (Colwill, 2009)

4 EXPERTENINTERVIEWS UND ANALYSE

Um aktuelle Erkenntnisse zu IT-Sicherheitsmaßnahmen zu erhalten und nicht nur auf die bereits vorhandene Literatur einzugehen, wurden im Rahmen dieser Diplomarbeit fünf Experteninterviews durchgeführt. Diese Interviews sollen aktuelle Maßnahmen aufzeigen und die wichtigsten hervorheben. Zusätzlich wird auf die Forschungsfrage und die Hypothesen eingegangen, um diese in Kombination mit der Literaturrecherche zu beantworten.

4.1 Vorgangsweise Interviews

Die Experteninterviews wurden sowohl vor Ort als auch über Remote durchgeführt. Zur Anonymisierung der Experten wurden die Tonaufnahmen transkribiert und Erkennungsmerkmale wie ausgesprochene Namen und Unternehmen ersetzt bzw. ausgenommen.

Die Remote-Interviews wurden mit Hilfe der XBOX Game Bar und die Vor-Ort-Interviews mit Mikrofonen aufgezeichnet. Die Aufzeichnungen wurden dann mit Hilfe von Adobe Premiere Pro transkribiert und manuell nach der Methodik von Dresing & Pehl ausgebessert. Dabei ist es zu erheblichen Aufwänden gekommen, da gerade Fachterminologien für Transkriptions-Programme eine erhebliche Herausforderung darstellen.

Die Experten wurden auf die Interviews mit einem kurzen Vorgespräch vorbereitet und haben den groben Ablauf inklusive den Hauptfragen zur Verfügung gestellt bekommen.

Für einen ordnungsgemäßen Ablauf wurde ein interner Leitfaden erstellt.

Leitfaden Experteninterview	
Begrüßung	
Einstiegsfragen	**Anmerkungen**
Seit wie vielen Jahren sind Sie in der IT bzw. der IT-Sicherheit tätig?	
In wie vielen Unternehmen haben Sie in der Zeit gearbeitet bzw. für wie viele Unternehmen waren Sie in Ihrer Karriere tätig?	
Kurzer Umriss des Themas	
Hauptfragen	**Anmerkungen/Rückfragen**
Frage 1: Welche technischen Maßnahmen sind zur Netzwerkabsicherung Ihrer Meinung nach sinnvoll?	Kurze Erklärung über die Vorteile der genannten Maßnahmen und kurz in die einzelnen Thematiken eintauchen.

Frage 2: Welche der genannten Maßnahmen bieten Ihrer Meinung nach den höchsten Schutz bzw. sind am wichtigsten?	
Frage 3: Wie hoch sind die Einschränkungen für die User durch die unterschiedlichen Maßnahmen?	Bekommt der User was davon mit bzw. stört es ihn beim Arbeiten?
Frage 4: Kann durch diese technischen Maßnahmen ein Netzwerk so gut geschützt werden, dass sogar bei mutwilliger oder grober Fahrlässigkeit der User keine Gefährdung für das Netzwerk entsteht?	Auf Maßnahmen zur Schadensminimierung hinweisen, falls nicht selbst angesprochen.
Frage 5: Bieten durch eine Firewall getrennte Subnetze einen Sicherheitsvorteil?	Wenn ja, welche Vorteile hat man dadurch? Welche Nachteile hat man dadurch?
Frage 6: Bei welchen der angeführten Maßnahmen sehen Sie Ihren Erfahrungen nach bei den meisten Unternehmen Verbesserungspotenzial?	Sowohl auf technische Aspekte als auch auf den menschlichen Faktor abzielen.
Frage 7: Gibt es Ihrer Meinung nach eine Sicherheitstechnologie, die zukünftig technische Sicherheitskonzepte bzw. das allgemeine Denken im Bereich IT-Sicherheit reformieren könnte?	
Informationen, wie es weitergeht	
Verabschiedung	

Tabelle 1: Leitfaden Experteninterview

Die Experten wurden zu den Hypothesen als auch bezüglich der Forschungsfrage wie in Tabelle 1 zu sehen befragt. Die Interviews dauerten zwischen 20 und 35 Minuten und deren Erkenntnisse werden im Folgekapitel ausgearbeitet.

4.2 Analyse

In diesem Kapitel werden die Antworten auf die gestellten Fragen analysiert. Die Fragen werden einer zusammenfassenden Inhaltsanalyse nach Mayring unterzogen und dadurch auf das Wesentliche reduziert. Dies wird unter anderem mit Hilfe der Paraphrasierung und Generalisierung geschehen. (Mayring, 2015, S. 51-55)

4.2.1 Interviewauswertung

In der Interviewauswertung werden die Antworten auf die 7 Hauptfragen analysiert und die Erkenntnisse daraus zusammengefasst.

Welche technischen Maßnahmen sind zur Netzwerkabsicherung Ihrer Meinung nach sinnvoll?

Antwort	Paraphrasierung	Generalisierung
1.1	Es gibt viele Maßnahmen bei vielen Angriffsvektoren vom Kabel bis zur Applikation. Zu beachten sind Computer, Laptop, Antiviren-Softwarestand, Zwei-Faktor-Authentifizierung und User Policies. Im Backend-Bereich benötige ich beispielsweise eine Firewall, Virenscanner und Datensicherung.	Antivirensoftware MFA User Policies Firewall Backup
2.1	Die Maßnahmen sind abhängig von der IT-Infrastruktur und Netzwerkgröße, wobei Firewall, Virenscanner und Backup je nach Szenario die essenziellen sind.	Firewall Backup Antivirensoftware
3.1	Die Firewall ist ein wichtiger Bestandteil der IT-Sicherheit auf mehreren Layern des OSI-Schichtenmodells. Weitere wichtige Punkte sind die Themen Verschlüsselung, Antivirensoftware, Asset-Management, Multi-Faktor-Authentifizierung, Mail-Sand Boxing und Endgeräte-Sicherheit.	Firewall Verschlüsselung Antivirensoftware Asset Management MFA Mail-Sand Boxing Endpoint-Security
4.1	Das Kernstück jeder IT-Sicherheitsstruktur ist die Firewall, wobei auch Thematiken wie Backup-Strategien, Netzwerk-Architekturen und Segmentierungen wichtige Maßnahmen sind. Im Basisbereich geht es auch um WSUS, Mail-Absicherungen, Endpoint-Security und Antivirensoftware.	Firewall Netzwerkarchitektur, Segmentierung Patch-Management Mail-Absicherung Endpoint-Security Antivirensoftware
5.1	Firewall, Netzwerk-Segmentierung, Backup und Antivirensoftware sind neben organisatorischen Maßnahmen wie Schulungen, Business-	Firewall Netzwerk-Segmentierung Backup

	Continuity-Management und Zertifizierungen sinnvoll.	Antivirensoftware

Tabelle 2: Qualitative Analyse Frage 1

Das Thema der technischen Sicherheitsmaßnahmen zur Absicherung von Unternehmensnetzwerken ist breit gefächert. Dementsprechend gibt es auch bei Frage 1 unterschiedliche Antworten. Dabei gilt festzuhalten, dass je nach Spezialisierungsgebiet der Experten die Antworten variieren können. Die Antworten zu Frage 1 sollten als Basisempfehlungen und nicht als Einschränkungen gewertet werden.

Welche der genannten Maßnahmen bieten Ihrer Meinung nach den höchsten Schutz bzw. sind am wichtigsten?

Antwort	Paraphrasierung	Generalisierung
1.2	Keine Aussage getroffen	----
2.2	Das Wichtigste ist die Firewall.	Firewall
3.2	Firewall-Einstellungen, Netzwerksegmentierung, Mail-Absicherung, User-Überwachung, Endpoint-Security und ein ordentliches Patch-Management sind alles wichtige Sicherheitsmaßnahmen, wobei es immer am wichtigsten ist, die User von kompromittierendem Verhalten abzuhalten.	In Hinsicht auf Userverhalten: Firewall (Einstellungen/Netzwerk-segmentierung) Mail-Absicherung Endpoint-Security User-Überwachung Patch Management
4.2	Insgesamt müssen alle Komponenten in einer Basisform vorhanden sein, danach stellen die Firewall und Netzwerk-Architektur aus technischer Sicht die wichtigsten Komponenten dar.	In Basisform alle Dann: Firewall, Netzwerkarchitektur
5.2	Wenn ein Basisschutz vorhanden ist, sind ein Patch-Management und eine Firewall-Konfiguration und zukünftig vermutlich die Umsetzung eines Zero-Trust Modells die wichtigsten Maßnahmen.	In Basisform alle Dann: Firewall, Patch-Management

Tabelle 3: Qualitative Analyse Frage 2

Grundsätzlich sind sich alle Experten, die eine Aussage zu Frage 2 getroffen haben, einig, dass die Firewall eine der effektivsten Maßnahmen in Bezug auf IT Security ist. Dies betrifft nicht nur den Schutz des Netzwerks vor Malware und Hackerangriffen von innen und außen, sondern auch die Schadensbegrenzung im Falle einer Sicherheitsverletzung. Es ist wichtig anzumerken, dass, auch wenn die Firewall als wichtigstes Glied eines ganzen Maßnahmen-Katalogs hervorsticht,

eine gewisse Basis sämtlicher Maßnahmen vorhanden sein muss, damit eine IT-Infrastruktur auf Dauer bestehen kann.

Wie hoch sind die Einschränkungen für die User durch die unterschiedlichen Maßnahmen?

Antwort	Paraphrasierung	Generalisierung
1.3	Das kommt auf die Infrastruktur an. Bei einer homogenen Umgebung wird es weniger Einschränkungen geben. Bei korrekter Konfiguration sollte es kaum Einschränkungen geben.	Kaum (nicht genauer definiert)
2.3	Wenn die Schutzmechanismen auf ein Level eingestellt sind, der ein guter Kompromiss ist, dann sollte den Usern nur selten etwas auffallen. Der Schutz ist dann allerdings auch nur „mittelgut". Wenn das System so eingestellt ist, dass die Security an erster Stelle steht, gibt es Performance-technisch kaum Einbußen, aber die Usability leidet darunter.	Bei Kompromisslösung kaum Bei Fokus auf Security Usability Schwächen
3.3	Das E-Mail-Sandboxing ist für die meisten Leute die größte Störung, da diese Maßnahme immer wieder auf Unverständnis stößt. Das Antivirenprogramm bekommen die User nicht mit und dass wegen der Firewall nicht jede beliebige Seite am Arbeitsplatz angesurft werden kann, verstehen die Benutzer meistens.	E-Mail-Sandboxing
4.3	Unerwartete Einschränkungen werden die User nur selten entdecken. Userschulungen sollten Einschränkungen wie E-Mail-Sandboxing erklären, damit diese Maßnahmen für die Benutzer verständlich sind. Viele Maßnahmen sind abhängig vom Geschäftsalltag der User und können durch organisatorische Maßnahmen umgangen werden.	Bei guter Organisation kaum
5.3	Die Einschränkung sind von der organisatorischen Umsetzung abhängig, wobei unter anderem eine E-Mail-Sandbox und ein Virenscanner Verzögerungen hervorrufen können. Viele Einschränkungen und Störfaktoren können mit	E-Mail-Sandboxing Antivirensoftware

	durchdachten Zeitmanagement abgeschwächt werden.	

Tabelle 4: Qualitative Analyse Frage 3

Die Meinungen über die Einschränkungen der Sicherheitsmaßnahmen variieren je Experte. Besonders wichtig zur Beantwortung dieser Frage war der Einbezug der organisatorischen Thematik. Viele Usability-Einbußen können mit wohlüberlegten organisatorischen Maßnahmen umgangen bzw. reduziert werden. Darunter fällt sowohl ein nächtlicher Backup-Prozess, der das System nur außerhalb der Geschäftszeit belastet, als auch der Aufbau des Systems mit übergreifenden Sicherheitskontexten, damit der Benutzer nicht alle fünf Minuten zu einer Authentifizierung aufgefordert wird. Zu den organisatorischen Hilfsmitteln zählen auch Userschulungen. Dort sollte den Benutzern auch der Hintergrund von gewissen Maßnahmen erklärt werden, damit ein gewisses Grundverständnis für „nervige" Einschränkungen wie z. B. die E-Mail-Sandbox oder Firewall-Restriktionen vorhanden ist. Das Ziel ist es das gesamte System so reibungslos wie möglich zu machen und den Usern näher zu bringen, dass die vorhandenen Einschränkungen wichtig sind. (Furnell, 2016)

Kann durch diese technischen Maßnahmen ein Netzwerk so gut geschützt werden, dass sogar bei mutwilliger oder grober Fahrlässigkeit der User keine Gefährdung für das Netzwerk entsteht?

Antwort	Paraphrasierung	Generalisierung
1.4	Das Löschen von Daten stellt kein Problem dar, sie können zurückgeholt werden. Problematischer sind Malware-Angriffe. Wenn ein unerfahrener User Malware in das System bringt, ist auch ein gut aufgebautes System nur minimalst sicher.	Nein
2.4	Das Netzwerk so gut schützen zu wollen ist unrealistisch, da die User bei zu starken Einschränkungen andere noch gefährlichere Wege suchen.	Nein
3.4	Eine komplette Gefährdung des Netzwerks ist nie auszuschließen, aber der Schadensumfang kann mit der Hilfe von Endpoint-Security und Netzwerksegmentierung bzw. Zero Trust eingeschränkt werden.	Nein (Schadenseinschränkung möglich)
4.4	Ein böswilliger oder grob fahrlässiger User wird immer eine Gefahr für das System sein, wobei etwaige Maßnahmen zur Schadensbegrenzung möglich sind.	Nein (Schadenseinschränkung möglich)

5.4	Wenn der User mit genug Wissen beziehungsweise dem notwendigen Ehrgeiz ausgestattet ist wird er für das Netzwerk immer eine Gefahr darstellen. Zukünftig dürfte Zero-Trust im Bereich der Schadensminimierung eine essenzielle Rolle spielen.	Nein (Schadeneinschränkung zukünftig gut möglich)

Tabelle 5: Qualitative Analyse Frage 4

Grundsätzlich ist es nicht möglich ein System so gut zu schützen, dass ein User, der mit grober Fahrlässigkeit bzw. mit bösen Absichten agiert, keinen Schaden verursachen kann. Es ist allerdings sehr wohl möglich, dass System so zu konfigurieren, dass der anfallende Schaden möglichst gering ist. Besonders das Sicherheitskonzept Zero Trust ist in dieser Hinsicht vielversprechend.

Bieten durch eine Firewall getrennte Subnetze einen Sicherheitsvorteil?

Antwort	Paraphrasierung	Generalisierung
1.5	Die Trennung der Subnetze durch eine Firewall ist heutzutage absolut notwendig.	Ja
2.5	Sicherheitstechnisch bietet die Netzwerksegmentierung nicht nur bei der Abwehr gewisse Vorteile, sondern insbesondere bei einem aktiven Malwareangriff. Da sollte nur das einzelne Netzwerksegment betroffen sein.	Ja
3.5	Durch die Netzwerksegmentierung besteht die Möglichkeit im Falle einer Sicherheitsverletzung die laterale Bewegung des Angreifers zu unterbinden. Die Abriegelung des Schadens auf einen begrenzten Teil des Netzwerks ist der größte Vorteil der Segmentierung.	Ja
4.5	Die getrennten Subnetze bieten einen Sicherheitsvorteil, insbesondere wenn eine Malware-Attacke vorliegt.	Ja
5.5	Im Falle einer erfolgreichen Malware-Attacke bieten getrennte Subnetze durch die Gefährdungseinschränkung einen großen Vorteil.	Ja

Tabelle 6: Qualitative Analyse Frage 5

Durch eine Firewall getrennte Subnetze bieten in jedem Fall einen Sicherheitsvorteil, wobei zu beachten gilt, dass dies einen kompletten Infrastrukturumbau mit sich bringt und im laufenden

Betrieb mit einer höheren Auslastung zu rechnen ist. Falls dieser Schritt getätigt wird, sollte im Vorhinein eine Anforderungsanalyse durchgeführt werden, damit neue Netzwerkkomponenten in der richtigen Dimension verwendet werden. Der Hauptvorteil der Netzwerksegmentierung liegt im Abgrenzen der einzelnen Netzwerkbereiche, wodurch bei einem Malwarebefall der Schaden eingedämmt werden kann.

Bei welchen der angeführten Maßnahmen sehen Sie Ihren Erfahrungen nach bei den meisten Unternehmen Verbesserungspotenzial?

Antwort	Paraphrasierung	Generalisierung
1.6	Aufholbedarf besteht bei den meisten Unternehmen insbesondere bei der Aktualität der Mittel, die eingesetzt werden. Dabei geht es um Thematiken wie Verhaltensüberwachung, „Need-to-Know“-Prinzip, Immutable Backups und automatische Auswertung der Logs. Es scheitert an Maßnahmen der Erkennung bzw. der Wiederherstellung.	Software- und Hardwarestand Verhaltensüberwachung „Need-to-Know“-Prinzip Immutable Backups Auswertung der Logs Erkennungs- und Wiederherstellungs-Maßnahmen
2.6	Die mit Abstand größte Schwäche stellt Human Error dar, wobei dies nicht nur das Fehlverhalten der User, sondern auch das Unverständnis der Geschäftsführungen mit einbezieht. Aus technischer Sicht gibt es kaum Unterschiede.	Organisatorische Maßnahmen User-Schulungen
3.6	Veraltete Hardware und Software sind eine Schwachstelle in vielen Unternehmen, da es hier seitens der Organisationen an Verständnis und Unterstützung mangelt. Auch eine Netzwerksegmentierung in fortgeschrittener Form fehlt den meisten Unternehmen.	Patch Management Netzwerksegmentierung
4.6	Auf technischer Seite gibt es die Möglichkeit zur Überprüfung von Firewall-Regeln, Hardware- und Softwareaktualität, wobei die organisatorischen Mängel meistens stärker ausgeprägt sind.	Firewall-Konfiguration Patch-Management Organisatorische Maßnahmen
5.6	Langsame Update-Zyklen und unvollständige Backupstrategien stellen meistens größere Schwachstellen dar und haben dementsprechend viel Verbesserungspotenzial, wobei auch eine	Patch-Management Backup Firewall

	Firewall-Konfigurations-Nachschärfung und WLAN-Absicherung beliebte Thematiken sind.	WLAN-Absicherung

Tabelle 7: Qualitative Analyse Frage 6

Bei der Frage des Verbesserungspotenzials ergeben sich aus den Experteninterviews unterschiedliche Meinungen. Einerseits fällt die organisatorische Seite als einer größten Bremsfaktoren auf. Dabei geht es um Thematiken wie fehlende Userschulungen, nicht vorhandene Priorisierung im Unternehmen oder Ressourcenmangel innerhalb der IT-Administration. Im technischen Bereich ist laut den Experteninterviews das Patch Management am ehesten verbesserungswürdig.

Gibt es Ihrer Meinung nach eine Sicherheitstechnologie, die zukünftig technische Sicherheitskonzepte bzw. das allgemeine Denken im Bereich IT-Sicherheit reformieren könnte?

Antwort	Paraphrasierung	Generalisierung
1.7	In der Heuristik bzw. bei der KI könnte es noch große Reformen geben, insbesondere im Bereich der Verhaltensanalyse.	Künstliche Intelligenz
2.7	Es gibt zwei große sicherheitstechnische Themen, die bereits populär sind und zukünftig vermutlich eingesetzt werden. Das sind IPv6 und Zero Trust. Beide Technologien bieten sicherheitstechnisch neue Möglichkeiten, wobei auch noch einige Schwachstellen zu beseitigen sind.	IPv6 Zero Trust
3.7	Das Thema KI wird sich in Zukunft noch weiter im Bereich der IT-Security verbreiten. Im Incident Response Management ist die KI bereits im Einsatz, wobei die zukünftigen Einsatzgebiete wie KI-gesteuerte Firewalls oder KI-gestützte Verhaltensanalysen noch weitere Fortschritte bringen werden. Insgesamt ist ein Trend zu Sicherheitsmaßnahmen zu erkennen, die dem User helfen „sicherer“ zu sein.	Künstliche Intelligenz
4.7	Es wird keine große Reformation der IT-Sicherheitskonzepte geben, aber neuartige Technologien wie der Einsatz von KI im IT-Security-Bereich und Zero Trust werden stark unterstützend wirken.	Reformation nein Zukunftsträchtige Technologien: Zero Trust Künstliche Intelligenz

5.7	Zero-Trust wird noch eine spannende Thematik werden, welche Sicherheitskonzepte abändern wird. Sicherheitskonzepte werden nicht mehr wirklich reformiert werden, wobei zukünftig das zeitnahe hinzufügen von neuen Technologien und Konzepten in den Sicherheitsstandard wichtiger werden wird.	Reformation nein Zukunftsträchtige Technologie: Zero Trust

Tabelle 8: Qualitative Analyse Frage 7

Bezüglich der zukünftigen Technologien im IT-Sicherheitsbereich geht keiner der Experten davon aus, dass es etwas geben wird, was die derzeitigen IT-Sicherheitskonzepte komplett revolutionieren würde. Es gibt allerdings interessante Themengebiete wie Zero Trust, IPv6 und KI im IT-Sicherheitskontext, die große Fortschritte bringen werden. Künstliche Intelligenz bietet viele interessante Möglichkeiten im Sicherheitsbereich, obwohl diese zurzeit nur sehr begrenzt eingesetzt wird. Von Interesse sind vor allem IT-Sicherheitsmaßnahmen, die sich darauf beziehen den User „besser“ zu machen, weil die Sicherheitssysteme selbst schon durchaus ausgereift sind.

4.2.2 Beantwortung Forschungsfrage & Hypothesen

Um die Forschungsfrage und die Hypothesen zu beantworten, wird die Literaturrecherche als Basis angewendet und durch die Experteninterviews angereichert.

Welche technischen Maßnahmen mit vertretbaren Einschränkungen für den operativen Betrieb schützen Firmennetzwerke effektiv vor Angriffen?

Sicherheitsmaßnahmen wie Firewall-Konfigurationen, Netzwerksegmentierungen, Endpoint-Security, Backup-Verfahren, Antivirenscans, E-Mail-Absicherung und Patch-Zyklen können mit vertretbaren Einschränkungen für die User in einer homogenen IT-Infrastruktur, in der organisatorisch auf Usability-Anforderungen im Sicherheitskonzept geachtet wurde und sicherheitstechnisch ein Kompromiss eingegangen wird, zur Absicherung von Unternehmensnetzwerken eingesetzt werden.

Im Allgemeinen gilt es festzuhalten, dass unter den soeben genannten Aspekten sämtliche in der Literaturrecherche als auch im Experteninterview behandelte Sicherheitsmaßnahmen zu Einschränkungen für die User in einem akzeptierbaren Bereich führen.

Dabei gilt es zu beachten, dass für ein reibungsloses IT-Sicherheitssystem viele Faktoren ineinandergreifen und dies auch ein gewisses Verständnis der User für Schutzmaßnahmen voraussetzt.

Zur Unterstützung der Forschungsfrage wurden folgende Hypothesen behandelt:

Hypothese 1:

- H0: Mehrere kleine, durch eine Firewall getrennte Subnetzwerke sind sicherer als ein großes Netz.
- H1: Viele kleine durch eine Firewall getrennte Subnetzwerke bieten keinen messbaren Sicherheitsvorteil gegenüber einem einzelnen großen Netzwerk.

Hypothese 1 wird vollständig von der Fachliteratur als auch von Experten unter normalen Umständen bestätigt. Die einzige Ausnahme zur Hypothese bildet ein Szenario, wo die Firewall vor Einführung der Subnetze bereits kurz vor der Überlastung stand.

Hypothese 2:

- H0: Ein technisch laut neuesten Sicherheitsanforderungen gut geschütztes Netz kann auch durch Anwendungsfehler und bewusste Manipulation von berechtigten Usern nicht gefährdet werden.
- H1: Selbst laut neuesten Sicherheitsanforderungen gut geschützte Netze können durch Anwendungsfehler und bewusste Manipulation von berechtigten Usern gefährdet werden.

Hypothese 2 wird auf Basis der Experteninterviews abgelehnt. In der Fachliteratur gibt es zwar Konzepte bezüglich der Schadensminimierung, die zumindest in der Theorie so weit gehen, dass der User nur sich selbst schaden kann, aber dies ist in der Praxis aus Gründen der Komplexität und den vorhandenen technischen Mitteln nicht realistisch.

4.3 Umgesetzte Konzepte Fallbeispiel

In diesem Kapitel werden umgesetzte Sicherheitsmaßnahmen basierend auf den Ergebnissen dieser Arbeit in einem Fallbeispiel gezeigt.

4.3.1 Ausgangsszenario

Bei diesem Fallbeispiel geht es um einen realen Malware-Angriff, der im Sommer 2020 in einem Unternehmen stattgefunden hat. Es handelt sich dabei um eine mittelständische Firmengruppe, in der für die Dachgruppe als auch für fünf der mehreren Subfirmen die IT-Infrastruktur administriert und zur Verfügung gestellt wird. Die User arbeiten großteils auf einem reinen Remote-Citrix-System und die Infrastruktur umfasst eine Vielzahl von Hardware, Anwendungen und Servern.

Folgende Eckdaten sind in der Infrastruktur vorhanden:

- 516 virtualisierte Server
- Drei VCenter auf ESX-Server zur Verwaltung von virtuellen Servern

- Eine gespiegelte Allflash-SSD-Nimble Storage[1]
- SAP ERP Server & Datenbank
- Zusätzliche Sicherungs-NAS

4.3.1.1 Malwareangriff

Durch eine forensische Untersuchung im Nachgang und eine Nachbesprechung mit den IT-Mitarbeitern kann davon ausgegangen werden, dass die Sicherheitslücke durch falsches Userverhalten entstanden ist. Der verantwortliche Userkreis konnte auf Basis der Usermeldungen auf drei Personen eingeschränkt werden, wobei nicht ausgeschlossen werden kann, ob nicht ein weiterer User der Verursacher war.

In diesem Fall war bei allen Usern ein „Klick“ auf einen Link in einer gut gefälschten E-Mail der Infektionspunkt. Es wird davon ausgegangen, dass die Malware unauffällig am Server gelegen ist, bis sie sich über einen Administratornutzer im gesamten Netzwerk verteilen konnte.

Bei der Malware selbst handelte es sich um die Ransomware DoppelPaymer[2], welche einen Großteil des Systems verschlüsselte.

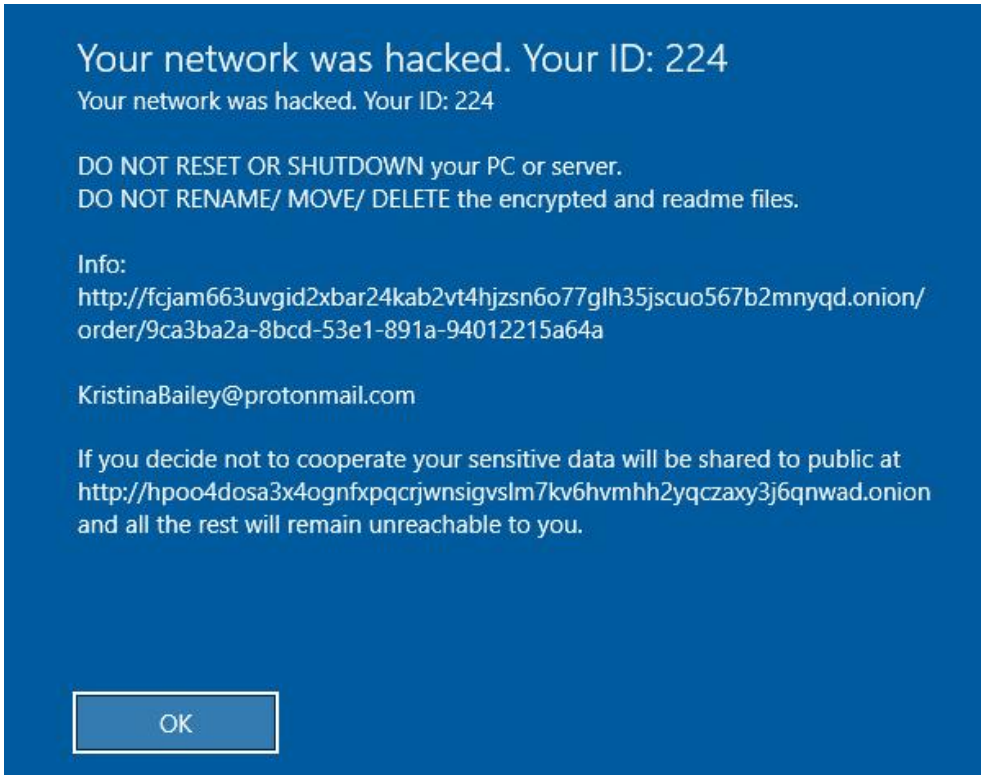

Abbildung 15: Verschlüsselungsnachricht

[1] https://buy.hpe.com/at/de/storage/disk-storage-systems/alletra-storage-arrays/alletra-storage-6000-arrays/hpe-alletra-6000/p/1013540188

[2] https://malpedia.caad.fkie.fraunhofer.de/details/win.doppelpaymer

Auf allen Remoteclients und befallenen Servern ist die in Abbildung 15 zu sehende Meldung eingeblendet, die das gesamte System blockierte. Die Vcenter ESX Server waren nicht von der Malware betroffen. So auch der SAP und SAP-Datenbankserver.

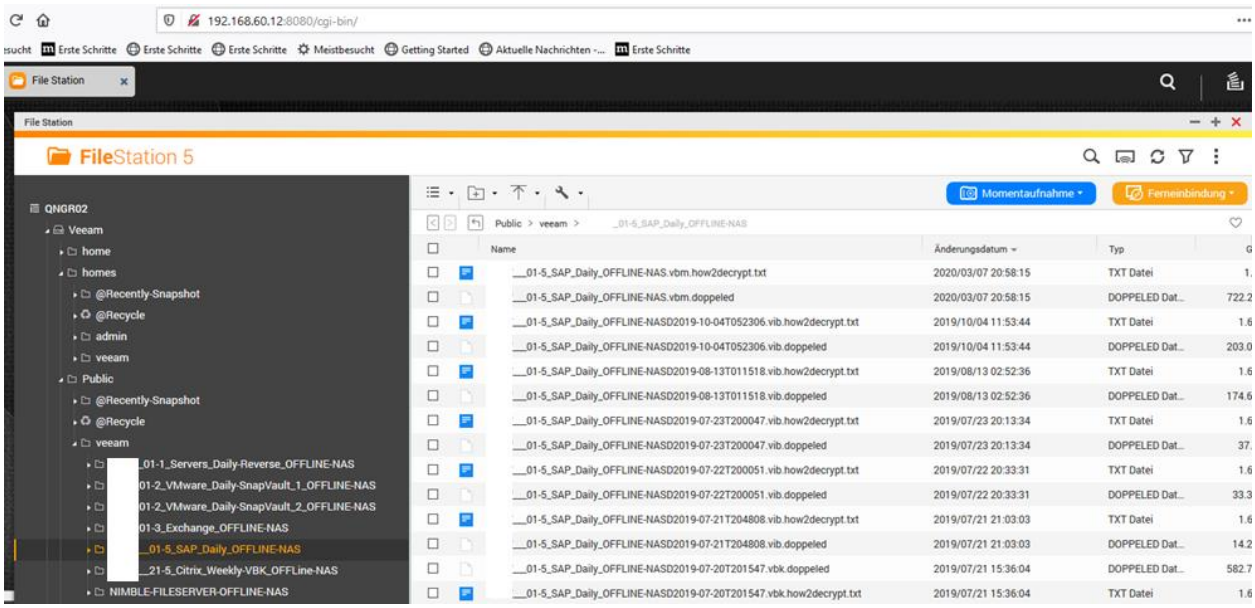

Abbildung 16: Verschlüsselte Dateien auf Sicherungsserver

In Abbildung 16 sind auch gut die verschlüsselten Sicherungsdateien zu erkennen. Die Dateien am Sicherungsserver sind mit der Dateiendung „*.doppeled“ verschlüsselt. Und es wird bei jeder Datei die Entschlüsselungsanleitung in einer Textdatei beigelegt. Die Sicherung zur Offline NAS war gerade am Laufen, als der Virus aktiv wurde, was auch die Daten dort unbrauchbar machte. Glücklicherweise wurde vorsorglich eine weitere NAS außerhalb der Domäne installiert, wodurch diese von der Malware verschont geblieben ist.

4.3.1.2 Systemrettung

Nach Entdeckung des Malware-Befalls wurde als Erstes das gesamte System vom Netz genommen, um etwaige Kommunikation nach außen zu unterbinden. Dann wurde mit einer Schadensanalyse angefangen und versucht das System wiederherzustellen.

Zum Verständnis über die Vorgangsweise bei der Systemrettung ist wichtig anzumerken, dass die ESX Server, die den virtuellen Servern die Ressourcen liefern, alle Diskless sind und so die Server datenseitig auf der Nimble-Storage bzw. der NetApp[3] gelegen sind. Dadurch stehen auch sämtliche Datensicherungsmöglichkeiten einer Storage zur Verfügung.

Um die Server in einem funktionalen Zustand zurückzuholen, wurde von allen auf der Nimble befindlichen Servern ein Snapshot von drei Tagen früher geladen, was sich im Nachhinein eigentlich als Fehler herausstellte. Die Malware fing bereits eine volle Woche früher an sich im System zu verbreiten, was dazu führte, dass zwar sämtliche Server durch den Snapshot wieder

[3] https://www.netapp.com/de/data-storage/

unverschlüsselt waren, aber die Virendateien trotzdem auf einer Vielzahl Server bereits vorhanden waren. Da zu diesem Zeitpunkt nicht bekannt war, wann genau die Verbreitung des Virus stattgefunden hat, gab sich die IT-Abteilung mit dem infizierten, aber voll funktionsfähigen Snapshot-Stand zufrieden.

Nach etwaigen Versuchen mit unterschiedlichen Anti-Malwareprogrammen die infizierten Server wieder sauber zu bekommen, wurden alle Server mit einer Kombination aus Malwarebytes, dem Kaspersky-Removal-Tool und der Roguekiller-Software gescannt und gefundene Viren beseitigt. Ein zufälliger Glücksfall war auch, dass die Malware durch das vom Netz-Nehmen und über Snapshot-Zurückholen in einem „schlafenden“ Zustand war. Die gesamte Serverlandschaft wurde auf die wichtigsten Server heruntergebrochen, die dann mit allen drei Tools mehrfach gescannt worden sind.

Wichtige Server, die auf der NetApp gelegen sind, konnten von der NAS, welche außerhalb der Domäne gelegen war, zurückgeholt werden.

Essenzielle Infrastruktur-Server wie z. B. die Domänencontroller wurden mit der Hilfe eines externen Dienstleisters komplett neu aufgesetzt. Insgesamt war der Ausfall für die User von kurzer Dauer. Das gesamte Kernproduktivsystem stand den Mitarbeitern gerade eineinhalb Tage nach dem Bekanntwerden des Vorfalls wieder zur Verfügung, was vor allem auf den intensiven Einsatz der lokalen IT-Abteilung, welche von Montag in der Früh bis Dienstagnachmittag durcharbeitete, zurückzuführen ist.

Mittags am dritten Tag nach dem Vorfall waren alle als wichtig definierten Server bereits mindestens zwei Mal mit den Tools überprüft worden und wurden langsam den Usern wieder zur Verfügung gestellt. Es wurde auch die Woche darauf noch ein dritter Scan durchgeführt, der ohne Virenfunde blieb.

Insgesamt wurden von den 516 Servern 225 wiederhergestellt und überprüft, wobei die restlichen Server nicht mehr notwendig waren und nur ein geringer Anteil nach expliziter Anforderung vom Langzeit-Backup zurückgeholt wurde. Insgesamt war die lokale IT noch drei bis vier Wochen nach dem Vorfall mit Nachbesserungen beschäftigt, bevor mit Hilfe eines Sicherheitsdienstleisters ein Sicherheitskonzept ausgearbeitet wurde. In den folgenden Kapiteln werden ausgewählte Maßnahmen, welche auch in dieser Diplomarbeit behandelt wurden, vorgestellt.

4.3.2 Firewall Upgrade & Netzwerksegmentierung

Einer der Hauptgründe, warum die schnelle Ausbreitung der Malware möglich war, lag unter anderem an einer unzureichenden Netzwerksegmentierung im ehemaligen Unternehmensnetzwerk. Dabei gilt festzuhalten, dass die Firewall zu diesem Zeitpunkt schon älter und von der Auslastung her an der Grenze war.

Um eine feinere Netzwerksegmentierung durchzuführen, war es notwendig, eine aktuellere und auf die höhere Last ausgelegte Firewall zu kaufen. Da die Mitarbeiter im Unternehmen bereits

Erfahrungen mit Fortinet Firewalls[4] gehabt haben, wurden nach einer Auslastungsanalyse zwei Stück der Fortinet 101F Firewall bestellt und konfiguriert.

Netz	Standort / Type	VLAN	Net	ALT	Kurz	DEVICE
Unt1 Gebäude						
DMZ	Graz RZ	8	8		Unt1_DMZ	FWGR01
MPLS	Graz RZ	9	9	9	Unt1_MPLS	A1 GW
ILO	Graz RZ	10	10	10	Unt1_ILO	FWGR01
ISCSI-Mgmt	Graz RZ	14	14		Unt1_ISCSI14	FWGR01
ISCSI-Data	Graz RZ	15	15		Unt1_ISCSI15	FWGR01
Voice Graz	Graz RZ	20	20	20	VoiceGraz	FWGR01
Unt1 - LAN Guest	Graz RZ	56	56		Unt1_LAN56	FWGR01
Unt1 - WLAN Guest	Graz RZ	57	57		Unt1_WLANG57	FWGR01
Unt1 - Infra Mgmt + Drucker	Graz RZ	58	58		Unt1_InfraMGMT58	FWGR01
Unt1 - Netz Mgmt (Secure)	Graz RZ	59	59		Unt1_NetMGMT59	FWGR01
Unt1 - Server	Graz RZ	60	60	60	Unt1_SERVER60	FWGR01
Unt1 - Client LAN	Graz RZ	61	61	61	Unt1_CLIENT61	FWGR01
Unt1 - Client LAN Reserve	Graz RZ	62	62		Unt1_CLIENT62	FWGR01
Unt1 - WLAN	Graz RZ	63	63		Unt1_WLAN63	FWGR01
Unt1 - WLAN Reserve	Graz RZ	64	64		Unt1_WLAN64	FWGR01
Unt1 - Reserve	Graz RZ	65	65		Unt1_NET65	FWGR01
Unt1 - Citrix TECH	Graz RZ	66	66		Unt1_Citrix66-TECH	FWGR01
Unt1 - Citrix KAUF	Graz RZ	67	67		Unt1_Citrix67-KAUF	FWGR01
Unt1 - Citrix Unt2	Graz RZ	68	68		Unt1_Citrix68-Unt2	FWGR01
Unt1 - Citrix Unt3	Graz RZ	69	69		Unt1_Citrix69-Unt3	FWGR01
Unt1 - Citrix IT	Graz RZ	70	70		Unt1_Citrix70-IT	FWGR01
Unt1 - Citrix Unt4	Graz RZ	71	71		Unt1_Citrix71-Unt4	FWGR01
Unt1 - Citrix 72 free	Graz RZ	72	72		Unt1_Citrix72-free	FWGR01
Unt1 - Citrix 73 free	Graz RZ	73	73		Unt1_Citrix73-free	FWGR01
Unt1 - Citrix 74 free	Graz RZ	74	74		Unt1_Citrix74-free	FWGR01
Unt1 - Citrix 75 free	Graz RZ	75	75		Unt1_Citrix75-free	FWGR01
Voice Unt2	Graz	30	30	30	VoiceUnt2	FWGR01
Unt2 - Server	Graz	32	32		Unt2_SERVER32	FWGR01
Unt2 - Clients	Graz	33	33		Unt2_CLIENT33	FWGR01
Unt2 - WLAN	Graz	34	34		Unt2_WLAN34	FWGR01
Unt2 - WLAN GUEST	Graz	35	35		Unt2_WLANG35	FWGR01

Abbildung 17: Netzwerksegmentierung Fallbeispiel

In Abbildung 17 sind die einzelnen Netze des Hauptstandorts der Unternehmensgruppe zu sehen. Die Detailspalten wie z. B. IP-Ranges mussten aus Sicherheitsgründen ausgeblendet werden. Es bietet aber trotzdem die Möglichkeit die Netzwerksegmentierung gut nachvollziehen zu können. Am Hauptstandort des Unternehmens sind zwei Firmen untergebracht. Vor der Netzwerksegmentierung wurden sämtliche Bereiche in nur fünf VLANs (MPLS VLAN ausgenommen) unterteilt und es wurde auf der Firewall keine Threat-Detection zwischen den internen Netzen angewendet.

Mit der neuen Firewall wurden die Subnetze von fünf auf 31 VLANs erhöht und es wurde je nach Firewall-Richtlinien die Threat-Detection aktiviert. Dies war nicht bei allen Subnetzen notwendig, da es VLANs gibt, die keine Berechtigung haben im internen Netz zu agieren, wie beispielsweise VLAN 57 für das Gäste-WLAN.

Auch die Absicherung der extern gelegenen Standorte der Unternehmensgruppe wurde überarbeitet und über Netzwerksegmentierung und neuere Firewalls gesichert.

[4] https://www.fortinet.com/de

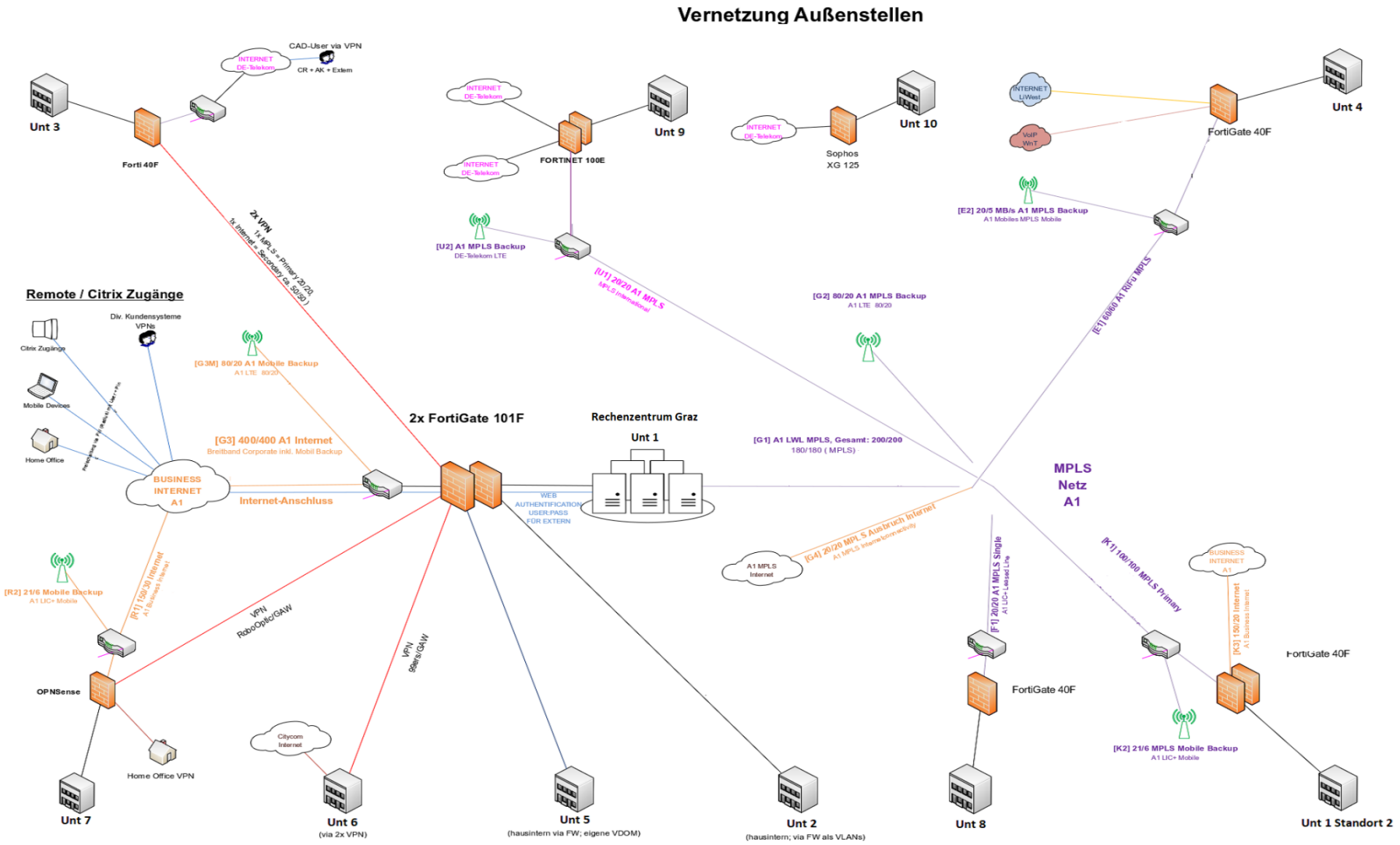

Abbildung 18: Beispiel Unternehmensnetzwerk

Wie in Abbildung 18 zu sehen ist, können Unternehmensnetzwerke schnell komplexere Ausmaße annehmen, wobei die Unternehmensgruppe insgesamt „nur“ 650 Mitarbeiter hat. Es ist gut zu erkennen, wie die einzelnen Unternehmen und Standorte verknüpft sind. Leider kann aus Datenschutz- und Sicherheitsgründen nicht genauer im Detail auf das Netzwerk eingegangen werden.

In den Unternehmen, wo die zentrale IT verantwortlich ist, wurde nach dem Malwareangriff eine Anforderungsanalyse bezüglich den Firewall-Kapazitäten erstellt, falls notwendig neue Hardware gekauft und eine Netzwerksegmentierung wie in Abbildung 17 dargestellt mit Threat-Detection durchgeführt.

4.3.3 Antivirus Suite

Vor der Malware-Attacke war im System zwar ein Kaspersky-Antivirus vorhanden, allerdings wurde dieser nur in der Basis-Version eingesetzt. Dieser wurde nach der Wiederherstellung des Systems komplett neu aufgesetzt.

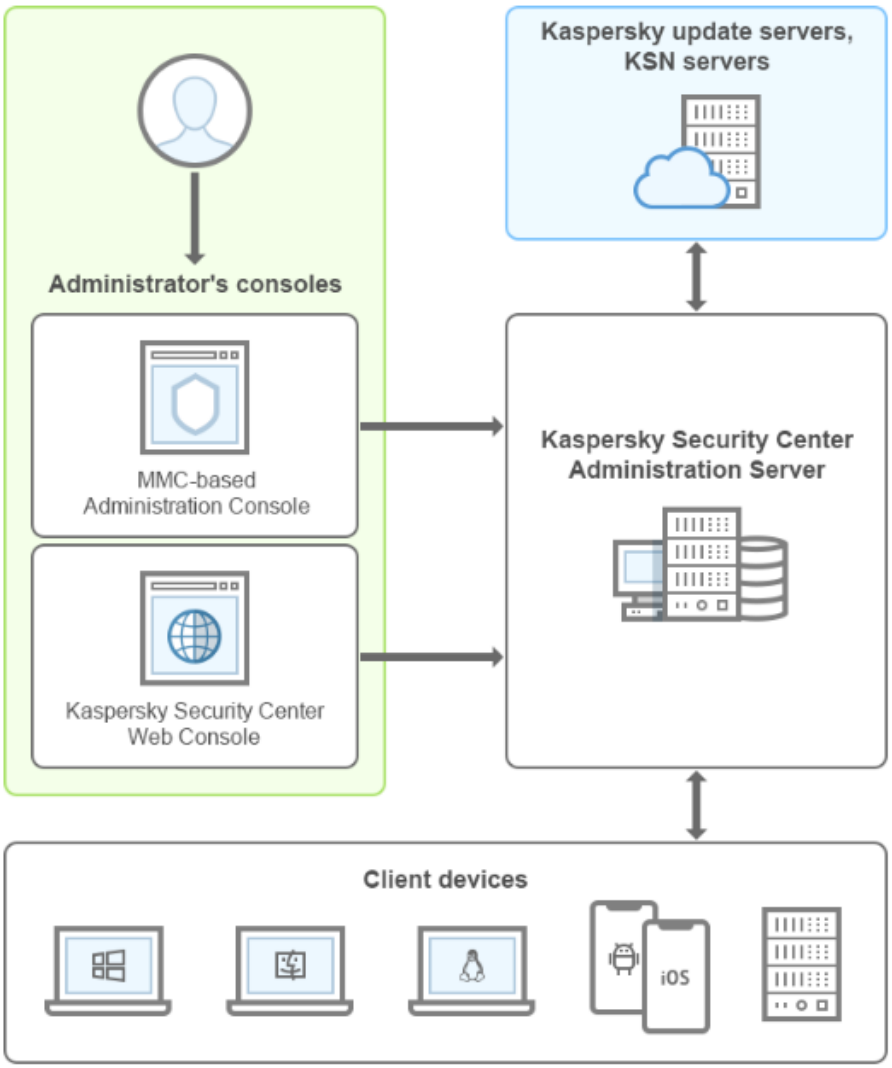

Abbildung 19: “Kaspersky Security Center”-Architektur (t.ly/iS5j)

Die Basis-Version der Software wurde komplett entfernt und von einem Kaspersky-Security-Center (KSC) ersetzt. Das KSC bietet wie in Abbildung 19 zu sehen den Administratoren über den KSC-Administrationsserver die Möglichkeit, je nach Endgerät unterschiedliche Einstellungen und Sicherheitsstufen zu definieren. Dadurch kann auf Standardgeräten ein etwas lockerer Schutz entstehen, was zu weniger Meldungen für die Admins und vor allem User führt und auf den essenziellen Servern und Geräten kann die Endpoint-Security auf die höchste Stufe gestellt werden. Dies führt dazu, dass für den User das Arbeiten auf solchen Geräten aufwendiger wird, da sämtliche Interaktionen und Dateien, die nicht im Vorhinein definiert wurden, gesperrt sind.

Da in der Unternehmensumgebung in vielen Bereichen im Remotedesktopsystem Citrix gearbeitet wird, wurde den Usern, die teilweise auf die kritischen Services zugreifen müssen, als Kompromisslösung ein zusätzlicher Desktop zur Verfügung gestellt. Dadurch gibt es für diese User den „sicheren“ Server mit starken Einschränkungen wie z. B. kein regulärer Internetzugang, kein freier Filesystemzugriff und starke Verhaltensüberwachung und den Standardarbeitsserver, wo der Antivirus anwenderfreundlicher eingestellt ist. Auf die essenziellen Programme kann der User nur am hochsicheren Server zugreifen.

4.3.4 E-Mail-Absicherung

Sowohl in der forensischen Untersuchung als auch bei der Nachbesprechung des IT-Teams nach dem Malware-Angriff kristallisierte sich die Infektion über gefährliche E-Mails als wahrscheinlichster Angriffsvektor heraus. Aus diesem Grund wurde seitens des großangelegten Security-Projekts insbesondere auf die E-Mail-Absicherung geachtet. Nach Rücksprache mit IT-Sicherheitsdienstleistern wurde unternehmensseitig für eine E-Mail-Sandbox des Anbieters Fortinet entschieden. Fortinet wurde ausgewählt, weil durch das vorhandene Vorwissen über Fortinet und die verwendeten Fortinet Firewalls eine möglichst homogene Umgebung geschaffen wurde. Sämtliche E-Mails, die von nicht whitegelisteten Adressen kommen, werden in der Fortinet Sandbox überprüft und je nach Ergebnis blockiert, weitergeleitet oder in die Quarantäne verschoben. Die E-Mails, die in der Quarantäne landen, sind beim Security-Check nicht eindeutig identifiziert worden. Das Sand-Box-System überprüft die E-Mails nach unterschiedlichsten Punkten und vergibt eine Benotung. Insofern am Ende der Untersuchung die Werte passen, wird das E-Mail weitergeleitet. Dabei gilt erwähnen, dass es natürlich Kriterien in der Überprüfung gibt, welche die E-Mails sofort blockieren.

Seit der Einführung der E-Mail-Sandbox kommen nur noch in seltenen Fällen gefährliche E-Mails an den Endanwender. In den meisten Fällen liegt dies daran, dass der Absender bereits bekannt und öfters als sicher bewertet wurde, aber nun von einer Malware infiziert ist. Insgesamt haben sich die Malware- und Phishing-E-Mails auf unter ein Zehntel der ursprünglichen reduziert.

5 RESÜMEE/AUSBLICK

Die IT-Sicherheit ist in gerade in der heutigen Zeit ein Brennpunkt für Unternehmen und Privatpersonen. Es vergeht kaum eine Woche, wo in den Nachrichten nicht darüber berichtet wird, dass ein Unternehmen von einem Malware-Angriff getroffen wurde. Dies betrifft aber nicht nur private Unternehmen, sondern auch Institutionen des öffentlichen Bereichs. So wird bei erfolgreichen Angriffen auch immer wieder die IT-Infrastruktur von Ämtern und Landesregierungen lahmgelegt.

Die IT ist aus sämtlichen modernen Unternehmen fast nicht mehr wegzudenken. Viele Prozesse benötigen die IT als Basis, damit diese vonstattengehen können. Sämtliche E-Mail- und VoIP-Kommunikation ist ohne die entsprechende Infrastruktur unmöglich und in Unternehmen nicht mehr wegzudenken.

Cyber-Attacken kommen immer häufiger vor und werden besser und auch professioneller. Mit dem „Ransomware as a Service“-Modell wurde durch Sodinokibi ermöglicht, dass sogar Laien ganze Systeme lahmlegen und ausbeuten können. Aus der Sicht der angreifenden Partei bietet das Modell eine Win-Win-Situation. Der Laie ohne besondere Ausbildung stellt den Malwarebetreibern die notwendigen Angriffsvektoren zur Verfügung und die Malwarebetreiber eliminieren, wenn sie im System sind, die restlichen Hürden so weit wie möglich. Dadurch wird die Erfolgschance für einen Ransomware-Angriff erhöht, was bei einer Lösegeldzahlung zum Gewinn von sämtlichen Beteiligten führt.

IT-Sicherheitskonzepte bieten eine Vielzahl an möglichen Maßnahmen, um den Malwarebefall zu verhindern beziehungsweise den angerichteten Schaden zu minimieren. Ein Kernstück der IT-Sicherheit ist die Firewall, die heutzutage wesentlich mehr Faktoren als reine Netzwerkrichtlinien abdeckt. Die Firewall-Systeme bieten Unified-Threat-Management, Überprüfungen von Applikationsdatenverkehr, Deep-Inspection, HSTS-Überprüfung und viele weitere Funktionen an. Spannenderweise ist gerade dabei ein gewisser Konflikt der Philosophien zu erkennen, wo es noch keinen klaren Gewinner gibt. Die zwei Features von Deep Inspection und HSTS stehen im direkten Konflikt miteinander. Das Ziel von Deep Inspection ist verschlüsselte Kommunikation aufzubrechen und zu überprüfen, ob das Übertragene auch wirklich sicher ist. Bei HSTS wird explizit darauf geachtet, dass diese Verschlüsselung nicht angegriffen wird und so der Datenverkehr authentisch ist. Der kritische Punkt ist, wenn zukünftig Applikationen auf HSTS-Kommunikation bestehen und so Firewalls den Datenstrom nicht mehr aufbrechen dürfen. Wie dies genau gelöst wird, ist bis jetzt nicht geklärt.

Die Firewall bietet aus Usersicht kaum irgendwelche Einschränkungen und ist eine Pflichtmaßnahme für Unternehmen. Die einzigen Szenarien, wo ein User mit der Firewall in Kontakt kommen könnte, ist beim Arbeiten auf Hochsicherheitsservern, wo ein gewisser Datenverkehr verboten ist, bei einer Überlastung, sodass ganze Datenbündel verloren gehen, oder beim bewussten beziehungsweise unbewussten Ansurfen von fragwürdigen Webseiten.

Weitere Maßnahmen zum Schutz vor Malware mit nur wenigen Berührungspunkten für die User sind Patch-Management, Netzwerkarchitektur und Segmentierung, Sicherungen und die

Antivirensoftware. Hierbei spielt der organisatorische Aufbau der einzelnen Maßnahmen eine große Rolle. Ein Server-Update ist für die Endanwender meistens belanglos, solange diese nicht während der Arbeitszeit eingespielt werden. Dies betrifft beispielsweise auch die Backups, welche sofern möglich nur über Nacht geschehen sollten, damit die Systemressourcen nicht überlastet werden.

Die Maßnahmen, bei denen es auch bei guten Sicherheitskonzepten zu Einschränkungen für die User kommt, sind E-Mail-Sandboxing, Endpoint-Security und WLAN-Absicherung. Dies trifft vor allem dann zu, wenn die Sicherheit einen höheren Stellenwert hat. Endpoint-Security kann Prozesse und Programme auf den Geräten der User blockieren. Die WLAN-Absicherung kann je nach Sicherheitsstandard sogar dazu führen, dass nur authentifizierte Geräte, welche einen gewissen Sicherheitslevel nachweisen können, in das WLAN dürfen. Das E-Mail-Sandboxing kann je nach Prozess des Freigabeverfahrens zu Reibungsstellen mit Usern führen. Wenn die freizugebenden E-Mails beispielsweise von einem IT-Fachpersonal nachüberprüft werden, muss mit Wartezeiten gerechnet werden. Die Wahrscheinlichkeit, dass ein gefährliches E-Mail durchkommt, wird reduziert, aber das Warteintervall kann zu Komplikationen in einem schnelllebigen Geschäftszweig führen.

Die Netzwerksegmentierung ist ein gutes und verhältnismäßig günstiges Tool zur Absicherung der Unternehmensstruktur. Gerade bei einer erfolgreichen Malwareattacke wird der Schaden stark reduziert und kann im besten Fall durch Sicherungen in kurzer Zeit wieder rückgängig gemacht werden.

Wie sich sämtliche Experten einig waren, stellt selbst bei bester IT-Security der User immer noch die mit Abstand größte Gefahr dar. Aus diesem Grund kommen immer mehr Sicherheitsmaßnahmen zum Einsatz, die nicht nur das System von außen, sondern eben auch von innen schützen. Diese Maßnahmen dienen nicht nur zur Einschränkung vom Schaden, der durch den User generiert werden kann, sondern sollen auch den Usern helfen „sicherer“ im System zu agieren.

Zukünftige Technologien werden diese Maßnahmen noch weiter voranbringen. Das Sicherheitskonzept von Zero Trust bietet einen maximalen Schutz gegen Schadensausbreitung, weil der User nur die Ressourcen gefährdet, auf die er auch Zugriff hat. Firewalls, die durch KI-Systeme gestützt werden, können zukünftig große Vorteile in Bezug auf dynamische Gefahrenerkennung und Verhinderung bringen. Auch die Analyse von Echtzeit-Logs durch Analyseprogramme auf Basis von künstlicher Intelligenz kann in dieser Hinsicht von Vorteil sein.

Im Allgemeinen ist festzuhalten, dass sowohl die Angriffsmethoden als auch die Schutzmaßnahmen immer besser werden. Voraussichtlich wird es auch zukünftig keinen heiligen Gral im technischen IT-Sicherheitsbereich geben. Bereits in der heutigen Zeit stellt der humane Faktor die größte Schwachstelle einer jeden IT-Security dar. Die Organisationen, die keine Ressourcen für die IT-Security zur Verfügung stellen, sind sich den Risiken meistens nicht bewusst beziehungsweise nehmen diese nicht ernst genug. IT ist aus kaufmännischer Sicht in unreiferen Unternehmen, wenn alles gut geht, nur ein Kostenfaktor, der erst dann relevant wird, wenn etwas geschieht. Der ungeschulte User stellt die vermutlich größte Gefahr dar und es

sollten in jeglichen Unternehmen, die ihre laufenden IT-Infrastrukturen wertschätzen, regelmäßige IT-Sicherheitsschulungen stattfinden.

Die Einschränkungen, die durch moderne technische Sicherheitsmaßnahmen auferlegt werden, dienen meistens dazu den User immer sicherer und besser zu machen, wobei homogene Systeme die sicherheitstechnisch ineinandergreifenden Reibungsstellen auf ein annehmbares Minimum reduzieren sollten.

Insgesamt ist der gesamte IT-Securitybereich in einem spannenden permanenten Wandel, den wir alle über die nächsten Jahre miterleben werden und in den einzelnen Unternehmen mitprägen dürfen.

ANHANG A - Interviews

H: Host

E: Experte

Interview 1:

H: Passt. Gut, dann danke fürs Kommen. Wie wir es schon festgehalten haben, bist du jetzt seit knapp über 25 Jahren im IT-Bereich tätig und warst insgesamt bei acht Unternehmen angestellt. Und du hast dort in der Zwischenzeit IT-Konzepte für weit über 50 Firmen umgesetzt. Gut, dann starten wir gleich hinein. Welche technischen Maßnahmen zur Netzwerk-Absicherung sind deiner Meinung nach sinnvoll?

E 1.1: Das sind relativ viele Maßnahmen, im Endeffekt geht es darum zu betrachten, wo und von wem wird an welchen Punkten auf das Netzwerk oder auf das Service oder wo auch immer noch zugegriffen. Und da es relativ viele Punkte sein können, wenn man das OSI-Schichtenmodell betrachtet, mehr oder weniger vom Kabel bis zur Applikation, hat man an allen Ecken und Enden Maßnahmen zu setzen, um das System und das Gesamtsystem abzusichern. Und wenn man da schaut, geht es vom OSI-Layer 0 der Person, mit Awareness-Trainings bis hin zu, wenn ich wen einstelle, einmal zu überprüfen, ob der gefährlich sein kann oder nicht.

Dies gehört mittlerweile eigentlich im Rahmen einer ISO-Zertifizierung normalerweise zum Standardprozess dazu. Bis hin zur Zugänglichkeit vom Netzwerk. Die physische Zugänglichkeit von den Systemen. Sei es eine Netzwerkdose. Ist die aufgepatcht? Ist da was dahinter? Meldet sich da was?

Wie zugänglich sind die Räume? Es zählen auch Computer, Laptop, Antivirensoftware, Patches, zwei Faktoren-Authentifizierung, regelmäßige Kennwortänderung, wobei sagen wir nicht regelmäßige Kennwortänderung, darüber kann man streiten, aber eine gewisse Kennwortkomplexität. Wenn man dann in das Backend zurückschaut, dort brauche ich dann Datensicherung und Virenscanner.

Die Verschlüsselung gehört da genauso dazu. Und ja es gibt mehr oder weniger gibt eigentlich kaum eine Komponente in der IT, wo Sicherheit keine Rolle spielt.

H: Grundsätzlich von deiner Erfahrung jetzt gesehen. Wo siehst du zurzeit bei den meisten Unternehmern Aufholbedarf oder wo hast du die größten Schwachstellen gesehen sozusagen?

E 1.1 + 1.6: Viele Unternehmen sehen die noch. Ah, ich habe eine Firewall, ich habe ein Backup und die Nutzer müssen alle 180 Tage ihr komplexes Kennwort ändern und dann glauben sie, sie

sind sicher. Aufholbedarf gibt es, sage ich jetzt mal, bei fast allen Unternehmen, die ich so sehe, als Angestellter bei einem IT-Dienstleister sieht man relativ viel.

Es gibt Aufholbedarf in Sachen der Aktualität der Mittel, die eingesetzt werden. Habe ich eine aktuelle Firewall, das alles auf Next Generation?

Werden alle IP-Pakete, die von innen nach außen und umgekehrt gehen, gescannt? Beherrschen meine Systeme oder meine Sicherheitssysteme Verhaltens-Überwachung? Bis hin zu der ganzen Geschichte eines „Need to Know"-Prinzips. Der User braucht nur das zur Verfügung gestellt bekommen, was er benötigt und keinen Strich mehr.

Ist vielleicht etwas mehr Verwaltungsaufwand, aber das liegt nachher dann mehr oder weniger in den Händen der IT oder des Dienstleisters das effizient zu gestalten, dass zeitlich dann wenig reinrinnt.

Der größte Aufholbedarf liegt bei Unternehmen in der Führungsebene. Das erkannt wird, ja, auch wenn jetzt jahrelang nichts passiert ist, irgendwann kommt einmal die „Intrusion" und dann wird es richtig teuer. Und da ist der größte Aufholbedarf, dass die Leute das erkennen.

H: Und von den technischen Maßnahmen mal klar, Firewall-Konfig und weiß Gott was, was man halt so alles kennt. Das, was du jetzt da angesprochen hast mit „Need to Know"-Bedarf, ist ja mehr oder weniger basierend auf dem Zero-Trust-Prinzip. Der User sieht nur das, was er braucht und gleichzeitig weiß er nicht, wo es herbekommt, sondern einfach hat.

E: Genau. Und von den Maßnahmen her kann man das von unten nach oben betrachten, nämlich am Netzwerk zum Beispiel mit einer 802.1x Authentifizierung. Ich habe im Moment jetzt wieder zwei Projekte in der Pipeline von Kunden, die einfach ein bisschen fortgeschritten denken und die das einfach haben wollen, oder abgesetzte Backup-Netzwerke. Immutable Backup, das nicht mehr manipulierbar ist bis hin zu Logging.

Und da im Prinzip beim Logging ist es wichtig, nicht einfach irgendwo Logs mitzuschreiben, sondern dass da auch eine Heuristik dahinter ist. Ja, kostet alles Geld, aber wenn man einen Angriff verhindert hat oder möglichst früh aufgedeckt hat, dann hat man die Kosten von Jahren an einem Tag meistens herinnen.

Ja, Virenscanner usw. hat eigentlich jeder. Aber im Großen und Ganzen geht es wirklich darum: Es scheitert im Moment meistens an Maßnahmen der Erkennung bzw. der Möglichkeiten der Wiederherstellung.

H: Eigentlich, wenn man es genau betrachtet, dann sind die Maßnahmen, die von vielen Leuten als Basics betrachtet werden, dann halt in der Praxis auch nicht mehr so ganz sicher gegeben. Viele Leute sagen ja, ja ein Backup haben wir! Ja, wo ist das Backup? Das hängt am PC dran. Oder ist in der Serverfarm irgendwo live geschalten.

E: Nicht nur das. Es geht auch darum, was ist, wenn wirklich ein Angriff erfolgreich stattgefunden hat und die Firma steht? Was kostet das? Ja, und das müssen sich die Firma dann mal ausrechnen. Und dieses Bewusstsein fehlt oft noch.

H: Man hört immer wieder. Mehr oder weniger vergeht keine Woche, wo man irgendwo hört, dass wieder eine Firma gehackt worden ist und einen Ransomware-Angriff auf sich lasten hat, als auch Regierungen. Ich denke, dass da gerade die Dunkelziffer extrem hoch ist, weil viele Firmen das natürlich jetzt nicht groß ausplaudern.

E: Ja, kriegt man regelmäßig mit.

H: Grundsätzlich bei den Schutzmaßnahmen gerade beim User-Schutz, stellt sich oft die Frage, wie schafft man die Balance gut zu halten zwischen: Wir haben jetzt ein sicheres System und gleichzeitig ist die Usability für Nutzer nicht eingeschränkt.

Es gibt ja unterschiedliche Systeme, wo dem User auch während dem Arbeiten auffällt: „Aha, okay, da ist jetzt irgendeine Sicherheitsmaßnahme im Hintergrund“. Ob das jetzt ein Sandbox-Mail-System ist, wo eventuell potenziell gefährdende E-Mails geflaggt werden und dann freigegeben werden müssen usw.

Welche Maßnahmen stellen für die User fast keine Usability-Einschränkungen dar bzw. welche Maßnahmen bringen so viel, dass man sie trotzdem umsetzt, auch wenn die User mitkriegen, dass das Leben im IT-System etwas schwieriger wird?

E 1.3: Ja, also ich sag es kommt drauf an, wie gut die ganze IT-Landschaft oder auch die Landschaft der ganzen Services designt ist. Wenn ich jetzt her gehe und sage ich kaufe aus allen Ecken und Enden und schustere mir mein System zusammen, dann habe ich viele verschiedene Systeme die eine komplett inhomogene Umgebung.

Und wenn ich nachher absichern will, dann muss ich die User natürlich traktieren. Für alles haben sie ein eigenes Kennwort dort einen Token dort einen Authenticator usw. Und somit ist dann die Usability im Keller.

Man muss halt heutzutage auf eine integrierte Sicherheit schauen sowie Single-Sign-On ein Kennwort für alles. Heutzutage muss man schon fast sagen, eine mehrfach Multi-Faktor-Authentifizierung für vielleicht die meisten Systeme sollte reichen. Und da muss ich schon mal schauen, welche Authentifizierungs-Systeme verwende ich und wo kann ich sie überall einsetzen? Beispiel: Die komplette Umgebung in der Microsoft Cloud. Das Ganze kann wirklich viel. Die meisten Leute oder Firmen wissen gar nicht, was das Zeug alles kann. Ich habe dort meine Active-Directory User, die in den meisten Firmen die treibende User-Datenbank sind. Ich kann auch dort meine MFA machen. Und es gibt so wahnsinnig viele Systeme. Nur ein Beispiel fast jedes System kann LDAP bzw. Radius-Authentifizierung.

Ich kann meinen Windows Server Richtung Azure verbiegen. Es können auch zwei Server sein, wenn es redundant sein soll. Dann hat der User überall sein Windowskennwort und Single-Signe-on. Die Cloud erkennt das System. Sie erkennt, ob ich von intern oder extern komme.

Intern brauche ich keine MFA von extern schon und dann muss das halt am Handy bestätigt werden.

Im Prinzip hat der User immer das gleiche System. Er hat den Benutzer, das Kennwort. Und ich glaube, dass man so die Sicherheit hochschrauben kann, ohne den User großartig zu traktieren.

H: So dann, wenn man sagt okay, man hat jetzt gut das Sicherheitskonzept homogener in einem System umgesetzt, eventuell auch mit Zero Trust System. Besteht dann die Möglichkeit, dass man es zusammenbringt, dass wenn ein User, mit Laienwissen, grob fahrlässig oder bewusst böswillig agiert, dass die Sicherheit vom Netzwerk und von der Server-Umgebung trotzdem gegeben ist?

Wo man sagt, ja gut, er kann jetzt da Dateien löschen oder Viren einfangen?

Kann man das System durch die Sicherheitsmöglichkeiten so absichern, dass das System trotzdem nur minimalst gefährdet ist, selbst wenn die User einen kompletten Schwachsinn machen?

E 1.4: Ich sehe das so: Daten löschen hin und her ja passt. Mit Backup kann ich es wiederherstellen. Ich kann auch wenn ich will alle fünf Minuten einen Snapshot ziehen, von was auch immer. Da sehe ich nicht so die Gefahr. Die Gefahr ist aber eher, ich sage jetzt mal Viren, Malware.

Und da ist aus meiner Sicht, der unerfahrene User am gefährlichsten. Er erkennt am wenigsten, dass das eine gefakte E-Mail ist. Und auch wenn man noch so eine tolle Firewall und einen tollen Virenscanner hat und ich weiß nicht was alles noch.

Sicherheitslücken gibt es immer. Und so ist vielleicht der unerfahrene User am gefährlichsten, weil er keine Erfahrung hat. Wenn der irgendwas Falsches anklickt und wenn man anschaut, dass die meisten Hackerangriffe dadurch passieren, dass diese Gruppen halt eher über Schwachstellen Bescheid wissen, über die die anderen halt noch nicht Bescheid wissen.

Und das ist halt deren Vorteil. Und genau Unerfahrene sind dann halt das Opfer, die ausführende Person zu sein. Also ich kann ein Backup schon mal wiederherstellen. Aber ich sage jetzt mal, was ist heutzutage sicher.

Es ist nichts sicher oder von minimaler Sicherheit kann man jetzt reden, man muss nicht immer den Teufel an die Wand malen, aber ich glaube, dass es am besten ist, wenn man die Systeme so betreibt, dass man davon ausgeht, dass nichts sicher ist.

Und nicht sagen ja, das ist nur minimal gefährdet. Man kann nur schauen, regelmäßig observieren und Reviews machen. Was hat sich jetzt geändert? Welche Angriffs-Vektoren habe ich? Habe ich jetzt vielleicht was gefunden, was ich vielleicht ausschalten kann?

Aber mehr kann man nicht tun.

H: In deiner Erfahrung bestehen Angriffs-Vektoren eher durch unterlassene Wartungsmaßnahmen oder durch Exploits?

E: Ich glaube, das ist fifty fifty. Es gibt genug. Firmen oder IT-Abteilungen, die einfach nicht patchen. Vor zwei Jahren war ja das große Exchange-Server-Schlachten. Da war der Fix von Microsoft glaube ich drei Wochen vorher draußen und in Deutschland waren trotzdem über 20.000 Exchange Server nicht gepatcht und waren auf einem Stand aus dem Jahre Schnee.

H: Ja, wenn der Stand dann so alt ist, dass man sagt, okay, nur Knöpfchen drücken reicht nicht, weil man halt nicht nur Updates, sondern dann Upgrades machen muss. Ja, dann wird es problematisch, weil wenn die IT selbst sagt, dass dauert zwei Wochen und dann wird es spannend.

E: Aber wenn man anschaut, wie schnell es gehen kann im Hause (FIRMA) ist es rausgekommen und am selben Tag eingespielt worden. Ich glaube, die User haben es nicht einmal gemerkt. Ja, und das System war up to date, also quasi es ist ein Maximum gemacht worden.

Also es geht schon. Also es ist schon sehr viel Wurschtigkeit dahinter, auch, das merkt man schon. Aber zuerst ist die Zero-Day-Lücke und danach kommt die Wurschtigkeit.

H: Um auf den Anfang zurückzukommen … Du sagst, dass in vielen Abteilungen einfach ein Ressourcenmangel herrscht und dass viele Abteilungen glücklich sind, dass das System einfach läuft. Zum Teil ist allerdings auch die Reife von der Abteilung und von der Führung noch nicht gegeben, dass ggf. ein eigener Mann abgestellt wird, der sich um saubere Patch-Cycles usw. kümmert.

E: Absolut. Wir wissen, die Systeme werden immer komplexer. Das ist auch ein Grund dafür, warum Firmen ein bisschen mehr zahlen um in die Cloud gehen. Die Firmen sparen Personal ein und ich sage jetzt mal, die Ausbildung der Leute ist aufwendig geworden.

Und dadurch hat man Leute in den internen ITs mit relativ geringem Wissensstand und die sagen gut es läuft, never change a running system. Wenn ich eine Industrieanlage habe, die abgeschottet ohne Internet ist, dann ich brauche das nicht. Aber bei allem, was irgendwie verbunden ist, ist never change a running system ein absolutes no go heutzutage. Tragisch, aber wahr.

H: Dann würde ich sagen, zum Abschluss ganz kurz noch. Wir haben ja jetzt geredet über Zero Trust und anderweitige Technologien. Siehst du irgendeine Technologie, die in dieser Hinsicht zukünftig Sicherheitskonzepte durchaus transformieren oder reformieren könnte?

E 1.7: Darauf kann ich ganz schwer was sagen. Fast jeden Tag gibt es irgendetwas Neues mit Security im Großen und Ganzen. Es gibt ja eigentlich kaum mehr was heutzutage, was man nicht irgendwie absichern kann. Es gibt nichts mehr. Alles was auf den Markt kommt ist irgendwie auf Sicherheit getrimmt.

Zukünftige technische Sicherheit. Das Einzige, wo es noch vielleicht eine große Reform oder Änderung geben wird, das ist in der Heuristik Schrägstrich Richtung künstliche Intelligenz. Dass die ganze Sicherheit in Zukunft auf Verhaltens-Überwachung, dass die Systeme lernen, das tun sie auch jetzt schon teilweise.

Das Verhalten von Teilnehmern, Usern oder Externen zu analysieren und danach noch entsprechende Maßnahmen zu setzen.

Das war früher die Heuristik, heutzutage sagt man KI dazu. Das ist vielleicht schon ein bisschen was anderes, aber ich glaube, dass es in der Zukunft eine Rolle spielen wird, dass die Systeme einfach lernen.

H: Gut und jetzt die endgültig abschließende Frage. Bieten Subnetze, die über Firewall getrennt worden sind, im Endeffekt Sicherheitsvorteile im Vergleich zu einem großen Netz, was hinter der Firewall von der Außenwelt abgeschottet ist und welche Vorteile und Nachteile bilden die unterschiedlichen Architekturen?

E 1.5: Ich sage jetzt, das ist heutzutage absolut notwendig. Es kommt auf den Verkehr drauf an, ich muss vielleicht nicht unbedingt eine Firewall zwischen einem Windows Client und einem Windows Server mit aktiver und gepflegter Firewall haben. Denn in der Praxis schaut es schon oft so aus, ich habe zwar eine Firewall dazwischen, aber es ist heutzutage alles verschlüsselt. Das Problem ist einfach, dass die Angreifer heutzutage kaum über einen offenen Port kommen, sondern meistens über eine Applikation, über ein Protokoll, das sowieso offen ist.

Da sind heutzutage eher die Verwundbarkeiten, dass die Firewall alles absichert, das war vor 20 Jahren. Aber im Endeffekt ja, es ist ein Basic, ich lass nur jenen Traffic durch, der notwendig ist.

Was aber wichtiger ist, wenn ich das schon mache. Dann muss sich in den Traffic reinschauen können und das tut keiner.

H: Es ist allerdings in der heutigen Zeit mit dem Hineinschauen nicht ganz einfach, wenn alles verschlüsselt ist.

E: Ja, ich sage in einen SMP3-Verkehr muss ich nicht unbedingt reinschauen. Da sehe ich sofort, was da geschieht. Aber zum Beispiel über HTTPS, da sehe ich sehr wohl und das haben wir auch bei den Kunden im Einsatz, dass auf der Firewall Deep-Inspection für gewisse Policies aktiv ist.

Und da holt sich die Firewall sehr wohl was raus. Bis hin, dass auf der Firewall eine gewisse Applicationen-Awareness konfiguriert ist. Die Firewall kann es. Das braucht aber Ressourcen und auch Dienstleister, die Firewalls verkaufen wissen oft nicht wie viele Ressourcen. Wie viel Ressourcen eine Deep-Inspection oder Application Tools dann wirklich benötigen, wissen die oft nicht.

Deswegen haben auch die Firmen damit gar nicht die Möglichkeit, das aufzudrehen, weil sie es nicht haben. Das kostet richtig Geld.

Dann bringt die Firewall richtig was.

H: Heißt das, dass gerade bei Firewall-Konzepten, wenn man mit unerfahrenen Dienstleistern arbeitet, es bei der Aktivierung von Deep-Inspection zu Problemen kommen kann? Auch zum Teil von Unternehmen verschuldet, weil Ressourcen und Kosten gespart wurden und wenn man die vollen Funktionen aktivieren will, kommt es zu Überlastungen?

E: Genau. Es ist vielleicht ein bisschen weniger Komfort, weil die Firewall das Zertifikat austauscht, dass öfter mal was passiert, aber im Endeffekt wie viel Internet brauchen die Leute wirklich im Alltag?

Es werden gewisse Seiten benötigt. Die kann man sogar freischalten. Das kann jede FW. Alles, was irgendwie auf Microsoft.com geht oder auf Microsoft online geht. Ja, da brauche ich keine Deep-Inspection. Dort habe ich nachher Performance … auf den Rest der Welt für YouTube und sonstiges da soll er das ruhig machen. Ich meine natürlich, es kostet, aber das bringt wirklich Sicherheit, das fischt so viel heraus. Da gibt es ja noch weitere System-Click-Protection usw. Das Maximum, was das Geld hergibt, muss man heute herausholen.

Und das Zweite sind Vorteile. Ich sage ganz klar, ich kann auch Netzwerke komplett abschotten. Ich habe eh z. B. mein Backup-Netz.

Dann muss der Angreifer die Firewall kassieren, um im Prinzip ins Backup-Netz reinzukommen.

Nachteile hat es natürlich auch. Getrennte Subnetze. Um Gottes Willen, es ist mehr Verwaltungsaufwand. Die Firma muss mehr zahlen.

Das ist der einzige Nachteil.

H: Alles klar. Wunderbar. Dann, wenn wir schon kurz über Cloudauslagerungen und AI geredet haben. Hast du irgendeine Erfahrung mit Anti Viren Cloud Software?

E: Antivirus kommt aus der Cloud. So wie es früher war, wo er noch mit Signaturen gearbeitet hat, das gibt es heute nicht mehr. Und egal welchen Hersteller, ob Crowdstrike, Cisco, Trendmicro, Kaspersky oder sonst was, die leben alle aus ihrer Cloud. Signaturen sind nur ein Bruchteil.

Security kommt heutzutage aus der Cloud. Woher weiß eine Firewall, was gut und böse ist? Wenn jemand einen Link angeklickt hat. Der im Prinzip ein böses JavaScript oder sonst was runterholt. Das nutzt wieder irgendeine Sicherheitslücke im Office aus. Das kann der Virenscanner mit der Signatur nicht abfangen. Die Firewall, aber hat das vielleicht schon der Datenbank drinnen den Link und die kann das dann aktiv blocken. Und das ist alles Cloud.

Interview 2:

H: Gut, danke, dass du dir die Zeit nimmst. Sämtliche Namens-Thematiken und so weiter werden dann noch im Rahmen vom Transkript einfach entfernt, sodass Anonymität weiterhin gegeben ist.

E: Ja gerne bitte.

H: Seit wie vielen Jahren bist du im IT-Bereich tätig?

E: Generell begonnen mit Firma vor 20 Jahren und alles in allem 40 Jahre.

H: In wie vielen Unternehmen warst du in dem Zeitraum tätig? Als auch für wie viele Unternehmen hast du Sachen umgesetzt?

E: Vor Ort, also wirklich im Unternehmen waren das 10.

Und Remote mit Betreuung 25 und Kunden an sich kommen noch so ca. 90 dazu.

H: Ja, dann zur Hauptfrage. Also meine Diplomarbeit handelt eben von technischen Sicherheitsmaßnahmen, die man in Unternehmens-Netzwerken verwenden kann, um halt das Netzwerk, das Unternehmen und die Infrastruktur so gut wie möglich zu schützen.

Wobei ich mir natürlich bewusst bin, dass dies sowohl durchaus organisatorische Maßnahmen mit hineinzieht als auch den humanen Faktor, wobei ich mich halt explizit auf die technischen Sicherheitsmaßnahmen spezialisiere.

Ich bin mir über den humanen Faktor bewusst, aber das würde die Diplomarbeit sprengen. Insofern jetzt eben die Hauptfrage: Welche technischen Maßnahmen sind eben im Sinne von Netzwerk-Absicherung deiner Meinung nach sinnvoll?

E 2.1 + 2.2: Gut. Es ist für die Absicherung aus meiner Sicht das Wichtigste die Firewall. Das ist mit Abstand sicher der größte Punkt. Da gibt es viele Punkte und Faktoren. Keine Ahnung wie tiefgreifend wir das jetzt generell besprechen sollen.

H: Also ich meine jetzt unter Netzwerk-Absicherung nicht nur das Netzwerk selbst, sondern die gesamte IT-Infrastruktur also auch die Server, Sicherung usw. Wenn wir jetzt noch kurz über die Maßnahmen reden, können wir im Anschluss dann bez. Firewall, was für dich ja der wichtigste Punkt war, in die Tiefe gehen.

E 2.1: Okay. Grundsätzlich muss ich unterscheiden zwischen zwei Sichten. Die eine Sicht am Gerät selbst. Also wie sichere ich ein Gerät ab? Es wäre recht geschickt, wenn man die Windows-Schiene hernimmt. Dann sollte noch ein Virenscanner drauf sein und in Kombination mit diesem die lokalen Firewall-Einstellungen kontrollieren.

Somit ist wahrscheinlich der Benutzer an sich schon gut geschützt. Wenn man jetzt weitergeht, um das feiner abzusichern, dann sind am Gerät selbst noch User-Einstellungen zu treffen wie zum Beispiel „nicht Admin“ sein. Nun, dann hängt es davon ab, wie groß ist die Firma? Hat sie ein Active-Directory?

Dann könnte man sagen, okay, das Gerät ist vielleicht Mitglied in der Domäne, was in dem Fall dann höchstwahrscheinlich sehr sinnvoll sein wird. Da müsste man dann schauen, wie geht man damit um. Bei größeren Unternehmen ist das Gerät jetzt mit einem Zertifikat angemeldet oder nicht?

Welche Rechte der Benutzer am Gerät? Wie wird jetzt in dem Unternehmen weitergearbeitet? Das Beispiel hier ist in einer Citrix-Umgebung und aus dieser Sicht nicht so interessant. Für kleinere Unternehmen ist sie aber sehr interessant, denn die betreiben eine ganz andere Herangehensweise an ihre eigene Infrastruktur.

Da ist es meistens so, dass man eine Reihe von Clients hat und 1-2 Server betreibt. Mehr wird es in dem Unternehmen nicht sein. Plus dann natürlich ein File-Server. Da sind wir schon fertig. Mehr ist nicht. Wenn man jetzt es auf dem Gesichtspunkt betrachtet, ist eigentlich das Wichtigste, dass der Virenscanner aktuell ist auf den Clients plus am File-Server.

Für Kleinunternehmen ist das eigentlich der STANDARD und ist ausreichend. Die gesamten Geräte für Kleinunternehmen, wie gesagt, gehen über Firewall ins Internet. Bei größeren geht es natürlich dann schon weiter. Aber jetzt? Wie interessant ist es für dich jetzt: kleine oder größere?

H: Ich würde schon auf größere Unternehmen eingehen, wenn es möglich wäre? Es ist relativ spannend, wenn man da bisschen mehr in konzeptionelle Ideen abschweifen kann.

E 2.1: Okay. Also bei größeren finde ich es dann immer spannend, denn da kommt die Cloud-Nutzung mit hinein. Die Unternehmen musst du zuerst mal überzeugen, generell in Schutz zu investieren. Das ist die größte Hürde.

Dann geht es weiter, dass man sagen kann, okay, welches Konzept? Zum Beispiel ein Hybrid mit Cloud oder nur On-Premise-Schutz? Und dann entscheidet sich automatisch gleich mit, wie schaut es aus mit … Welche Dienste? Weil grundsätzlich das Wichtigste im Unternehmen ist meistens der File-Server und der Mailserver. Das sind die zwei Hauptpunkte, auf die Unternehmen abzielen.

Dann, wenn jetzt diese Unternehmen zum Beispiel Applikationen hosten, wie machen wir das? In den meisten Fällen macht man das nicht mehr On-Premise … Das ist alles in der Cloud. Dann gibt es die Entscheidung, gehst du zu Amazon oder in Richtung Microsoft?

Meine persönliche Erfahrung mit Amazon ist, dass das nicht gern genommen wird. Den Grund dessen kann ich ehrlicherweise nicht sagen. Microsoft wird sehr gern genommen, dort kommt am meisten durch das Mail und der SharePoint.

H: Also quasi wieder die Online-Varianten von Exchange und File-Server.

E: Nicht ganz, denn die Exposure aus Internetsicht vom SharePoint ist ja massiv. Du hast viel mehr Kanäle, wesentlich mehr Kanäle. Und du beziehst automatisch auch externe Kontakte mit ein, für Projekte.

Heißt, du legst ein Projekt an. Deine ganzen externen Lieferanten und Kunden oder Mitarbeiter ladest du ein, gibst denen Rechte und somit sind automatisch, ohne dass man sich dessen bewusst ist, alle möglichen Firmen-Informationen öffentlich. Jetzt hängt es davon ab, wie gut das Gegenüber den Zugang schützt. Dementsprechend öffentlich diese geheimen Dokumente für das Projekt sind. Das wird gern vergessen.

H: Dann, weil wir am Anfang über die Firewall geredet haben, was sind deiner Meinung nach gerade bei moderneren Firewalls die Vorteile, die diese mit sich bringen.

E: Die Vorteile werden noch nicht benutzt, meiner Meinung nach. Weil das wäre, zum Beispiel die zukünftig IPV6 und Zero Trust. Dies wird eigentlich von keinem Unternehmen genutzt, weil IPV6 gemieden wird. Und Zero-Trust auch gerade erst im Kommen ist. Da ist es schwer Schätzungen zu machen.

Aber eigentlich ist genau das, wo die größte Änderung wäre. Was wir jetzt noch ausgelassen haben, sind die Strategien, die im Unternehmen sonst noch greifen. Wie zum Beispiel Backup oder so. Hat jetzt mit einer Firewall an sich nichts zu tun.

Aber das Backup-Szenario ist ein ganz wichtiges, speziell für große Unternehmen, weil man damit natürlich, wenn die Firewall einmal versagt hat, auch zu seinen Daten kommen kann. Das wäre was ganz Wichtiges, was wir vielleicht noch besprechen sollten. Aber später.

Aber nun zum Thema Firewall. Das, was die Unternehmen heute machen, ist einfach eine klassische IP Firewall. Wenn die Unternehmer mehr Geld ausgeben möchten, dann hat man schon die Chance den ganzen Traffic zu filtern.

Das funktioniert mehr oder weniger gut. Das Hauptproblem ist: Es wird immer schwieriger, das überhaupt zu tun. Das heißt, die Firewall ist einfach ein zentraler Punkt, der filtert den Traffic. Jetzt ist es in den heutigen Zeiten nicht mehr ausreichend, weil immer mehr Verbindungen sind, SSL-Verbindungen, sprich sind kryptographisch dunkel, in die niemand mehr reinschauen kann.

Das wird immer schwieriger. Das heißt, eigentlich ist das Konzept mehr oder weniger veraltet und nicht mehr zielführend. Und deswegen der Ansatz mit Zero Trust. Weil da zieht man dann den Tunnel lustigerweise vom Client direkt auf die Firewall und dann hat man alle Möglichkeiten reinzuschauen. Dort wird der Traffic erst gebündelt, gefiltert und wieder woanders hin durchgelassen. Und es ist egal, wie segmentiert das Netz innerhalb der Firma ist.

H: Das heißt aus der Client Computer Sicht ist es dann so bei Zero Trust: Ich sage einfach zur Firewall, ich will dorthin, die Firewall delegiert mich dorthin. Aber der Client selbst hat eigentlich keine Ahnung, wo was ist.

E: Grundsätzlich richtig genau. Das setzt aber voraus und dann funktioniert das Konzept. Der Client installiert sich diesen VPN Client, denn es ist nichts anderes als ein ehrliches VPN und über den gesicherten Tunnel spricht er nur mit der Firewall und sonst niemanden. Im Idealfall gibt es kein einziges IP-Paket, das den Client verlassen kann.

Und damit wiederum ist es so, dass es komplett irrelevant ist für den Client, ob dieser im Unternehmen oder zu Hause oder in Amerika oder in Asien ist.

H: Und dann eine kurze Frage Es gibt ja bei FW nicht nur das Feature der Paketfilterung, sondern auch Paket-Inspection, wo dann wirklich zum Teil, wenn die Firewall die notwendigen Ressourcen hätte, das bereits bei der Firewall sozusagen durchschaut wird.

Wobei ich jetzt durch andere Experten auch schon weiß, dass das in den seltensten Fällen gemacht wird, weil man da einfach bei der Firewall immense Ressourcen braucht. Hast du in deiner Erfahrung schon mal den Fall gehabt, dass ein Unternehmen die Security so hochstellt, dass es sagt, es wäre zumindest darüber nachzudenken, dass man das organisiert?

Oder ist das ressourcentechnisch einfach so gigantisch, dass die meisten Firmen sagen: „Das ist uns das Geld nicht wert!“

E: Ich glaube, da geht es gar nicht so sehr um Geld oder Aufwand, sondern es geht um Praktikabilität. Das ist in keinster Weise praktikabel, weil wenn du diese Features alle aktivieren würdest, könnte niemand mehr in einer Art und Weise arbeiten, die für den User überhaupt noch brauchbar ist.

Jetzt gar nicht wegen Performance, sondern wegen Einschränkungen. Du kommst dann eigentlich zu deinen eigenen Diensten schon noch. Aber allerspätestens, wenn du Cloud-Dienste oder andere Firmen über andere VPN-Strecken oder ganz normale Webserver, die im Internet stehen, erreichen willst, wirst du dann in keiner zufriedenstellenden Art und Weise dort hinkommen.

H: Also müsste man, damit alles geht, wieder alles aufmachen, wodurch wieder kein Schutz gegeben ist.

E: Erstens das. Oder die Gegensicht, was aufgrund von HSTS immer spannender wird. Du hast andere Firmen oder deine gegenüber werden immer mehr dazu tendieren, das Aufbrechen des SSL-Kanals zu verbieten. Da gibt es eigene Mechanismen und das kann man setzen. Und wenn man das Flag setzt und dieser Kanal darf nicht aufgebrochen werden, somit ist diese ganze Inspection nicht mehr möglich … darf nicht mehr möglich sein. Damit hat auch die Firewall keine Möglichkeit mehr als „man in the middle attack“ reinzuschauen. Das heißt du hast jetzt das Riesenproblem, dass du teure Infrastruktur kaufst und die eigentlich gar nicht verwenden darfst, weil viele, die das mir gegenüber verbieten. Und da sind wir dann beim Punkt.

Somit ist eigentlich das, wo es hingehen muss, eigentlich. Es hat sich selbst überholt. Eigentlich.

H: Und bei Zero Trust würde es dann so ausschauen, dass dieser SSL-Tunnel quasi von der Firewall ausgeht und dann nochmal getunnelt zum Client geht?

E: Genau. Die Firewall ist in Wirklichkeit dann ein Application-Level-Proxy. Vor 20 Jahren war das ein Socks4 / Socks5 Proxy. Der hat es eigentlich genauso gefiltert mit Store and Forward. Und jetzt ist es aber noch ein Level höher. Dass die Streams in der Firewall erkannt werden. Das Ding ist in der Lage zu erkennen. Ist es jetzt Gif? Ist es ein Videostream? Ist das ein Textstream? Ist es ein Zip? Ist es Mail? Das ist ein echter Application-Level-Proxy.

Die kann das auseinanderdividieren und kann aufgrund vom Protokoll oder vom Port oder von der Kombination von diesen oder von User-Credentials erkennen. Was für Daten werden da transportiert. Ist es überhaupt sinnvoll, in den Stream reinzuschauen? Muss ich nur die ersten paar Pakete vom Stream filtern und dann ist es eh obsolet? Oder den gesamten durchgängig. Ist es ein Realtime-Stream? Wie Voice oder RDP-Protokolle. Da hat es keinen Sinn, die laufend zu filtern zum Beispiel. Hat man ein Mail oder Text oder sonst einen Download sehr wohl. Das ist dann das echte Plus einer Firewall, die diesen Stream dann filtern kann.

H: Was ich dem entnehme ist, dass die FW, insbesondere wenn man an Zukunfts-Szenarien mit Zero Trust denkt, den höchsten Schutz von außen anbietet.

E 2.7: Nicht nur von außen, auch zwischen den einzelnen Usern in Wirklichkeit. Das ist der größte Vorteil von Zero Trust. Benutzer eins und zwei sitzen am selben Schreibtisch nebeneinander und sprechen trotzdem nur über die FW miteinander. Es wird wirklich jedes Gerät, jeder Zugriff und jeder User gefiltert. Ich kann einstellen, dass der User 1 auf Gerät 1 komplett andere Rechte hat als User 2 auf Gerät 2.

H: Was natürlich durch die zwischengeschaltete Firewall dann im Falle eines durchgegangenen Virenangriffs wieder gigantische Vorteile bietet.

E: Genau. Die Profile sind total fein granuliert. Und zum nächsten Problem. Dieses gesamte Zero-Trust-Modell, was du da aufbaust, das Implementieren von dem Ding ist sehr kompliziert. Ist eine irrsinnige Hürde, denn du musst sehr viel Regeln und Layer definieren. Du setzt damit automatisch auf einen Hersteller, auf eine Software.

Ist grundsätzlich nicht schlecht. Aber das Problem ist, wenn diese Software, wenn dieser Hersteller Probleme hat oder wenn du da einen Konfig-Fehler hast, ist eigentlich das gesamte Konzept mehr oder weniger sehr kompromittiert.

H: Spannend trotzdem! Und bevor wir jetzt zu den Subfragen kommen, die ich noch habe, können wir noch mal einen ganz kurzen Ausflug in Richtung zurück machen zu dem was wir schon kurz gesagt haben. Backup?

E: Also, wenn wir zum Beispiel einen Virenscanner auslassen. Würde es in dem Grundmodell zu Zero Trust zum Beispiel dann sogar untergeordnete Rolle spielen.

Beim herkömmlichen Ansatz natürlich nicht. Welches Szenario verfolgt man? Und damit entscheidet es sich. Wenn man jetzt sagt, Zero Trust ist die Zukunft, das setzt man auf, da geht man hin, ist aber jetzt nicht aktiv. Das heißt, jetzt sind wir noch in der herkömmlichen Welt. Jetzt gibt es eben die herkömmlichen Segmentierungsmaßnahmen, VPNs und die Firewall.

Dann gibt es natürlich auf den Clients und auf den Servern auch die Sicherheitsmaßnahmen, aber auf den Clients gibt es auch noch die lokalen Schutzmaßnahmen wie den Virenscanner.

Die gibt es zwar bei der Firewall auch, aber die Betrachtungsweise ist eine ganz andere, denn die lokalen Virenscanner zielen auf alle Daten, die bereits im oder am Gerät sind ab und filtern diese beim Öffnen, beim Schreiben, beim Verschicken, beim Manipulieren. Die Virenscanner, die in der Firewall sind, haben einen ganz anderen Fokus, die durchsuchen hier Streams.

Sie sind zwei komplett nicht vergleichbare Konzepte und somit aber eine gute Ergänzung.

Wenn ich ein Problem habe, brauche ich einmal ein gutes Backup. Da empfehle ich aus meiner Sicht mindestens zweistufige Backups. Sprich ich mache echte Backups, also nicht nur Snapshots.

Wirklich echtes Backup, wo ich die Daten vom File-Server extrahiere auf einem anderen Medium speichere und dort in eine zeitliche Linie einordne. Zum Beispiel tägliche Backups, wöchentliche monatliche, jährliche in einem zeitlichen Ablauf und dann damit einhergehend würde einen zweiten Backup-Zyklus vorschlagen, der dann dieses erste Linienbackup übernimmt und wo komplett anders hin nochmal repliziert.

In welcher Form ist dann komplett egal, ob das jetzt Copyjob ist, ob das wirklich auf der Storage selbst ist, wo diese Dateien, die erstellt werden, vom Backup noch einmal kopiert werden oder ob das auf anderen Synchronisierungs-Mechanismus geht, je nachdem was das Ziel Storage für Möglichkeiten von Backups hat.

Ist die Ziel Storage so wie eine Nimble, kann die das sowieso bitweise synchronisieren zwischen zwei Rechenzentren. Natürlich ist das vorzuziehen. Ist das eine billigere Storage, nimmt man andere Mechanismen. Je nachdem wie viel man investieren möchte in das ganze Thema.

H: Ich nehme an als dritte Stufe? Könnte man sich ein Offline-Backup zusätzlich vorstellen.

E: Auf jeden Fall, egal wie jetzt, auf eine NAS oder auf Tape, das ist so oder so das maximale Desaster-Backup.

H: Das ist das ist ein Thema, was nicht jeden Tag geschieht, sondern wird, wenn es hochkommt, einmal die Woche gemacht. Im Endeffekt, wenn es mal ein Problem gibt, das System steht und alle anderen Stricke reißen, ist man froh darüber.

E: Genau. Das Desaster-Backup ist es ja nur so lang sinnvoll, dass man das besitzt, wenn man das dann auch speziell physisch sichert. Das macht eigentlich schon kaum jemand, weil das Desaster-Backup müsste man, ja, wenn man konsequent ist, in einen Tresor legen, der auch vor elektromagnetischen Strahlen schützt.

Zum Beispiel bleiben dann herausnehmbare Festplatten oder Tapes über. Das macht fast niemand mehr. Aber das wäre eigentlich in einem seriösen Umfeld schon zu empfehlen.

H: Alles klar. Wunderbar. Dann mal zur nächsten Frage. Wenn man da diese unterschiedlichen Schutz-Szenarien implementiert oder einsetzt und die unterschiedlichen Maßnahmen verwendet. Wie hoch ist die Einschränkung dann für die User? Das ist von dem Szenario abhängig. Aber wenn man jetzt von einem realistischen Jetztzeit-Szenario nur ohne Zero Trust ausgeht.

Wie sehr schränken die Maßnahmen dann die User in ihrem alltäglichen Leben ein? Wie hoch ist die Usability? Wie oft kriegt man irgendwo eine Warnung?

E 2.3: Wenn man die Schutzmechanismen auf ein Level einjustiert, das ein guter Kompromiss ist, würde ich sagen selten. Natürlich und das ist die Kehrseite der Medaille. Wenn man das auf genau dieses Level einstellt, ist der Schutz in Wirklichkeit nur mehr mittelgut.

Das kann nicht anders sein, weil wenn ich dem System viel abverlange, und sage verbiete mir viel, scanne viel, kontrolliere viel, dann leidet gar nicht so sehr die Performance, das ist nicht das Hauptthema. Die Systeme sind so gut, dass man das nicht merkt, aber die Usability leidet.

Also wenn ich dem Benutzer so viel verbiete, dass ich aus meiner Admin-Sicht glücklich wäre und sage ok das Gerät oder die System Infrastruktur ist gut geschützt, kann niemand mehr arbeiten. Vermutlich erreichst du in Wirklichkeit dann nur mehr die Grey-IT. Du erreichst damit ein Level, dass die User so behindert sind in der täglichen Arbeit, dass sie was viel Gefährlicheres machen.

Sie suchen sich Löcher, die noch offen sind und bespielen dann die Löcher massiv, ohne dass du merkst, dass eigentlich in Wirklichkeit die Gesamtsituation darunter leidet. Darum ist es aus meiner Sicht eine sehr gute Entscheidung nur ein Mittelmaß einzustellen und die User zu trimmen und zu sagen: Bitte nutzt das System so, wie es angedacht ist. Und dann muss man auf Awareness und auf Schulungen der User setzen, dass sie die Blödsinnigkeiten nicht machen.

H: Gut. So ist zumindest deiner Meinung nach, selbst wenn man sagt, okay, ich mach das bestmögliche Netz mit jetzigen Standards nicht möglich, das Netz so zu schützen, dass selbst durch grobe Fahrlässigkeit oder sogar mutwillige Zerstörung der User das Netz nicht gefährdet ist.

E 2.4: Exakt. Genau. Das ist komplett sinnlos und eine komplette Illusion.

H: Inwiefern, wenn man jetzt die gleiche Fragestellung hernimmt, würden sich die Parameter dazu ändern, wenn man sagt man setzt das Ganze in der Zukunft mit Zero Trust auf?

E: Ich glaube nur bedingt. Weil das Hauptproblem bleibt bestehen. Jeder Schutz, egal in welcher Art, limitiert immer Gerät und User, sonst ist es ja kein Schutz. Und sobald du auf Schutz setzt, erzwingt es automatisch Frust. Das ist so! Und wenn jetzt dieser Frust zu groß wird, wird sich der User immer in jedem Szenario einen Ausweg suchen.

Der User will sich nicht limitieren lassen und sucht einen Ausweg. Und wenn man alle Auswege blockiert, dann ist das aus meiner Sicht komplett egal, ob man auf herkömmliche Modelle oder auf Zero Trust setzt. Bei Zero Trust kommt man vielleicht ein Stückchen weiter, weil auch die Einstellmöglichkeiten viel besser sind.

Also ich bin nur schwer misstrauisch und schwer skeptisch, dass das überhaupt auch in Zukunft gut funktionieren kann. Also ich glaube, du wirst immer Kompromisse machen müssen, die in jeder Firma und in jedem Bildungslevel bezüglich der IT von den Usern anders sein müssen.

Da gibt es keine Aussage, die für alles immer zutrifft. Das kann nicht möglich sein.

H: Bieten durch getrennte Subnetze Sicherheitsvorteile und welche Vorteile wären das?

E 2.5: Also grundsätzlich ja, natürlich. Der größte Zugewinn ist auch der, wenn man sich einen Virus einfängt und der sucht benachbarte IPs oder Geräte oder was auch immer, dann segmentiert man das einfach durch genau das schon runter.

Und die Anzahl der Geräte, die auffindbar sind und angreifbar sind, reduziert sich drastisch. Der Escape aus dem VLAN ist schwieriger. Du brauchst genau Zugriff auf diesen Hub oder diesen zentralen Punkt, über den du drüber musst, damit du wo anders hinkommst bzw. was anderes findest. Dies ist eine wirklich sehr kostengünstige und einfache Methode, der fast keine Performance-Einbußen bringt, den man sofort umsetzen kann.

H: Also kann man von Nachteilen technisch maximal davon reden, dass wenn die Firewall bereits am absoluten Limit ist, von der Performance her, dass es dann schwierig ist das umzusetzen.

E: Genau.

H: Wo siehst du basierend auf deinen Erfahrungen bei den Unternehmern in der STANDARD IT von der Infrastruktur her die größten Schwachstellen?

Gibt es da Muster sozusagen oder ist das wirklich komplett unterschiedlich?

E 2.6: Die mit Abstand größte Schwäche ist Human Error und die Awareness ist eigentlich mit Abstand im Faktor 1 Million zu eins das größte Problem. Es ist der Mensch an sich, das Nicht-Erkennen der Gefahr, das Nicht-Wahrnehmen der Geschäftsführung des Themas IT und Security, das allergrößte Problem.

Du musst immer zuerst die Geschäftsführung überhaupt motivieren und zum Investieren überreden. Dann kommt es darauf an, wie viel es ist. Das ist aus meiner Sicht das allergrößte Problem. Sobald du einmal Geldmittel hast, ist die Verteilung von diesen in einen vernünftigen Virenscanner, in eine vernünftige Firewall, in ein vernünftiges Backup und sonstige Dinge eine Kleinigkeit.

Das Hauptproblem ist das Akzeptieren überhaupt, dass die IT die finanziellen Funds braucht.

H: Okay, das heißt aber grundsätzlich, wenn man jetzt bei rein technischen Maßnahmen sieht, ist eigentlich kaum ein Unterschied, sondern es ist halt wirklich der humane Faktor, der das größte Verbesserungspotenzial hat.

E 2.6: Genau.

Weil wir sprechen vom Geldbörsel. Je nachdem wie viel man dann an hineinwirft in den Topf, wird es besser oder schlechter. Aber nur jeder Euro, der investiert wird, macht es automatisch besser.

H: Und dann zur letzten Frage, wenn man jetzt sagt, okay, Zukunft, Sicherheitskonzepte, was sind dort die Möglichkeiten, auch mit eventuell zukünftig herauskommenden Technologien? Wird da deiner Meinung noch rauskommen, was sozusagen die STANDARD-Security-Gedanken, wie man ein Netzwerk aufbaut, wie man es absichert, komplett revolutionieren wird? Oder ist da zurzeit noch nichts am Horizont? Wir haben jetzt schon über Zero Trust geredet, was man ja eigentlich in der Hinsicht sagen kann. Was mir in der Literatur-Recherche immer wieder untergekommen ist, wobei das alles sehr in den Sternen steht, wären AI unterstützte Firewalls.

E 2.7: Das kann ich nicht sagen. Das zweite Thema, das große was auf uns zukommen wird, ist IPV6, weil der Hauptunterschied zu IPV6 ist erstens die verschlüsselte Kommunikation an sich und zweitens die über Grenzen hinweg vorhandene Root-Fähigkeit. Das bringt noch sehr viele Probleme und nicht geahnte Türen, die dort geöffnet werden.

Da gibt es auf jeden Fall noch sehr viele Probleme, die mit IPV6 kommen werden. Und natürlich auch Chancen und Möglichkeiten. Aber wir reden hier über Probleme und über Risiken.

H: Alles klar, also könnte man durchaus sagen, dass unter die Zukunftstechnologien, die Verbesserungen bringen könnten, wir im Bereich von Zero Trust unterwegs sind und von der problematischen Seite, aber auch von den Chancen her, dürfte IPV6 noch eine spannende Herausforderung darstellen.

E 2.7: Genau richtig.

Interview 3:

H: Los geht's. Ja. Vielen Dank, dass du dir Zeit genommen hast fürs Interview.

Jetzt einfach mal ganz kurz. Damit du dich kurz vorstellen kannst. Seit wie vielen Jahren bist du in dem Bereich tätig?

E: Also seit neun Jahren. Also da ist jetzt die Ausbildung nicht drin. Also das zähle ich nicht dazu. Jetzt neun Jahre, wo ich wirklich dabei bin Vollzeit im Job.

H: Alles klar. Wie viele Jahre davon hat die Security Context?

E: Sieben … Ja wir sind jetzt bei sieben Jahren.

H: Perfekt. Bei wie vielen Unternehmen warst du in den letzten neun Jahren? Bzw. für wie viele Unternehmen warst du im Laufe deiner Karriere tätig?

E: In Bezug auf Netzwerk-Sicherheit, das hast du mir ja geschrieben, dass das das Thema deiner Diplomarbeit ist. Ja, da haben wir schon die 25. Plus natürlich hier bei uns im eigenen Unternehmen.

H: Alles klar. Ja, eh wie du es gerade vorher kurz gesagt hast. Netzwerk-Sicherheit, technische Maßnahmen sind das Thema für meine Diplomarbeit. Nochmals vielen Dank, dass du dir die Zeit dazu nimmst.

Welche technischen Maßnahmen sind deiner Meinung nach und vor allem deiner Erfahrung nach natürlich zur Netzwerk-Absicherung sinnvoll?

E 3.1: Da haben wir natürlich, wenn ich jetzt beim Thema Netzwerk-Sicherheit an die Ausbildung denke, das OSI-Modell im Kopf, das muss man können. Und beim Modell, wenn du dir das ganze vorstellst zum Datensichern, nehmen wir einfach die Firewall. Wir haben auf Schicht zwei, das mit MAC-Adresse, auf Schicht 3 die IP-Adresse auf Schicht 4 das TCP Protokoll, da gibt es überall sicherheitstechnische Maßnahmen, die da den Datenverkehr weiterleiten oder blockieren können.

Also ich glaube für das Netzwerk Thema mit dem OSI-Schichtenmodell mit der Firewall, da kann man schon mal richtig viel machen und das solltest du auch gemacht haben. Man kann natürlich darauf noch einen Proxy laufen lassen, das wäre Schicht 7. Da kannst du auch wieder mehr Sachen machen. Also beim Thema Firewall würde ich sagen ist schon richtig viel möglich.

H: Und dass die Firewall dann bei dementsprechender Einstellung möglicherweise sogar ein Application Proxy darstellt.

E: Genau das meinte ich. Ich hoffe, ich habe mich nicht unklar ausgedrückt. Ja, dann haben wir natürlich hier das VPN. Mit den englischen Fachbegriffen geht es ja schon los.

Nein, wir müssen uns halt einfach auch beim Thema Netzwerke über Verschlüsselung unterhalten, dass die Daten halt auch verschlüsselt sind. Ob das jetzt mit TLS, mit SSH oder mit IPV6 verschlüsselt ist, das ist im Grunde genommen egal. Hauptsache wir haben halt VPN oder wir haben eine Daten-Verschlüsselung bei der Kommunikation, weil die Daten hin und her zu schicken, wenn jeder im Netzwerk mitlesen kann, wäre unklug.

Ja, das Thema Netzwerk-Absicherung … Technische Maßnahmen … Ich weiß jetzt nicht, ob du Antivirus-Software dazu zählst. Also für mich ist das ja schon wieder fast wieder Software und geht weniger technisch rein.

H: Grundsätzlich ist für mich der Begriff der Netzwerk-Absicherung ein bisschen breiter gefasst und bezieht sich nicht nur auf die Netzwerke Firewall und Routing usw., sondern tatsächlich auf das Firmen-Netzwerk. In dieser Netzwerk-Landschaft gibt es Server, Switches und so weiter und so fort.

E: Ja, für das ganze System im Netz, da brauchen wir dann natürlich in Asset Management drüber. Damit wir wissen, welche Geräte sind da. Und falls sich da ein neues Gerät einloggt ins Netzwerk, dass wir das sofort erkennen können.

Asset Management ist da super wichtig. Zugangs-Richtlinien sind super wichtig. Ich kann ja sagen, wer hat Zugriff auf die Hardware, wer hat Zugriff auf welche Bereiche im Netzwerk. Also das Identity und Access Management, das kannst du ja dann dementsprechend auch schärfen, bis hin zur Kontrolle von dem Nutzer.

Superwichtig ist halt das Thema Multi-Faktor-Authentifizierung. Das merken wir auch immer, wie häufig das angefragt und umgesetzt wird. Einfach, wenn sich die User beim Kunden einloggen wollen, dass sie da nicht nur mit Passwort, sondern halt nur mit Multi-Faktor-Authentifizierung drauf zugreifen können.

Weitere technische Maßnahmen … Wenn wir jetzt an klassische User denken, die schicken sich ja die ganze Zeit Mails hin und her. Und was heute unverschlüsselt über Mails verschickt wird, das ist grausam. Ich würde da sagen, wir brauchen dann eine Mail-Absicherung.

Ich rate da gern zum Mail-Sand Boxing. Das ist natürlich aufwendig, kostet Zeit, aber es hat natürlich da auch die Vorteile, wo dann sowas wie Phishing oder Malware, die mitgeschickt wird, geblockt wird. Wir hatten ja vorhin noch das Thema Asset Management, da musst du natürlich auch Endgeräte-Sicherheit machen.

Also da ist ja nicht nur Mobile-Device-Management, wir haben ja alle unsere Firmenhandys plus Notebook, Laptop und diese ganzen Unternehmens-Geräte. Du bist ja selber auch noch häufig im Homeoffice.

Ich bin auch noch zwei Tage die Woche mal im Office da, da brauchst du halt solche Themen. Da sind die Netzwerk-Sicherheitsanforderungen einfach gestiegen.

In welche Richtung wollen wir gehen? Über welche Maßnahmen möchtest du mehr wissen?

H: Wir haben jetzt schon einiges gesagt. Grundsätzlich deiner Meinung nach, gibt es irgendeine dieser Maßnahmen, die wir jetzt kurz durchgesprochen, wo du sagst, das ist sozusagen der Fels in der Brandung? Welche ist für dich die wichtigste Maßnahme sozusagen da?

E 3.2: Für mich sind alle Maßnahmen wichtig, die den User daran hindern kompromittierende Vorgänge zu machen. Oder halt das Customizing von einer gescheiten Firewall-Einstellung, das ist mit einer Benutzer-Überprüfung, das ist mit einer Mail-Absicherung, aber das betrifft auch Netzwerk-Segmentierung. Das ist bei einem Unternehmen, wenn die halt klassisch Management und Produktion haben, halt einfach eine Aufteilung der Netze. Da kann man auch schon viel machen.

Auch bei der Endgeräte-Sicherheit, da schau einfach, dass der User so wenig wie möglich falsch machen kann, indem du ihm durch technische Maßnahmen so viel Sicherheit wie möglich gibst. Und das Ganze nicht dem User überlassen, immer schön die Updates von zentraler Stelle aus verwalten.

Nicht, dass der User da noch mit dem Klick das Update bestätigen muss. Die Updates betreffen nicht nur die Enduser, sondern eben auch die Netzwerkkomponenten.

H: Wir haben jetzt schon von einigen Maßnahmen geredet und auch, dass das die User unter anderem betreffen kann. Mit welchen Einschränkungen kann der User sozusagen rechnen, wenn diese Maßnahmen umgesetzt sind?

Bzw. welche Maßnahmen schränken den User am meisten ein oder stören ihn am meisten im Alltag?

E 3.3: Also das, was wir jetzt mitbekommen haben, ist, dass Mail-Sand Boxing die meisten Leute stört, weil sie halt bei der E-Mail denken, ich drück auf Senden und das Ding fliegt los und das kommt an.

Ich frage mich immer dann … Wir haben die sicheren Unternehmens-Netzwerke mit File-Shares mit allem aufgesetzt und die schicken sich die Unternehmensberichte immer noch per E-Mail hin und her. Dann kriegen wir leider vor allem auch aus der höheren Führungsebene zu hören: Warum müssen wir Mail-Sand Boxing machen?

Das würde sie ja so sehr einschränken. Ich glaube, das ist kein Problem. Das kriegen wir dann meistens gut argumentiert, dass es da doch auch um die Sicherheit von dem ganzen Unternehmen geht. Ja, was heißt gut? Da gibt es natürlich immer wieder Verschwörungen, aber ich würde schon sagen, dass so was den User einschränken könnte.

Sonst würde ich das eher gering sehen, ob da jetzt ein Antiviren-Programm läuft, ob ich da Updates mach, wie die Firewall eingestellt ist, das kriegt der User nicht mit … Der soll ja auch

nicht auf allen Webseiten unterwegs sein. Also es ist ja auch Arbeitszeit und da soll er auch arbeiten und produktiv sein, da braucht er auch nicht alle Ports freigeschaltet.

H: Ja, das stimmt. Ja dann von dem, was wir jetzt geredet haben. Wenn man jetzt davon ausgeht, dass man ein komplett neues Sicherheitssystem aufsetzen kann … Eine komplett neue Netzwerke-Infrastruktur … Budget so viel, wie man braucht.

E: Na also, das ist ja echt unrealistisch. Aber können wir gerne mal machen.

H: Ja, lass uns einen Gedanken zu Ende spielen. Bestünde dann irgendwie die Möglichkeit, dass man das Netzwerk tatsächlich technisch so gut absichert, dass man sagt, Okay, selbst bei grober Fahrlässigkeit oder Böswilligkeit kann der User das Netz nicht gefährden oder die Firmen-Infrastruktur nicht gefährden.

E 3.4: Ja, wir können einfach keine User nehmen, dann wäre das auf jeden Fall gegeben. Also wenn, wenn wir keine User haben, dann ist das natürlich auch von dem User nicht gefährdet. Ich würde sagen, das geht nicht. Da sind wir noch nicht.

Du hast ja auch gesagt, ein mutwilliger User. Also wenn der User wirklich dem Unternehmen schaden will … Das kriegt man ja auch ab und zu mal mit, wenn ein Mitarbeiter entlassen wird und nicht schnell genug die Zugänge gesperrt werden.

Da gibt es ja auch dann richtige Probleme, die der User machen kann. Geht aber auf jeden Fall so, dass wir da den Schaden einschränken können. Vor allem, wenn du sagst, wir haben Budget ohne Ende, kann man auch überlegen, ob man so was wie Zero Trust macht.

Wir können uns überlegen, wie wir die Endpoint Security umsetzen, dass wir da Unified Endpoint Security machen, da geht viel. Aber ist es wie überall, wir haben keine hundertprozentige Sicherheit, die gibt es einfach nicht. Wir sind bei 99,9 %, aber bei diesem 1 %, kann der User, wenn er gut ist, auch was machen.

H: Dann die grundsätzliche Frage: Bieten durch eine Firewall getrennte Subnetze einen Sicherheitsvorteil?

E 3.5: Natürlich also einfach, dass ich bei den Firewalls zwischen den Netzen noch mal den Traffic überwachen kann, da die noch mal filtern kann. Wenn wir einen Angriff haben, wir haben einen Breach da drin, dass sich der …

Wir nennen das immer die laterale Bewegung. Da kann sich der Angreifer innerhalb des Netzwerks nicht von rechts nach links bewegen. Da können wir schon viel machen. Du kannst

dann auch überlegen, ob du da wieder eine Multi-Faktor-Authentifizierung rein baust, aber das wäre dann wieder zu viel.

Also ich würde sagen, getrennte Subnetze durch Firewall hat viele Vorteile, einfach für die Sicherheit und dass der Schaden halt abgeriegelt ist und sich natürlich dann nur auf dieses eine Subnetz bezieht.

H: Gibt es irgendwelche Nachteile diesbezüglich?

E: Die Nachteile würde ich da eher sehen. Ist die Budgetierung oder die Führungsebene. Wir haben kein Problem normalerweise das Budget rauszuschlagen, weil IT Security kostet halt. Die User, wissen wir, sind ein kritischer Punkt bei Sicherheit. User müssen geschult und kritisiert werden.

Nachteil bei solchen komplizierteren Maßnahmen, die über den STANDARD-Schutz gehen, ist, dass es schwierig ist das bei den Geschäftsführungen durchzuboxen. Da gibt es teilweise dann echt Leute, die sich dagegenstellen und sagen: Brauchen wir das? … Ist doch alles Schwachsinn. Also das sehe ich bei vielen von solchen weiterführenden Maßnahmen wie z. B. von der Firewall getrennte Subnetze. Nachteil ist da einfach nur, das überhaupt bei dem Kunden implementieren zu können, auch wenn das auf den Preis ausschlägt. Dazu kommt natürlich, dass der Konkurrent das nicht mit aufnimmt und sagt: Das brauchen Sie nicht.

Dann habe ich auf einmal für uns halt Nachteile. Der Kunde hat davon keine Nachteile, der hat ja eigentlich nur eine bessere Sicherheit.

H: Von den ganzen Maßnahmen, die wir durchgesprochen haben, wo siehst du da so in der Regel das größte Verbesserungspotenzial?

E 3.6: Ich glaube, das größte Verbesserungspotenzial sehe ich da definitiv in den Einstellungen. Also wenn du dir da die Hardware anschaust, wie die gehandhabt wird, da kann viel gemacht werden. Was aber genauso groß ist, würde ich sagen, einfach die ganzen veralteten Geräte, veraltete Sicherheitssoftware, veraltete Standards. Also da sollte mal wirklich gescheit drüber überlegt werden, ob die technischen Maßnahmen alle noch up to date sind. Und wenn, dann sollte das Update mal passieren. Also da sind viele Sicherheitslücken, die schon längst geschlossen werden könnten, die immer noch bestehen, weil da auch aus der obersten Führungsebene so viel Widerstand gegen das Thema besteht.

Und zu sagen, das brauchen wir nicht so genau. Da reicht es doch, wenn wir das noch aus dem letzten STANDARD nehmen oder das System von vor drei Jahren.

Da muss halt einfach mehr Geld, Budget und Unterstützung hinter das Thema.

Netzwerk-Segmentierung haben noch wenige in einer fortgeschrittenen Form oder auch in einer Zero-Architektur. Also da würde für mich auch Verbesserungspotenzial bestehen, aber ist das halt nicht das, was die Unternehmen umgesetzt haben.

H: Jetzt dann noch ein kleiner Ausblick, was zukünftig möglich ist. Was sind deiner Meinung nach potenzielle zukünftige Sicherheits-Technologien, die eventuell die Denkweise, wie man heutzutage an IT-Security-Konzepte herangeht, reformieren könnten?

E 3.7: Da ist definitiv das Thema AI zu nennen. Wir haben jetzt bereits Artificial Intelligence bei der beim Incident Response Management im Einsatz bzw. bei der Erkennung.

Die AI kann das Ganze analysieren, die kann Nutzerverhalten analysieren und sieht dann okay, das ist nicht der Nutzer, der verhält sich jetzt gerade komplett anders. Ja, ich kann mit einer AI das Ganze viel schneller finden, als wenn ich das von Menschen untersuchen lasse. Die findet das halt innerhalb von Sekunden oder Minuten, wo ein Level-drei- oder Level-vier-Analyst, halt einfach fünf Stunden sitzt.

Und wir haben natürlich den Riesenvorteil, wenn wir das Ganze automatisiert laufen lassen, das reduziert die Zeit. Wir brauchen da die Rechenleistung, die dafür die Zeit uns wiedergibt.

Da können wir AI viel machen … Wo wir noch nicht ganz sind, aber wo der Weg hingehen wird, ist die AI nicht nur falls etwas passiert einzusetzen, sondern auch aktiv im Schutz zu verwenden.

Wir haben ja schon gesagt, dieses Nutzerverhalten wird analysiert. Ich kann ja dieses Nutzerverhalten mir anschauen und Tendenzen sehen. Wenn dieser Nutzer dazu neigt, dass er Security-bedenkliches Verhalten den Tag legt, dann kommt er halt wieder in eine Schulung rein.

Also alles das, wo wir den User steuern können, da kann die AI viel übernehmen. Wenn die AI am Ende nicht sogar unsere Firewalls macht oder managed. Die können ja so viel lernen, das ist ja ein Riesenthema, was da alles geht. Gut, wir haben halt da Rechenleistung, die wir dahinter brauchen, aber das ist schon schön.

H: Aber wenn ich deine Gedankengänge ein bisschen durchforste, sieht es für mich so aus, dass du der Meinung bist, dass die technischen Sicherheitsmaßnahmen schon reformiert werden, aber dass wir zukünftig vor allem technische Sicherheitsmaßnahmen sehen werden, die halt eben die User besser machen.

E 3.7: Genau bzw. wir haben die Technologie, die besser wird. Eine der Gefahrenquelle ist eindeutig der User. Und wir hatten ja vorhin die Frage, bez. mutwilliger oder grober Fahrlässigkeit. Die technischen Maßnahmen können AI-gestützt auf jeden Fall so viel besser werden, dass der User immer und immer weniger machen kann.

Das zielt nicht darauf ab, dass der User besser wird, sondern einfach, dass der User weniger schlecht machen kann oder dass wir schon vorher erkennen, dass der User was Falsches macht. Aber ich denke schon, das Thema AI, das kann viel machen.

Wir haben unser Asset Management, haben ganz am Anfang ja drauf geschaut. Wir müssen schauen, welche Geräte sind drin. Wenn ich da ein neues Gerät habe, wie schnell das ein Mensch erkennt? Schwierig. Wie oft schaut er sich das im Jahr an? Wie oft schaut er sich das am Tag an?

Wie viele Geräte sind gerade angemeldet oder wo ist mein neues Gerät? Die künstliche Intelligenz hat das innerhalb von Millisekunden. Überprüft das mal bitte.

Bei der Incident Response, da nutzen wir AI mittlerweile schon. Wir können damit natürlich auch ein bisschen unsere Controls, die Effektiveness damit überprüfen. Wir können bei Pentests, da wird sicher die AI deutlich bessere Ergebnisse liefern.

Also ich denke, das Thema Artificial Intelligence für Cybersecurity, da beschäftigen sich ja auch die großen Unternehmen mit.

Da steckt ja Geld und Manpower dahinter, dass die entwickelt wird und das wird. Wenn wir da dann standardisierte Lösungen bekommen, die wir dann auch für unsere Kunden in dem Sinne einsetzen können … Das wird sicher das Zukunftsthema werden.

Interview 4:

H: Ja. Vielen Dank, dass du Zeit gehabt hast fürs Interview. Ich schreibe jetzt gerade eine Diplomarbeit in Richtung technische Sicherheitsmaßnahmen zur Absicherung von Unternehmens-Netzwerken. Und fangen wir kurz mit einer Vorstellung an! Seit wie vielen Jahren bist du jetzt eigentlich schon im Zeitbereich tätig?

E: Ja. Tätig im IT-Bereich bin ich seit circa 20 Jahren und im Security-Kontext bin ich seit 15 Jahren unterwegs.

H: Alles klar, super. Vielen Dank. In wie vielen Unternehmern bzw. für wie viele Unternehmen warst du in deiner Karriere bereits tätig?

E: Über die 20 Jahre habe ich für sieben Unternehmen gearbeitet. Wobei ich gerade als IT-Dienstleister eben auch zum Aufsetzen von unterschiedlichen Security-Konzepten immer wieder für andere Firmen gearbeitet habe.

H: Okay und circa nur ganz grob eine Kennzahl: Für wie viele Firmen warst du da bereits tätig bzw. hast du technische Umsetzungen gemacht?

E: Grob über den Daumen gepeilt werden das schon so um die 30 bis 40 Firmen gewesen sein.

H: Super. Ja, also wie vorher schon angesprochen, handelt meine Diplomarbeit von technischen Maßnahmen zur Netzwerk-Absicherung.

Die Hauptfrage ist, welche technischen Maßnahmen sind im Rahmen einer IT-Sicherheitsumsetzung für eine ordentliche Netzwerk-Umsetzung notwendig?

E 4.1: Also das ist natürlich ein sehr breitgefächertes Thema. Wir reden da von unzähligen Komponenten, die aufeinander einfließen. Persönlich würde ich sagen, ein absolut essenzieller Bestandteil wird natürlich schon die Firewall sein. Das ist das Kernstück einer jeden IT-Sicherheitsstruktur.

Und gleichzeitig kann man da natürlich auch über Backup-Strategien und Netzwerk-Architektur im Allgemeinen reden. Also reden wir hier von sauber getrennten Subnetzen … denkt man eventuell auch an zukunftsträchtigere Thematiken. Reden wir jetzt zum Beispiel von Software-Defined-Networks oder von Zero Trust?

Oder wir können natürlich auch über die Thematiken reden, wo man sagt, das ist heutzutage im IT-Security-Lingus im Basis-Bereich, was aber trotzdem nicht unterschätzt werden kann, denn ohne diese Maßnahmen hat man trotzdem das Problem, dass es dann immer wieder zu Lücken kommt.

Also da reden wir im Basis-Bereich von WSUS, Backup-Strategien und auch von Mail-Absicherungssystemen in der Hinsicht, dass die User nicht einen jeden Müll zugestellt bekommen. Aber das geht auch in Richtung Endgeräte-Sicherung, mit Anti-Viren-Software, mit allgemeinen Einschränkungen für die Endgeräte im Unternehmen.

H: Das ist ja schon mal eine ziemliche Menge, die wir jetzt angesprochen haben. Welche Maßnahme ist im Sicherheitskontext und vor allem dem technischen Sicherheitskontext deiner Meinung nach die wichtigste bzw. welche bietet den besten Schutz?

E 4.2: Grundsätzlich ist es auf jeden Fall so, dass man schon sagen muss, dass in einer Basis-Form alle Komponenten passen müssen. Also man kann jetzt nicht hergehen und sagen, ich baue mir eine Firewall und der Rest ist egal, sondern es muss tatsächlich so sein, dass sämtliche Bereiche in einer gewissen Basis-Form vorhanden sein müssen, wie sie ja bei einem einzelnen Endgerät auch vorhanden sind.

Beim einzelnen Endgerät einem Windows-10-Rechner zum Beispiel ist es ja so, dass der Windows Rechner per se schon viele Basis-Komponenten hat. Es gibt einen Windows Defender, der gleichzeitig auch als Antivirus- Software agiert und eben auch gewisse Programm-Behaviours nachvollzieht.

Windows hat eine integrierte Firewall. Es gibt eigene Updatezyklen und wo dich Windows mehr oder weniger dazu zwingt ein Update zu machen. Also die Basis per se muss schon einmal gegeben sein und erst dann kann man sich darüber Gedanken machen, welche Maßnahmen tatsächlich noch großen Schutz bieten.

Wenn man sagt, die Basis passt, dann ist aus technischer Sicht meiner Meinung nach die Netzwerk-Architektur, als auch die Firewall schon einer der Kernpunkte, weil das natürlich die große Schnittstelle nach außen ist, die angegriffen werden kann.

H: Gut, dann auf jeden Fall schon mal vielen Dank. Wo sind bei der Netzwerk-Absicherung und der Firewall oder wie wir auch kurz geredet haben, bei der Anti-Viren-Software Einschränkungen für die User? Stören sie die User beim Arbeiten?

E 4.3: Es ist schon so, dass der User möglicherweise was mitbekommt. Aber wir reden ja jetzt auch von vielen Maßnahmen, die für den User auch, solange er in einem Unternehmen tätig ist, selbstverständlich sein sollten.

Man sagt ein User, der in einem Unternehmen ist, wird nicht auf seinem Rechner im Browser alle Webseiten aufrufen können. Und das wird auch von den Usern heutzutage schon verstanden und wahrgenommen.

Also das ist jetzt nicht so, dass die Nutzer kein Verständnis dafür haben. Es gibt da natürlich gewisse Einschränkungen, wo die User dann sehr schnell an ihre Schmerzgrenze stoßen. Das ist dann meistens, wenn es tatsächliche Performance-Einbußen durch die Sicherheitskomponenten gibt.

Da redet man zum Beispiel von einer Anti-Viren-Software, die mitten am Tag auf einmal das gesamte System halb lahmlegt, weil ein Gesamtcheck durchgeführt wird. Oder man redet auch zum Teil von einer E-Mail Sandbox, wo man halt eben hergeht, und sagt: Okay, es gibt diese Sandbox, die E-Mails landen dort drinnen und werden von der Sandbox durchgecheckt und dann halt zugestellt.

Und wenn halt fragwürdiger Content gefunden wird, wird je nach fragwürdigem Content der User informiert, dass ein Mail angekommen ist, und er soll das freigeben, oder der User wird halt einfach darauf hingewiesen, dass ein E-Mail gekommen ist, und ein Virus drin war.

Das kann, wenn der User mit schnelllebigen Geschäften zu tun hat, durchaus zu Ärgernissen führen. Also wir reden da, wenn ein User gewohnt ist, dass seine E-Mails quasi wie Chat-Nachrichten hin und her gespielt werden, dann wird es das mit der Sandbox nicht spielen. Dies betrifft insbesondere grenzwertige bzw. für die Sandbox spannende Inhalte. Wir reden da von Excel Files oder halt einfach Worddateien, die Links enthalten können oder PDFs, die Links enthalten können. Also da gibt es schon einige Maßnahmen, die den User halt auch stören können.

Aber letztendlich kann da viel durch gute Organisation weggemacht werden, also Updatezyklen oder auch Backupzyklen können in der Nacht gleich gut gemacht werden wie am Tag. Aber auch

dem User selbst kann durch Schulungen und beigebracht werden, dass das halt einfach notwendig ist.

Diese fünf Minuten Verzögerung, die er insgesamt am Tag hat, sind für die Firma ein verhältnismäßig kleiner Nachteil im Vergleich zu dem, was passieren würde, wenn die gesamte Firma von einer Ransomware ganz lahmgelegt wird.

Wenn einmal die Firma steht und kein Backup mehr vorhanden ist und die Infrastruktur quasi einfach verschlüsselt daliegt und keiner kann mehr was machen. Das kostet richtig Geld.

H: Das macht natürlich durchaus Sinn. Angenommen man hat jetzt im Budget technisch freie Hand. Kann durch technische Maßnahmen das Netzwerk so gut geschützt werden, dass sogar mutwillige oder böswillige User bzw. User, die grob fahrlässig agieren, keine Gefährdung für das System darstellen?

E 4.4: Die kurze Antwort zu dieser Frage ist nein! Das ist nicht möglich. Ein User, der böswillig oder grob fahrlässig in einem System agiert, wird immer ein Risiko sein und ein riesiges Gefahrenpotenzial haben.

Was allerdings durchaus durch moderne Sicherheitskonzepte und auch eventuell zukünftig anwendbare Technologien möglich sein könnte, ist, dass der Schaden, den der User verursachen kann, möglichst geringgehalten wird. Also wir reden da jetzt von verhaltensmustererkennender Firewall oder auch Anti-Viren-Software, die sich halt eben antrainieren und anlernen, wie gewisse Programme oder User agieren.

Da ist schon sehr viel zukünftig möglich und eventuell besteht dann auch die Möglichkeit, durch eine gewisse Abschottung des gesamten Benutzers, dass eben nicht mehr das gesamte System gefährdet wird, sondern halt nur ein Teil des Systems.

Das ist natürlich für die Firma noch immer ärgerlich, aber wenn nur ein Teil des Systems steht und dies hoffentlich nur ein produktiver Teil ist und nicht unbedingt der Teil, wo auch gewisse Backups liegen. Dann besteht die Möglichkeit, dass man relativ zeitnah diese Systeme wieder zurückholt und eigentlich kein praktischer Schaden entsteht.

H: Dann nur kurz. Weil wir es kurz angesprochen haben mit Netzwerk-Architektur und Zero Trust, bieten durch eine Firewall getrennte Subnetze einen Sicherheitsvorteil?

E 4.5: Natürlich bieten diese einen Sicherheitsvorteil, das ist ganz klar. Dadurch bringt man es zusammen, dass ein User, selbst wenn er befallen wird … Der Virus trotzdem noch einmal irgendwie über die Firewall muss, um weitere Netzwerkparzellen anzugreifen.

Es ist natürlich gegeben mit der Netzwerk-Segmentierung hier, dass es darauf ankommt, was alles betroffen ist. Also was liegt alles im Netz des Users? Und das ist halt trotzdem alles in Gefahr. Da ist dann möglicherweise zukünftig ein Zero-Trust-Konzept durchaus the way to go.

H: Gibt es bezüglich getrennter Sub-Netze auch Nachteile?

E: Kaum. Also maximal als Nachteil kann man sagen, dass die Einrichtung aufwendig ist und dass es im laufenden Betrieb einen höheren Ressourcenverbrauch gibt.

Also wenn man ein Netz hat, wo die Firewall bereits permanent auf voller Auslastung fährt und das System sich gerade irgendwie erhält. Dann wird es nicht möglich sein, die Subnetze untereinander in VLANs zu trennen, dass die nicht miteinander reden können und alles über die Firewall läuft. Dadurch würde die Firewall komplett überlastet werden und alles beginnt zu stecken.

Andererseits gibt es die Frage, wie ernst es eine Firma meint, wenn sie wissen, unsere Firewall ist zehn Jahre alt, sie ist am Anschlag, wir wollen ein neues Security-Konzept aufsetzen, aber wir wollen keine Firewall tauschen.

H: Im Zeitraum von den ganzen IT-Systemumsetzungen, die du gemacht hast … Wo hast du bei Unternehmern das größte Verbesserungspotenzial gesehen? Du kommst zum Unternehmen, du machst die Basisanalyse. Gibt es ein gewisses Muster bei Unternehmern, wo man sieht okay, da ist Verbesserungspotenzial.

E 4.6: Vom allgemeinen Stand, also von den allgemeinen technischen Maßnahmen, ist es eigentlich meistens so, dass die Unternehmen gar nicht so schlecht aufgestellt sind. Es gibt natürlich immer Verbesserungspotenzial, man kann Firewall-Regeln nachschärfen, man kann neue Netzwerk-Architekturen einführen, man kann Netzwerksegmentierung betreiben, man kann sich auch durchaus die Aktualität der unterschiedlichen Server und Hardware anschauen und Software natürlich auch.

Aber letztendlich erfahrungsgemäß ist es eigentlich meistens eher auf der organisatorischen Seite. Ein absolut ungeschulter User, der keine Ahnung davon hat, was alles er im System anrichten kann, ist eine gigantische Gefahr für das Netzwerk. Eine weitere riesige Gefahr ist ein Top Level Management, das nicht weiß, wie groß die Gefahr sein kann und was für ein Schaden entstehen kann.

Es gibt nichts Schlimmeres, als eine IT, die ihr Möglichstes tut, um das System zu sichern, aber keinen Rückhalt von oben bekommen. Und dann ist das genau die IT, der die ganze Schuld zugeschoben wird, wenn etwas passiert und die gesamte Firma steht.

H: Also siehst du die Verbesserungspotenziale definitiv eher auf der organisatorischen Seite als eigentlich auf der technischen Seite.

E: Ja genau.

H: Dann kommen wir jetzt zur letzten Frage Auf jeden Fall vielen Dank für dieses tolle Interview.

Siehst du irgendeine Sicherheitstechnologie am Horizont, die eventuell zukünftig das Denken in IT-Security als auch zurzeit aktuelle Sicherheitskonzepte revolutionieren könnte?

E 4.7: Von den bisher bekannten Technologien finde ich das eher unwahrscheinlich. Also wir reden jetzt davon, was gerade sehr stark im Kommen ist zum Beispiel von so etwas wie Zero Trust. Dort ist schon ein gewisser Zukunftswert da. Aber Zero Trust ist mehr oder weniger nichts anderes als eine heruntergebrochene, fertig gedachte Netzwerksegmentierung.

Es gibt dann halt pro Netzwerk nur noch einen User, der auch nur die Ressourcen sieht, die er wirklich benötigt. So gesehen wird das die Sicherheitskonzepte meiner Meinung nach nicht revolutionieren. Was eventuell noch kommt und zurzeit in aller Munde ist, ist, dass durch eine gewisse KI technische Analyseverfahren, Firewall-Verhalten verbessert und auch die Erkennung der Muster wesentlich zügiger und schneller vonstattengehen.

Also ich könnte mir vorstellen, dass Sicherheitskonzepte, die KI involvieren, tatsächlich noch einmal dem IT-Security-Denken einen ordentlichen Ruck nach vorne geben werden.

H: Gut, dann auf jeden Fall vielen Dank für die Zeit und ich werde dich natürlich am Laufenden halten. Und danke nochmals, dass du dir Zeit genommen hast.

Interview 5:

H: Ja, dann vielen Dank, dass du dir Zeit genommen hast. Ich würde vorschlagen, fang einfach mal mit deiner kurzen kleinen Vorstellung an, also, seit wie vielen Jahren bist du in dem Bereich tätig?

E: Gerne. Ja. Ich bin jetzt seit 14 Jahren im IT-Bereich tätig und habe damals angefangen und bin jetzt seit acht Jahren in IT-Security. Das ist jetzt seit acht Jahren mein Berufsfeld.

H: In wie vielen Unternehmen hast du gearbeitet bzw. Für wie viele Unternehmen warst du bereits im Kontext tätig?

E: Ja, ich bin Security mäßig im dritten Unternehmen. Natürlich im ersten Unternehmen nur für das Unternehmen zuständig bez. Security. Und jetzt dann später durch die Beratung für mehrere Kunden. Jetzt auch für viele kleine mittelständische Unternehmen, aber auch Behörden in Deutschland.

H: Kannst du das circa grob nur sagen. In welchen Bereich reden wir?

E: Wir sind sicher bei 30 auf jeden Fall. Die könnte ich jetzt so nennen. Wenn ich jetzt nachsehen müsste, dann würden wahrscheinlich sogar noch ein paar mehr rauskommen. Aber man weiß ja nicht mehr von den ganzen Jahren, die wichtigen Projekte, die bleiben aber natürlich dann im Kopf.

H: Passt perfekt. Ja, Meine Diplomarbeit handelt grundsätzlich von technischen Maßnahmen zur Netzwerk Absicherung. Dementsprechend natürlich die Hauptfrage… Welche technischen Maßnahmen zur Absicherung sind deiner Meinung nach in einem Unternehmens Netzwerk sinnvoll?

E 5.1: Also bei technischen Maßnahmen, da gibt es natürlich eine Vielzahl, die sinnvoll sind. Es ist schön, dass du auf die technischen Maßnahmen eingehst.

Ich möchte dabei immer noch betonen, das mache ich meist gegenüber dem Kunden ja auch, mit den technischen Maßnahmen ist es leider nicht gegeben. Das Thema IT-Security beziehen wir jetzt ja auf die technischen Maßnahmen. Das Thema Security oder auch Netzwerk-Sicherheit lebt natürlich von einem ganzheitlichen Ansatz.

Das heißt, wir brauchen natürlich auch organisatorische Maßnahmen oder auch Schulungen oder Zertifizierung und so was. Das ist auch wichtig, nur dass das hier nicht untergeht, dass das hier auch mal genannt wird.

Sonst würde in mir natürlich mein Herz bluten, wenn das Thema sonst unter den Tisch fällt. Technische-Maßnahmen, wo fangen wir an? Sagen wir als erstes, wir brauchen natürlich Anti-Viren-Software. Ja, das ist ganz einfach gemacht.

Ich mache eine Anti-Viren-Software auf den Client von jedem Anwender. Das ist schon mal ein grundlegender Schutz. Der sollte auch im privaten Umfeld überall gegeben sein. Und natürlich im Unternehmens Umfeld wird das für den Nutzer meistens durch die Administration übernommen.

Also der bekommt davon ja nicht mal was mit. Aber es muss halt gegeben sein und die sollte natürlich auch dementsprechend immer auf dem aktuellen Stand sein die Anti Viren Software, sonst bringt das nichts, da veraltete Anti Viren Software laufen zu lassen.

Für Netzwerk-Sicherheit würde ich natürlich sagen, das größte Thema ist die Firewall. Ja Firewall haben, schön und gut, eine richtige Firewall haben, darauf kommt es dann an! Oder auch die Anzahl der Firewalls. Wenn ich mir jetzt überlege, am besten ist da natürlich so eine DMZ zu haben.

Und da ist auch schon meine Empfehlung zu sagen, wir haben zwei Firewalls, schon mal eine vor und eine dahinter, um den Schutz zu verstärken. Und was ich jetzt als gut das Best Practices für mich oder auch im Umfeld und etabliert hat es natürlich dann, die Firewalls von

unterschiedlichen Herstellern zu nehmen. Das heißt, wenn ich jetzt eine Schwachstelle bei dem einen Hersteller identifiziert habe, ist nicht direkt der Zugang durchgängig geöffnet, sondern weil der andere Hersteller hoffentlich die gleiche Schwachstelle nicht in seiner Firewall hat, kommen wir darüber relativ gut raus, dass durch die doppelte Firewall von unterschiedlichen Herstellern wir schon mal gegenüber dieser einen Schwachstelle gesichert sind.

H: Immer mal andere auch ein bisschen eine Anspielung zu der Thematik mit Zero Day Exploits. Das mal falls es bei einem bekannten Firewall Hersteller Probleme gibt, dass man da halt nicht in diese Falle hineingerät.

E: Genau das ist ein super Beispiel, was du genannt hast mit dem Zero-Day-Exploit einfach zu sehen… Hey, ich habe zwei unterschiedliche technische Maßnahmen, die eigentlich die gleiche sind. Ja das gleiche. Ich mache eine Firewall dahin, aber durch die unterschiedliche Ausrichtung von den beiden komme ich schon viel weiter. Also es ist bei den technischen Maßnahmen häufiger so man kann jetzt natürlich Maßnahmen doppelt nehmen, aber bei manchen ist das natürlich nicht, während das bei anderen dann überflüssig ist.

H: Ja, ich glaube auch wenn man unter System-Sicherheit jetzt auch nicht nur von Fremdeinwirkung, sondern auch von normalen Gebrechen ausgeht. Es ist ja ein Vorteil, wenn man eine gewisse Redundanz bei den Geräten im Netz hat.

E 5.1: Das auf jeden Fall. Wir brauchen Redundanz. Das ist natürlich für die Ausfallsicherheit gegeben. Wir haben ja unsere drei großen Ziele Confidentiality, die Integrity und Availability. Und die Availability ist natürlich durch Redundanz abgedeckt. Da kommt es natürlich auf die Anwender und auf die Anforderungen an, die in dem Fall gegeben sind.

Aber wenn wir von Unternehmens-Netzwerken reden, die sind alle gut durch Redundanz aufgesetzt. Da sind wertvolle Kundendaten drauf. Die können ohne diese Daten oder ohne diese Netzwerke nicht arbeiten. Da sind dann wieder natürlich größere Themen drin.

Da kommt Business-Continuity-Management mit rein. Aber es ist ganz eindeutig, dass in den heutigen Unternehmen ohne die IT sowieso nichts mehr geht. Und dementsprechend ist das ganz wichtig. Zum Thema Redundanz geht es dann auch Richtung Backup. Was passiert, wenn das Ganze ausfällt?

Ich brauch einen Backup von meinen Sachen und das gehört für mich eindeutig zum Thema Netzwerk-Sicherheit, weil das natürlich dann auf Hardwareebene umgesetzt wird. Ja, wir können auch mit Software ein Backup machen, aber es ist einfach essenziell, dass ich da sage… Hey, ich habe hier ein gespiegeltes Netzwerk und natürlich ist es dann auch wichtig, dass die Backups regelmäßig gemacht werden, damit ich dann im Falle eines Angriffs oder wenn das System kontaminiert ist, dass ich dann halt wieder den vorherigen Stand wiederherstellen kann.

Ja, was können wir noch sagen zu Netzwerk-Absicherung? Es wäre auch wichtig, dass man bei den Netzwerken ein bisschen segmentiert. Jetzt ein großes Netzwerk und wir kennen das alle, das Unternehmens-Netzwerk ist eins, aber wenn man das Ganze noch mal segmentiert mit dazwischen liegenden Firewalls, kann man auch noch viel erreichen.

H: Bei der Netzwerk-Segmentierung, wenn wir schon darüber reden. Gibt es da irgendwelche Zukunfts-Maßnahmen, die eventuell ein Umdenken hervorrufen werden?

E: Ja natürlich. Da sprichst du genau auch auf ein Thema an, das wir bei uns jetzt viel diskutieren. Das ist Zero-Trust, dass muss man sich ganz ein bisschen so vorstellen… Man hatte bisher die IT-Security als so eine Burg mit so einem Graben, wo Wasser drin ist, verstanden.

Ja, ich versuch meine Unternehmens-Netzwerke nach außen hin richtig gut abzusichern und damit natürlich kein Angreifer da reinkommt. Jetzt ist es aber so, wenn man sich das überlegt, wenn der Angreifer einmal drin ist, gehört ihm die ganze Burg.

War ja vorher auch so, das ist mittlerweile das veraltete Denken. Hauptsache es kommt nichts von draußen rein. Bei dem Zero-Trust haben wir einen sehr interessanten Ansatz, dadurch, dass der einzelne Client auch abgeschirmt ist, weil er nichts und gar keinem vertraut.

Das heißt, er vertraut nicht nur keinen externen Sachen, sondern er vertraut auch keinen internen Sachen, so würde einfach alles über die Firewall gesteuert werden. Dementsprechend wäre auch ein Breach von einem einzelnen Client. Der würde nicht das Unternehmensnetz gefährden. Also ist es auf jeden Fall ein Thema, da können wir uns Stunden drüber unterhalten, was das für Vorteile und Nachteile mit sich bringt. Einfach weil dieses Umdenken, das damit in Gang gesetzt wird für das Thema Security, das werden wir sicher noch in der Zukunft jetzt für uns gebrauchen.

H: Dann welche von den jetzt genannten technischen Maßnahmen bieten deiner Meinung nach den höchsten Schutz bzw. sind am wichtigsten im Allgemeinen zur Netzwerk Sicherheit?

E 5.2: Also ja, es gibt natürlich Sachen, die brauchen wir einfach grundlegend, weil ohne die können wir keinen höheren Schutz herstellen. Wir brauchen halt eine grundlegende Firewall, die auf den unterschiedlichen Schichten mit den Protokollen arbeitet und Sicherheit herstellt. Wir brauchen auch eine Antivirensoftware.

Das sind einfach solche grundlegenden Sachen. Aber wenn wir jetzt solche Konzepte Zero-Trust nehmen, das würde natürlich den Schutz enorm erhöhen. Er kommt dann natürlich auch wieder darauf an wie hoch ist der Schutzbedarf von dem Unternehmensnetz oder von den Daten, die hier gerade drin sind.

Weil das natürlich dann auch noch einen deutlichen Mehraufwand darstellt in der technischen Umsetzung. Ich würde aber sagen, das könnte den höchsten Schutz mit sich bringen. Einfach nur, falls etwas passiert, habe ich halt nicht das ganze Netzwerk kompromittiert.

H: Gut, und wenn man jetzt hergeht, zum Unternehmens Netzwerk, wo man nicht, wie es für Zero-Trust ja notwendig ist, die gesamte Netzwerk Architektur umkrempeln und upgraden will …

Wo würdest du da als erstes hin greifen und sagen bei diesen Punkt da wissen wir, da gibt es in den meisten Unternehmen Verbesserungspotenzial?

E 5.2: Also was ich da gerne mir als erstes anschaue ist, wie das Ganze mit den Updates steht, wie die Updates geregelt werden. Viele haben Leute haben Windows Server und die Windows Server Update Services sind natürlich immer eine Sache, die wir da empfehlen oder die wir da nahelegen.

Einfach, weil häufig auch von der Abteilung die Updates geschwänzt werden, sodass Sicherheitslücken, die bereits bekannt sind, für die auch schon Lösungen bereitstehen, einfach dann noch im Unternehmens-Netzwerk weiterhin bestehen, weil einer zu faul ist das Update zu machen.

Wenn man das am Ende erklärt, fragt sich natürlich ein wie konnte das passieren? Die Security ist auch manchmal einfach nur gesunder Menschenverstand. Einfach darüber nachzudenken okay, was fehlt uns hier gerade? Oder auch, dass das Backup gescheit gemacht wurde.

Oder auch was, was für mich auch eine der Top-Maßnahmen ist, sich einfach im kontinuierlichen Verbesserungsprozess das Ganze alljährlich anzuschauen. Ich review meine technischen Maßnahmen, ich sehe okay, welche funktionieren gut und bei welchen habe ich auf jeden Fall noch Aufholbedarf.

Das passt natürlich gut, wenn man dann auch nach einem Standard zertifiziert ist. Also so eine Zertifizierung hilft auf jeden Fall auch dabei, selbst da an dem Thema dranzubleiben und reinzuschauen.

Was uns auffällt ist, dass wir häufig in den Firewalls, in den Konfigurationen Sachen verbessern können. Meistens ist ein bisschen was zu verschärfen. Oder auch die Zugangskontrolle oder Zugangsberechtigung, dass die richtig eingestellt sind. Wir haben dann teilweise Benutzer, die Zugriff auf Sachen haben, die sie gar nicht haben dürften.

Und wenn man da einfach mit den beiden Prinzipien antwortet... „Need-to-know“ also er darf nur auf das zugreifen, was er wissen muss und natürlich „least-privileg“. Grundsätzlich hat er erst mal kein Privileg und dann muss er nach und nach zugeordnet werden.

Darüber geht viel. Wir haben viele kleine technische Maßnahmen, an denen Optimierungsprozesse bei den Unternehmen durchgeführt werden können.

H: Dann jetzt eben von vielen technischen Maßnahmen gesprochen. Existieren durch diese technischen Maßnahmen Einschränkungen für die User? Also wird die Usability für die User dadurch eingeschränkt? Merkt man was in der System-Performanz oder wie schaut das aus?

E 5.3: Ja, das ist jetzt ein bisschen schwierig, denn das kommt immer drauf an. Grundsätzlich haben wir natürlich durch die Sicherheitsmaßnahmen einen erhöhten Aufwand, also wir brauchen mehr Rechenleistung. Wir haben kompliziertere Kommunikationswege und wir haben Verzögerungen dadurch. Ja, zum Beispiel beim Sandboxing oder natürlich ein Virenscanner, der über die Emails drüber läuft und vieles mehr.

Da gibt es natürlich schon Einschränkungen für den User in der Performance. Ob der davon was mitbekommt, ist fragwürdig. Da nehme ich gerne das Beispiel des Updates. Wir machen Updates, natürlich werden die normalerweise außerhalb der Geschäftszeiten gemacht, meistens zwischen null und null Uhr fünf, halt mitten in der Nacht.

Wie viele von den Mitarbeitern werden zu der Zeit arbeiten und merken okay, mein Unternehmen ist gerade nicht erreichbar, weil es ein Update macht. Die Updates werden dann ja auch meistens vorher groß angekündigt. Jeder Mitarbeiter kann sich ja dementsprechend drauf einstellen und ich denke, das ist für das Thema Usability das Größte.

Wenn die technischen Maßnahmen das ein bisschen einschränken, der Virenscanner macht den Computer langsamer, dann kann man das sicher durch organisatorische Maßnahmen so regeln, dass diese Auswirkungen auf den Nutzer deutlich abgeschwächt sind. Einfach, dass der User davon noch was mitbekommt, aber es stört ihn nicht bei seiner Arbeit.

H: Gut, dann zu folgender Frage: Wir wollen uns Unternehmens Netzwerk so sicher wie es nur geht machen. Besteht die Möglichkeit, dass man so durch rein technische Maßnahmen Unternehmens - Netzwerke so gut absichert, dass selbst durch mutwillige oder grobe Fahrlässigkeit der User keine Gefährdung für das System entsteht?

E 5.4: Das ist natürlich immer eine Frage, die ich gerne höre. Wo man dann sagt… Wir machen hier Netzwerk-Sicherheit auf Knopfdruck oder mit Zauberhand und dann gibt es kein Problem, sie können machen was sie wollen. Das ist grundsätzlich natürlich nicht der Fall.

Je nachdem, wie wissend der User ist und wie mutwillig er an die Sache rangeht, kommt man ja durch. Wir hören unter dem Fall ja auch immer, dass wenn einer wirklich einen Angriff starten möchte, dass man ja auch viele von den Sicherheitsmaßnahmen einfach überbrücken kann.

Je nachdem, wie viel Effort hinter der Attacke steckt, kommt der Angreifer durch. Es geht darum das Ganze so schwer und unattraktiv und einfach schwieriger zu machen, dass er sich darauf nicht konzentrieren möchte.

Wenn wir jetzt von grober Fahrlässigkeit der User sprechen, da kann viel abfangen, würde ich sagen. Einfach weil wir aus technischer Sicht sagen können… okay, wir haben zum Beispiel eine Password - Richtlinie, der Nutzer kann sich da jetzt nicht eins bis drei als Passwort nehmen.

Wir können schauen, dass bevor der Nutzer auf die Unternehmensdaten zugreifen überprüft wird und da geht schon viel durch die technischen Maßnahmen. Aber zurück zur Frage noch kann man das, glaube ich, noch nicht erreichen.

Ich weiß nicht, ob das in Zukunft sogar möglich wäre. Unter dem Zero-Trust-Prinzip wäre das sicher interessanter anzuschauen, weil auch wenn der User grob fahrlässig handelt, kann er nur seinen eigenen Client kompromittieren.

Der Rest des Unternehmens - Netzwerks sollte bei gescheiter Umsetzung kaum betroffen sein und vor allem bei der Firewall sollte der Angriff spätestens ja stoppen und dann wäre nur ein geringer Teil des Unternehmens - Netzwerks betroffen. Aber betroffen ist es natürlich immer noch. Wir haben immer noch einen Schadensfall, also einen super geringen Schadensfall, aber es ist nach wie vor ein Schadensfall.

Deswegen würde ich diese Frage auch in der Hinsicht immer noch mit Nein beantworten. Mutwillige oder grobe Fahrlässigkeit führt unweigerlich zu einer Gefährdung.

H: Gut, jetzt mit Zero Trust. Das ist heruntergebrochen mehr oder weniger die nächste Stufe nach einer ordentlich sauberen Netzwerk Segmentierung.

E: Ja, das könnte man so sagen.

H: Bietet eine ordentliche Netzwerk-Segmentierung Vorteile? Und wenn ja, welche Vorteile wären das bzw. gibt es auch Nachteile dadurch?

E 5.5: Wir haben natürlich durch die Netzwerk-Segmentierung die gesteigerte Sicherheit dadurch, dass wenn wir uns durch Phishing einen Virus eingefangen haben, diesen einen Teil vom Netzwerk isolieren können.

Das heißt, wenn wir eine Gefährdung haben, ist die nicht auf das ganze Unternehmensnetz, sondern nur auf einen Teil von diesem Netz. Die anderen Teile von den Unternehmensnetzen wären noch arbeitsfähig.

Das ist natürlich erst mal wieder ein Sicherheitsvorteil. Nachteil ist natürlich der höhere Aufwand. Um die Sicherheit zu erreichen, muss ich halt meine Netzwerke segmentieren, muss dazwischen auch den Traffic wieder durch Firewalls schützen und überwachen und dementsprechend auch wieder einen…

Ja, das würde ich so gar nicht sagen, das ist interessant… Wie das Ganze dann beim Incident-Response-Management aussieht. Weil… natürlich müssen die dann nicht das ganze Netzwerk betrachten, sondern können sich dann auf das eine Netzwerk fokussieren.

Also ich würde sagen, auch fürs Incident Response Management später wäre das sicher auch von Vorteil. Vielleicht sind in dem Fall die Kosten zu nennen, aber das sind keine technischen Maßnahmen. Wenn wir von technischen Maßnahmen reden, würde ich da eher sagen, dass es eigentlich nur Vorteile hat.

H: Ja, das ist klar. Okay. Wenn du wieder mal zu einem Unternehmen hingeschickt wirst und sozusagen eine Anfangs - Analyse machst. In welchen Teilbereich siehst du meistens das größte Verbesserungspotenzial?

E: In Bezug auf technische Maßnahmen oder generell.

H: Wenn du die Zeit hast, würde ich gerne auf beides ganz kurz eingehen.

E 5.6: Sicher doch. Generell würde ich sagen, dass wir beim Thema Sensibilisierung das größte Verbesserungspotenzial, also noch mehr als bei den technischen Maßnahmen, haben. Einfach, weil viele Nutzer sich dem Thema Security nicht bewusst sind.

Es gibt Schulungen mittlerweile für Phishing-E-Mails und trotzdem, wenn wir Phishing Kampagnen bei Unternehmen machen…. Was wir da für Klickzahlen erreichen, das sollte nicht passieren.

Das sollte einfach nicht passieren, dass da 30 % der Nutzer draufklicken. Ist leider so, also ich würde sagen das Thema Sensibilisierung IT-Security ist nicht mal eben so gemacht, gehört aber dazu. Das muss auf jeden Fall umgesetzt werden.

Bei den technischen Maßnahmen sind wir vorhin schon darauf eingegangen. Da habe ich gesagt Updates sind zu langsam, die Backup - Strategien sind unvollständig, die Firewall Konfigurationen sind meistens schon recht gut, könnten vielleicht ein bisschen schärfer sein, aber dann gibt es auch sowas wie WLAN-Absicherung.

Also das ist von Unternehmen zu Unternehmen sicher unterschiedlich. Generell auf Security würde ich schon sagen, dass durch Schulungen oder vor allem Sensibilisierungsprogramme auch viel bei den Nutzern klar gemacht werden kann. Es ist ja nicht der große Aufwand, aber wenn man vom Sicherheitsdenken nur einen ganz kleinen Teil dem Endnutzer beibringen kann, wäre da sicher schon viel gemacht.

H: Sehr gut. Dann zur abschließenden Frage. Wird es deiner Meinung nach irgendwann mal in näherer Zukunft irgendeine Sicherheitsmaßnahme, irgendein Gadget, ein Tool oder eine Hardware geben, die das derzeitige Denken von Sicherheit und Sicherheitskonzepte komplett revolutionieren wird?

E 5.7: Komplett revolutionieren. Das ist stark. Wir betrachten gerne mal auch die Themen, die halt die Hype - Themen sind. Es gibt natürlich immer Themen, die aufkommen, die auch dann heiß diskutiert werden, ob da wirklich was kommen kann…

Ich sehe das Ganze eher kritisch. Ich bin derzeit von Zero-Trust sehr gut überzeugt, dass das definitiv gescheit ist, so etwas auch als Standarddenken umzusetzen.

Das könnte ich mir gut vorstellen, dass das in Zukunft kommen würde. Das wir vom Sicherheitskonzept her in Richtung Zero-Trust oder halt diese Netzwerk-Segmentierung gehen. Wie wir es schon besprochen haben, ist es ja ein anderer Ansatz und so was könnte ich mir vorstellen, dass wir da eher was haben, als dass wir eine neue Technologie haben, die uns Sicherheit gibt.

Nur durch eine Technologie ist das auf jeden Fall nicht gegeben. Es wird immer ein Thema sein, dass die technischen und organisatorischen Maßnahmen zusammen kombiniert und deswegen würde ich sagen, da gibt es keine Technologie.

Aber es gibt halt gute Konzepte und Ansätze oder einfach Technologien, die müssen dann relativ schnell in den Standard gebracht werden. Das ist natürlich auch wieder mit Kosten verbunden. Aber wenn die Sicherheitsvorteile so dermaßen überwiegen, dann sollten die halt einfach schneller zur Standard-Absicherung dazugehören und dementsprechend dann auch bei den Unternehmen oder beim Kunden eingeführt werden.

H: Vielen Dank für deine Zeit.

E: Bitte gerne.

ABKÜRZUNGSVERZEICHNIS

RaaS	Ransomware as a Service
AES	Advanced Encryption Standard
NAC	Network Access Control
UTM	Unified Threat Management
WAF	Web Application Firewall
DMZ	Demilitarized Zone
NIST	National Institute of Standards and Technology
RADUIS	Remote Authentication Dial-In User Service
BYOD	Bring Your Own Device
MDM	Mobile Device Management
SDNs	Software Defined Networks
DDOS	Distributed Denial of Service
PEP	Policy Enforcement Point
PDP	Policy Decision Point
MFA	Multi-Faktor-Authentifizierung
HSTS	HTTP Strict Transport Security

ABBILDUNGSVERZEICHNIS

TABELLENVERZEICHNIS

LITERATURVERZEICHNIS

Agham, V. (2016, April). Unified Threat Management . *International Research Journal of Engineering and Technology (IRJET)*, pp. 32-36.

Agrawal, A., & Wahie, K. (1016). Analyzing and optimizing cloud-based antivirus paradigm. *2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH)* (pp. 203-207). Greater Noida: IEEE.

Ahmad, I., Namal, S., Ylianttila, M., & Gurtov, A. (2015). Security in Software Defined Networks: A Survey. *IEEE Communications Surveys & Tutorials, 17*(4), pp. 2317-2346.

Alani, M. M. (2014). Securing the Cloud: Threats, Attacks and Mitigation Techniques. *Journal of Advanced Computer Science and Technology*, pp. 202-213.

Al-Asli, M., & Ghaleb, T. A. (2019). Review of Signature-based Techniques in Antivirus Products. *2019 International Conference on Computer and Information Sciences (ICCIS)* (pp. 1-6). Sakaka: IEEE.

Armando, A., Costa, G., & Merlo, A. (2013). Bring your own device, securely. *SAC '13: Proceedings of the 28th Annual ACM Symposium on Applied Computing* (pp. 1852-1858). Coimbra: Association for Computing Machinery.

Ayodele, A., Henrydoss, J., Schrier, W., & Boult, T. (2011). Study of Malware Threats Faced by the Typical. *CNSA 2011: Advances in Network Security and Applications*, (pp. 513-525). Chennai.

Bellovin, S., & Cheswick, W. (2014, September). Network firewalls. *IEEE Communications Magazine*, pp. 50-57.

Bilge, L., & Dumitras, T. (2012). Before we knew it: an empirical study of zero-day attacks in the real world. *CCS '12: Proceedings of the 2012 ACM conference on Computer and communications security* (pp. 833-844). Raleigh: Association for Computing Machinery.

Brewer, R. (2016, September). Ransomware attacks: detection, prevention and cure. *Network Security*, pp. 5-9.

Buck, C., Olenberger, C., Schweizer, A., Völter, F., & Eymann, T. (2021, November). Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust. *Computers & Security, 110*, pp. 2-26.

Byrne, P. (2006, September). Application firewalls in a defence-in-depth design. *Network Security*, pp. 9-11.

Cadieux, P., Grady, C., Schultz, J., & Valites, M. (2019, April 30). *Talos Intelligence: Sodinokibi ransomware exploits WebLogic Server vulnerability*. Retrieved from Cisco Talos Intelligence Group: https://blog.talosintelligence.com/2019/04/sodinokibi-ransomware-exploits-weblogic.html

Caputo, D. D., Pfleeger, S. L., Freeman, J. D., & Johnson, M. E. (2014, Januar - Februar). Going Spear Phishing: Exploring Embedded Training and Awareness. *IEEE Security & Privacy*, pp. 28-38.

Chamorro, E., Han, J., & Beheshti, M. (2012). The Design and Implementation of an Antivirus Software Advising System. *2012 Ninth International Conference on Information Technology - New Generations* (pp. 612-617). Las Vegas: IEEE.

Chandrasekaran, M., Narayanan, K., & Upadhyaya, S. (2006). Phishing email detection based on structural properties. Buffalo, New York, USA.

Chen, Y., Hu, H.-C., & Cheng, G.-z. (2019, März 19). Design and implementation of a novel enterprise network defense system by maneuvering multi-dimensional network properties. *Frontiers of Information Technology & Electronic Engineering*, pp. 238-252.

Cheng, Y., Wang, W., Wang, J., & Wang, H. (2011, Juli). FPC: A New Approach to Firewall Policies Compression. *TSINGHUA SCIENCE AND TECHNOLOGY*, pp. 65-76.

Cisco. (2021, Juni 4). *CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide, 9.8*. Retrieved from Cisco Configuration Guides: https://www.cisco.com/c/en/us/td/docs/security/asa/asa98/configuration/general/asa-98-general-config/ha-failover.html

Clincy, V., & Shahriar, H. (2018). Web Application Firewall: Network Security. *42nd IEEE International Conference on Computer Software & Applications* (pp. 835-836). Tokio: IEEE.

Colwill, C. (2009, November). Human factors in information security: The insider threat – Who can you trust these days? *Information Security Technical Report*, pp. 186-196.

ComputerWeekly. (2016, Dezember). *Out-of-band Patch*. Retrieved from Computer Weekly Webseite: https://www.computerweekly.com/de/definition/Out-of-band-Patch

Department of Homeland Security. (2016, September). *Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies.* Retrieved from Cybersecurity & Infrastructure Security Agency: https://www.cisa.gov/uscert/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

Department of Homeland Security CISA. (2020). *Ransomware Guide CISA*. Retrieved from CISA Homepage: https://www.cisa.gov/stopransomware/ransomware-guide

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. *CHI '06: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 581-590). Montreal: Association for Computing Machinery.

Dixit, V. H., Kyung, S., Zhao, Z., Doupé, A., Shoshitaishvili, Y., & Ahn, G.-J. (2018). Challenges and Preparedness of SDN-based Firewalls. *SDN-NFV Sec'18: 2018 ACM International Workshop on Security in Software Defined Networks Network Function Virtualization* (pp. 33-38). Tempe: Association for Computing Machinery.

Dukinfield, D., & Richardson, P. (2019, November). *Zero Trust, Zero Touch (Enabling Security for Software-Defined Networking).* Retrieved from Website Cisco: https://www.cisco.com/c/dam/en/us/services/collateral/sdn-security-white-paper.pdf

Fortinet. (2021). *Fortinet: Cybersecurity Statistics*. Retrieved from Fortinet Website: https://www.fortinet.com/resources/cyberglossary/cybersecurity-statistics

Foster, I. D., Larson, J., Masich, M., Snoeren, A. C., Savage, S., & Levchenko, K. (2015). Security by Any Other Name: On the Effectiveness of Provider Based Email Security. *CCS '15: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security* (pp. 450-464). Denver: Association for Computing Machinery.

Furnell, S. (2016, September). The usability of security – revisited. *Computer Fraud & Security*, pp. 5-11.

Garba, A. B., Armarego, J., & Murray, D. (2015, Februar). BRING YOUR OWN DEVICE ORGANISATIONAL INFORMATION SECURITY AND PRIVACY. *ARPN Journal of Engineering and Applied Sciences*, pp. 1279-1287.

Gazet, A. (2008, Juli 04). Comparative analysis of various ransomware virii. *Journal of Computer Virology and Hacking Techniques*, pp. 77-90.

Hancock, J., & Tessian. (2022). *Understand the mistakes that compromise your company's security.* Retrieved from Tessian Website: https://www.tessian.com/research/the-psychology-of-human-error/

Hatem, S. S., Wafy, M. H., & El-Khouly, M. M. (2014). Malware Detection in Cloud Computing. *International Journal of Advanced Computer Science and Applications*(5), pp. 187-192.

Hudson, B. (2014, Februar). Advanced Persistent Threats: Detection, Protection and Prevention. Oxford, Vereinigtes Königreich.

Hunt, R. (1998, April). Internet/Intranet firewall security—policy, architecture. *Computer Communications 21*, pp. 1107-1123.

IBM. (2020, Juli). IBM: Cost of a Data Breach Report 2020. Armonk, New York, USA.

IBM Global Technology Services. (2014, May). IBM Security Services 2014 Cyber Security Intelligence Index. Somers, New York, USA. Retrieved from Webseite : https://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/custom/IBMSecurityServices2014.PDF

Iskandar, A., Virma, E., & Saleh Ahmar, A. (2018). Implementing DMZ in Improving Network Security of Web Testing in STMIK AKBA. *International Journal of Engineering & Technology*, pp. 99-104.

Jarschel, M., Oechsner, S., Schlosser, D., Pries, R., Goll, S., & Tran-Gia, P. (2011). Modeling and performance evaluation of an OpenFlow architecture. *Proceedings of the 23rd International Teletraffic Congress* (pp. 1-7). San Francisco: IEEE.

Kim, S., Kim, J., & Kang, B. B. (2018, August). Malicious URL protection based on attackers' habitual behavioral analysis. *Computers & Security*.

Kindervag, J., Balaouras, S., & Coit, L. (2012, November 15). *Build Security Into Your Network's DNA: The Zero Trust Network Architecture.* Retrieved from Website Forrester: https://www.forrester.com/report/build-security-into-your-networks-dna-the-zero-trust-network-architecture/RES57047

Koret, J., & Bachaalany, E. (2015). *The Antivirus Hacker's Handbook.* John Wiley & Sons Inc.: Indianapolis.

Kreutz, D., Ramos, F. M., & Verissimo, P. (2013). Towards secure and dependable software-defined networks. *HotSDN '13: Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking* (pp. 55-60). Hong Kong: Association for Computing Machinery.

Kulkarni, G., Sutar, R., & Gambhir, J. (2012, Jänner-Februar). Cloud Computing-Storage as Service. *International Journal of Engineering Research and Applications (IJERA)*, pp. 945-950.

Luber, S., & Schmitz, P. (2017, Juni 5). *Definition Remote Authentication Dial-In User Service: Wie funktioniert RADIUS?* Retrieved from Security Insider Website: https://www.security-insider.de/wie-funktioniert-radius-a-613266/

Marks, E., & Lozano, B. (2010). *Executive's Guide to Cloud Computing.* Hoboken: John Wiley & Sons, Inc.

Masoudi, R., & Ghaffari, A. (2016, May). Software Defined Networks: A survey. *Journal of Network and Computer Applications*(67), pp. 1-25.

Mayring, P. (2015). *Qualitative Inhaltsanalyse - Grundlagen und Techniken.* Weinheim: Beltz Verlagsgruppe.

McCormack, C. (2019, November 22). *Is encryption rendering your firewall irrelevant?* Retrieved from Sophos News: https://news.sophos.com/en-us/2019/11/22/is-encryption-rendering-your-firewall-irrelevant/

Mcginthy, J. M., & Michaels, A. J. (2019, Oktober). Secure Industrial Internet of Things Critical Infrastructure Node Design. *IEEE Internet of Things Journal, 6*(5), pp. 8021-8037.

Meland, P. H., Fahmy Bayoumy, Y. F., & Sindre, G. (2020, Mai). The Ransomware-as-a-Service economy within the darknet. *Computers & Security*.

Mhaskara, N., Alabbadab, M., & Khedri, R. (2021, April). A Formal Approach to Network Segmentation. *Computers & Security*.

Microsoft. (2021, Dezember 15). *Monatliche Qualitätsupdates*. Retrieved from Microsoft Dokumentationen: https://docs.microsoft.com/de-de/windows/deployment/update/quality-updates

Miloslavskaya, N. (2021, März 4). Network Protection Tools for Network Security Intelligence Centers. *Procedia Computer Science*, pp. 597-603.

Min-kyu, C., Rosslin, K. R., Chang-hwa, H., & Tai-hoon, K. (2008, Juli). Wireless Network Security: Vulnerabilities, Threats and Countermeasures. *International Journal of Multimedia and Ubiquitous Engineering*, pp. 77-86.

Mohurle, S., & Patil, M. (2017, Juni). A brief study of Wannacry Threat: Ransomware Attack 2017. *International Journal of Advanced Research in Computer Science*, pp. 1938-1940.

Morrisey, C. (2021, Juli 21). *Windows quality updates primer*. Retrieved from Mircosoft TechCommunity: https://techcommunity.microsoft.com/t5/windows-it-pro-blog/windows-quality-updates-primer/ba-p/2569385

Nakamura, S., Nakayama, K., & Nakagawa, T. (2009). Optimal backup interval of database by incremental backup method. *Proceedings of the IEEE International Conference on Industrial Engineering and Engineering Management* (pp. 218-222). Hong Kong: IEEE.

Nakhjiri, M., & Nakhjiri, M. (2005). *AAA and Network Security for Mobile Access: Radius, Diameter, EAP, PKI and IP Mobility.* West Sussex: John Wiley & Sons.

Naous, J., Erickson, D., Covington, G. A., Appenzeller, G., & McKeown, N. (2008). Implementing an OpenFlow switch on the NetFPGA platform. *ANCS '08: Proceedings of the 4th ACM/IEEE Symposium on Architectures for Networking and Communications Systems* (pp. 1-9). San Jose: Association for Computing Machinery.

Nath, B. (2022, April 4). *Cloud Backup Vs. Local Backup: Which Is Better?* Retrieved from Geekflare Website: https://geekflare.com/cloud-backup-vs-local-backup/

Nelson, S. (2011). *Pro Data Backup and Recovery.* Berkeley: Apress.

Oberheide, J., Cooke, E., & Jahanian, F. (2007, August 7). Rethinking Antivirus: Executable Analysis in the Network Cloud. *Proceedings of the 2nd USENIX workshop on Hot topics in security (HOTSEC).* Boston: Usenix.

Oberheide, J., Cooke, E., & Jahanian, F. (2008). CloudAV: N-Version Antivirus in the Network Cloud. *17th USENIX Security Symposium*, (pp. 91-106). San Jose.

Obrutsky, S. L. (2016). Cloud Storage: Advantages, Disadvantages and Enterprise Solutions for Business. *Conference: EIT New Zealand.* Hawke's Bay: Eastern Institute of Technology.

Pandove, K., Jindal, A., & Kumar, R. (2010, August). Email Security. *International Journal of Computer Applications*, pp. 23-26.

Parsons, K., McCormac, A., Butavicius, M., & Ferguson, L. (2010, Oktober). *Human Factors and Information Security: Individual,Culture and Security Environment .* Retrieved from Website Defense Technical Information Center (Australian Department of Defence): https://apps.dtic.mil/sti/pdfs/ADA535944.pdf

Perakovic, D., Husnjak, S., & Remenar, V. (2012). RESEARCH OF SECURITY THREATS IN THE USE OF MODERN TERMINAL DEVICES. *Annals of DAAAM for 2012 & Proceedings of the 23rd International DAAAM Symposium* (pp. 545-548). Wien: DAAAM International.

Porter, C. (2012). *Email Security with Cisco IronPort.* Indianapolis: Cisco Press.

Roeckl, C. (2014). Stateful Inspection Firewalls. *Juniper Networks Whitepaper*.

Rose, S., Borchert, O., Mitchel, S., & Conelly, S. (2020, August). *Zero Trust Architecture (NIST Special Publication 800-207).* Retrieved from Website NIST: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

Ruofan, X., Xiaoyan, Y., Javier, A. L., Fumio, M., & Kishor, S. T. (2014, Juli/August). Performance and Availability Modeling of IT Systems with Data Backup and Restore. *IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING*, pp. 375-389.

Samaniego, M., & Deters, R. (2018). Zero-Trust Hierarchical Management in IoT. *2018 IEEE International Congress on Internet of Things* (pp. 88-95). San Francisco: IEEE.

Sarkar, K. R. (2012, August). Assessing insider threats to information security using technical, behavioural and organisational measures. *Information Security Technical Report, 15*(3), pp. 112-133.

Scarfone, K., & Hoffman, P. (2009, September 28). Guidelines on Firewalls and Firewall Policy. Gaithersburg, Maryland, USA: NIST: National Institute of Standards and Technology.

Schneier, B. (2000). *Secrets & Lies: Digital Security in a Networked World.* New York: John Wiley & Sons, Inc.

Serrao, G. J. (2010). Network access control (NAC): An open source analysis of architectures and requirements. *44th Annual 2010 IEEE International Carnahan Conference on Security Technology* (pp. 94-102). San Jose: IEEE.

Singleton, C. (2021, Februar). X-Force Threat Intelligence Index 2021. Armonk, New York, USA.

Souppaya, M., & Scarfone, K. (2012, Februar). Guidelines for Securing Wireless Local Area Networks (WLANs). Gaithersburg, Maryland, USA: National Institute of Standards and Technology.

Sukwong, O., Kim, H., & Hoe, J. (2011). Commercial Antivirus Software Effectiveness: An Empirical Study. *Computer*(44), pp. 63-70.

Thomas, J. E., & Galligher, G. C. (2018, Jänner 3). Improving Backup System Evaluations in Information Security Risk Assessments to Combat Ransomware. *Computer and Information Science*, pp. 14-25.

TitanHQ. (2022). *Email Protection, Security and Email Filtering*. Retrieved from TitanHQ Website: https://www.titanhq.com/email-protection/

Tobias, E. (2012, Februar 15). *128 or 256 bit Encryption: Which Should I Use?* Retrieved from Ubiq Security Website: https://www.ubiqsecurity.com/128bit-or-256bit-encryption-which-to-use/#:~:text=With%20the%20right%20quantum%20computer,than%20the%20universe%20has%20existed.

Tuttle, H. (2021, März). Ransomware Attackers Turn to Double Extortion. *Risk Management*, pp. 8-9.

Voronkov, A., Iwaya, L. H., Martucci, L. A., & Lindskog, S. (2017, Dezember). Systematic Literature Review on Usability of Firewall Configuration. *ACM Computing Surveys*, pp. 1-35.

Wagner, N., Şahin, C. Ş., Pena, J., Riordan, J., & Neumayer, S. (2017). Capturing the security effects of network segmentation via a continuous-time markov chain model. *Proceedings of the 50th Annual Simulation Symposium (ANSS '17).* (pp. 1-12). San Diego: Society for Computer Simulation International.

Wagner, N., Sahin, C. S., Winterrose, M., Riordan, J., Pena, J., Hanson, D., & Streilein, W. W. (2016). Towards automated cyber decision support: A case study on network segmentation for security. *IEEE Symposium Series on Computational Intelligence (SSCI)* (pp. 1-10). Athen: IEEE.

Wilcox, J., & Poulson, H. (2021, Juli 29). *Microsoft: Windows 10 update servicing cadence*. Retrieved from Microsfot Techcommunity Website: https://techcommunity.microsoft.com/t5/windows-it-pro-blog/windows-10-update-servicing-cadence/ba-p/222376

Wu, Z., & Li, H. (2014, September 12). Analysis of data backup and recovery system. *Applied Mechanics and Materials*, pp. 1207-1210.

Yong, W., Jinpeng, W., & Vangury, K. (2014). Bring your own device security issues and challenges. *2014 IEEE 11th Consumer Communications and Networking Conference (CCNC)* (pp. 80-85). Las Vegas: IEEE.