MASTERARBEIT

IT-SICHERHEIT FÜR KRITISCHE INFRASTRUKTUREN

ausgeführt am

Studiengang
Informationstechnologien und Wirtschaftsinformatik

Von: Stefan Anton Maggale
Personenkennzeichen: 1910320009

Graz, am 10. Dezember 2020 .....

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

Zuerst möchte ich mich bei meinem Betreuer Herrn DI(FH) Christian Schmid, MSc für die Betreuung und Begutachtung dieser Masterarbeit bedanken. Ich bedanke mich auch bei Herrn Christian Hofer, Bakk., BSc, MSc der mich auf dieses spannende Thema aufmerksam gemacht hat. Des Weiteren bedanke ich mich bei Herrn DI Daniel Knauder, BSc für das Korrekturlesen dieser Arbeit. Ein besonderer Dank gebührt auch meiner Familie, die mich bei dieser Arbeit immer unterstützt hat und mir das Studium erst ermöglichte.

KURZFASSUNG

Das Ziel dieser Masterarbeit ist die Analyse der IT-Sicherheit von kritischen Infrastrukturen. Es soll gezeigt werden, ob eine Absicherung kritischer Infrastrukturen mit Hilfe von Methoden aus der IT-Sicherheit möglich ist und welche Auswirkung eine Vernetzung der einzelnen Systeme hat. Nicht behandelt werden Absicherungen für Cloud und mobile Geräte. In den vergangenen Jahren hat die Vernetzung der kritischen Infrastrukturen stark zugenommen und die Angriffe auf diese sind deutlich gestiegen. Aufgrund dessen werden in dieser Masterarbeit zunächst vergangene Angriffe beschrieben und analysiert. Großen Wert wird hierbei auf die NIS-Richtlinie gelegt, die als EU-Richtlinie wichtige Punkte für ganz Europa vorgibt. Aus den gewonnenen Erkenntnissen werden anschließend technische IT-Maßnahmen abgeleitet wie kritische Infrastrukturen in Zukunft besser geschützt werden können. Folgend werden die einzelnen Maßnahmen auch technisch in einer extra dafür aufgesetzten Testumgebung umgesetzt und im Detail beschrieben. Unter anderem wird gezeigt, wie wichtig es ist eine Verschlüsselung einzusetzen und dass es nicht ausreichend ist, die Zugänge nur mit einem starken Passwort abzusichern, sondern auch ein zweiter Faktor eingesetzt werden sollte.

Durch Umsetzung der Sicherheitsmaßnahmen, zusätzlich zu den normalen IT-Schutzvorkehrungen, kann die IT-Sicherheit erhöht werden. Ein kompletter Schutz vor Angriffen ist jedoch nicht möglich, da durch die Vernetzung der Systeme immer ein Angriffsvektor entsteht, der ausgenutzt werden kann. In Zukunft könnten kritische Infrastrukturen besser abgesichert werden, wenn die aufgezeigten Sicherheitsmaßnahmen umgesetzt werden.

ABSTRACT

This master thesis analyzes IT security for critical infrastructure. The author explores IT security techniques to secure key infrastructure and assesses the risks of interconnecting systems. Cloud and mobile-device security is beyond the scope of this thesis. Critical infrastructure networking has grown in complexity, as have attacks on it. The thesis opens by describing historical attacks. A focus is on the NIS guideline, the main guideline for European systems. Countermeasures are implemented to protect these systems from future attacks. Subsequently, individual measures are technically implemented and described in a bespoke test environment. Encryption is important, but a password is insufficient for account protection; two-factor authentication is strongly recommended. IT security can be improved by implementing security measures in addition to the standard IT-protection measures. Perfect protection is impossible as system networking always opens potential attack vectors. In future, critical infrastructure can enjoy improved secured if they implement the security measures described.

INHALTSVERZEICHNIS

1 EINLEITUNG

Unsere moderne Gesellschaft treibt eine laufende Weiterentwicklung von Technologien voran. Die Digitalisierung schreitet besonders schnell vorwärts und wird in den unterschiedlichen Bereichen eingesetzt, um die Flexibilität und auch den Komfort zu steigern. Es gibt bestimmte Bereiche die wichtiger sind, da diese unsere Grundversorgung sicherstellen und daher zu kritischen Infrastrukturen zählen. Unsere Gesellschaft ist abhängig von den kritischen Infrastrukturen, daher ist es notwendig diese entsprechend zu schützen. Ein Ausfall hätte große Auswirkungen auf unser tägliches Leben. Um das zu verhindern, gibt es in den Ländern verschiedene Pläne, die zum Schutz von kritischen Infrastrukturen beitragen. In Österreich gibt es dafür einen Masterplan APCIP (*Österreichisches Programm Zum Schutz Kritischer Infrastrukturen (APCIP)*, 2014). Dieser Masterplan wurde mit dem European Programme for Critical Infrastructure Protection (EPCIP) entwickelt und angepasst.

Da Hacker (AngreiferInnen) auch vor kritischen Infrastrukturen nicht Halt machen, wird es immer wichtiger diese bestmöglich abzusichern. In der Fallstudie von Dännart et al. (2018) wurde die IT-Sicherheit in kritischen Infrastrukturen betrachtet. Dabei wurden sowohl Angriffe von außen als auch das Fehlverhalten der MitarbeiterInnen analysiert. Angriffe von außen werden durch Ausnutzen von Sicherheitslücken oder Einschleusen von Malware durchgeführt. Ein Fehlverhalten der MitarbeiterInnen liegt dann vor, wenn es zu einer falschen Handlung eines Mitarbeiters oder einer Mitarbeiterin kommt und dadurch ein Eindringen der Hacker ermöglicht wird. Aus diesem Grund müssen MitarbeiterInnen regelmäßig geschult und auch die Systeme von kritischen Infrastrukturen abgesichert werden (Dännart et al., 2018).

Leider kommt es immer wieder vor, dass Unternehmen Updates nicht zeitgerecht installieren, mit der Begründung, dass es nach Updates zu gewissen Problemen kommen kann, wie beispielsweise ein System fährt nach dem Einspielen der Updates nicht mehr hoch. Dabei werden häufig auch die Sicherheitsupdates vernachlässigt. Dies kann dann zu erheblichen Schwachstellen in Systemen und zu potenziellen Lücken führen. Diese Lücken können dann von Hackern ausgenutzt werden, um kritische Infrastrukturen anzugreifen. Häufig werden die Bedienbarkeit und Performance (Reaktionszeit der Systeme) der Sicherheit vorgezogen. Sicherheit beeinflusst die Performance, da bei Einsatz einer Verschlüsselung ein Rechenaufwand nötig ist.

Zum besseren Schutz von kritischen Infrastrukturen werde ich in dieser Arbeit unterschiedliche IT-Sicherheitsmaßnahmen vorstellen. Eine kritische Infrastruktur ist weitaus mehr Gefahren (Umwelteinflüssen) als nur IT-Angriffen ausgesetzt. Da die Anzahl der IT-Angriffe immer weiter zunimmt, wird in dieser Masterarbeit auf diese genauer eingegangen. Cybersecurity (IT-Sicherheit) spielt zur Absicherung gegen Hackerangriffe eine wichtige Rolle. Unter IT-Sicherheit versteht man den Schutz von IT-Systemen und deren Daten vor Beschädigung, Diebstahl, Missbrauch oder Unterbrechung (Bendel, 2018).

1.1 Problemstellung und Zielsetzung

In den letzten Jahren nahm die Vernetzung in allen Bereichen immer weiter zu und auf die IT-Sicherheit wurde nicht immer viel Wert gelegt. Dies stellt uns jetzt vor neue Herausforderungen, denn ein nachträgliches Implementieren von Sicherheit in ein bestehendes System ist schwieriger als ein neues System von Grund auf sicher zu planen und zu implementieren. Das betrifft auch die kritischen Infrastrukturen, da diese nicht immer auf den neuesten Stand der Technik sind und dennoch vernetzt und weiterbetrieben werden. Mit Angriffen aus der Vergangenheit wird gezeigt, dass es immer häufiger zu Angriffen auf kritische Infrastrukturen kommt.

Um in das weitgreifende Thema „IT-Sicherheit für kritische Infrastrukturen“ Ordnung zu bringen und das Thema einzugrenzen, wurde folgende Forschungsfrage festgelegt:

„Wie ist es möglich kritische Infrastrukturen, trotz der Gefahren durch die Vernetzung über das Internet, aus Sicht der IT-Sicherheit abzusichern?“

Zu dieser Forschungsfrage wurden passende Hypothesen H0 und H1 aufgestellt, die in dieser Arbeit erforscht und genauer beantwortet werden.

H1: Die kritischen Infrastrukturen können mittels Härten der IT-Systeme abgesichert werden.

H0: Die kritischen Infrastrukturen können mittels Härten der IT-Systeme nicht abgesichert werden.

Zusätzlich sollte die folgende Frage im Zuge der Masterarbeit beantwortet werden:

“Welche Rolle spielt die Vernetzung von kritischen Infrastrukturen?“

Das Ziel der Arbeit ist es Möglichkeiten aufzuzeigen wie eine kritische Infrastruktur abgesichert werden kann, um die Angriffsfläche für Hacker zu minimieren. Dazu wird die Abfolge von Angriffen aus der Vergangenheit beschrieben und analysiert. Es wird eine Gliederung erstellt wer die potenziellen Hacker sind und welche Motive sie haben eine kritische Infrastruktur anzugreifen. Die Maßnahmen werden anhand vom Stand der Technik ausgearbeitet, die zu diesem Zeitpunkt verfügbar sind.

Um das Themengebiet weiter einzugrenzen, wird nur auf die IT-Sicherheit von Client-Server-Architektur im Netzwerk der kritischen Infrastrukturen eingegangen und welche technischen Maßnahmen es gibt, um diese zu schützen. Als Server und Client Betriebssysteme wird in dieser Masterarbeit auf Windows Systeme eingegangen, es gibt jedoch auch weitere Betriebssysteme wie Linux und Mac OS. Nicht eingegangen wird auf mobile Geräte wie Mobiltelefone, Clouddienste und auch Webanwendungen werden nicht behandelt. Diese sollten wenn möglich nicht mit den kritischen Infrastruktur Systemen vernetzt werden, da eine Absicherung sehr aufwendig ist. Clouddienste sollten nicht für kritische Infrastrukturen gewählt werden, da einerseits vertrauliche Informationen verarbeitet werden und viele Cloudanbieter die Datenschutzrichtlinien nicht erfüllen. Andererseits darf bei einem Ausfall der Verbindung zur Cloud, die Versorgung nicht unterbrochen werden.

1.2 Aufbau der Arbeit

Zuerst wird ein Überblick über kritische Infrastrukturen geschaffen. Anhand von Beispielen wird veranschaulicht, wie wichtig bestimmte Bereiche für unsere Sicherheit und Versorgung in unserem täglichen Leben sind. Es werden wichtige Begriffe im Zusammenhang mit kritischen Infrastrukturen und der IT-Sicherheit erklärt. Um den Stand der Forschung darzustellen, werden die Pläne für den Schutz kritischer Infrastruktur aufgelistet und deren Ziele beschrieben. In der Beschreibung der Pläne wird auf die Länder Deutschland, Österreich und die Schweiz besonders Wert gelegt. Es wird die EU-Richtlinie beschrieben, da diese für alle Mitgliedsstaaten gültig ist. Danach werden die Gefahren, die durch die Vernetzung entstehen aufgezeigt und mit Beispielen weiter veranschaulicht.

Im Kapitel „Angriffe“ wird definiert was unter Hackerangriffen verstanden wird und anhand eines Diagramms gezeigt, wie sich die Angriffe in den letzten Jahren weiterentwickelt haben. Anschließend werden Angriffe anhand ihrer Risiken gegliedert. Um Sicherheitsmaßnahmen zu erstellen, werden die Motive und die Motivation der Hacker betrachtet. Anschließend werden Angriffe beschrieben, die in der Vergangenheit auf kritische Infrastrukturen stattgefunden haben. Anhand der Vorgehensweise dieser Angriffe, wurden Erkenntnisse abgeleitet und nach Möglichkeiten gesucht, um eine kritische Infrastruktur, bestmöglich vor zukünftigen Angriffen zu schützen.

Anschließend wird im Kapitel „Absicherung nach Stand der Technik“ zuerst definiert was unter dem Begriff Stand der Technik verstanden wird und welche Stufen es gibt. Danach werden die drei wichtigsten Schutzziele der IT aufgezählt und beschreiben was darunter verstanden wird. Damit die technischen Maßnahmen der NIS-Richtline entsprechen, wurden diese aus der Handreichung zum Stand der Technik entnommen, die von Teletrust veröffentlicht wurde und theoretisch beschrieben. Ein Unterkapitel wurde der physischen Absicherung gewidmet, denn wenn diese Absicherung nicht sorgfältig umgesetzt wird, könnten viele Maßnahmen umgangen werden. Außerdem wird beschrieben wie wichtig der Einsatz von Verschlüsselung ist und welche Arten es gibt.

Der praktische Teil besteht aus der Umsetzung der zuvor ausgearbeiteten Maßnahmen. Dafür wurde eine Testumgebung aufgesetzt. Diese wird benötigt, um zu überprüfen, ob es möglich ist die beschriebenen Maßnahmen technisch umzusetzen. Daher wird zuerst der Aufbau der Testumgebung beschrieben. Bei der Auswahl der eingesetzten Programme wird versucht auf Open Source Software zurückzugreifen. Die Vorteile von Open Source Software werden im Kapitel „Umsetzung der Schutzmaßnahmen“ beschrieben. Die Wahl der Verschlüsselungsalgorithmen und verwendeten Zertifikate, wurden anhand der Empfehlungen die vom BSI (Bundesamt für Sicherheit in der Informationstechnik) veröffentlicht wurden getroffen.

In der Diskussion werden die Maßnahmen aus unterschiedlichen Perspektiven betrachtet und beurteilt, ob sie kritische Infrastrukturen schützen können. Die fortschreitende Vernetzung wird kritisch betrachtet, da diese viele Möglichkeiten für einen Angriff bieten.

2 KRITISCHE INFRASTRUKTUREN

Im folgenden Kapitel werden zunächst die kritischen Infrastrukturen definiert und die strategischen Ziele beschrieben. Um einen Überblick zu erhalten, wie wichtig diese für unser tägliches Leben sind, wird dies anhand von zwei Beispielen veranschaulicht. Zudem werden die einzelnen Bereiche, welche von kritischen Infrastrukturen betroffen sind, grafisch dargestellt. Die Abhängigkeit von den zwei wichtigsten Bereichen der kritischen Infrastrukturen, wird anschließend genauer erläutert. Es werden die Pläne zum Schutz der kritischen Infrastrukturen der D-A-CH Staaten (Deutschland, Österreich, Schweiz) beschrieben und die strategischen Ziele, die von den Staaten verfolgt werden, aufgezählt. Es wird außerdem beantwortet, was der Begriff Widerstandsfähigkeit bedeutet und wieso kritische Infrastrukturen eine hohe Widerstandsfähigkeit gegen Angriffe besitzen sollten. Am Ende werden die Vorteile und Nachteile, die durch die Vernetzung von kritischen Infrastrukturen entstehen können, beschrieben.

2.1 Definition der kritischen Infrastrukturen

Ein wichtiger Begriff, der immer wieder auftaucht, wenn man über kritische Infrastrukturen liest ist Widerstandsfähigkeit. Der Begriff Widerstandsfähigkeit ist für kritische Infrastrukturen von großer Bedeutung, denn Widerstandsfähigkeit bedeutet Zurückkehren oder Zurückspringen zum ursprünglichen Stabilitätszustand. Für kritische Infrastrukturen genügt der Begriff Zurückspringen nicht, denn sie sollten sich auch Veränderungen, Transformationen oder Weiterentwicklungen anpassen können. Daher wurde der Begriff erweitert und so versteht man unter Widerstandsfähigkeit auch die Überwindungsfähigkeit von Krisen eines Systems. Das kann auch Veränderungen oder neue Gegebenheiten mit sich ziehen, an die sich ein System oder der Mensch anzupassen hat. Daher ist die Widerstandsfähigkeit kritischer Infrastrukturen besonders wichtig, da diese auch in Krisen funktionieren sollten, um den Schutz und die Versorgung der Bevölkerung aufrecht zu erhalten. Ein Telefonnetz sollte durch einen Ausfall eines Sendemastes oder einer Überlastung des Netzes nicht gänzlich zum Erliegen kommen und auch lokal schnell wiederhergestellt werden können (Fekete, 2013).

Nachfolgend werden die strategischen Ziele der Länder Österreich, Deutschland und der Schweiz beschrieben, die zum Schutz kritischer Infrastrukturen beitragen. Diese drei Länder wurden gewählt, da sie auch D-A-CH Staaten genannt werden und regelmäßig den „Trilateraler Workshop D-A-CH“ für den Schutz kritischer Infrastrukturen abhalten. Dieser Workshop fand bereits vier Mal statt. Dabei treffen sich Personen aus den Bereichen Sicherheitspolitik und Bevölkerungsschutz der drei Länder. Hierbei werden grenzübergreifende Maßnahmen zum Schutz kritischer Infrastrukturen besprochen. Im zweiten Teil des Workshops 2018 wurde auch das europäische Programm zum Schutz kritischer Infrastrukturen besprochen und zielte darauf

ab, das europäische Programm zu überarbeiten, da die grenzüberschreitende Vernetzung immer weiter zunimmt. Betroffen sind dabei die Organisationen: Weltbank, die Internationale Energieagentur, die NATO, die Vereinten Nationen und die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (Maduz & Roth, 2018).

2.1.1 Österreich

Österreich hat leistungsfähige Infrastrukturen, wie beispielsweise Gesundheitsversorgung, Lebensmittelversorgung, Verkehrsbetriebe, Energieversorgung, Finanzdienstleistungen und Telekommunikationsdienstleistungen, welche eine hohe Versorgungssicherheit bieten. Um diese Infrastrukturen zu schützen, wurde 2008 das österreichische Programm zum Schutz kritischer Infrastrukturen beschlossen. Daraus wurde der „Masterplan APCIP“ (Austrian Program for Critical Infrastructure Protection) 2008 entwickelt. Auf dieser Basis wurde dann 2014 ein neuer Masterplan APCIP 2014 entwickelt und bis auf Länderebene runter gebrochen. Das strategische Ziel dieses Masterplans ist es, strategische Unternehmen dabei zu unterstützen, eine umfangreiche Sicherheitsarchitektur zu implementieren. Die strategischen Unternehmen sollten die folgenden vier Punkte aufweisen, um einen Ausfall der Versorgung zu verhindern.

- Vorhandene Risikoanalyse, um über die bestehende Verwundbarkeit informiert zu sein.
- Verfügen über ein Risikomanagement zur Verringerung der Verletzlichkeit.
- Verfügen über ein Business Continuity Management, um Störungen und Notfälle besser bewältigen zu können.
- Richten ein Sicherheitsmanagement ein.

Bei diesem Masterplan ist außerdem sichergestellt, dass er mit dem EPCIP (Europäisches Programm zum Schutz kritischer Infrastruktur) komplementär und kompatibel ist. Das ist durch die aktive Beteiligung Österreichs am EPCIP gegeben (*Österreichisches Programm Zum Schutz Kritischer Infrastrukturen (APCIP)*, 2014).

In Österreich zählen laut dem Masterplan 2014 Systeme, Anlagen, Prozesse, Netzwerke oder Teile davon, die zur Aufrechterhaltung wichtiger gesellschaftlicher Funktionen dienen, zu den kritischen Infrastrukturen. Diese müssen nicht öffentlich betrieben werden. Es können auch private Betreiber dahinterstehen. Ein Ausfall dieser kritischen Infrastrukturen hätte jedoch schwerwiegende Auswirkungen auf große Teile der Bevölkerung sowie staatliche Einrichtungen. Dies würde die Gesundheit, Sicherheit oder das wirtschaftliche und soziale Wohl unserer Gesellschaft beeinflussen. Aus diesem Grund ist es wichtig diese kritischen Infrastrukturen zu schützen. Sollte ein Ausfall dennoch geschehen, muss die Zeit für ein „Wieder-hochfahren“ so gering als möglich gehalten werden. Der Masterplan wird dann auf die einzelnen Bundesländer herunter gebrochen, um die regionalen kritischen Infrastrukturen zu schützen. Um die Komplementarität sicherzustellen, tauschen die Länder und der Bund ihre Erkenntnisse in bestimmten Zeitabständen aus (*Österreichisches Programm Zum Schutz Kritischer Infrastrukturen (APCIP)*, 2014, S. 6).

2.1.2 Deutschland

In Deutschland hingegen gibt es die „Nationale Strategie zum Schutz kritischer Infrastrukturen“ (KRITIS-Strategie). Diese teilt die kritischen Infrastrukturen in neun Bereiche (Energie, Gesundheit, IT und Telekommunikation, Transport und Verkehr, Medien und Kultur, Wasser, Finanz- und Versicherungswesen, Ernährung, Staat und Verwaltung) ein. Wenn man Abbildung 1: Kritische Infrastrukturen Österreichs betrachtet, ist eine Ähnlichkeit zu Österreich erkennbar. Die strategischen Ziele Deutschlands sind:

- **Prävention:** Die Prävention soll sicherstellen, dass die Risiken im Vorfeld analysiert und Schutzmaßnahmen abgeleitet werden, sowie die regelmäßige Durchführung von Übungen.
- **Reaktion:** Bei einem Ausfall wird durch gutes Krisenmanagement die Ausfallzeiten so kurz wie möglich gehalten und der Normalbetrieb schnellstmöglich wieder aufgenommen.
- **Nachhaltigkeit:** Die Nachhaltigkeit soll sicherstellen, dass die laufende Weiterentwicklung der Schutzvorkehrungen gegeben ist. Die dafür erforderlichen Informationen können von Ereignissen der Betreiber anderer Länder oder dem Inland oder den Gefährdungsanalysen kommen.

Deutschland geht den Weg, dass es eine gemeinsame Aufgabe von Staat und den Betreibern kritischer Infrastrukturen ist, zum Schutz beizutragen. Es sollte auch eine Verhältnismäßigkeit der Maßnahme zum Schutzniveau gegeben sein. Zusätzlich sieht der Staat vor, dass alle kritischen Infrastrukturen, die strategischen Ziele Prävention, Reaktion und Nachhaltigkeit aufweisen. Dafür wurde der Risikomanagementkreislauf als Schutzsystem entwickelt. Der Risikomanagementkreislauf besteht aus Prävention, Umsetzung (Übung), Reaktion und Analyse (Evaluation). Durch die Umsetzung dieser Ziele ist gewährleistet, dass kritische Infrastrukturen einen nachhaltigen Schutz erhalten (“Nationale Strategie Zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie),” 2009, S. 5).

In Deutschland gibt es neben der nationalen Strategie zum Schutz kritischer Infrastrukturen auch das IT-Sicherheitsgesetz. Das IT-Sicherheitsgesetz ist 2015 in Kraft getreten und schreibt gesetzliche Sicherheitsstandards für kritischen Infrastrukturen vor. Betroffen von diesem Gesetz sind die Sektoren: Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen. Laut dem IT-Sicherheitsgesetz besteht eine Meldepflicht bei einem IT-Sicherheitsvorfall. Die Absicherungen müssen alle zwei Jahre mit einem Audit geprüft werden und die IT-Sicherheit muss nach Stand der Technik umgesetzt werden. Das Gesetzt ist Pflicht und sollte die Sicherheit von IT-Systemen erhöhen, damit kritische Infrastrukturen trotz steigender Abhängigkeit der IT zuverlässig funktionieren (Rosenthal & Schmitz, 2017).

2.1.3 Schweiz

In der Schweiz gibt es eine nationale Strategie zum Schutz kritischer Infrastrukturen (SKI) für den Zeitraum von 2018 bis 2022. Diese wurde am 08. Dezember 2017 veröffentlicht und ist somit die neueste Strategie der drei beschriebenen Länder Österreich, Deutschland und Schweiz. Die kritischen Infrastrukturen der Schweiz werden auch in neun Bereiche (Behörden, Energie, Entsorgung, Finanzen, Gesundheit, IKT, Nahrung, Öffentliche Sicherheit und Verkehr) eingeteilt. Die strategischen Ziele der Schweizer Strategie sind:

- Kritische Infrastrukturen sind widerstandsfähig, um Ausfälle zu vermeiden oder die Funktionsfähigkeit schnell wieder herstellen zu können.
- Bevölkerung und Wirtschaft sind widerstandsfähig, um schwere Schäden bei Ausfällen von kritischen Infrastrukturen zu vermeiden.
- Behörden handeln angemessen bei einem Ausfall von kritischen Infrastrukturen.
- Unterstützung der Betreiber von kritischen Infrastrukturen.

Mit diesen strategischen Zielen will die Schweiz eine Verbesserung der Widerstandsfähigkeit von kritischen Infrastrukturen erreichen. Die Schweiz möchte damit den wirtschaftlichen Wohlstand aufrechterhalten und den Schutz der Bevölkerung sicherstellen. Dazu wurde ein Prozess entwickelt der aus fünf Stufen (Analyse, Bewertung, Schutzmaßnahmen, Umsetzung und Überprüfung) besteht. Dieser nennt sich „Regelkreis zur Überprüfung und Verbesserung der Resilienz“, damit sollte eine laufende Verbesserung sichergestellt werden (Bundesamt für Bevölkerungsschutz BABS, 2017, S. 516).

2.2 NIS-Richtlinie

Die NIS-Richtlinie ist eine EU-Richtlinie, die 2016 in Kraft getreten ist. Bis zum 09. Mai 2018 haben die Mitgliedsstaaten die erforderlichen Rechts- und Verwaltungsvorschriften zu erlassen die notwendig sind, damit die NIS-Richtlinie erfüllt werden kann. Durch die Richtlinie sollten technische Ausfälle und Hackerangriffe vermindert werden. Weiters erhöht die Richtlinie die Zusammenarbeit der EU-Mitgliedsstaaten, indem Vorfälle ausgetauscht werden und dadurch anschließend neue Schutzmaßnahmen umgesetzt werden. Folgende Sektoren sind von der NIS-Richtlinie betroffen:

- Energie
- Verkehr
- Bankwesen
- Finanzmarktinfrastrukturen
- Gesundheitswesen
- Trinkwasserlieferung und -versorgung
- Digitale Infrastruktur

Diese Sektoren sind betroffen, da diese laut NIS-Richtline „Betreiber wesentlicher Dienste“ sind. Das schließt auch kritische Infrastrukturen ein, daher müssen diese auch die NIS-Richtline erfüllen. Durch die NIS-Richtlinie sollte ein hohes Niveau an Sicherheit in allen EU-Staaten gewährleistet werden. Zudem bietet die NIS-Richtlinie eine rechtliche Grundlage für die Sicherheit von Netz- und Informationssystemen, für die oben genannten Sektoren. Die Richtlinie schreibt kritischen Infrastrukturen vor, dass die Sicherheitsmaßnahmen „Stand der Technik“ sein müssen (Rosenthal & Schmitz, 2017).

Unternehmen die eine kritische Infrastruktur betreiben, sollten auch ISO 27001 zertifiziert sein. Für diese Unternehmen ist die NIS-Richtline auf das ISMS (information security management system) bezogen kein Problem, da sich die Anforderungen nahezu decken. In der ISO 27001 werden Anforderungen an ein ISMS definiert. Das ist ein weltweit einheitlicher Standard für IT-Sicherheit den Unternehmen mit der ISO 27001 Zertifizierung erfüllen. Diese Norm ist ein kontinuierlicher Prozess zur Verbesserung und ist auch in Deutsch verfügbar. Kritische Infrastrukturen sollten alle Normen der ISO 27000 Reihe erfüllen, jedoch kann nur die ISO 27001 zertifiziert werden (Kersten et al., 2016).

2.3 Bereiche der kritischen Infrastrukturen

Der Masterplan APCIP verzichtet auf eine Aufzählung der Bereiche von kritischen Infrastrukturen. Das liegt daran, dass die Wirtschaft in Österreich sehr komplex ist. Um dennoch einen Überblick zu erhalten, sind in Abbildung 1: Kritische Infrastrukturen Österreichs, die Bereiche nach der Gliederung der „Cyber Security Austria“, dargestellt.

Abbildung 1: Kritische Infrastrukturen Österreichs

Quelle: https://www.cybersecurityaustria.at/images/kritische-infrastrukturen.jpg (19.08.2020)

In dieser Abbildung ist klar ersichtlich, dass dies Bereiche sind, die uns alle betreffen und ein Ausfall erhebliche Auswirkung auf unser Leben hätte. Daher ist der Schutz kritischer Infrastrukturen sehr wichtig. In den nachfolgenden Beispielen wird nochmals verdeutlicht, welche Auswirkungen ein Ausfall haben könnte. Das zweite Beispiel veranschaulicht, welche Abhängigkeiten zwischen den kritischen Infrastrukturen bestehen und dass es bestimmte Bereiche gibt die wichtiger sind als andere.

Ein Beispiel ist der Bereich Elektrizität. Ohne Strom würde unser täglicher Ablauf anders aussehen da kein elektrisches Licht, keine Tankstellen und in der Küche fast gar keine Geräte, wie Kühlschrank oder E-Herd, funktionieren würden. Aus diesem Grund ist es wichtig, dass es in Österreich einen Masterplan für kritische Infrastrukturen gibt. Ein Nachteil ist, dass Unternehmen freiwillig in die erhöhte Sicherheit investieren müssen, wie beispielsweise die Anschaffung einer Firewall oder USV (unterbrechungsfreie Stromversorgung) Anlage, damit die IT gestützte Steuerung der Anlagen auch bei Stromausfall reibungslos funktioniert.

Ein weiteres Beispiel, welches mehrere kritische Infrastrukturen betrifft, wäre ein Krankenhaus. Dieses fällt in den Bereich Gesundheit, benötigt aber für die Gesundheitsversorgung Energie, um die Versorgung der Geräte aufrecht zu erhalten. Des Weiteren werden auch die Kommunikationswege benötigt, um Medikamente bestellen zu können oder einen Krankenwagen zu koordinieren. Das Beispiel verdeutlicht, wie abhängig die einzelnen Infrastrukturen voneinander sind und wie wichtig die Vernetzung dabei ist. Jedoch wird auch ersichtlich, dass es bei einem Ausfall einer kritischen Infrastruktur zur Kettenreaktion kommen kann. Die beschriebenen Beispiele zeigen, wieso kritische Infrastrukturen so wichtig sind und diese einen besonderen Schutz benötigen (Kuhn, 2005, S. 6).

Es ist schwierig eine Gewichtung über die Notwendigkeit der Infrastrukturen zu erstellen. Dennoch gibt es die zwei Bereiche Elektrizität und die Informations- und Kommunikationstechnik (IKT), die die anderen Bereiche miteinander verbinden. Diese zwei Bereiche werden auch zentrale Infrastruktursektoren genannt, da sie vieles miteinander vernetzen oder andere Bereiche davon abhängig sind. Von den zentralen Infrastruktursektoren hängen beispielsweise die meisten Versorgungsbereiche ab. Ein Ausfall dieser zwei Bereiche könnte eine Kettenreaktion auslösen. Dabei würden die Bereiche nacheinander ausfallen und das könnte zu einem Chaos führen. Daher sind laut „Cyber Security Austria“ die zwei Sektoren besonders wichtig und es gilt diese zu schützen. Dies wird auch durch „Cyber Security Austria“ verdeutlicht, wo sehr häufig auf Smart Grid eingegangen wird, da das Stromnetz von großer Bedeutung ist und immer mehr vernetzt wird. Ein Blackout über mehrere Tage könnte verheerende Auswirkungen haben (Cyber Security Austria - Verein zur Förderung der Sicherheit Österreichs strategischer Infrastruktur).

Sollte ein Ausfall einer kritischen Infrastruktur dennoch geschehen, sollte in kürzester Zeit ein Wiederhochfahren möglich sein, besonders wenn es einen zentralen Infrastruktursektor wie die Elektrizität betrifft. Ein neuer Ansatz wäre hier das Smart Emergency Grid, mit dem Konzept der selektiven Versorgung bei Unterspannung. Ein Vorteil ist, dass diese Schaltung keine Angriffsfläche für IT-Angriffe bietet, da es rein durch elektrische Verschaltungen möglich ist. Es ist jedoch eine Anpassung des Stromnetzes nötig. Dies könnte durch eine Modifikation der

Smart Meter (Intelligenter Stromzähler) erfolgen (Wakolbinger et al., 2012). Bei diesem Konzept könnten bei einem Stromausfall nur kritische Verbraucher zugeschaltet und die Versorgung für kritische Infrastrukturen schneller wiederhergestellt werden.

2.4 Gefahren und Vorteile der Vernetzung

Kritische Infrastrukturen sind zahlreichen Gefahren ausgesetzt, wie Naturereignisse, Terrorismus, Kriminalität, Krieg und technisches sowie menschliches Versagen. Die Vernetzung bietet aus Sicht der IT-Sicherheit eine große Angriffsfläche. Aus diesem Grund wird der Fokus dieser Masterarbeit auf die Vernetzung gelegt. Durch die Vernetzung steigt die Angriffsfläche für Hackerangriffe und somit nimmt die Internetkriminalität (Cybercrime) stetig zu. Als Internetkriminalität werden strafbare Taten bezeichnet, die Lücken von Informationstechnik und Telekommunikationstechnik ausnutzen, um strafbare Handlungen zu begehen. Beispielsweise das Verschlüsseln von Daten mit anschließender Erpressung und Lösegeldforderung. Bei Internetkriminalität ist davon auszugehen, dass Taten oft unentdeckt bleiben oder nicht gemeldet werden. Unternehmen sehen von einer Strafanzeige häufig ab, da sie eine Rufschädigung oder einen Imageverlust befürchten, wenn ein Hackerangriff bekannt wird. Eine Gefahr, die durch die globale Vernetzung entsteht, ist die schnelle Verbreitung von Schadsoftware über die vernetzten Systeme. Das kann zur Folge haben, dass Hacker eine kritische Infrastruktur lahmlegen (Vetter, 9-10 ;27;77).

Die technische Vernetzung ist ein neuer Trend geworden und schreitet immer weiter voran. Alles soll immer weiter miteinander verbunden werden, um Informationen auszutauschen und die Geschwindigkeit, Zuverlässigkeit und Flexibilität der Prozesse zu erhöhen. Durch die Vernetzung kann zusätzlich Geld gespart werden, indem durch die Informationstechnik vieles automatisiert wird und dadurch das Personal reduziert werden kann. Der Trend geht hin zur zentralen Steuerung, wie beispielsweise ein Kontrollsystem zur Steuerung von 50 Kraftwerken, die von einer Leitwarte aus gesteuert werden. Neuere Phänomene sind das Cloud Computing und Smart Grids, die immer mehr an Bedeutung gewinnen, da sie eine zentrale Steuerung ermöglichen (Gaycken, 2011). Dadurch wird nur eine Leitwarte und in Folge weniger Personal benötigt. Dies führt zu einer Reduktion der Baukosten. Durch die Automatisierung werden auch die laufenden Kosten zusätzlich verringert. Das führt zu einem Wettbewerbsvorteil, wenn eine Vernetzung in einem Betrieb vorgenommen wird.

Die Vernetzung der Systeme führt nicht zwangsweise zur Vernetzung der beteiligten Menschen. Oft geht jedoch damit einher, dass Menschen mitvernetzt werden. Es werden mit Hilfe der Vernetzung Informationen über das tägliche Leben und deren getroffenen Entscheidungen gesammelt. Diese Entscheidungen werden als Zustände gesehen, die dann wie Schaltelemente beobachtet und gesteuert werden können. Der Mensch wird als ein Element eines Systems gesehen, das die einzelnen Elemente verändern kann, er kann sich jedoch selbst entfalten (Meixner, 2016, S. 3). Das veranschaulicht uns, dass die Vernetzung eine größere Dimension angenommen hat als am Anfang erwartet wurde. Der Vorteil dabei ist, dass durch den hohen Informationsaustausch viele Systeme oder Geräte miteinander kompatibel sind und einfach

gesteuert werden können. Darunter fallen die Sprach-Assistenten, wie beispielsweise Alexa von Amazon, Siri von Apple oder der Google Assistent, da diese Geräte mit vielen Systemen bereits kompatibel sind und diese ansteuern können. Der Nachteil dabei ist, dass Informationen an die Hersteller übermittelt und ausgewertet werden und wir dadurch immer mehr zum gläsernen Menschen werden. Das geschieht auch, wenn ein solches Gerät in einer kritischen Infrastruktur betrieben wird.

Durch die Vernetzung ist es möglich, dass MitarbeiterInnen von zu Hause aus oder von unterwegs arbeiten. Technisch umsetzbar ist das mit Hilfe einer VPN (Virtual Private Network) Verbindung. Eine VPN Verbindung bringt jedoch auch Gefahren mit sich und muss auf mehreren Ebenen abgesichert werden. Eine Gefahr bildet das Netzwerk, von dem eine Verbindung aufgebaut wird. Das Netzwerk sollte bereits über eine entsprechende Sicherheitsstruktur verfügen und kein ungesichertes öffentliches Netzwerk sein, denn diese Sicherheit kann vom Unternehmen nicht überwacht werden, da der lokale Netzwerkbetreiber dafür die Verantwortung übernimmt (Steinmann, 2018, S. 53). Die Verschlüsselung und die Wahl der Software für Server und Client, die für die VPN Verbindung erforderlich ist, kann vom Unternehmen gewählt und auch abgesichert werden. Für kritische Infrastrukturen ist daher ein sicherer Fernzugriff wichtig. Die Steuerung der Anlagen und Systeme einer kritischen Infrastruktur muss auch in Krisenzeiten zuverlässig funktionieren. Gesehen haben wir das bei Covid-19, da mussten viele MitarbeiterInnen von zu Hause aus arbeiten, um die Infrastrukturen am Laufen zu halten.

Die steigende Vernetzung bringt nicht nur Vorteile mit sich, denn es entstehen immer mehr Abhängigkeiten. Durch die Vernetzung, die in vielen Bereichen der Technik vorhanden ist, kommen wir von den Möglichkeiten immer weiter zu den Notwendigkeiten. Die Prozesse und Abläufe werden den neuen Möglichkeiten, die durch die Vernetzung möglich sind, angepasst. Ein Beispiel für die Abhängigkeit ist, wenn die verarbeitende und transportierende Großindustrie mit der Steuerung, Verwaltung bis hin zum Warenaustauschsystem vernetzt ist. Bei einem solchen System sind die einzelnen Strukturen nur mehr schwer trennbar, da die gesamten Abläufe darauf ausgelegt sind, dass diese vernetzt funktionieren. Das bietet hohe Flexibilität und es ist ein weniger spezifisch geschultes Personal notwendig, da die Prozesse durch die Informationstechnologien zusätzlich überwacht werden. Eine Trennung der Systeme ist nach einem Vernetzen nur mehr schwer möglich und somit entsteht eine Abhängigkeit der einzelnen Systeme durch die Vernetzung (Gaycken, 2011, S. 3).

Für die Hacker bedeutet das, dass sie nur einen Teil des Systems kompromittieren oder lahmlegen müssen und in Folge kommt das gesamte System zum Erliegen, sofern es keine redundanten Systeme gibt. Bei einem redundanten System kommt es zu einer Umschaltung, wenn ein System ausfällt. Ein Beispiel dafür ist, wenn der Computer für die Steuerung doppelt vorhanden ist und bei einem Ausfall des ersten Computers, der zweite die Steuerung übernimmt. Das ist mit höheren Kosten verbunden, da das System in zweifacher Ausführung vorhanden sein muss. Wenn das nicht der Fall ist, kann durch die Abhängigkeiten der einzelnen Strukturen ein Betrieb oder eine Infrastruktur ausfallen. Auch die Angriffsfläche der gesamten Infrastruktur wird durch die Vernetzung erhöht. Derzeit überwiegen die Vorteile der Vernetzung, da es nur wenige Angriffe in der Vergangenheit gegeben hat und es noch nicht zu einem

Totalausfall der gesamten kritischen Infrastrukturen gekommen ist. Eine weitere Globalisierung der Infrastrukturen ist mit der Vernetzung möglich.

Es gibt jedoch auch Angriffe, die ohne Vernetzung möglich sind, wie beispielsweise über einen infizierten USB-Stick. In einer Studie wurden 297 USB-Sticks auf einem Universitätscampus verteilt. Das Ergebnis war erschreckend, denn ein Angriff wäre mit einer Rate von 45-98% erfolgreich gewesen. Die Personen, die den USB-Stick fanden, haben ihn angeschlossen und Dateien geöffnet. Der erste USB-Stick, wurde sogar innerhalb von 6 Minuten gefunden, angeschlossen und die Dateien geöffnet. Auf den Stick waren nur HTML Dateien, die auf einen Server verlinkten, um zu prüfen ob ein USB-Stick gefunden und die Datei geöffnet wurde. Die meisten Personen bei dieser Studie wollten nur den Besitzer der USB-Sticks ermitteln und ihn an diesen zurückgeben. MitarbeiterInnen einer kritischen Infrastruktur gehören daher laufend geschult, um sie zu sensibilisieren. Als zusätzlicher Schutz, sollten die USB-Ports auf den Computer gesperrt werden (Tischer et al., 2016).

3 ANGRIFFE

Mit Angriffen sind in dieser Masterarbeit Hackerangriffe gemeint. Die Hackerangriffe (Angriffe aus dem Internet) in Österreich (in Abbildung 2 als Balkendiagramm dargestellt) nehmen laufend zu. Daher wird zuerst in diesem Kapitel eine Gliederung der Angriffe mit Hilfe der Cyberleiter beschrieben. Danach werden die Motive für potenzielle Hacker genannt, nach welchen Kriterien die Hacker kategorisiert werden können und welche Motive sie haben könnten, um ein Ziel anzugreifen. Im Anschluss werden Angriffe aus der Vergangenheit beschrieben und analysiert.

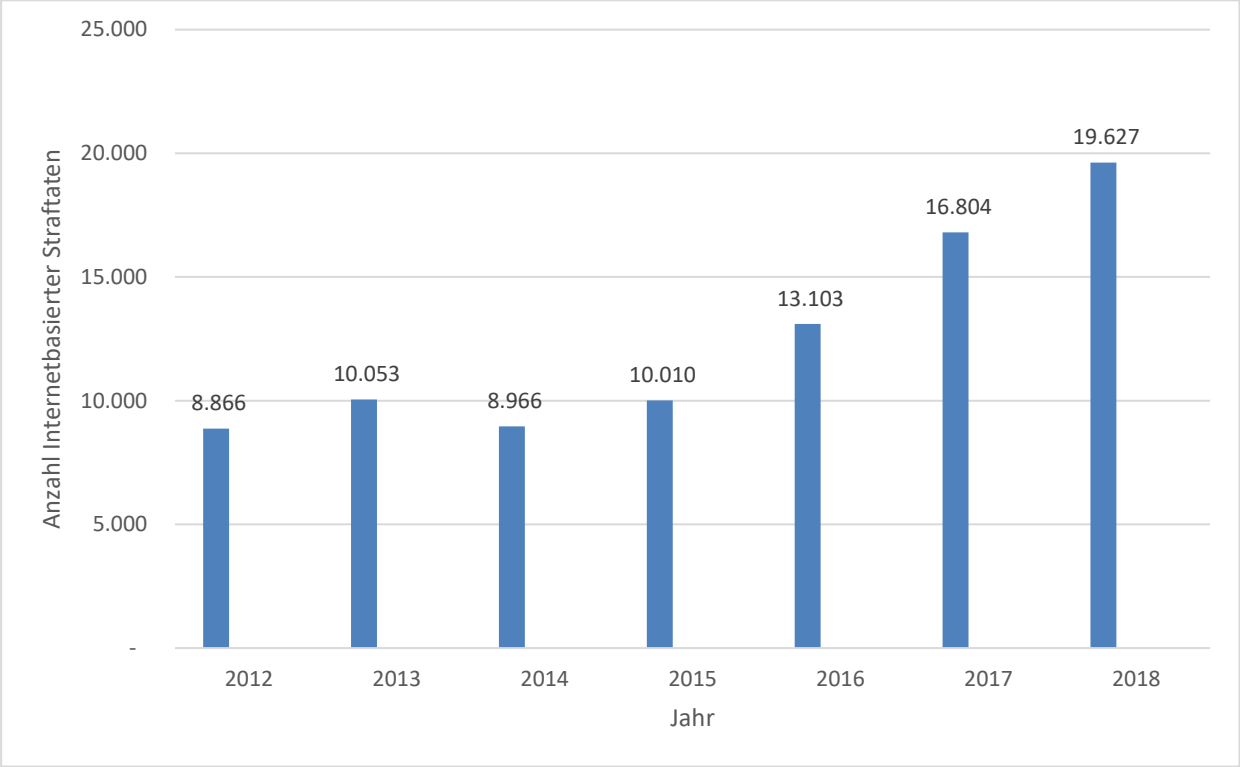

Abbildung 2: Anzahl der Cyberangriffe Österreichs von 2012 bis 2018

Quelle: https://www.bundeskriminalamt.at/306/files/Cybercrime_Report_18_web.pdf verändert

In der Abbildung 2 ist ab dem Jahr 2015 eine deutliche Steigerung (der Internetkriminalität) zu erkennen. Im Jahr 2018 ergab das eine Steigerung von +16,8% gegenüber dem Jahr 2017. Daraus lässt sich schließen, dass sich die Kriminalität immer mehr ins Internet verlagert und auch in Zukunft weiter zunehmen wird. Durch die Zunahme der Internetkriminalität wird die Gefahr für kritische Infrastrukturen immer größer.

3.1 Gliederung der Angriffe

Es gibt unterschiedliche Arten von Angriffen, die unterschiedlichen Schaden verursachen können, daher ist eine Gliederung der Angriffe wichtig. Eine übersichtliche Gliederung, wie Cyberattacken eingeteilt werden können, sind laut Dunn Cavelty (2010) die fünf Stufen auf der Cyberleiter. Je höher die Stufe (Nummer), desto höher ist das Schadensausmaß des Angriffs. Die Stufen als Nummerierung aufgezählt lauten:

1. Cybervandalismus
2. Internetkriminalität
3. Cyberespionage
4. Cyberterrorismus
5. Cyberwar

Zur ersten Stufe, dem Cybervandalismus, zählen virtuelle Änderungen des Inhalts oder auch dessen Zerstörung. Dazu zählen laut Dunn Cavelty (2010) Angriffe wie das Hacken einer Webseite oder das Erzwingen eines Webseitenausfalls durch Überfluten von Datenanfragen. Angriffe dieser Art werden als DDoS (Distributed Denial-of-Service) bezeichnet. Dies ist eine weit verbreitete Angriffsform und im Vergleich zu den anderen Angriffen auf der Cyberleiter relativ harmlos und zeitlich begrenzt. Auf der zweiten Stufe (Internetkriminalität) und der dritten Stufe (Cyberspionage) sind die Hauptopfer der Unternehmenssektor, es können jedoch auch Regierungsnetzwerke betroffen sein (Dunn Cavelty, 2010, S. 1–2).

Ein hohes Schadensausmaß haben Angriffe der Stufe vier dem Cyberterrorismus. Das sind illegale Angriffe von nicht staatlichen Akteuren. Sie greifen Computer, Netzwerke sowie die darin gespeicherten Daten mit dem Ziel an, eine Regierung und deren Bevölkerung einzuschüchtern oder auch ein bestimmtes Vorhaben durchzusetzen. Solche Angriffe werden nur als Cyberterrorismus gezählt, wenn bestimmte Kriterien erfüllt werden. Die Kriterien dafür sind, körperliche Gewalt an Personen, Schäden am Eigentum oder schwere ökonomische Schäden, welche erhebliche Angst erzeugen. Durch einen Angriff auf eine kritische Infrastruktur, könnte dieses Ziel schnell erreicht werden und eine Regierung würde dadurch zum schnellen Handeln gezwungen werden (Dunn Cavelty, 2010, S. 1–2).

SCADA-Systeme (Supervisory Control and Data Aquisition-Systeme) spielen eine wichtige Rolle bei kritischen Infrastrukturen, da die meisten durch diese Systeme gesteuert werden. Diese Systeme bestehen hauptsächlich aus Komponenten wie Sensoren, Steuerungselementen, lokalen Prozessoren, Nahbereichskommunikation, Computer und Fernkommunikation. SCADA-Systeme sammeln die Informationen, übermitteln diese an zentrale Stellen und werten diese dann aus. Die ausgewerteten Daten werden anschließend auf einem Bildschirm des Bedieners dargestellt. Dieser kann dann Kontrollaktionen durchführen und die Anlage steuern. Daher werden zur Steuerung und Überwachung von kritischen Infrastrukturen meistens SCADA-Systeme eingesetzt. Der Vorteil liegt darin, dass diese durch die Vernetzung zentral steuerbar sind (Robles et al., 2008, S. 99–100).

Auf der obersten Stufe der Cyberleiter befindet sich der Cyberkrieg. Hierbei geht es um kriegerische Konflikte im virtuellen Raum. Der Begriff Cyberkrieg ist ein Unterbegriff der Informationskriegsführung. Dieses Konzept zielt darauf ab, Angriffe im Cyberraum durchzuführen, die die Entscheidungsfähigkeit der politischen Führung, des Militärs sowie der zivilen Bevölkerung des Feindes beeinflussen. Das ist eine neue technologische Art des Krieges im Informationszeitalter, wo die Vernetzung laufend zunimmt und auch Bereiche des Militärs betroffen sind (Dunn Cavelty, 2010, S. 1–2).

Besonders gefährlich für kritische Infrastrukturen sind daher Angriffe der Stufe vier und fünf, da diese einen erheblichen Schaden anrichten können. In Stufe fünf könnte der Angriff auf die Uranzentrifugen im Iran fallen. Dieser Angriff wurde mittels Stuxnet im Jahr 2010 durchgeführt und sabotierte das Nuklearprogramm des Irans. Wie der Angriff funktioniert wird im Kapitel „Angriffe der Vergangenheit“ beschrieben (Dunn Cavelty, 2010, S. 1–2).

3.2 Potenzielle AngreiferInnen

Um ein System wie kritische Infrastrukturen, aus Sicht der IT-Sicherheit absichern zu können, ist es wichtig zu wissen von wem ein Angriff erfolgen kann, um entsprechende Gegenmaßnahmen einzuleiten. Dazu müssen die Motive der Hacker bekannt sein und kategorisiert werden. Einen guten Überblick über die potenziellen Hacker bietet das Buch „Secrets and Lies: Digital security in a networked world“ von Bruce Schneier (2015).

Es gibt unterschiedliche Motive für einen Angriff: finanzieller Gewinn, geheime Informationen, Wettbewerbsvorteil und militärische Geheimnisse. Beispielsweise werden Spionageangriffe durchgeführt, um einen Wettbewerbsvorteil zu erlangen oder Kriminelle sind auf der Suche nach finanziellem Gewinn. Die Kriminalität hat sich somit in den digitalen Bereich verlagert. Um einen guten Schutz zu gewährleisten, ist es wichtig die AngreiferInnen zu kennen. Die Hacker können kategorisiert werden nach: Zugriff, Fachwissen, Ressourcen, Ziele und Risiko (Schneier, 2015, S. 42–43).

3.2.1 Zugriff

Ein hohes Risiko birgt der Zugriff. Je mehr Rechte ein Hacker hat, desto leichter kann er ins System eindringen. Somit ist für interne Angestellte ein Angriff leichter möglich. Vor allem wenn die Angestellten in der IT-Abteilung arbeiten, da diese Personen auch über das nötige Fachwissen verfügen. Für externe Angreifer und Angreiferinnen ist es schwieriger, da im Regelfall diese keine detaillierten Kenntnisse über die interne Infrastruktur haben. Bei kritischen Infrastrukturen muss bei der Auswahl des Personals genau darauf geachtet werden wie vertrauenswürdig und zuverlässig diese Person ist und welchen Zugriff sie erhält, da eine Bestechung oder Erpressung der MitarbeiterInnen nicht auszuschließen ist (Schneier, 2015, S. 42–43).

3.2.2 Fachwissen

Es gibt Angriffe die viel Fachwissen erfordern, dafür jedoch wenig Zugriff auf das zu hackende System. Dazu zählt das Brechen eines Verschlüsselungsalgorithmus. Daten werden verschlüsselt kopiert oder bei einer Übertragung abgefangen und anschließend wird die Verschlüsselung aufgebrochen. Die breitere Masse jedoch hat wenig Fachwissen und versucht es daher eher über Social Engineering (Schneier, 2015, S. 42–43).

Beim Social Engineering wird der Mensch so manipuliert, dass er einen Fehler macht, wie etwa sensible Daten preiszugeben, Daten die Schadsoftware beinhaltet zu öffnen oder Zahlungen an die Hacker zu tätigen. Hacker geben sich hierbei oft als Behörden oder namhafte Unternehmen aus. Beim Social Engineering wird die Gutgläubigkeit der Menschen ausgenutzt, da sich das Opfer nichts Schlimmes denkt und daher nicht mit der Dreistigkeit der Täter rechnet (Steinmann, 2018, S. 57–58).

3.2.3 Ressourcen

Ein weiterer wichtiger Teil bei einem Angriff sind die Ressourcen des Hackers. Ein Team mit guten finanziellen Mitteln kann einfacher einen erfolgreichen Angriff durchführen als eine Einzelperson mit wenig Zeit und Geld. Ein Hacker mit guten finanziellen Mitteln könnte Experten anstellen oder in eine Firma einschleusen und minimiert so auch das Risiko erwischt zu werden (Schneier, 2015, S. 42–43).

3.2.4 Ziele

Die verschiedenen Hacker haben unterschiedliche Ziele: Schaden anrichten, sensible Daten zu stehlen oder finanziellen Gewinn zu erzielen. Hier ist es wichtig dies zu differenzieren, um die Gegenmaßnahmen auf die AngreiferInnen anzupassen. Gegenmaßnahmen die einen Angriff stoppen würden, könnten von einem anderen Hacker einfach umgangen werden. Bei kritischer Infrastruktur wäre das Stehlen von Daten ein geringeres Übel als ein Angriff, der die Infrastruktur zum Erliegen bringt (Schneier, 2015, S. 42–43).

3.2.5 Risikobereitschaft

Hacker haben eine unterschiedliche Risikobereitschaft. Oft wollen Hacker nur Aufmerksamkeit erregen, jedoch keine Freiheitsstrafe riskieren. Kriminelle hingegen sind bereit ins Gefängnis zu gehen, wenn sie erwischt werden. Terroristen sind sogar bereit für ihre Sache zu sterben (Schneier, 2015, S. 42–43). Anhand dieser Beispiele, wird deutlich, wie unterschiedlich das Risiko ist, welches Hacker eingehen, um beispielsweise eine kritische Infrastruktur anzugreifen oder auszuspionieren.

3.3 Angriffe der Vergangenheit

In diesem Kapitel werden Angriffe aus der Vergangenheit aufgelistet und beschrieben. Da hier nicht alle Angriffe beschrieben werden können, werden folgende Angriffe besonders betrachtet:

- Stuxnet
- Regin
- BlackEnergy
- Angriff auf die Zentralbank von Bangladesch
- WannaCry

Die Gliederung der Angriffe erfolgt nach dem Datum beginnend mit dem ältesten Angriff. Es wird beschrieben wie die Angriffe die Systeme infiziert und welchen Schaden sie angerichtet haben. Die Beschreibung dieser Angriffe, dient dann in weiterer Folge dazu, eine Eingrenzung für die Absicherung von kritischen Infrastrukturen durchzuführen. Anhand dieser Eingrenzung und dem Stand der Technik werden dann Maßnahmen zur Absicherung beschrieben.

Bei den meisten Angriffen kommt ein sogenannter Dropper zum Einsatz. Dieser wird in ein System eingeschleust und damit ein Einfallstor geöffnet. Der Dropper lädt dann den Schadcode. Dieser Schadcode wird auch als Payload bezeichnet. Ein Dropper ist somit ein Trägerprogramm, das Malware benötigt, um funktionsfähig zu werden. Dabei werden auch zero-day Exploits ausgenutzt. Zero-day Exploits nutzen eine Sicherheitslücke aus, die dem Hersteller/Autor der Software noch unbekannt ist. Dem Softwarehersteller bleiben also null Tage, da die Lücke noch am selben Tag ausgenutzt wird. Wenn einem Hersteller eine Lücke in seinem Produkt bekannt wird, bringt er in der Regel schnellstmöglich ein Update heraus, um diese Lücke zu schließen (Minnich, 2016).

3.3.1 Stuxnet

Die Malware Stuxnet wurde 2010 entdeckt. Sie griff Industriecomputer an und verbreitete sich über USB-Sticks und Netzwerke. Stuxnet ist darauf konzipiert SCADA Systeme anzugreifen und sich zu verbreiten. Wenn Stuxnet auf einem PC installiert ist, verwendet er die Standardpasswörter von Siemens. Dadurch erhält er Zugriff auf die Systeme, auf denen die Programme WinCC und PCS 7 ausgeführt werden. Die Programme können den Code der SPS (speicherprogrammierbare Steuerung) steuern und ändern und so die Anlage sabotieren. Liam O'Murchu ist bei Symantec ein Security Response Supervisor. Ihm zufolge arbeitet Stuxnet nach einer Infektion in zwei Schritten. Als erstes werden Konfigurationsinformationen über das Siemens System, welches auf infizierten Computern läuft auf einem Server hochgeladen. Die Hacker können dann die Funktionsweise der SPS neu programmieren und so entscheiden wie diese arbeiten soll. Den bearbeiteten Code senden sie dann zurück an den infizierten Computer, der dann die Funktionsweise der SPS ändert. Das eigentliche Ziel von Stuxnet war das Iranische Nuklearprogramm zu sabotieren. Hier gelang es Stuxnet die Einrichtungen zu infizieren, welche mit den Hochgeschwindigkeitszentrifugen verbunden waren (Thabet, 2011).

3.3.2 Regin

Regin ist eine Malware die 2013 entdeckt wurde, jedoch schon seit 2008 im Umlauf ist und bereits in mehreren Versionen existiert. Sie ist eine sehr komplexe Malware, die über Jahre von mehreren Entwicklern mit viel Ressourcen entwickelt wurde. Es ist eine 32Bit und 64Bit Version im Umlauf, die auch zero-day Exploits von damals beinhalten. Auch in Österreich waren Computer mit Regin infiziert. Regin ist darauf ausgelegt ihre Ziele auszuspionieren und Daten zu stehlen, was es zu einem erstklassigen Spionagetool macht. Regin kann zusätzlich angepasste Funktionen laden und ist damit flexibel erweiterbar (Symantec, 2015).

Das Regin Framework ist darauf ausgelegt modular zu sein, um noch präziser angreifen zu können. Symantec gelang es daher nicht immer zu ermitteln welche Daten gestohlen wurden, da Regin sehr geschickt vorgeht und die Daten häufig nicht auf die Festplatte schreibt. Dadurch ist eine Analyse der gestohlenen Daten im Nachhinein nur schwer möglich. Das Regin Framework arbeitet in sechs Schritten. Im Schritt null, dem sogenannten Dropper wird Regin auf dem Zielcomputer installiert, danach folgt Schritt eins wo die Treiber installiert werden. Dies ist der einzige Schritt, wo der Code auf dem Computer sichtbar ist. Dieser wird auch als Supportmodul bezeichnet. Danach ist alles verschlüsselt und es wird Schritt zwei ausgeführt, wo ein Kernel Treiber installiert wird. In Schritt drei, wird eine Kernel Mode DLL verschlüsselt, in der Registry abgelegt und es wird ein Framework eingerichtet, welches für die nächsten Schritte benötigt wird. Im Schritt vier, werden zwei verschlüsselte Container erstellt und Kerneltreiber geladen. Der letzte Schritt fünf, beinhaltet die Payload Module und Daten Files. In den verschlüsselten Container sind die DLLs und benutzerspezifischen Payload Daten wie gestohlene Passwörter oder gesammelte Computerinformationen. Angegriffen wurde mit Regin beispielsweise Internetserviceprovider, die Telekommunikationsinfrastruktur, die Krankenhäuser, der Energie Sektor und Fluglinien. Das bedeutet, dass auch kritische Infrastrukturen durch Regin angegriffen wurden (Symantec, 2015).

3.3.3 BlackEnergy

Die Malware BlackEnergy sorgte 2015 für Schlagzeilen, da sie in der Ukraine am 23. Dezember 2015 für einen massiven Stromausfall sorgte, der über mehrere Stunden dauerte und unterschiedliche Regionen in der Ukraine betraf. Das war das erste bestätigte zivile Ziel, dass durch einen Cyberwar Angriff attackiert wurde. Diese Malware ist bereits in drei Versionen vorhanden. Der Hauptunterschied zwischen BlackEnegry2 und BlackEnergy3 ist, dass die Version drei auch ohne Administratorrechte auskommt. BlackEnergy kann mit verschiedenen Modulen flexibel erweitert werden. Diese werden in separaten verschlüsselten Dateien abgelegt. Der Angriff 2015 lief folgendermaßen ab. Es wurden Phishing Mails an das Ziel gesendet, diese Mails beinhalteten Microsoft PowerPoint Dateien. In diesen Dateien befand sich in den Makros ein Schadcode, welcher zusätzlich Microsoft Office zero-day Lücken von damals ausnutzte. Wenn der Benutzer oder die Benutzerin die Makros erlaubte, dann wurde eine .JAR Datei ausgeführt, welche den BlackEnergy Dropper auf dem Computer installierte. Damit das erfolgreich funktioniert muss auf dem Zielcomputer eine Java Laufzeitumgebung

installiert sein. Im Netzwerk kommuniziert BlackEnergy über HTTP (Hypertext Transfer Protocol), welche mit dem RC4 Algorithmus verschlüsselt ist. Erst später wurde eine HTTPS (Hypertext Transfer Protocol Secure) Verbindung aufgebaut. Damit wird das gesamte Netzwerk ausspioniert und weitere Computer und auch Server infiziert. Die gesammelten Informationen werden dann den Hackern übermittelt. Hiermit versuchen sie immer mehr Berechtigungen bis hin zum Domänenadministrator zu erhalten. Beim Angriff 2015 auf die Ukraine wurden am Schluss wichtige Daten von der Festplatte gelöscht, die Windows logs gelöscht und der erste Sektor auf der Festplatte überschrieben damit der Computer nicht mehr booten konnte (Cherepanov & Lipovsky, 2016). Daraus lernen wir, dass auch der HTTP Datenverkehr genauestens überwacht werden sollte, um einen Angriff frühzeitig zu erkennen. In den meisten Fällen sind die Hacker über längere Zeit im Netzwerk, um Informationen zu sammeln. Anhand dieser Informationen wird dann nach Lücken gesucht, die ausgenützt werden können.

3.3.4 Angriff auf die Zentralbank von Bangladesch

Das auch der Bereich Finanzen der kritischen Infrastrukturen nicht sicher ist, zeigt der Angriff im Jahr 2016 auf die Zentralbank von Bangladesch. Bei diesem Angriff wurden 81 Millionen US-Dollar gestohlen. Wäre der gesamte Angriff erfolgreich gewesen, hätten die Diebe fast 1 Milliarde US-Dollar erbeutet. Diese Summe hätte katastrophale Folgen für die Wirtschaft von Bangladesch haben können. Der Angriff auf die Bank startete mit mehreren Phishing Mails in denen Bewerbungsschreiben enthalten waren. In den Mails befand sich ein Link zum Lebenslauf, welcher auf den Server verwies, der die Malware beinhaltete. Das ermöglichte das erste Eindringen auf den Bank Computer. Danach installierten die Hacker weitere Schadsoftware, welche das Netzwerk ausspionierte und infizierte. Den Hackern gelang es, mit Hilfe eines benutzerdefinierten Binärprotokolls zu kommunizieren und keinen Alarm auszulösen. Das verwischte auch die Spuren da es als authentisch verschlüsselte Verbindung betrachtet wurde. Damit gelang es die Systeme, die für den Cyberangriff notwendig waren, ausfindig zu machen und zu infizieren. Das war schlussendlich das sogenannte SWIFT System, welches die Transaktionen von mehreren Banken verwaltet. Der Raub fand am Donnerstag dem 04. Februar 2016 statt, als die Hacker 35 Transaktionen starteten. Die Hacker berücksichtigten die Feiertage und Zeitverschiebungen der Länder. Daher wählten sie diesen Tag und starteten die Transaktionen und löschten anschließend die Daten, um ihre Spuren zu verwischen. Es wurde sogar auf den SWIFT Drucker gedacht, der normalerweise jede Transaktion ausdruckt. Damit es keine Aufzeichnungen über den Vorgang der Hacker gibt wurde der Drucker deaktiviert (Sullivan et al., 2019).

Warum scheiterte dieser Angriff? Die Hacker machten einen Tippfehler bei einer Transaktion. Sie schrieben „Fundation“ anstelle von „Foundation“. Das löste einen Alarm im System aus woraufhin sich ein Mitarbeiter der New York Fed Bank die Transaktion ansah und bemerkte, dass es mehrere Transaktionen mit hohen Summen gab. Der Mitarbeiter wollte sich vergewissern und kontaktierte die Bank in Bangladesch, doch durch den Feiertag konnte er niemanden erreichen. Daher ließ er das restliche Geld der noch offenen Transaktionen einfrieren und verhinderte so einen noch größeren Bankraub (Sullivan et al., 2019).

Damit wurde auch das als sicher geltende SWIFT System angegriffen. Die Firma brachte danach ein Update heraus, welches Lücken schloss, die von den Hackern ausgenutzt wurden. Schlussendlich verhinderte ein Mensch der misstrauisch wurde den großen Bankraub. Ein Mensch der gut geschult ist kann somit besser reagieren als ein Computer. Das SWIFT System löste zwar einen Alarm aus, doch das geschieht öfter und am Ende entscheidet der Mensch, ob die Transaktion legitimiert wird oder nicht.

3.3.5 WannaCry

Im Mai 2017 richtete die Ransomware (Erpressungstrojaner) WannaCry (WanaDecrypt0r 2.0) großen Schaden an und sorgte damit für Schlagzeilen. Sie befiel in Großbritannien viele Computer des NHS (National Health Service) im Bereich Gesundheit. Das führte zu Ausfällen in der Behandlung, wo beispielsweise Krebspatienten oder auch Herzpatienten nach Hause geschickt oder in andere Kliniken umgeleitet wurden, da die Patientendaten nicht verfügbar waren. In Deutschland war die Deutsche Bahn von diesem Angriff betroffen. In Portugal und Spanien waren Netzbetreiber von dieser Ransomware betroffen. Die Ransomware breitete sich weltweit aus und verschlüsselte die Daten auf tausenden PCs. Anschließend verlangte sie Lösegeld in Form von Bitcoins, um die Daten wieder zu entschlüsseln. Wenn das Lösegeld nicht innerhalb einer bestimmten Zeit bezahlt wurde, wurde mit einer Löschung der Daten gedroht. Das hätte ohne Backup zum Verlust der Daten geführt. WannaCry breitete sich in zwei Schritten aus. Einerseits durch gefälschte Mails, wie die meisten Ransomware Angriffe, andererseits jedoch auch über das Netzwerk. Die Ausbreitung innerhalb des Netzwerkes gelang durch Ausnutzen einer Sicherheitslücke im SMB (Server Message Block) Protokoll, welches für Dateifreigaben in Windows genutzt wird. Microsoft gab im März 2017 das Sicherheitsupdate MS17-010 zum Schließen dieser Lücke heraus, doch durch die schnelle Ausbreitung ist zu erkennen, dass Updates nicht rechtzeitig installiert werden. Forscher haben durch die Registrierung einer Domäne einen Notaus für WannaCry entdeckt, was zu einer schwächeren Ausbreitung führte. WannaCry prüft vor der Verbreitung, ob eine bestimmte Domäne erreichbar ist. Wenn das der Fall ist, wird keine Verbreitung mehr durchgeführt. Das wurde jedoch in einer erweiterten Version umgangen (Briegleb, 2017).

3.3.6 Erkenntnisse

Diese Angriffe lassen uns erkennen, dass die Angriffe gut geplant waren und sorgfältig ausgeführt wurden. Dadurch, dass bei einigen Angriffen wie oben beschrieben zero-day Exploits ausgenutzt wurden, ist klar, dass diese langfristig geplant waren und sogar Regierungen im Hintergrund involviert sein könnten. Eine wichtige Erkenntnis ist, dass Hersteller schnell auf kritische Sicherheitslücken reagieren und ein Update zur Verfügung stellen. Daher sollten sicherheitsrelevante Updates immer schnellstmöglich eingespielt werden, um die Lücken und dadurch auch die Angriffsflächen zu schließen.

Anhand der oben beschriebenen Angriffe aus der Vergangenheit können wir erkennen, dass die meisten Angriffe immer gleich ablaufen oder zumindest ähnlich. Der Ablauf ist meist so, dass

zuerst ein Dropper in das anzugreifende System eingeschleust wird. Dann wird laufend Code mittels Module nachgeladen und die Hacker erhalten immer mehr Informationen und erschleichen sich immer höhere Berechtigungen. Wenn sie dann die nötigen Informationen und Berechtigungen haben, werden die geplanten Schritte umgesetzt. Am Schluss erfolgt meistens eine Verschleierung der Spuren damit keine Rückschlüsse auf die Täter gemacht werden.

Daraus lässt sich schließen, dass kritische Infrastrukturen, die vernetzt sind, nur bestmöglich abgesichert werden können, um Angriffe zu verhindern. Wenn Hacker jedoch genügend Motivation und Ressourcen zur Verfügung haben kann jedes System, welches vernetzt ist, angegriffen werden. Bei kritischen Infrastrukturen, die nicht vernetzt sind, ist wie im Beispiel von Stuxnet ein Angriff mittels infiziertem USB-Stick möglich. Sogar nicht IT gestützte Systeme können mittels Sabotage angegriffen und ein Ausfall erzwungen werden. Somit kann die Schlussfolgerung gezogen werden, dass es wichtig ist eine kritische Infrastruktur mittels IT-Sicherheit bestmöglich abzusichern, um ein Angriffsrisiko zu minimieren. Dazu sollte auch auf Resilienz Wert gelegt werden, denn falls ein Angriff einmal erfolgreich war, muss der Schaden schnell eingedämmt werden.

4 ABSICHERUNG NACH STAND DER TECHNIK

"Das Sprichwort stimmt, dass Sicherheitssysteme immer gewinnen müssen, der Angreifer hingegen muss nur einmal."

– Kevin Mitnick

Basierend auf dem Sprichwort von Kevin Mitnick, ist es schwer möglich ein System komplett abzusichern. Hacker mit genügend Zeit und Ressourcen finden immer einen Weg, in ein System einzudringen. Daher sollten kritische Infrastrukturen bestmöglich abgesichert werden, um es den Hackern möglichst schwer zu machen. Dazu sollten die Sicherheitsstandards der IT möglichst hoch und immer am neuesten Stand sein.

Die in dieser Masterarbeit aufgezählten Maßnahmen, sind nur eine Möglichkeit kritische Infrastrukturen abzusichern. In der Praxis sind mehr Technische und Organisatorische Maßnahmen (TOM) erforderlich und eine individuelle Anpassung an die jeweiligen Systeme vorzunehmen.

4.1 Stand der Technik

Wie bereits erwähnt schreibt die NIS-Richtlinie für kritische Infrastrukturen Schutzmaßnahmen nach Stand der Technik vor. Dabei handelt es sich um einen Entwicklungsstand, der technologisch abgrenzbar ist. Der Stand der Technik wird wie in Abbildung 3 abgegrenzt und befindet sich über den allgemein anerkannten Regeln der Technik und unter dem Stand der Wissenschaft und Forschung (Bartels, 2017).

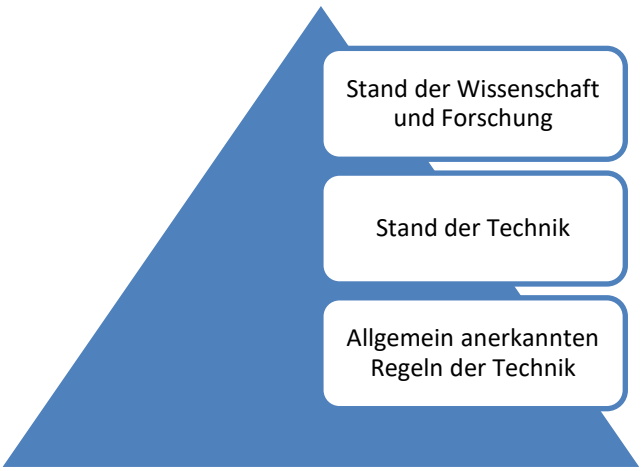

Abbildung 3: Abgrenzung Stand der Technik

Quelle: https://www.aquaetgas.ch/media/4672/buerki_fig1.jpg?width=800 verändert

Die allgemein anerkannten Regeln der Technik sind die Mindeststandards die technisch einzuhalten sind und zweckdienlich sind. Die allgemeine Anerkennung ist für diesen Stand sehr hoch, daher wird es in der Praxis häufig eingesetzt und die Techniken sind ausgereift. In der Abbildung 3 ist das die unterste Ebene der Pyramide. Um den Stand der Technik handelt es sich, wenn zu einem bestimmten Zeitpunkt die technologische Möglichkeit gegeben ist und die Erkenntnisse auf Erfahrung, Wissenschaft und Technik basieren. Der Stand der Wissenschaft und Forschung hat nur wenig allgemeine Anerkennung und ist in der Praxis noch nicht bewährt. Dieser Stand befindet sich noch in der Entwicklung (Bürki, 2019).

4.2 Schutzziele der IT

Informationen zählen heute zu wertvollen Vermögenswerten und sollten daher geschützt werden. Durch die Schutzziele ist es möglich festzustellen, wie gut ein Unternehmen die IT-Systeme abgesichert hat. Die drei wichtigsten Schutzziele sind: Vertraulichkeit (**C**onfidentiality), Integrität (**I**ntegrity) und Verfügbarkeit (**A**vailability). Sie werden auch als CIA Schutzziele bezeichnet. (Siriu, 2019).

Vertraulichkeit

Mit Hilfe der Vertraulichkeit wird sichergestellt, dass nur Personen, die befugt sind Daten bearbeiten und einsehen dürfen. Dafür muss festgelegt werden welche Personen Zugriff auf welche Daten erhalten. Ein Beispiel hierfür sind E-Mails. Diese beinhalten vertrauliche Informationen und sollten nur von berechtigten Personen eingesehen werden können. Sichergestellt werden kann das durch Verschlüsselung der E-Mail. Eine Person, die den Schlüssel nicht hat, wäre der Zugriff auf die Informationen nicht möglich (Siriu, 2019).

Integrität

Die Integrität sollte gewährleisten, dass es nicht möglich ist Daten unerkannt zu verändern. Es muss möglich sein, Änderungen von Daten nachzuvollziehen. Unterschieden wird zwischen einer starken Integrität und einer schwachen Integrität. Bei der starken Integrität lässt das System keine Möglichkeit der unbemerkten oder unerkannten Datenänderungen zu. Bei einer schwachen Integrität lässt das System eine Änderung zu, diese können jedoch nicht unerkannt erfolgen. Da in den meisten Unternehmen eine Veränderung der Daten nicht verhinderbar ist, sollte eine Datenveränderung nicht unerkannt erfolgen können. Für Unternehmen kann eine Änderung der Daten wie Abändern, Löschen oder Einfügen zu einem verfälschten Produkt führen und dies kann existenzbedrohend werden (Siriu, 2019).

Verfügbarkeit

Unter der Verfügbarkeit versteht man, dass ein System jederzeit für die berechtigten Personen verfügbar ist. Ziel der Verfügbarkeit ist es, die notwendigen Systeme eines Unternehmens vor einem Systemausfall oder einem Angriff zu schützen. Ein Beispiel dafür ist ein Stromausfall, der für Ausfälle von Systemen sorgen kann und in weiterer Folge die Abläufe beeinträchtigt. Die Auswirkung von Schäden bei einem Ausfall der unterschiedlichen Systeme, ist in jedem Unternehmen unterschiedlich und muss individuell abgewogen werden (Siriu, 2019).

4.3 Technische Maßnahmen

Um den Technologiestand einer technischen Maßnahme zu bestimmen, gibt es vom Bundesverband IT-Sicherheit e.V. (TeleTrusT) eine Handreichung zum Stand der Technik die 2020 erschienen ist. In diesem Dokument wird eine Methode zur Bestimmung des Technologiestandes vorgestellt. Diese Methode beinhaltet einfache Leitfragen, um die Dimensionen „Grad der Anerkennung“ sowie den „Grad der Bewährung in der Praxis“ zu bestimmen. Es stehen bei jeder Frage drei Antwortmöglichkeiten zum Ankreuzen und zusätzlich muss die Antwort begründet werden. Erst nach Beantwortung aller Fragen wird der Mittelwert gebildet und es kann der Technologiestand bestimmt werden, indem die Werte in ein Diagramm eingetragen werden (Bartels et al., 2020, S. 12–13).

Nachfolgend werden die technischen Maßnahmen die den Qualitätssicherungsprozess der Handreichung des Bundesverband IT-Sicherheit e.V. (TeleTrusT) entsprechen beschrieben. Diese Maßnahmen wurden von mehreren Experten ausgearbeitet und dienen als Handlungsempfehlung.

4.3.1 Bewertung der Passwortstärke

Für die User ist es wichtig sichere Passwörter zu verwenden, damit diese nicht durch erraten oder mit der Brute-Force-Methode geknackt werden können. Bei der Brute-Force-Methode werden alle möglichen Kombinationen nacheinander durchprobiert, bis das Passwort gefunden wird. Diese Methode steht für rohe Gewalt und führt nur bei kurzen unsicheren Passwörtern schnell zum Ziel. Bei komplexen Passwörtern dauert diese Methode zu lange. Die Computer werden jedoch immer leistungsfähiger und können in kürzerer Zeit immer mehr Kombinationen durchprobieren. Um ein sicheres Passwort erstellen zu können, spielt der Begriff Entropie eine wichtige Rolle.

Die Entropie ist ein Maß für die Unordnung oder Zufälligkeit. Bei einem Passwort bedeutet dies, je zufälliger es ist, desto höher ist die Entropie. Einfach gesagt, wird bei der Entropie jedem ASCII Zeichen in einem Passwort ein Wert zugewiesen. Der Wert hängt von den möglichen Zeichen ab, welche im Passwort enthalten sein können. Dieser Wert wird in Bit angegeben und beschreibt dann die Stärke des gewählten Passwortes. Ein Beispiel ist, wenn wir eine Münze werfen, kommt mit gleicher Wahrscheinlichkeit Kopf oder Zahl, dies entspricht einer Entropie von einem Bit. Somit sollte ein Passwort eine möglichst hohe Entropie aufweisen (Schneier, 2015, S. 104).

Passwörter sollten nicht im Klartext gespeichert werden, sondern mit einer Hashing-Funktion. Es sollte eine möglichst langsame kryptografische Hashfunktion sein wie sha3. Damit wird sichergestellt, dass die Passwörter vor unbefugten Zugriff geschützt sind und verhindert, dass bei Diebstahl der Datenbank, die Passwörter im Klartext wiederhergestellt werden können. Dadurch wird jedoch auch eine Bewertung der Passwortstärke erschwert. Ein Passwort-Sicherheit-Assessment simuliert einen Angriff, indem es Schwachstellen wie vorhersehbare oder schwache Passwörter der BenutzerInnen erkennt. Durch diese Maßnahme wird verhindert, dass trotz strikter Regeln ein schwaches Passwort gewählt wird (Bartels et al., 2020).

4.3.2 Durchsetzung starker Passwörter

Starke Passwörter sind lang und komplex. Mit komplex ist gemeint, dass es Buchstaben, Sonderzeichen und Zahlen beinhaltet, die in zufälliger Reihenfolge auftreten. Es sollten keine Wörter sein, die in einem Wörterbuch zu finden sind, da Hacker häufig Wörterbücher verwenden, um Passwörter zu knacken. Daher sollten Passwörter zufällig generiert werden. Laut NIST special publication 800-63B sollten zufällig erstellte Passwörter eine Mindestlänge von 8 Zeichen haben (Grassi et al., 2017).

Sehr oft findet man eine Empfehlung, dass ein Passwort 10 Zeichen lang sein sollte. Bestehen sollte das Passwort aus Sonderzeichen, Zahlen, große und kleine Buchstaben. Dann gäbe es für eine Brut-Force-Methode im schlechtesten Fall 72 hoch 10 Möglichkeiten zum Probieren. Die Autoren Dirscherl und Arne empfehlen jedoch ein Passwort mit 16 Zeichen zu verwenden, um auch gegen Angriffe wie Wörterbuchattacken gerüstet zu sein (Dirscherl & Arne, 2020).

Es sollte außerdem darauf geachtet werden, dass niemand mit Administratorrechten im Tagesgeschäft arbeitet, da es meistens nicht notwendig ist. Bei einem Angriff auf den Account, hätte der Hacker sofort Administratorrechte. Mit Administratorrechte hätte es ein Hacker leichter sich weitere Berechtigungen wie Domänenadministratorrechte zu erschleichen. Daher sollten BenutzerInnen immer mit so wenig Berechtigungen wie möglich arbeiten und nur bei Bedarf weitere Rechte erhalten. Das könnte über einen zweiten Account einfach gelöst werden. Ein Standard Account, wird zum Arbeiten benutzt und ein zweiter Account mit Administratorrechten, um sich bei Bedarf mit den erhöhten Rechten zu authentifizieren. Dabei sollte darauf geachtet werden, wo die Berechtigungen zwischengespeichert werden. Es kann notwendig sein sich als Administrator zu authentifizieren, um beispielsweise Einstellungen zu verändern, Programme zu installieren oder sonstige Tätigkeiten durchzuführen, die nur mit Administrator Berechtigungen möglich sind. Hat man sich als Administrator authentifiziert und benötigt die erhöhten Rechte nicht mehr, sollte danach der Computer neu gestartet werden, da sonst der Hash vom Passwort zwischengespeichert ist und ausgelesen werden kann. Durch einen einfachen Neustart wird das verhindert, da der RAM (Random Access Memory) gelehrt wird (Metcalf, 2014).

4.3.3 Multi-Faktor-Authentifizierung

Wenn möglich sollte eine MFA (Multi-Faktor Authentifizierung) verwendet werden. Dabei wird zusätzlich zu einem sicheren Passwort ein weiterer Faktor zur Authentifizierung verwendet. Durch eine MFA wird die Sicherheit bei der Authentifizierung erhöht und der Identitätsdiebstahl erschwert. Bei der MFA kommen zwei oder mehrere voneinander unabhängige Faktoren zur Berechtigungsüberprüfung zum Einsatz. Beispielsweise könnten es folgende Faktoren sein:

- geheimes Wissen wie ein Passwort, PIN, Antworten auf Sicherheitsfragen
- biometrische Merkmale wie beispielsweise Fingerabdruck, Iris-Scan, Stimmerkennung
- der Besitz eines Gegenstandes wie eine Magnetkarte oder ein Token

Wichtig ist, dass die Faktoren voneinander unabhängig sind. MFA ist vom Online Banking bekannt, denn meistens erfolgt die Anmeldung mit den Zugangsdaten und einem Passwort und je nach Bank und vereinbartem zusätzlichen Faktor häufig mit SMS, Card TAN, TAN Generator, App und TAN Liste. Das Beheben von Bargeld bei einem Bankomaten erfordert auch zwei Faktoren, die Bankomatkarte und den PIN. Vermehrt wird bei der Authentifizierung auch das Smartphone als zweiter Faktor eingesetzt. Das kann mittels SMS, die auf das Smartphone gesendet wird und einen Code enthält, der für eine gewisse Zeit gültig ist, erfolgen. Eine andere Variante wäre eine App die einen OTP (One-time password) Token generiert, der üblicherweise für 30 Sekunden gültig ist, dies funktioniert auch offline. Es gibt auch noch eine Variante wo das Smartphone eine Internetverbindung benötigt, wie die Microsoft Authenticator App. Da wird bei einem Anmeldeversuch eine Benachrichtigung an die App gesendet und der User bestätigt diese am Smartphone (Schmitz, 2017a).

Der Vorteil der MFA ist, die erhöhte Sicherheit des Systems. Ebenso erschwert es den Identitätsdiebstahl durch einen Passwortklau. Für einen Hacker ist durch den MFA ein Passwortklau nicht ausreichend, um sich am System anzumelden. Ein Angriff, der auf einen Passwortklau abzielt, kommt häufig zum Einsatz da die meisten Systeme nur mit Benutzername und Passwort gesichert sind. Daher wird auch vom BSI der Einsatz vom MFA empfohlen. Die Nachteile sind jedoch, dass eine Anmeldung aufwendiger ist und mehr Zeit erfordert. Sollte ein Faktor verloren gehen, ist eine Anmeldung am System nicht mehr möglich und der Faktor ist zu ersetzen. Das ist aufwendiger als ein Zurücksetzen des Passworts (Schmitz, 2017a).

4.3.4 Verschlüsselung

Verschlüsselung bedeutet das Informationen so verändert werden, dass sie ohne Schlüssel nicht lesbar sind. Vergleichbar ist das mit einem Text, der durch Chiffrierung unlesbar wird und nur wer den Schlüssel kennt, kann mit Dechiffrierung den Text wieder lesbar machen. Bei der Verschlüsselung unterscheidet man zwischen symmetrischen und asymmetrischen Verfahren. Häufig werden hybride Verfahren eingesetzt die eine Kombination aus symmetrischen und asymmetrischen Verfahren bilden (Lauterschlag, 2017).

Symmetrische Verfahren verwenden zum Verschlüsseln und Entschlüsseln den gleichen Schlüssel, daher ist dieses Verfahren vom Berechnungsaufwand geringer als ein asymmetrisches Verfahren. Dies wird zum Verschlüsseln von Daten, Laufwerken oder Container eingesetzt. Vorsicht ist bei diesem Verfahren beim Austausch des Schlüssels geboten und auch bei der Verwahrung des Schlüssels. Beispielsweise zählen AES (Advanced Encryption Standard), Twofish und Serpent zu diesem Verfahren (Lauterschlag, 2017).

Asymmetrische Verfahren verwenden zum Verschlüsseln einen öffentlichen Schlüssel und zum Entschlüsseln einen privaten Schlüssel. Eingesetzt wird dieses Verfahren für Nachrichten oder den Schlüsselaustausch, da es sehr rechenintensiv ist. Der Vorteil vom asymmetrischen Verfahren ist jedoch, dass der öffentliche Schlüssel einfach mitgesendet werden kann, da dieser nur zum Verschlüsseln dient. Ein bekanntes Beispiel für dieses Verfahren ist PGP (Pretty Good Privacy) (Lauterschlag, 2017).

Festplattenverschlüsselung

Eine Festplattenverschlüsselung schützt die Daten bei Diebstahl oder Verlust von Geräten. Immer mehr Geräte haben einen TPM (Trusted Platform Module) Chip verbaut. Dieser Chip gibt die Schlüssel frei, wenn sich das Gerät in einem sogenannten „sicheren Zustand“ befindet. Die Schlüssel werden dann beispielsweise vom Bitlocker zum Entschlüsseln der Festplatte benötigt. Werden Manipulationen an der Hardware oder Software gemacht, wird das vom TPM erkannt (Pössneck, 2008).

Objektverschlüsselung

Die Objektverschlüsselung beinhaltet die Verschlüsselung von beispielsweise Dateien, Container und Ordner. Viele Verschlüsselungsprogramme arbeiten transparent, somit können die BenutzerInnen arbeiten als wären die Objekte unverschlüsselt. Diese Verschlüsselung bietet Schutz, um Daten sicher zu transportieren, so dass ein Verlust oder Diebstahl keinen Missbrauch oder unbefugten Zugriff der Daten zur Folge hat. Im schlimmsten Fall könnte ein „Nicht-Verschlüsseln“ der Daten zum Missbrauch persönlicher Daten oder sogar die Existenzgrundlage gefährden. Ein weiteres Problem wäre, wenn durch „Nicht-Verschlüsseln“ die Datenschutzrichtlinien nicht eingehalten werden und es zu einem Diebstahl kommt, dann müsste mit Strafen gerechnet werden (Bartels et al., 2020, S. 26–27).

Verschlüsselung von E-Mails

E-Mails werden standardmäßig unverschlüsselt übertragen, daher sollten keine vertraulichen Informationen versendet werden. Eine E-Mail kann wie eine Postkarte gesehen werden, sie kann von unbefugten Personen abgefangen und gelesen werden. Durch den Einsatz einer Verschlüsselung kann verhindert werden, dass der Inhalt der E-Mail mitgelesen werden kann. Für die Verschlüsselung von E-Mails, sind die zwei bekanntesten Standards, OpenPGP und S/MIME. Zur Transportverschlüsselung sollte TLS (Transport Layer Security) in aktueller Version eingesetzt werden. Diese Verschlüsselung ist jedoch nicht so stark wie eine OpenPGP Verschlüsselung, daher wird im Kapitel „Umsetzung der Schutzmaßnahmen“ diese Variante verwendet (Rentrop & Will, 2020).

4.3.5 Sicherung des elektronischen Datenverkehrs mit PKI

Damit die Identität des Absenders sowie die Echtheit der Daten geprüft werden können, können Zertifikate oder Signaturen eingesetzt werden. Zertifikate werden verwendet, um Identitäten zu prüfen, Signaturen hingegen werden zum Prüfen von Dokumenten und Nachrichten eingesetzt. Voraussetzung dafür ist eine PKI (Public Key Infrastructure), um Zertifikate zu erzeugen, managen und zu prüfen. Unternehmen können zur Umsetzung eine eigene PKI einrichten oder eine externe PKI nutzen (Bartels et al., 2020).

Mit Hilfe der PKI kann ein verschlüsselter Kommunikationskanal eingerichtet werden, mit diesem sicher kommuniziert werden kann. Die höchste Instanz einer PKI ist die Root CA (Certificate Authority), diese autorisiert darunterliegende CAs und diese können weitere Zertifikate ausstellen. Kommt es bei einem Angriff auf eine darunterliegende CA, kann die

Identität anhand der Root CA weiterhin verifiziert werden. Wichtig für die Sicherheit ist, dass die Kontrolle der Root CA gesichert ist. Zudem fordert auch die NIS-Richtlinie den Einsatz einer PKI (Andreas, 2020).

4.3.6 Einsatz von VPN

Der Anteil an Homeoffice Nutzern nimmt stetig zu. In einer Umfrage des Bayerischen Forschungsinstituts für Digitale Transformation wurde festgestellt, dass in Deutschland der Anteil der MitarbeiterInnen, die von zu Hause aus arbeiten seit Beginn der Coronakrise von 35% auf 43% gestiegen ist, was einen Anstieg von 8% ergibt. Das zwingt die Betriebe die Digitalisierung voranzutreiben und wird einen Einfluss auf die Arbeitswelt der Zukunft haben (Beiersmann, 2020). Für Betriebe wird es daher immer wichtiger, eine sichere Verbindung zwischen Homeoffice und dem Arbeitsplatz oder verschiedenen Firmenstandorten aufzubauen.

Eine Möglichkeit eine sichere Verbindung zu realisieren, ist mit Hilfe einer VPN Verbindung gegeben. Dabei wird ein **V**irtuelles **P**rivates **N**etzwerk über das Internet aufgebaut. Diese VPN Verbindung sollte dann unbedingt mit einer Verschlüsselung abgesichert werden, damit die Verbindung von anderen nicht mitgelesen werden kann. Eine VPN Verbindung für die Homeoffice User, ist eine Verbindung vom Computer des Users, zum Firmennetzwerk. Wenn eine VPN Verbindung aufgebaut ist, kann der User so arbeiten als würde er direkt mit dem Netzwerk der Firma verbunden sein. Notwendig ist dafür ein VPN Server und häufig eine Software, um sich mit dem VPN Server zu verbinden. Die meisten Firewalls haben bereits einen VPN Server vorinstalliert, dieser muss jedoch für seinen Einsatzzweck speziell konfiguriert werden. Eine VPN Verbindung kann man sich daher wie einen Tunnel in einer Firewall vorstellen, der den Zugriff auf das dahinter liegende Netzwerk ermöglicht. Abgesichert wird die VPN Verbindung mit Hilfe von Anmeldeverfahren zur Authentifizierung und strikten Regeln die festlegen was zugelassen oder geblockt wird (Schneier, 2015, S. 193–194).

4.3.7 Verschlüsselung auf Layer 2

Eine VPN Verbindung kann auf unterschiedlichen Schichten (Layer) nach dem OSI Modell abgesichert werden. Dieses Modell besteht aus sieben Schichten. Mit Layer 2 ist die zweite Schicht des OSI Modells gemeint, sie nennt sich Sicherungsschicht. Eine Verschlüsselung wird auf Ethernet-Frames und nicht auf IP-Pakete angewendet, da IP-Pakete in die dritte Schicht fallen. Diese Verschlüsselung ist schneller, da die IP-Header nicht verarbeitet werden, entsteht kein Verschlüsselungs-Overhead und somit kann die ganze Leitungsbandbreite genützt werden. Voraussetzung ist ein Netzwerk, welches auf Ethernet-Frame basiert. Die Einsatzgebiete sind, WAN-Backbone Leitungen, Anbindungen an Rechenzentren, Leitungen des Backbones die über fremde Grundstücke verlegt sind und Anbindungen zu vertrauenswürdigen Cloud Providern. Der Vorteil dieser Verschlüsselung ist, dass sie für höhere Schichten im OSI Modell transparent ist und keine Auswirkung auf die Geschwindigkeit vom Netzwerk hat (Bartels et al., 2020).

4.3.8 Routersicherheit / Firewall

Eine Firewall wird eingesetzt, um eingehenden und ausgehenden Datenverkehr zu kontrollieren. Sie befindet sich meistens zwischen dem Internet und dem lokalen Netzwerk und filtert unerwünschten Datenverkehr heraus. Leider setzen laut Anderson (2010) manche Firmen teure Firewalls ein, anstatt Firewalls die den geforderten Schutz bieten. Firewalls kontrollieren die Pakete im Netzwerk und wenden definierte Regeln auf diese Pakete an. In den Regeln ist definiert welche Pakete gedroppt, rejected oder allowed werden. Beim droppen eines Pakets, wird keine Rückmeldung an den Absender übermittelt. Der Absender erhält dann ein Timeout. Wenn ein Paket rejected wird, wird das Paket verworfen und es wird eine Nachricht (ICMP Typ3: Ziel nicht erreichbar oder TCP Reset) an den Absender übermittelt. Wenn ein Paket allowed wird, wird das Paket durchgelassen. Bei den meisten Firewalls gibt es eine Log Funktion die eingeschaltet werden sollte, damit unter anderem ein Debuggen leichter möglich ist (Anderson, 2010, S. 654).

Die Hauptaufgabe von Firewalls ist es, Hacker draußen zu halten und autorisierte BenutzerInnen in das LAN (Local Area Network) zu lassen. Wenn ein Hacker im LAN ist, ist eine Firewall nutzlos. Dafür sollten interne Firewalls eingerichtet werden. Mit Hilfe einer internen Firewall können Netzwerke segmentiert werden. Dabei werden verschiedene Netzwerke eingerichtet und voneinander getrennt. Zwischen den Netzwerken kann der Datenverkehr komplett unterbunden werden oder es wird nur ein definierter Datenverkehr zwischen den Netzwerken zugelassen. Um eine Firewall als Hacker zu überwinden, gibt es laut dem Buch Secrets and Lies (Schneier, 2015) drei grundlegende Möglichkeiten:

1. Eine Möglichkeit ist es, die Firewall zu umgehen. Das ist möglich da große Netzwerke viele Verbindungen haben wie beispielsweise große Kopierer mit Internetverbindung oder es besteht eine Verbindung zu Lieferanten oder Kunden. Diese Verbindungen sind meistens schlechter abgesichert. Oft schließen MitarbeiterInnen ein Modem an ihren Computer an und öffnen damit eine Hintertür, um von zu Hause aus arbeiten zu können. Diese Hintertüren können dann auch von Hackern ausgenutzt werden.
2. Ein komplizierter Angriff wäre, etwas durch die Firewall zu schleusen. Dafür muss der Firewall eine vertrauenswürdige Verbindung vorgetäuscht werden. Hierzu muss ein Code, den die Firewall durchlässt ins Netzwerk eingeschleust werden. Damit wird dann eine Verbindung zum Hacker der sich außerhalb der Firewall befindet und einem Computer, der innerhalb der Firewall ist, aufgebaut. Dadurch kann der Hacker in das Netzwerk einsteigen. Wie schwer oder unmöglich dieser Angriff ist, hängt stark von der Konfiguration der Firewall ab.
3. Die dritte Möglichkeit ist die Firewall zu übernehmen und anschließend anders zu konfigurieren. Das ist möglich, wenn ein verwundbarer Code auf der Firewall ausgeführt wird oder das Betriebssystem, auf dem die Firewall läuft, Sicherheitslücken aufweist. Dieser Angriff ist stark von der eingesetzten Firewall abhängig.

Auf dem Markt sind weit über 100 verschieden Firewall Produkte verfügbar und es werden laufend mehr. Die Produkte werden laufend weiterentwickelt und verbessert, um die Sicherheit

zu erhöhen. Es ist schwierig diese Produkte zu vergleichen, daher vergeben Firmen sogenannte „Siegel“ für getestete und für gut befundene Produkte. Die meisten Hacker finden das jedoch lächerlich, da diese Tests nur grundlegende Angriffe abdecken. Eine gute Firewall sollte laut Schneier ordentlich konfiguriert sein und alle Sicherheitsupdates und Patches installiert haben (Schneier, 2015, S. 188–193).

4.3.9 Netzwerküberwachung mittels Intrusion Detection System

Ein IDS (Intrusion Detection System) überwacht das Netzwerk und versucht außergewöhnliches Verhalten, was auf einen Angriff hindeutet, zu erkennen. Wenn durch IDS ein Angriff erkannt wird, wird dieser gemeldet. Ein Eingreifen, um den Angriff zu verhindern, wird nicht vorgenommen. Die Probleme bei einem IDS sind die Falschmeldungen und die Verzögerung bei der Alarmierung. Schlägt das System zu früh Alarm, gibt es zu viele falsche Alarmierungen. Aufgrund dessen wird der Schwellwert oft höher angesetzt, dadurch kommt es zu einer verspäteten Erkennung bei langsamen Angriffen (Schneier, 2015, S. 194–197).

Ein IPS (Intrusion Protection System) hingegen setzt aktiv Gegenmaßnahmen, um den Angriff zu verhindern und schützt dadurch das Netzwerk. Bei einem erkannten Angriff setzt das IPS Regeln in der Firewall, die den Zugriff blockieren. Ein IPS greift durch Regeln, Machine Learning oder anhand einer erkannten Signatur selbständig ein und kann einen Angriff durch blockieren des Datenverkehrs verhindern (Schmitz, 2018).

Bei den IDS wird zwischen HIDS (Host Based Intrusion Detection Systems) und NIDS (Network Intrusion Detection Systems) unterschieden. Ein HIDS überwacht einzelne Computer, indem es aufzeichnet welche Anwendungen gestartet wurden, auf welche Dateien zugegriffen wurde und welche logs aufgetreten sind. Bei einem NIDS wird das ganze Netzwerk überwacht, dies geschieht durch Mitlesen und Analysieren des Netzwerkverkehrs. HIDS und NIDS sammeln Informationen vom Netzwerk und Computer, um die Informationen mit den Mustern von bekannten Angriffen zu vergleichen. Es werden auch Information zum normalen Verhalten der Computer und Netzwerke gespeichert (Saxena, 2020).

4.3.10 Server-Härtung

Auf den Servern laufen oft wichtige Dienste und es werden sensible Daten gespeichert, daher sollten Server geschützt werden. Unter den Begriff Härten versteht man die Absicherung des Betriebssystems. Standardmäßig sind Betriebssysteme so konfiguriert, dass sie eine hohe Kompatibilität aufweisen, was meist zu Lasten der Sicherheit geht. Beispielsweise sind veraltete Protokolle aktiv, die bereits Sicherheitslücken aufweisen. Nicht benötigte Dienste und Funktionen sollten daher deaktiviert werden, da diese für Angreifer als Einfallstor dienen können. Bei der Härtung werden daher alle nicht benötigten Funktionen und Schnittstellen deaktiviert und die Einstellungen so konfiguriert, dass sie möglichst sicher sind. Diese Maßnahmen sollten von jedem Unternehmen umgesetzt werden, nicht nur von kritischen Infrastrukturen. Folgende Maßnahmen sollten, laut der Handreichung zum Stand der Technik (Bartels et al., 2020), umgesetzt werden:

- Deaktivierung von nicht benötigten Komponenten
- Aktivierung von hardwarenaher Schutzfunktionen
- Sicherheitseinstellungen
- Minimale Vergabe von Berechtigungen
- Userverwaltung und Kennwörter
- Netzwerkkomponenten einschränken

Diese Maßnahmen sollten auf neue Server, unmittelbar nach der Installation, angewandt werden, da ein nachträgliches Härten zu Problemen führen kann. Wird ein Server nachträglich gehärtet, sollte ein vollständiges Backup erstellt werden und erst danach die Härtung durgeführt werden. Anschließend müssen alle Funktionen sorgfältig getestet werden (Bartels et al., 2020).

4.3.11 Endpoint Detection und Response

Ein Endpoint Detection und Response System zielt darauf ab, Schutz vor neuen Angriffen zu bieten. Da die Hacker immer neue Techniken entwickeln und oft auch mehr investieren, um einen Angriff durchzuführen, genügen Prüfungen auf Signaturen, Einschränkungen der Zugriffe und Regeln nicht mehr. Wenn Angriffe in mehreren Stufen und über lange Zeit erfolgen, sind diese nur schwer zu erkennen. Bei solchen Angriffen stürzen keine Rechner ab und keine Schwellwerte werden überschritten. Ein Endpoint Detection und Response System fasst Aktivitäten und Ereignisse von den Endgeräten zusammen und speichert diese auf eine zentrale Datenbank. Anhand weiterer Datenbanken, welche Informationen zu Sicherheitslücken und Cybergefahren beinhalten, wird dann verglichen, ob ein Angriff stattgefunden hat. Wenn ein Angriff erkannt wird, greift das System schnell und angemessen ein, damit das Ausmaß des Angriffs sichtbar wird (Marwan, 2018).

4.3.12 Erkennung von Angriffen und Auswertung

Um Angriffe zu erkennen wird häufig ein SIEM (Security Information and Event Management) eingesetzt. Mit Hilfe eines SIEM ist es möglich Ereignisse in den IT-Systemen zu erkennen. Dazu werden Daten von verschiedenen Stellen gesammelt und anschließend ausgewertet. Das Sammeln der Ereignisse erfolgt meist mit Softwareagents, die auf den Geräten wie Server oder Firewall installiert werden. Die Softwareagents senden die Daten an eine zentrale Managementkonsole, wo die Daten ausgewertet werden und so abweichende Muster erkannt werden. Weicht ein Muster ab, kann das SIEM warnen und Maßnahmen veranlassen. Das SIEM kann mittels Regeln oder anhand eines Korrelationsmodells konfiguriert werden (Rouse, 2020).

Ein Beispiel wäre, wenn 25 Anmeldeversuche von einem Account in 25 Minuten gemacht werden und alle fehlschlagen, dann ist davon auszugehen, dass das Passwort vergessen wurde. Werden hingegen 130 Anmeldeversuche von einem Account in 5 Minuten gemacht, könnte dies ein Brute-Force-Angriff sein. Wenn so ein Angriff erkannt wird, können sofort die

definierten Gegenmaßnahmen getroffen werden. Ein Eingriff kann dadurch automatisiert abgewehrt werden. Damit das möglich ist, ist eine gute Konfiguration des SIEM notwendig. (Rouse, 2020).

4.4 Physische Absicherung

Angriffe können nicht nur von außen kommen, daher sollten kritische Infrastrukturen auch physische Absicherungen erhalten. Eine Möglichkeit, um das Einschleusen von Malware mit einen USB-Stick zu verhindern, wäre die Sperre der USB-Ports. Damit wäre sichergestellt, dass auch kein Mitarbeiter und keine Mitarbeiterin einen USB-Stick anschließt und dadurch Malware installiert wird. Dadurch würde dieser Angriff erfolgreich verhindert werden. USB-Ports können Hardware- oder Softwareseitig deaktiviert werden. Softwareseitig kann dies unter Windows über die Gruppenrichtlinien oder Registry erfolgen. Hardwareseitig können bei einem PC die Front USB-Ports innen abgeschlossen werden oder es gibt auch von Kensington einen USB-Port Blocker. Eine etwas unprofessionellere Variante, welche in der Praxis auch angewendet wird, ist das Zukleben der USB-Ports.

Kritische Infrastrukturen sollten über eine Zugangskontrolle verfügen, diese schützt zusätzlich davor, dass unbefugte Personen Zugang zu den IT-Systemen (Computer, Server, Router, Switches und Peripheriegeräte) erhalten. Eine Zugangskontrolle erfolgt häufig durch die physische Zutrittskontrolle und der Zugriffskontrolle, um die IT-Systeme abzusichern. Dabei müssen sich die Personen identifizieren als auch authentifizieren. Dies kann unter anderem durch Eingabe von Benutzername und Passwort, Fingerabdruck und Chipkarten erfolgen. Die Identifikation wäre die Eingabe von Benutzername und die Authentifizierung wäre das Passwort (Schmitz, 2017b).

Die Zutrittskontrolle kann beispielsweise mittels Wachdienstes, Berechtigungsausweis, Videoüberwachung und Türkontrollsystemen erfolgen. Zudem sollte der IT-Bereich über einen Einbruchschutz verfügen und Alarmanlagen gesichert sein. Im IT-Bereich kommt häufig ein Türkontrollsystem zum Einsatz, welches mit Magnetkarten, RFID (Radio Frequency Identification) Chipkarten, biometrische Verfahren oder durch ein einfaches PIN-Verfahren gesichert sind. Bei einer Absicherung nur mittels PIN-Verfahren an einer Tür wäre die Sperre von einer einzelnen Person nicht so einfach möglich, da der PIN geändert werden müsste und der neue PIN den autorisierten Personen mitgeteilt werden muss. Mit Chipkarten oder Magnetkarten ist sichergestellt, dass eine Sperrung einer Person jederzeit möglich ist und in den meisten Systemen ist nachvollziehbar wann eine Person sich Zutritt verschafft hat. Vor allem zu IT-Systemen sollten nur berechtige Personen einen Zugang erhalten, da meistens von dort der Zugriff auf die einzelnen IT-Komponenten möglich ist und daher ein Angriff besonders gefährlich wäre. Mit der Zugriffskontrolle wird gesteuert welcher BenutzerIn welche Berechtigung erhält. Dabei werden für BenutzerInnen oder Benutzergruppen die Berechtigungen für Lesen, Schreiben oder Ausführen vergeben. Die Aktionen der BenutzerIn werden dabei protokolliert und überwacht (Schmitz, 2017b).

4.5 Defense in Depth

Der Defense in Depth Ansatz beinhaltet zur Absicherung von Cyberangriffen mehrere Schichten von Sicherheitsmaßnahmen. Ein Hacker muss bei Defense in Depth mehrere Schichten durchdringen, um ein System anzugreifen. Die Schichten kann man sich wie eine Burg vorstellen, ein Hacker müsste den Burggraben, die Burgmauern, die Verteidigungstürme und die inneren Mauern überwinden, um in die Burg zu gelangen. Die Norm IEC 62443 beschreibt Grundkonzepte für Defense in Depth, diese Norm wird häufig für kritische Infrastrukturen herangezogen. In der Normreihe IEC 62443 werden drei Basisrollen beschreiben:

1. Betreiber
2. Integrator
3. Hersteller

In der Norm IEC 62443, ist in der ersten Schicht die betreibende Firma für die Absicherung der Anlagensicherheit verantwortlich. In der zweiten Schicht kommt die Absicherung der Netzwerksicherheit, dafür ist der Integrator verantwortlich. Die dritte Schicht ist die Systemintegrität und dafür ist der Hersteller zuständig (DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE, 2020).

Defense in Depth wurde von der NSA (National Security Agency) für den Schutz der Informationssicherheit entwickelt und bietet eine gute Grundlage für die Verteidigung gegen Cyberangriffe. Abgeleitet wurde Defense in Depth von der gleichnamigen Militärstrategie. In der Militärstrategie als auch in der IT werden bei Defense in Depth mehrere Schichten von Sicherheitsmaßnahmen zur Verteidigung aufgebaut. Der Sinn von Defense in Depth ist es, einen Angriff nicht mit einer Maßnahme zu verhindern, sondern durch mehrere Maßnahmen. Wichtig dabei ist, dass die Maßnahmen hintereinander geschalten werden. Ein Beispiel wäre, wenn in einer Infrastruktur eine Firewall, Antivirus Software, Datenverschlüsselung und Zutrittskontrollen zum Einsatz kommen. Sollte einmal eine Sicherheitsmaßnahme in einer Schicht versagen, halten noch weitere Schichten einem Angriff stand. Mit Defense in Depth können unsichere Aktivitäten wie Fernzugriffe oder IoT (Internet of Things) Komponenten in einer separaten Schicht abgegrenzt werden (Tunggal, 2020).

4.6 Verteidigung gegen Social Engineering

Eine beliebte Angriffsvariante ist das Social Engineering, da diese oft am schnellsten zum Ziel führt und viele Sicherheitsmaßnahmen damit umgangen werden können. Die wirksamste Verteidigung gegen Social Engineering, bietet eine ausführliche Schulung der MitarbeiterInnen, um diese gegen Angriffe zu sensibilisieren. MitarbeiterInnen sollten dabei, über das dreiste Vorgehen der Hacker, aufgeklärt werden. Ein Beispiel für das Einschleusen eines Virus könnte sein, dass ein infizierter USB-Stick am Parkplatz der Geschäftsführung platziert wird. Danach wird gehofft, dass der USB-Stick gefunden wird und der ehrliche FinderIn den Stick zurückgeben möchte. Dafür wird der USB-Stick angeschlossen und geprüft, ob die enthaltenen

Daten Rückschlüsse auf den Besitzer geben. Doch durch das Anschließen kann es schon zu einer Infektion des Systems kommen. Im Beispiel wurde bewusst Geschäftsführung geschrieben, da diese meistens höhere Rechte haben als die meisten MitarbeiterInnen und oft nicht genug auf solche Angriffe geschult wurden. Daher ist es wichtig alle Personen im Unternehmen entsprechend zu schulen und aufzuklären (Steinmann, 2018, S. 57–58).

Eine weitere Maßnahme könnte sein, die Makros per Gruppenrichtlinie zu deaktivieren, damit die BenutzerInnen diese nicht durch einen einfachen Klick auf „Makros zulassen“ aktivieren können. Dadurch werden Angriffe mittels Office Makros verhindert. Das geht nur für Personen, die diese Funktion nicht benötigen, was meistens in einer Recruiting Abteilung der Fall ist. In dieser Abteilung kommen häufig infizierte Bewerbungsschreiben an und bei einem Bewerbungsschreiben sind keine Makros notwendig. Leider ist das eine gängige Vorgehensweise der Hacker und wurde auch im Kapitel „Angriffe der Vergangenheit“ beschrieben.

5 UMSETZUNG DER SCHUTZMAßNAHMEN

Security is a process, not a product.

– Bruce Schneier

Um kritische Infrastrukturen zu schützen, ist eine laufende Weiterentwicklung der Sicherheitsmaßnahmen erforderlich. Gerade im Bereich IT-Sicherheit gibt es nach jedem Angriff immer wieder neue Erkenntnisse, wie die Sicherheit weiter erhöht werden kann. Es sollte immer der Aufwand zum Nutzen abgewogen werden, bevor eine Maßnahme umgesetzt wird. Ein Beispiel für eine schlechte Maßnahme wäre, eine teure Firewall einzusetzen und diese falsch zu konfigurieren. Daher werden für die Absicherung die Punkte aus dem Kapitel „Technische Maßnahmen“ herangezogen und umgesetzt. Zur Auswahl der geeigneten und zulässigen Verschlüsselungsmethoden wurde die „BSI – Technische Richtlinie“ mit der Bezeichnung „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ (BSI, 2020a) herangezogen.

Bei der Ausarbeitung und Umsetzung der Maßnahmen wird großen Wert auf Open Source Software gelegt. Open Source bietet viele Vorteile wie geringere Kosten, innovative Lösungen, keine Bindung an die Lieferanten, hohe Anpassbarkeit, Zusammenarbeit in einer großen Community, weniger Fehler, hohe Qualität der Software, höhere Sicherheit und ermöglicht einfacheres auditieren. Für kritische Infrastrukturen ist der Punkt höhere Sicherheit besonders wichtig, dies wird erreicht durch die Offenlegung des Source Codes. Das ermöglicht, dass viel mehr Augen auf den Source Code achten und gefundene Fehler melden. Dadurch werden Fehler beseitigt was zu mehr Sicherheit und höherer Qualität der Software führt. Das Prinzip geht zurück auf Linus Torvalds, der auf „die Weisheit von Vielen“ bei der Entwicklung von Linux setzte. Immer mehr Unternehmen setzen daher auf Open Source Software. Beispiele von großen Unternehmen, die in den letzten Jahren neben der proprietären Software auch Open Source Software auf den Markt brachten sind: Microsoft, Google, IBM, Amazon, Intel, RedHat und SAP (Augsten, 2019).

5.1 Aufbau der Testumgebung

Um die Maßnahmen praktisch umzusetzen, wurde eine Testumgebung aufgesetzt. Verwendet wurden die aktuellsten Softwareversionen die verfügbar waren. Die Testumgebung beinhaltet einen Windows Server, Windows Clients und eine Firewall. Die Umsetzung der Maßnahmen in dieser Testumgebung ist nur eine Variante von Vielen. Die Maßnahmen sollten zusätzlich zu den normalen IT-Maßnahmen (regelmäßig Updates des Betriebssystems und der installierten Programme, Firewalls und Zugangsbeschränkungen) eingesetzt werden, um die Sicherheit weiter zu erhöhen.

Für den Windows Server wurde die Version 1809 mit dem Build 17763.1577 von Windows Server 2019 Standard auf einem PC installiert. Nach der Installation wurden alle Sicherheitsupdates installiert. Der PC wurde mit einer zweiten Netzwerkkarte ausgestattet. Als Computername wurde „SRV01“ vergeben und folgende Rollen und Features mit dem Server-Manager hinzugefügt, Active Directory-Domänendienste, Bitlocker und Hyper-V.

Als Client wurde die Testversion von Windows 10 Pro in der Version 20H2 mit dem Build 19042.630 als Virtuelle Maschine eingerichtet. Nach der Installation wurde auch wie beim Server als erstes alle Sicherheitsupdates installiert und der Client wurde anschließend zu der Domäne des Servers hinzugefügt. Die installierten Programme auf den Client sind: Thunderbird, KeepassXC, 7-Zip, VeraCrypt und WireGuard.

Als Firewall wurde OPNsense in der Version 20.7.5-amd64 verwendet. OPNsense ist eine Open Source Firewall Lösung und erhält regelmäßig Sicherheitsupdates. Es werden die wichtigsten Funktionen wie VPN, Zwei-Faktor Authentifizierung, IPS und IDS unterstützt. Hinzugefügt wurde das Plugin WireGuard, um eine VPN Verbindung einzurichten.

5.2 Bewertung der Passwortstärke

Um die Passwortstärke von Windows AD (Active Directory) User zu bewerten, gibt es für die PowerShell das Modul DSInternals. Dieses Modul bietet mehrere Funktionen, die es ermöglichen die Passwörter der User zu prüfen. Ein Befehl nennt sich Test-PasswordQuality, dieser prüft anhand einer vordefinierten Liste, ob es Duplikate gibt, User kein Passwort haben oder Passwörter vom Administrator gesetzt wurden und diese nie geändert wurden. Ein weiterer Befehl von DSInternals ist Get-AdReplAccount, dieser findet alle AD User vom angegebenen Server und der angegeben Domäne. Diese zwei Befehle können miteinander kombiniert werden um alle User aus einem AD auszuwählen und anschließend die Passwortstärke zu bewerten (Bertram, 2019).

Umgesetzt wurde die Bewertung der Passwortstärke indem auf dem Server, auf dem das AD installiert ist, das Modul DSInternals nachinstalliert wurde. Testweise wurde ein neuer AD User mit dem Namen „user2“ angelegt und das Passwort wurde auf „Passwort01“ festgelegt. Das ist kein sicheres Passwort und erfüllt dennoch die Richtlinien für starke Passwörter. Solche Sicherheitslücken sollten nicht von Hackern ausgenutzt werden können. Damit das verhindert wird, wurde mit dem PoweShell Befehl (Get-ADReplAccount -All -Server SRV1 | Test-PasswordQuality -WeakPasswordsFile „C:\Storage\SchlechtePasswoerter.txt“) ein Bericht generiert. Der daraus resultierende Bericht ist in Abbildung 4 dargestellt. Mit dem Parameter „-Server“ wurde der Name des Servers angegeben und mit „-WeakPasswordsFile“ wurde der Speicherort Textdatei angegeben, in der die schwachen Passwörter enthalten sind. Diesem Befehl können noch weitere Parameter mitgegeben werden wie beispielsweise, dass auch deaktivierte Accounts geprüft werden sollten. Wie im Bericht (Abbildung 4) zu sehen, wurde das Passwort von user2 in der Textdatei erfolgreich gefunden. Dadurch wurde ersichtlich, dass dieser User sein Passwort dringend ändern sollte.

Abbildung 4: Bericht der Passwort Qualität

Es ist wichtig solche Überprüfungen im AD regelmäßig durchzuführen und die Berichte auszuwerten. Solche Prüfungen sollten nicht nur für Windows durchgeführt werden, sondern auch für weitere Betriebssystemen. Für Linux gibt es zwei bekannte Module pam_pwquality und pam_cracklib, um die Passwortstärke zu ermitteln. Damit die Berichte aussagekräftig sind, sollten Wörterbücher benutzt werden, die auch von Hackern verwendet werden. Größere Wörterbücher erfordern jedoch eine längere Laufzeit des PowerShell Befehls, um den Bericht zu generieren.

5.3 Durchsetzung starker Passwörter

Wenn zum Verwalten Windows AD eingesetzt wird, kann mit Gruppenrichtlinien festgelegt werden, welche Richtlinien ein Kennwort erfüllen muss. Der Vorteil dabei ist, dass von einem zentralen Punkt die Richtlinien verwaltet und so starke Passwörter für alle BenutzerInnen erzwungen werden können. Die hier beschriebene Variante wäre eine gute Möglichkeit, um Angriffen entgegenzuwirken.

In der Testumgebung wurden die Kennwortrichtlinien wie in Abbildung 5 festgelegt. Das maximale Kennwortalter wurde auf 365 Tage festgelegt. Das BSI macht in der 2020er Ausgabe des BSI-Grundschutz-Kompendiums keine Empfehlungen mehr, dass Passwörter häufig geändert werden müssen. Häufiges Passwortändern führt dazu, dass schwache Passwörter verwendet werden und oft nur ein Zeichen verändert wird (Beispielsweise Kennwort1!,

Kennwort2! und Kennwort3!). Wenn jedoch der Verdacht besteht, dass es gehackt wurde oder nach einem Angriff wenn die Hacker sich nicht mehr im System befinden, sollten alle Kennwörter geändert werden (Schmidt, 2020). Die Kennwortsperrungsschwelle wurde auf drei festgelegt, somit wird nach drei falschen Eingaben der Account für 30 Minuten gesperrt. Die minimale Kennwortlänge für AD Accounts wurde auf 10 Zeichen festgelegt.

Kontorichtlinien/Kennwortrichtlinien

Richtlinie	Einstellung
Kennwort muss Komplexitätsvoraussetzungen entsprechen	Aktiviert
Kennwortchronik erzwingen\ngespeicherte Kennwörter	24 gespeicherte Kennwörter
Kennwörter mit umkehrbarer Verschlüsselung speichern	Deaktiviert
Maximales Kennwortalter	365 Tage
Minimale Kennwortlänge	10 Zeichen
Minimales Kennwortalter	1 Tage

Kontorichtlinien/Kontosperrungsrichtlinien

Richtlinie	Einstellung
Kontensperrungsschwelle	3 ungültige Anmeldeversuche
Kontosperrdauer	30 Minuten
Zurücksetzungsdauer des Kontosperrungszählers	30 Minuten

Abbildung 5: Kennwortrichtlinien für AD User

Durch Aktivieren der Richtline „Kennwort muss Komplexitätsvoraussetzungen entsprechen“, müssen die in Abbildung 6 ersichtlichen Bedingungen für das Kennwort erfüllt werden. Somit ist sichergestellt, dass das Kennwort eine bestimmte Komplexität aufweisen muss.

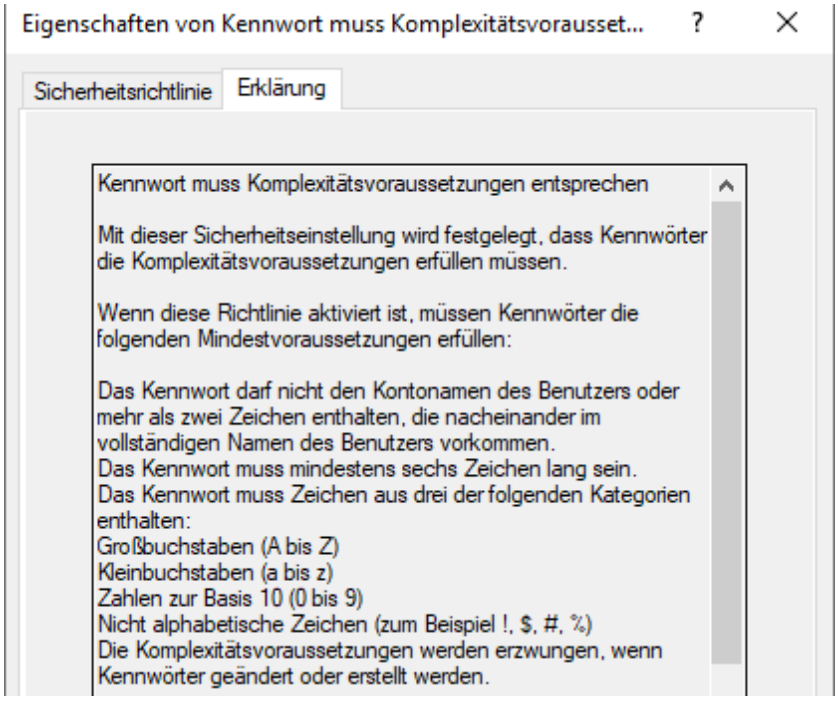

Abbildung 6: Komplexitätsvoraussetzungen für Kennwörter

Bei einem Brute-Force-Angriff müssten dadurch im schlechtesten Fall 95^{10} Kombinationen probiert werden. Die 95 Kombinationen setzen sich aus 26 Kleinbuchstaben, 26 Großbuchstaben, 10 Zahlen und 33 Sonderzeichen zusammen. Der schlechteste Fall wird jedoch nicht durch die Komplexitätsrichtlinie erzwungen, da nur drei Kategorien erfüllt sein müssen. Ein online Brute-Force-Angriff ist schwer möglich, da durch die zweite Richtlinie der Account nach drei Fehleingaben für 30 Minuten gesperrt wird.

Brute-Force wird nicht mehr so häufig angewendet, meistens kommen Wörterbücher oder Hybrid-Verfahren zum Einsatz, wo Wörter im Wörterbuch nach bestimmten Mustern abgeändert werden (Singh, 2020).

5.4 Multi-Faktor-Authentifizierung

Die Multi-Faktor-Authentifizierung dient wie oben beschreiben als zusätzliche Sicherheit und ersetzt nicht ein starkes Passwort. Wenn möglich sollte zur zusätzlichen Absicherung gegen Passwortdiebstahl ein zweiter Faktor aktiviert werden. Das ist besonders wichtig für Accounts, die vom Internet aus zugänglich sind. Technisch gibt es verschiedene Technologien für die Umsetzung eines weiteren Faktors. Beispiele für einen zusätzlichen Faktor wären HOTP (HMAC-based One-Time-Passwort), TOTP (Time-based One-Time-Passwort) und FIDO2.

HOTP und TOTP basieren beide auf dem One-Time-Passwort Verfahren. Der HOTP Algorithmus basiert auf HMAC (ist eine kryptographische Hash-Funktion) und einem Zähler. Es handelt sich um ein ereignisgesteuertes Verfahren. Bei der Generierung eines Einmalpasswortes wird der Zähler um eins erhöht. Am Server wird der Zähler bei erfolgreicher Verwendung auch erhöht. Bei diesem Verfahren kommt es vor, dass die Zähler nicht synchron sind, daher gibt es ein Validierungsfenster von mehreren Einmalpasswörtern und der Server akzeptiert in diesem Rahmen die generierten Einmalpasswörter. Wenn die Zähler außerhalb dieses Rahmens liegen werden die Eingaben abgelehnt und die Zähler müssen synchronisiert werden. Der TOTP Algorithmus basiert auch auf HMAC wie HOTP. TOTP ist zeitabhängig und tauscht bei der ersten Einrichtung einen geheimen Schlüssel und eine Zeitinformation mit dem Server aus. Die Zeitinformation wird als Unixzeit festgelegt und zählt die Sekunden von 01. Januar 1970 00:00 bis jetzt. Daraus wird ein Schlüssel generiert, der für meistens 30 Sekunden gültig ist. Da TOTP nur für eine geringe Zeitspanne gültig ist, gilt dieser Algorithmus im Gegensatz zu HOTP als sicherer (Schmitz, 2019).

FIDO2 ist der dritte und derzeit neueste Standard der FIDO Allianz (Fast Identity Online), diese Allianz verfolgt das Ziel offene und lizenzfreie Standards für sichere Authentifizierung zu entwickeln. Das Verfahren von FIDO2 funktioniert durch Generierung eines Schlüsselpaares auf einem Gerät, welches aus einem öffentlichen Schlüssel und einem privaten Schlüssel besteht. Der private Schlüssel bleibt auf dem Gerät gespeichert und ist nur dem Client bekannt. Der öffentliche Schlüssel wird beim Webdienst registriert. Die zukünftigen Anmeldungen sind nur durch eine Prüfung des privaten Schlüssels möglich. Entsperrt kann dieser Schlüssel durch PIN-Eingabe, Spracheingabe, Drücken einer Taste oder mit einem FIDO2-Token (Zwei-Faktor-Hardware) (“FIDO2: Der Neue Standard Für Den Sicheren Web-Log-in,” 2019).

Ein Beispiel wird hier für den neu angelegten Microsoft Testaccount durchgeführt. Dazu musste im Account zuerst eine Telefonnummer oder alternativ eine E-Mail hinterlegt werden. Danach konnte die zweistufige Überprüfung aktiviert werden. Wie bereits beschrieben kann hier OTP verwendet werden. Da bei diesem Verfahren keine zusätzliche Hardware benötigt wird, wurde diese Variante gewählt. Mehr Sicherheit würde FIDO2 bieten, dieses hat jedoch keine so hohe Kompatibilität und es wird eine zusätzliche Hardware benötigt. Eingerichtet wurde daher der zweite Faktor am Handy mit der App andOTP die vom Fdroid Store heruntergeladen wurde. Bei dieser App wurde die Datenbank zusätzlich mit einem Pin verschlüsselt. Der generierte Code von der andOTP App war sechs Stellen lang und nur für 30 Sekunden gültig. Beim Anmelden am Microsoft Konto war das Kennwort erforderlich und zusätzlich der sechsstellige Code, der sich alle 30 Sekunden geändert hat. Beim Einrichtungsprozess wurde am Schluss noch ein Code für die Wiederherstellung des zweiten Faktors angezeigt, dieser wurde verschlüsselt abgelegt. Dieser Code wird dann benötigt, wenn der zweite Faktor verloren geht wie beispielsweise bei Verlust des Handys.

5.5 Festplattenverschlüsselung

Um die Festplatte zu verschlüsseln, wurde die in Windows 10 Pro integrierte Funktion Bitlocker gewählt. Bitlocker nutzt das TPM und wurde vom BSI und dem Fraunhofer-Institut getestet mit dem Fazit, dass Bitlocker vertrauliche Daten gut vor physischen Angriffen bei richtiger Konfiguration schützt. Ein Mangel ist jedoch, dass Nutzer von Notebooks nicht den Energiesparmodus verwenden sollten, da dieser einen physischen Angriff ermöglichen würde (Pössneck, 2008).

Zum Verschlüsseln der Festplatte werden Administratorberechtigungen benötigt. Bitlocker nutzt das TPM, ist dieses nicht vorhanden oder nicht kompatibel erhält man eine Fehlermeldung. Durch Aktivieren der Gruppenrichtlinie „Zusätzliche Authentifizierung beim Start anfordern“ kann auch ohne TPM die Festplatte mit Bitlocker verschlüsselt werden. Der Wiederherstellungsschlüssel sollte sicher aufbewahrt werden. Dafür stehen mehrere Optionen zur Verfügung, wie das Speichern in einer Datei, auf einem USB-Stick speichern oder drucken des Wiederherstellungsschlüssels (Mierke, 2020).

Wenn die Option „in Datei speichern“ gewählt wird, sollte diese verschlüsselt in einem Passwortmanager abgelegt werden, wo nur berechtigte Personen Zugriff haben. Wird der Wiederherstellungsschlüssel ausgedruckt, sollte dieser auch sicher abgelegt werden, denn mit diesem Schlüssel kann die Festplatte entschlüsselt werden und auch ein sehr sicheres Passwort schützt dann nicht mehr. Von mir wurde die Option „in Datei speichern“ gewählt und danach wurde die Datei in einem Passwortsafe KeepassXC abgelegt, alternativ wäre auch ein VeraCrypt Container für die Ablage möglich gewesen. Als Verschlüsselungsmodus wurde der neue Verschlüsselungsmodus gewählt, da dieser eine bessere Verschlüsselung (XTS-AES) aufweist. Nach einem Neustart beginnt die Verschlüsselung und sobald diese abgeschlossen ist, erscheint im Explorer bei diesem Laufwerk ein Symbol mit einem Schloss wie in Abbildung 7

ersichtlich. Beim Starten ist ab dem Verschlüsseln zusätzlich das zuvor festgelegte Passwort zum Entschlüsseln einzugeben.

Abbildung 7: Bitlocker Festplattenverschlüsselung

Um einen Windows Server 2019 mit Bitlocker zu verschlüsseln, muss dieses Feature zuerst nachinstalliert werden. Es gibt noch weitere Möglichkeiten Festplatten sicher zu verschlüsseln wie beispielsweise die Sicherheitsfestplatte von Lenovo oder VeraCrypt. Diese Sicherheitsfestplatte hat ein Tastenfeld, welches Kennwörter von 8 bis 16 Stellen zulässt, die Festplatte mit AES-256 verschlüsselt und über behördliche Zulassungen verfügt.

5.6 Objektverschlüsselung

Zum Verschlüsseln von Objekten gibt es viele Tools, es sollte daher darauf geachtet werden welche Algorithmen diese verwenden und wie sie sich in das bestehende System integrieren. Das BSI nennt das Programm 7-Zip, da es Archive mit AES-256 verschlüsseln kann, TrueCrypt welches in Version 7.1a von Experten geprüft wurde und Gpg4Win welches auch Dateien verschlüsseln kann. TrueCrypt wird jedoch nicht mehr weiterentwickelt. Es gibt aber einen Fork, der sich VeraCrypt nennt und auch TrueCrypt Container weiterhin öffnen kann. Mit Gpg4Win können einzelne Dateien verschlüsselt und entschlüsselt werden, zudem bietet dieses Programm auch die Möglichkeit Daten zu Signieren (BSI, 2020b).

5.6.1 7-Zip

7-Zip wurde in Version 19.00 installiert. Nach der Installation integrierte sich dieses Programm in den Explorer und konnte durch einen Rechtsklick auf eine Datei oder einen Ordner aufgerufen werden. Zuerst wurde eine Textdatei angelegt, welche verschlüsselt werden sollte. Um die angelegte Datei zu verschlüsseln, wurde mit Rechtsklick auf die Datei die Option „Archivieren und versenden“ unter 7-Zip ausgewählt. Damit das erzeugte Archiv verschlüsselt wird, wurde in den Optionen ein Passwort vergeben und als Verschlüsselung wurde AES-256 gewählt. Das erstellte Archiv erhielt die Dateiendung „.7z“ und konnte nur durch Eingabe des zuvor vergebenen Passwortes geöffnet werden. Eine weitere nützliche Funktion des Programmes ist, dass es große Dateien in mehrere Teilarchive splitten kann, damit diese dann versendet werden können.

5.6.2 VeraCrypt

Das Programm VeraCrypt wurde in der Version1.24-Update7 installiert, da es der Fork von TrueCrypt ist. VeraCrypt bietet viele Möglichkeiten zu verschlüsseln wie Container und Partitionen oder Laufwerke. Um einen sicheren leeren verschlüsselten Container zu erzeugen, wurde die Option „verschlüsselte Containerdatei erstellen“ gewählt. Als Verschlüsselungsalgorithmus wurde AES gewählt, da dieser mit einer Schlüssellänge von 256 Bits laut BSI derzeit als sicher gilt. Für den Hash-Algorithmus wurde SHA-512 gewählt. VeraCrypt ermöglicht es einen weiteren Faktor in Form einer Schlüsseldatei zum Entsperren hinzuzufügen. Daher wurde eine Schlüsseldatei erzeugt, die zum Entschlüsseln des verschlüsselten Containers erforderlich ist. Damit bei der Verschlüsselung eine möglichst hohe Entropie erzeugt werden kann empfiehlt VeraCrypt zufällige Mausbewegungen durchzuführen. Damit der erstellte Container eingebunden werden kann, wurde ein Laufwerksbuchstabe vergeben, in diesem Fall wurde wie in Abbildung 8 ersichtlich, der Laufwerksbuchstabe A gewählt. Weiters ist die Eingabe des Pfades zum Container notwendig. Anschließend muss das Passwort eingegeben und die Schlüsseldatei ausgewählt werden. Wenn der Container erfolgreich eingebunden ist sieht man wie in Abbildung 8 das neue Laufwerk A im Explorer und in VeraCrypt erscheint unter dem Buchstaben A der Pfad vom Container. Der Container ist nun wie ein normales Laufwerk eingebunden und kann nun mit Daten befüllt werden.

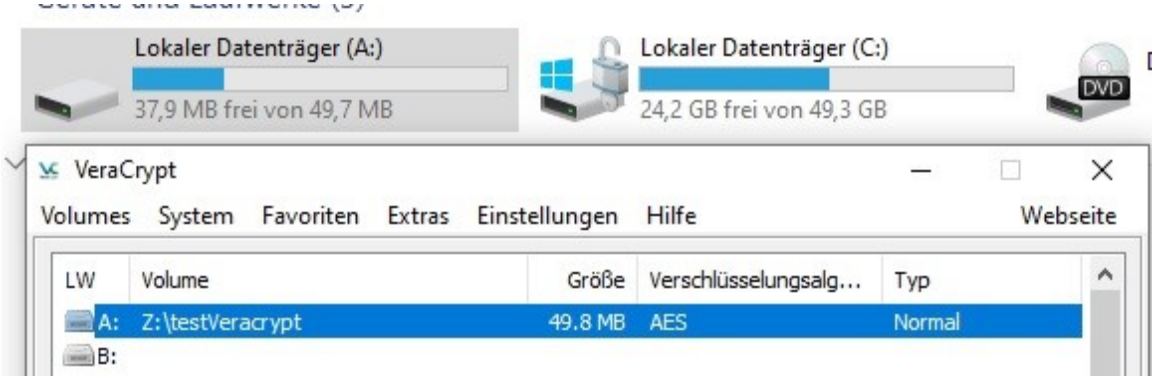

Abbildung 8: VeraCrypt Container als Laufwerk A eingebunden

Das Programm bietet auch die Option für versteckte Systeme oder versteckte Container. Diese werden innerhalb der verschlüsselten Container angelegt. Bei einem verstecken Container sind zwei verschieden Passwörter notwendig. Ein Passwort öffnet den Container mit den vertraulichen Informationen und das Zweite öffnet einen Container der Informationen enthält, die nur zur Ablenkung dienen. Wird die Person erpresst oder bedroht, gibt sie das Passwort für den Container ein, der nur zur Ablenkung dient und der Täter erhält dadurch keine vertraulichen Informationen. Die Funktion für versteckte Container, ist für sehr vertrauliche Informationen gedacht (Heise, 2020).

5.6.3 Gpg4Win

Als weitere Variante, die vom BSI empfohlen wird, wurde Gpg4Win in der Version 3.1.13 installiert. Auch dieses Programm integriert sich in den Explorer und kann einfach aufgerufen werden. Zum Verschlüsseln einer Datei oder eines Ordners wird durch Rechtsklick das Menü aufgerufen. Verschlüsselt wurde auch hier wieder eine Textdatei und als Optionen wurde „Mit Passwort verschlüsseln“ ausgewählt. Nach Vergabe des Passwortes wurde die Datei verschlüsselt und erhielt die Dateiendung „.gpg“. Diese verschlüsselte Datei konnte auch wieder durch Eingabe des vergebenen Passwortes entschlüsselt werden.

Dieses Programm bietet noch weitere Funktionen wie Entschlüsseln, Prüfen, Entschlüsseln und prüfen, Verschlüsseln, Signieren, Signieren und verschlüsseln, Zertifikate importieren, Prüfsummen erstellen und Prüfsummen überprüfen. Somit können auch Signaturen geprüft oder eigene Zertifikate erzeugt und verwaltet werden. Ein Anwendungsfall, der auch in der Testumgebung durchgeführt wurde, ist das Prüfen des Hashes anhand des Programmes KeepassXC. Dieses Programm wurde vom Internet heruntergeladen, danach wurde der Hashwert geprüft und die Signatur mit Zertifikat geprüft.

5.7 Verschlüsselung von E-Mails

Um E-Mails Ende-zu-Ende zu verschlüsseln wurde auf dem Client1 Thunderbird installiert und eine Mailadresse eingerichtet. Alternativ könnte auch Outlook verwendet werden und die Verschlüsselung S/MIME. Der Vorteil mit Thunderbird ist, dass in der aktuellen Version (78.4.3) OpenPGP Schlüssel ohne zusätzlichen Plugin erzeugt und verwaltet werden können. Es wurde ein Schlüssel erzeugt, der wie in Abbildung 9 ersichtlich drei Jahre gültig ist und mit dem Algorithmus RSA 4096 verschlüsselt wurde. Durch Austausch der öffentlichen Schlüssel können E-Mails verschlüsselt werden. Die einzelnen Schritte wurden wie von Mierke (2019) beschrieben durchgeführt, es wurde nur eine andere Schlüsselgröße gewählt. Diese wurde von 3072 auf 4096 erhöht, um mehr Sicherheit durch einen längeren Schlüssel zu erhalten. Der öffentliche Schlüssel wurde auf keinen Server hochgeladen. Zu beachten ist, dass der private Schlüssel sicher verwahrt wird. Bei einem Export sollte ein sicheres Passwort vergeben werden, da mit dem privaten Schlüssel die E-Mail wieder entschlüsselt werden kann.

Vorgeblicher Schlüsselbesitzer	testumgebungstefan@outlook.de <testumgebungstefan@outlook.de>
Typ	Schlüsselpaar (geheimer Schlüssel und öffentlicher Schlüssel)
Fingerabdruck	9DF7 068C 43C6 6A98 1804 BCD8 0B2D BB3F 61B2 977E
Erzeugt am	18.11.2020
Läuft ab am	18.11.2023

Abbildung 9: OpenPGP key Fingerabdruck

5.8 Einsatz von VPN (Layer 3)

Wie schon beschrieben sieht die Empfehlung der Handreichung von Bartels et al. (2020) eine VPN Verbindung von Layer 3 vor, dabei ist die dritte Layer Schicht im OSI-Modell gemeint. WireGuard wurde gewählt, da es die Anforderung erfüllt und auch Open Source ist. Zudem hat WireGuard eine geringe Programmgröße und hat nur etwas über 4000 Zeilen Code. Daher ist der Code übersichtlich und Fehler lassen sich leichter beheben, was die Sicherheit erhöht. Durch die geringe Größe bietet es auch eine schnellere Verbindungsgeschwindigkeit als vergleichsweise OpenVPN (Glenk, 2020).

Eine VPN Verbindung für die OPNsense Firewall ist die Open Source Software WireGuard. WireGuard wurde auf der OPNsense Firewall als Plugin nachinstalliert. Nach erfolgreicher Installation erschien das Plugin unter dem Menüpunkt VPN. Anschließend wurde WireGuard aktiviert und wie in Abbildung 10 ersichtlich konfiguriert. Der Public Key vom Client wurde auf der Firewall unter Endpoints hinterlegt. Die Firewall Regeln mussten für die WAN Schnittstelle und für die WireGuard Schnittstelle angepasst werden. Da im Netzwerk noch ein A1 Router vor der Firewall angeschlossen war, musste dort eine Portweiterleitung eingerichtet werden.

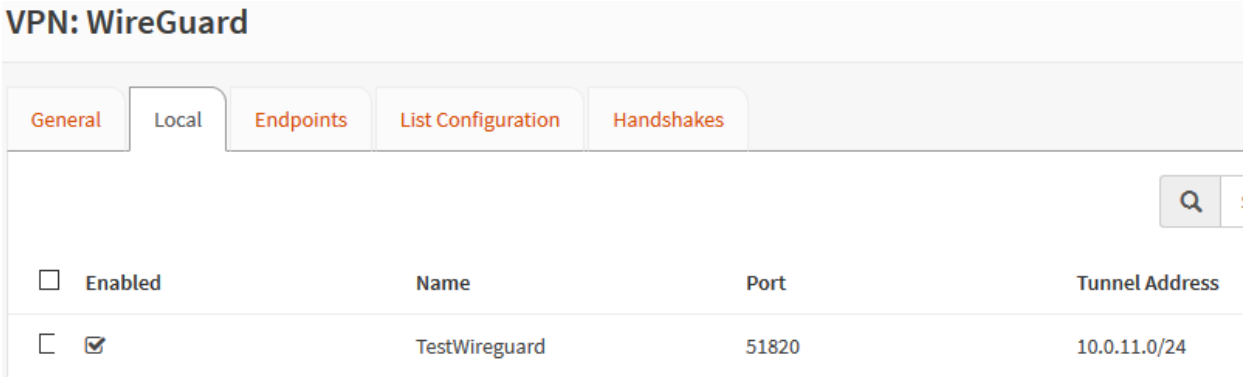

Abbildung 10: WireGuard Konfiguration in der OPNsense Firewall

Auf dem Client wurde die Software WireGuard in der Version 0.2.3 installiert und eingerichtet. Zum Einrichten des Tunnels wurde, wie in Abbildung 11 ersichtlich, der Public Key des Servers, die öffentliche IP-Adresse des A1 Routers, die zugelassen IP-Adressen und die IP-Adresse des Clients eingetragen. Durch den Eintrag AllowedIPs = 0.0.0.0 wurden alle Verbindungen durch den Tunnel geleitet.

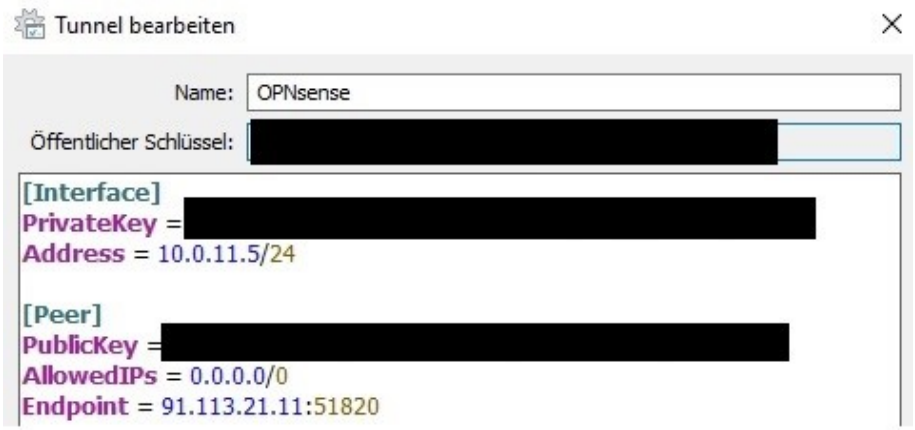

Abbildung 11: WireGuard Client Konfiguration

Durchgeführt wurde die Einrichtung dieser Maßnahme wie von Niedermeier (2019) beschrieben. Als Client wurde jedoch Windows 10 und nicht Ubuntu verwendet und die Einstellungen wurden angepasst. Eine weitere Möglichkeit eine Layer 3 VPN umzusetzen wäre mit IPsec.

5.9 Routersicherheit / Firewall

Im Businessbereich kommt es häufig vor, dass die Router, welche von den Providern zur Verfügung gestellt werden, nur vom Provider verwaltet werden können. Daher sollte nach diesem Router eine Firewall eingesetzt und diese abgesichert werden. Als erstes sollte der Zugang mit einem sicheren Passwort geschützt werden und wenn möglich eine zwei Faktor Authentifizierung eingerichtet werden. Damit die eingesetzte Firewall Updates erhält, sollten automatische Updates aktiviert werden und mit regelmäßigen manuellen Überprüfungen nachgebessert werden, wenn es zu Problemen kommt. In OPNsense ist mit einem Cron Job möglich regelmäßig nach Updates zu suchen und zu installieren. Die Firewall oder der Router sollte nur für Administratoren zugänglich sein, damit unbefugte keinen Zugriff haben. Es gibt auch Hardware, die mit einer GPS-Funktion ausgestattet ist und so prüfen kann, ob sich nach einem Stromausfall der Standort geändert hat. Network Ingress Filterung sollte eingesetzt werden, um die Angriffsfläche zu verringern. Ports und Schnittstellen (USB, Firewire und Netzwerkschnittstellen), die nicht benötigt werden, sollten, um weniger Angriffsfläche zu bieten, deaktiviert werden. Um das Zeitfenster eines Angriffs einzuschränken, ist es möglich die Internetverbindung zu trennen, wenn sie nicht benötigt wird. Ein sehr wichtiger Punkt ist die Segmentierung der Netze, um kritische Netze getrennt von den anderen zu betreiben. WLANs sollten mit dem höchstem Verschlüsselungsstandard abgesichert werden. Um die VPN-Verbindungen abzusichern, sollten starke Verschlüsslungen und eine zertifikatbasierte Verbindung gewählt werden (Bartels et al., 2020).

5.10 Netzwerküberwachung mittels Intrusion Detection System

Wie bereits beschrieben gibt es HIDS und NIDS, diese zwei Varianten sollten beide umgesetzt werden. Wie eine mögliche Lösung aussehen könnte, wird in diesem Kapitel genauer beschrieben. Zuerst wurde für die Clients ein HIDS in der Testumgebung umgesetzt, um die Informationen der Clients zentral auf einen Server zu speichern. Anschließend wurde ein NIDS für das Netzwerk umgesetzt. Das eingesetzte NIDS von OPNsense kann auch als NIPS erweitert werden, damit bei Erkennung eines Angriffs der Netzwerkverkehr unterbunden wird und einem Angriff entgegengewirkt werden kann.

5.10.1 HIDS

Als HIDS wurde OSSEC gewählt, da OSSEC von Unterfingher (2020) und Klein (2020) den ersten Platz bei den Open Source Tools belegt hat. Es ist kompatibel mit Windows, Linux, Unix und MacOS, daher eignet es sich auch für kritische Infrastrukturen in denen verschiedene Systeme eingesetzt werden.

Um den OSSEC Server zu installieren musste ein Linux Betriebssystem aufgesetzt werden, da es keine Windows Version für einen Server gibt. Gewählt wurde eine Debian10 64Bit Version ohne Graphische Oberfläche. Installiert wurde das Debian als VM in Hyper-V auf dem Windows Server 2019. Auf dieser VM wurde dann OSSEC Server installiert, heruntergeladen wurde dieser vom offiziellen Git Repository. Davor wurden noch die notwendigen Abhängigkeiten installiert. Nach der erfolgreichen Einrichtung des Servers wurde ein Agent hinzugefügt und so konfiguriert das dieser die logs an den Server übermittelt. Am Server konnten dann die logs wie in Abbildung 12 eingesehen und ausgewertet werden. Zusätzlich wurde noch eine Emailbenachrichtigung angeboten, dabei werden Alarme an eine zuvor konfigurierte Adresse gesendet.

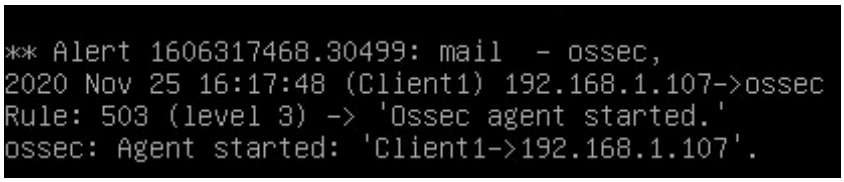

Abbildung 12: OSSEC Server log

Für die Clients wird ein OSSEC Agent Manager vom Hersteller bereitgestellt, dieser wurde heruntergeladen und auf dem Windows 10 (Client1) installiert. Anschließend wurde der Agent wie in Abbildung 13 konfiguriert. Dem Client wurde eine Statische IP-Adresse vergeben, um Problemen, die bei einer Dynamischen IP-Adresse entstehen können vorzubeugen. Damit es möglich ist eine Verbindung zum Server herzustellen, muss dies in der Firewall erlaubt werden. Standardmäßig werden die Daten über UDP Port 1514 übertragen. Am Server muss zuerst ein neuer Agent hinzugefügt werden, um einen Authentication key zu erhalten. Die IP-Adresse des Servers und der Authentication key muss dann im OSSEC Agent Manager eingetragen werden, um die Verbindung abzusichern. Anschließend wurde der Dienst gestartet und wie in Abbildung 12 ersichtlich wurden die Daten erfolgreich an den Server übertragen.

Abbildung 13: OSSEC Agent Manager

Es ist auch möglich die Verbindung mit SSL abzusichern. Diese Variante ist dann zu wählen, wenn eine kritische Infrastruktur mehrere Clients einrichten möchte, da ein manuelles Hinzufügen der Clients am Server zeitaufwendig ist. Damit mehrere Clients automatisch hinzugefügt werden können, muss ein SSL Development Tool in Debian installiert werden. Das wird benötigt, um Zertifikate erstellen zu können. Die Zertifikate sollten eine möglichst lange Schlüssellänge aufweisen und einen entsprechenden Gültigkeitszeitraum erhalten. Durch Anpassen der Datei mit der Endung „.conf“ kann der Agent auf mehrere Clients mit den vordefinierten Konfigurationen installiert werden (Birari, 2018).

5.10.2 NIDS/NIPS

Um ein NIDS und NIPS umzusetzen wurde OPNsense verwendet. Das in OPNsense integrierte System ist suricata welches auch getrennt aufgesetzt werden könnte. Der Unterschied zwischen IDS und IPS ist der letzte Schritt. Ein IDS erkennt einen Angriff und schlägt Alarm, ein IPS greift ein und blockiert die Verbindung. NIDS und NIPS wurde auf der OPNsense Firewall eingerichtet, da der gesamte Netzwerkverkehr über diese Firewall geht. NIDS lässt sich auch getrennt von NIPS aktivieren (Stubbig, 2019).

Zuerst wurde NIDS und NIPS für die WAN (Verbindung zum Internet) Schnittstelle aktiviert, da diese viel Angriffspotenzial bietet und diesen zusätzlichen Schutz benötigt. Es sollte auch LAN-seitig implementiert werden, da Angriffe auch häufig Clientseitig stattfinden. OPNsense bietet verschieden vordefinierte Regeln zum Download an. Es gibt auch die Möglichkeit selbst Regeln zu erstellen, damit je nach Infrastruktur die Regeln angepasst werden können. Um die Testumgebung optimal abzusichern wurden viele Regeln heruntergeladen, nach der Aktivierung der Regeln kam es jedoch zu hoher Hardwareauslastung von RAM und CPU. Dann sollte nicht die Lösung gewählt werden, weniger Regeln anzuwenden, sondern es sollte für die kritische Infrastrukturen eine stärkere Hardware angeschafft werden. Zuerst wurden die Regeln streng eingestellt, um möglichst viel zu blockieren. Anschließend wurden die Regeln gelockert damit der zugelassene Netzwerkverkehr erlaubt war und die Anzahl an falsch positiven Alarmen

akzeptabel war. Zum Schluss wurde noch unter „Schedule“ ein regelmäßiges Update eingerichtet damit die Regeln automatisch aktualisiert werden und so den neuesten Bedrohungen entgegengewirkt werden kann. Ein Beispiel wie ein Alarm aussieht, ist in Abbildung 14 dargestellt. In der Abbildung 14 ist zu erkennen, dass versucht wurde von der IP-Adresse 103.145.13.10 über den Port 443 auf die WAN Schnittstelle (IP-Adresse 10.0.0.25) zuzugreifen.

Alert info

Timestamp	2020-11-25T23:45:08.848674+0100
Alert	ET CINS Active Threat Intelligence Poor Reputation IP group 98
Alert sid	2403397
Protocol	TCP
Source IP	103.145.13.10
Destination IP	10.0.0.25
Source port	44014
Destination port	443
Interface	WAN

Abbildung 14: OPNsense NIDS Alarm

5.11 Fernzugriff auf Netzwerke / Fernwartung

Der Fernzugriff sollte mit einer stark abgesicherten VPN Verbindung umgesetzt werden. Eine VPN Verbindung sollte von beiden Seiten (helfende Person und hilfesuchende Person) zu einem Vermittlungsserver aufgebaut werden, damit die Verbindung auch jederzeit von beiden Seiten getrennt werden kann. Die VPN Verbindung sollte mit mehreren Faktoren abgesichert werden. Zur Nachverfolgung sollte die Protokollierung am Vermittlungsserver aktiviert werden. Wenn diese Verbindung aufgebaut ist, sind beide Computer im selben Netz und es kann beispielsweise mit SSH, VNC oder RDP zugegriffen werden. Die Absicherung sollte bis auf Layer 3 des OSI Modells eingeschränkt werden können, das bedeutet auf IP-Adresse, Port und Protokoll (Bartels et al., 2020).

Für die Umsetzung der Fernwartung wird OpenVPN verwendet, da diese VPN flexibler ist als WireGuard. Für unterschiedliche Clients eignet sich daher OpenVPN besser, da mehrere Verschlüsselungsalgorithmen unterstützt werden und mit Zertifikaten die Verbindung gesichert werden kann. WireGuard hingegen nutzt einen öffentlichen Schlüssel zum Verschlüsseln und einen privaten Schlüssel zum Entschlüsseln. Die öffentlichen Schlüssel müssen bei der Einrichtung ausgetauscht werden. OpenVPN bietet zudem bessere Logs, was für die Fernwartung wichtig ist, damit die Nachvollziehbarkeit sichergestellt werden kann. Somit kann nachvollzogen werden, welche Person zu welchem Zeitpunkt auf welche Clients zugegriffen

hat. WireGuard eignet sich dafür besser zum Vernetzten von Standorten, da diese Verbindung eine schnellere Übertragung bietet (Long, 2020).

Um diese Anforderungen zu erfüllen, wurde auf der OPNsense Firewall ein OpenVPN Server eingerichtet. Zu diesem Server wurde eine Verbindung mit Passwort und zweitem Faktor aufgebaut. OpenVPN ist in der Standardinstallation inkludiert und musste nicht als Plugin hinzugefügt werden. Die Verbindung wurde mit AES-256-GCM abgesichert und die Authentifizierung erfolgte mit SHA 512. Für die Zertifikate wurde eine Länge von 4096 bit festgelegt. Diese Einstellungen wurden gewählt, da sie derzeit als sicher gelten. Da die verwendete IP eine private Adresse ist und sich diese ändert, musste ein DDNS eingerichtet werden, dies sollte bei kritischen Infrastrukturen nicht der Fall sein. Denn es sollte ein Business Internetzugang vorhanden sein der eine Statische IP-Adresse hat. In OPNsense kann unter dem Menü OpenVPN der Punkt „Log File“ gewählt werden. Dieser zeigt die Details zu den VPN Verbindungen an. Am Client wurde die OpenVPN GUI installiert und die Konfigurationsdatei sowie die Zertifikate hinterlegt, die vom Server ausgestellt wurden. Am Client werden die Verbindungen zusätzlich protokolliert. Diese Protokolle wurden zum Suchen des Fehlers verwendet, da die Firewall den Verbindungsaufbau verhinderte. Nachdem eine Verbindung erfolgreich aufgebaut wurde, färbte sich das Symbol in der Taskleiste grün und am Server war der Verbindungsstatus wie in Abbildung 15 ersichtlich. Anhand des Verbindungsstatus ist die IP-Adresse ersichtlich die benötigt wird, um auf den entfernten Computer zuzugreifen.

OpenVPN Server TCP:443 Client connections

Common Name	Real Address	Virtual Address	Connected Since
stefan	91.141.3.164:43293	192.168.15.6	2020-11-28 22:20:36

Abbildung 15: OpenVPN Status der Verbindung

Als auch die zweite Seite eine Verbindung zum Netzwerk aufgebaut hatte, konnte auf den hilfesuchenden Computer zugegriffen werden. Für den Zugriff mit SSH musste der Port 22 in den Regeln der Firewall freigeschaltet werden. Um eine SSH Verbindung zum hilfesuchenden Computer aufzubauen wurde eine SSH Verbindung geöffnet, dazu wurde OpenSSH-Server nachinstalliert. Auf dem helfenden Computer wurde unter Windows das Programm Putty installiert. Nach dem Start von Putty kann die IP-Adresse des Zielrechners eingegeben werden und eine Verbindung wird aufgebaut. Beim erstmaligen Verbinden wurde die Echtheit der Zertifikate manuell geprüft und bestätigt. Alternativ könnte auch auf dem helfenden Computer OpenSSH-Client verwendet werden.

Wie schon im Kapitel „Gefahren und Vorteile der Vernetzung“ beschrieben, sollten die Netzwerke, von denen eine Verbindung aufgebaut wird, schon über entsprechende Sicherheitsmaßnahmen verfügen. Es sollten keine ungesicherten öffentlichen Netze sein von denen eine Verbindung aufgebaut wird (Steinmann, 2018, S. 53).

5.12 Server-Härtung

Zum Härten des Windows Servers 2019 werden die Punkte umgesetzt, die in der Theorie aufgezählt und beschrieben wurden. Diese Umsetzung muss je nach System angepasst werden. Einige Punkte sollten regelmäßig geprüft werden ob diese noch benötigt werden oder deaktiviert werden können. Bei der Konfiguration gilt, je weniger erlaubt ist, desto sicherer wird das System.

5.12.1 Deaktivierung von nicht benötigten Komponenten

Im Servermanager wurden alle nicht benötigten Rollen und Features entfernt. Dienste die den Status beendet hatten wurden deaktiviert, danach wurden weitere nicht benötigte Dienste deaktiviert. Dieser Schritt erforderte einige Neustarts damit geprüft werden konnte, dass keine wichtigen Dienste deaktiviert werden. Dateifreigaben wurden mit Berechtigungen geregelt und nicht benötigte Berechtigungen wurden entfernt. Die Übermittlung von Telemetriedaten wurde eingeschränkt und auch die Feedbackhäufigkeit von Windows wurde deaktiviert.

5.12.2 Aktivierung von hardwarenaher Schutzfunktionen

Die Funktion ASLR (Address Space Layout Randomization) wurde aktiviert, damit Sicherheitslücken in Programmen nicht einfach ausgenutzt werden können. Wenn ASLR aktiv ist, werden den Programmen zufällige Adressbereiche zugewiesen. Um Pufferüberläufe zu verhindern wurde geprüft ob DEP (Data Execution Prevention) aktiviert ist. Die Einstellung lässt sich am Windows Server 2019 mit dem Befehl „sysdm.cpl“ aufrufen und befindet sich im Reiter „Erweitert“ unter Leistung und dann im Reiter „Datenausführungsverhinderung“.

Im BIOS wurde ein Zugriffspasswort festgelegt und die Bootreihenfolge auf die Festplatte beschränkt. Die Funktion Secure Boot und Schutz gegen Seitenkanalangriffe konnte nicht eingestellt werden, da die verwendete Hardware zu alt ist und diese Features nicht anbietet. Mit der Funktion Secure Boot würden vor dem Starten des Bootloaders, wichtige Teile auf Manipulation geprüft werden. Bei neuer Hardware werden diese Features angeboten, daher ist es möglich diese Schutzmaßnahmen dort umzusetzen.

5.12.3 Sicherheitseinstellungen

Sensible Daten müssen sicher mittels Verschlüsselung übertragen werden, dazu sollten die Kommunikationsprotokolle aktiviert und regelmäßig überprüft werden, ob die Verschlüsselung aktiv ist. Der Austausch von kryptographischen Schlüsseln sollte mit Zertifikaten abgesichert werden. Nicht notwendige Zertifikate sollten aus den Vertrauensregeln entfernt werden. Wie schon beschrieben sollten BenutzerInnen nur die benötigten Rechte erhalten und auch die Benutzerkontensteuerung sollte aktiviert werden. Unter Windows nennt sich diese Benutzerkontensteuerung „User Account Control“. Auch die Dienste sollten mit minimalen Rechten sowie mit einem eigenen Account betrieben werden. Soweit möglich sollte nach außen

hin jeder Hinweis auf die installierten Services und dessen Versionen deaktiviert werden, da dies nützliche Informationen für Hacker wären. Der Server sollte so eingestellt werden, dass er sich bei Inaktivität der BenutzerIn von selbst sperrt. Umgesetzt kann das durch Einstellen eines Bildschirmschoners werden, indem die Option Kennwortschutz bei Reaktivierung aktiviert wird. Die Autostartfunktionen sollten deaktiviert werden, damit nicht bei Anschluss eines infizierten USB-Sticks Schadsoftware automatisch geladen wird. Protokolle sollten am Server aktiviert werden, damit Änderungen nachvollziehbar sind und auch bei einem Angriff erkannt werden kann, was verändert wurde (Bartels et al., 2020, S. 54).

5.12.4 Minimale Vergabe von Berechtigungen

Wie schon beschrieben sollten nur die notwendigen Berechtigungen vergeben werden, das gilt auch für Administratoren. Auch auf dem Dateisystem sollten strikte Berechtigungen für die Personen vorhanden sein. Mit dem Windows AD lässt sich das einfach umsetzen da die BenutzerInnen per Freigabeberechtigung individuell Berechtigungen zugewiesen werden können. Wartungszugänge sollten nur die Administratoren erhalten, die auch eine Wartung durchführen. Es sollten keine großzügigen Berechtigungen für Administratoren vergeben werden, die physikalische Zutrittsberechtigung zählt hier ebenfalls dazu. Hinzu kommt auch, dass USB-Schnittstellen und CD-Laufwerke, wenn diese nicht benötigt werden, deaktiviert werden sollten (Bartels et al., 2020, S. 54).

5.12.5 Userverwaltung und Kennwörter

Damit Kennwörter einer bestimmten Komplexität entsprechen und Änderungen der Richtlinien zentral gesteuert werden können, sollten für alle BenutzerInnen wie im Kapitel „Durchsetzung starker Passwörter“ die Richtlinien festgelegt werden. Dann ist auch sichergestellt, dass jeder Account mit einem Kennwort entsprechend der Kennwortrichtlinie abgesichert ist. Es sollte regelmäßig die Qualität der Kennwörter wie im Kapitel „Bewertung der Passwortstärke“ beschrieben, geprüft werden damit Standardkennwörter, die beispielsweise vom Administrator zur Einrichtung eines neuen Benutzers vergeben wurden, auch der Kennwortrichtlinie entsprechen. Es sollte keinen Administratoraccount für mehrere Personen geben, sondern jeder Account sollte personenbezogen sein, damit auch nachvollziehbar ist, wer die Änderung durchgeführt hat. Bei mehrmaliger Falscheingabe des Kennworts sollte auch der Administratoraccount gesperrt werden. Gastaccounts sind in vielen Systemen aktiv, diese sollten sofern nicht benötigt deaktiviert werden. Testaccounts und anonyme Accounts, die beim Installieren von Software erstellt wurden, sollten wieder gelöscht werden. Eine Anmeldung von lokalen Accounts sollte im Netzwerk gesperrt werden (Bartels et al., 2020, S. 54).

5.12.6 Netzwerkkomponenten einschränken

Windows bietet eine hohe Kompatibilität und daher unterstützt es viele Netzwerkprotokolle. Nicht benötigte und veraltete Protokolle gehören deaktiviert wie beispielsweise SMB1.0 (wurde von WannaCry ausgenutzt). Firewall Regeln des Servers sollten, wie auch in der Netzwerkfirewall, nur die benötigten Ports und Protokolle zulassen. Paketfilter sollten in der Firewall aktiviert werden und Dienste, über die mehrere Verbindungen laufen, sollten auf ein Minimum beschränkt werden (Bartels et al., 2020, S. 54–55).

5.13 Endpoint Detection und Response

Als Endpoint Detecton und Response wurde die Software Sophos Intercept X Endpoint gewählt, da diese im com-magazin mit der Note Sehr gut abgeschnitten hat (Selinger, 2019). Im AV-test hat diese Software im Bereich Schutzwirkung fünf von sechs Punkten, im Bereich Geschwindigkeit fünfeinhalb von sechs Punkten und im Bereich Benutzbarkeit sechs von sechs Punkten (AV-Test, 2020).

Die Software Sophos Intercept X Endpoint wurde in der Versin 10.8.9.2 installiert. Nach der Installation ist der Client im Admin Portal von Sophos sichtbar. Im Portal können verschiedene Richtlinien definiert werden wie: Schutz vor Bedrohungen, Überwachung von Peripheriegeräten, Überwachung von Anwendungen, Data Loss Prevention, Web Control, Update-Management und Windows Firewall. Die Computer können direkt vom Portal aus verwaltet werden und es bietet viele Sicherheitsstatusinformation wie in Abbildung 16 ersichtlich. Es könnte eine Verschlüsselung mittels Bitlocker mit Sophos Intercept X Endpoint durchgeführt werden. Doch dies wurde bereits im Punkt Laufwerksverschlüsselung erledigt. Das Portal wurde so abgesichert, dass für alle Administratoren eine mehrstufige Authentifizierung erforderlich ist.

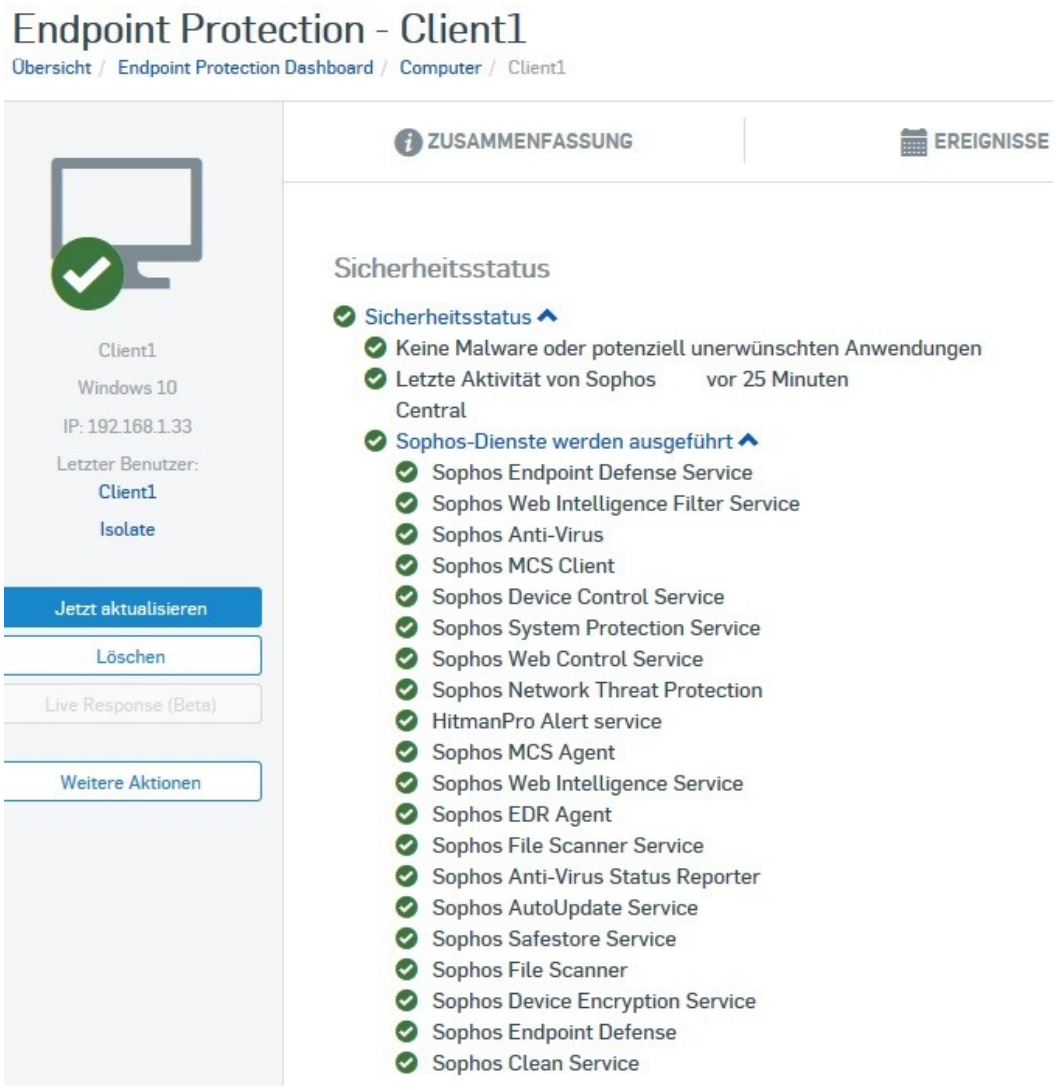

Abbildung 16: Sophos Endpoint Protection Client1 status

5.14 Erkennung von Angriffen und Auswertung

OSSIM ist eines der populärsten SIEM Tools, welches sehr viele Features wie Protokollierung, Überwachung, Bedrohungsbewertung über einen langen Zeitraum, automatisierte Antworten, Datenanalyse und Datenarchivierung beinhaltet. Es bietet auch Echtzeit Informationen über betroffene Clients. Ein Nachteil ist jedoch dass es sehr unflexibel und die Installation sehr aufwendig ist, besonders unter Windows (DNSstuff, 2019).

In der Testumgebung wurde OSSIM in einer VM am Windows Server 2019 aufgesetzt. Damit OSSIM bootet musste die Generation 1 für den virtuellen Computer ausgewählt werden. Bei der Installation war es wichtig, ein Passwort für Root zu vergeben. Ohne dieses Passwort funktionierte der Login trotz Hinzufügen eines Users nicht. Nach der Installation musste im Webinterface ein Account registriert werden. Mit dem Einrichtungsassistenten ließ sich das Netzwerk scannen und es konnten die Clients gewählt werden auf dem ein HIDS Agent installiert werden sollte. Dazu war die Eingabe eines Domänenadministrators notwendig. Für dieses Setup sollte ein eigener Domänenadministrator angelegt werden der anschließend

wieder entfernt wird. Um die Eingabe eines Domänenadministrators zu vermeiden, wurde der Client manuell installiert. Es wurde festgestellt, dass dies derselbe Agent war, wie er bei OSSEC zum Einsatz gekommen ist. Der Agent wurde so konfiguriert, dass er die Informationen an den OSSIM Server sendet. Weiters wurde noch der Windows Server 2019 und der Router hinzugefügt, der das Gateway zum Internet bildet. Eine Auflistung der Geräte, die zu OSSIM hinzugefügt wurden, sind in Abbildung 17 dargestellt. Diese Geräte wurden überwacht und es konnten Events konfiguriert werden. OSSIM bietet das Tool open threat exchange an für das eine Registrierung notwendig ist. Mit diesem Tool können bekannte Angriffe entdeckt werden.

HOSTNAME	IP	DEVICE TYPE	OPERATING SYSTEM
Server1	192.168.1.104	Server	Microsoft Windows Server 2019 Standard Edition on x64
Host-192-168-1-107	192.168.1.107		Windows
Host-192-168-1-1	192.168.1.1		
alienvault	192.168.1.11		AlienVault OS

Abbildung 17: OSSIM Assets

Damit ein SIEM richtig eingerichtet werden kann, muss festgelegt werden welche Informationen von einem SIEM gesammelt werden sollten. Die Daten werden dann von verschiedenen Quellen gesammelt und dargestellt. Bei der Entscheidung welche Informationen wichtig sind, könnte die Betrachtung von Worst Case Szenarien helfen. Durch eine Bedrohungsanalyse können gefährliche Aktivitäten im Netzwerk durch Auswerten von Netzwerkinformation erkannt werden. Daher ist eine Bedrohungsanalyse ein „Muss“. Ein SIEM sollte über alle IT-Umgebungen eingeführt werden, um ein einheitliches Monitoring über alle Systeme zu ermöglichen. Nur so können auch Gefahren auf allen Systemen erkannt werden. Damit ein Ausrollen auf allen Systemen möglich ist, sollte SIEM automatisiert werden. Zum Automatisieren eines SIEM kann ein USM (Unified Security Management) eingesetzt werden. Ein USM kann auch den Anforderungen an ein Compliance und Thread Management erfüllen. Die fünf wesentlichen Sicherheitsfunktionen sind Schwachstellenprüfung, Asset-Detection, Identifizieren von Bedrohungen, Verhaltensüberwachung und intelligente Netzwerksicherheit. Diese werden in einer USM Konsole vereinigt (Schmitz, 2013).

> *„Die richtigen Informationen zum richtigen Zeitpunkt zu bekommen, ist von entscheidender Bedeutung. Bei der Untersuchung von Sicherheitsvorfällen müssten sich Anwender ansonsten die meiste Zeit mit Events auseinandersetzen, die bereits geschehen sind. Mit den richtigen, aussagekräftigen Informationen steht und fällt die Leistung des Incident Response-Programms eines Unternehmens.“*
>
> *- Oliver Bareiss*

Der Einsatz eines SIEM bringt eine Flut an Informationen, die dann richtig eingeordnet werden müssen. Wie Oliver Bareiss in dem oben genannten Zitat sagt, helfen die Informationen nur, wenn sie zur richtigen Zeit verfügbar sind. Dabei kann ein SIEM helfen die Informationen zu sammeln und auszuwerten. Mit Regeln ist es dann möglich automatisiert gegen erkannte Bedrohungen zu reagieren. Es muss jedoch manuell geprüft werden, ob es sich tatsächlich um einen Angriff handelte oder ein Fehlalarm die Ursache ist. Wenn es an einem Fehlalarm liegt und das häufig auftritt, sollten die Regeln angepasst werden.

6 DISKUSSION

Um den Einfluss der Vernetzung auf die IT-Systeme von kritischen Infrastrukturen zu untersuchen, wurden Angriffe aus der Vergangenheit beschrieben und Schutzmaßnahmen ausgearbeitet. Die Forschung hat gezeigt, dass die Vernetzung einen großen Einfluss auf die Angreifbarkeit der IT-Systeme von kritischen Infrastrukturen hat. Jedoch bietet die Vernetzung auch viele Vorteile, auf die nicht immer verzichtet werden kann. Durch die richtige Umsetzung der erarbeiteten Maßnahmen, kann die Sicherheit stark erhöht werden, jedoch müssen die Maßnahmen immer an die jeweiligen Infrastrukturen angepasst werden.

Durch die gewonnenen Erkenntnisse wird die zuvor formulierte Hypothese H1 bestätigt, denn die kritischen Infrastrukturen können mittels Härten der IT-Systeme abgesichert werden. Es kann jedoch keinen kompletten Schutz der IT-Systeme geben der alle Angriffe erfolgreich verhindert. Wie bereits im Kapitel „Angriffe der Vergangenheit“ beschrieben, werden immer Angriffsflächen, die von Hacker ausgenutzt werden können, vorhanden sein. Man kann ihnen jedoch, durch Umsetzung der beschriebenen Maßnahmen, das Eindringen in ein System erschweren, so dass sich der Aufwand nicht mehr lohnt.

IT-Systeme, die nicht mit dem Internet verbunden sind und auch keine Funkverbindungen besitzen, können auch nicht aus der Ferne angegriffen werden. Das bedeutet sie sind vor möglichen Cyberangriffen geschützt. In Zukunft könnten daher Inselsysteme entstehen, die abgetrennt werden und keine Verbindung nach außen aufweisen. Innerhalb dieser Inseln könnten die Geräte miteinander kommunizieren und dadurch gesteuert werden. Für einen Angriff müsste ein physischer Zugriff gegeben sein. Entnetzung als eine Option zur Erhöhung der IT-Sicherheit, wird in der Arbeit „Entnetzung statt Vernetzung“ (Gaycken, 2011) genau beschreiben. Dieser Lösungsansatz ist jedoch nicht auf alle kritischen Infrastrukturen anwendbar. Daher wurden in dieser Masterarbeit verschieden Möglichkeiten beschrieben, um IT-Systeme besser abzusichern. Dadurch sollten kritische Infrastrukturen in Zukunft besser vor Hackerangriffen geschützt sein.

6.1 Erkenntnisse

Eine Bewertung der Passwortstärke lässt sich im AD von Windows, durch Auswertung des beschriebenen Berichtes einfach umsetzen. Bei regelmäßiger Durchführung dieser Maßnahme kann die Sicherheit deutlich erhöht werden. Dabei wird überprüft, ob die BenutzerInnen wirklich ein starkes Passwort verwenden oder die Richtlinien für die Durchsetzung eines starken Passwortes umgehen. Die Richtlinien helfen dabei, dass einfache Passwörter wie 12345678 nicht verwendet werden, denn dieser Account würde sehr schnell mit einem Wörterbuchangriff kompromittiert werden. Der Einsatz einer Multi-Faktor-Authentifizierung bringt zwar mehr

Sicherheit, hat jedoch einige Nachteile. Beispielsweise ist der Einrichtungsaufwand oder bei Verlust, der Wiederherstellungsaufwand, je nach verwendetem Faktor unterschiedlich hoch.

Ein wichtiges Thema ist die Verschlüsselung, daher wurde versucht unterschiedliche Möglichkeiten zu zeigen wie E-Mails, Daten, Ordner, Container, Festplatten und Verbindungen durch Verschlüsselungen abgesichert werden können. Die Wahl der Algorithmen ist jedoch immer an den aktuellen Stand der Technik anzupassen, da Computer immer leistungsfähiger und Algorithmen auch gebrochen werden können und dann nicht mehr sicher sind. Bei der Wahl von Verschlüsselungsprogrammen sollte darauf geachtet werden, dass eine starke Verschlüsselung verwendet wird, damit die Verschlüsselung ordentlich implementiert ist und keine Backdoors aufweist. Die Verschlüsselung sollte auch den neuesten Standards entsprechen. Einen guten Überblick bietet hierfür das BSI in den Publikationen zu Kryptographische Verfahren, welche auch in dieser Masterarbeit herangezogen wurden. Häufig wird Open Source Software bevorzugt, da jeder den Code frei einsehen kann und Fehler so schneller gefunden und ausgebessert werden. Zusätzlich bietet es den Vorteil, dass der Code angepasst oder erweitert werden kann, um noch mehr Flexibilität zu erhalten. Daher wurde auch in dieser Masterarbeit darauf geachtet, dass wenn möglich ein Open Source Programm verwendet wird.

Der Einsatz einer Firewall sollte selbstverständlich sein, denn nur so ist es möglich den Netzwerkverkehr in mehrere Netzwerke aufzutrennen (Segmentierung der Netze). Damit können kritische Bereiche abgetrennt werden und nur der festgelegte Datenverkehr zugelassen werden. Eine Firewall bietet noch viel mehr Möglichkeiten zur Sicherheit beizutragen, wie beispielsweise NIDS, NIPS, VPN-Verbindungen und Regeln zur Filterung (Protokolle, Ports und IP-Adressen). Damit kann sichergestellt werden, dass keine ungewollten Zugriffe in andere Netzwerke erfolgen.

Die Härtung des Servers trägt zur Erhöhung der Sicherheit bei, doch es sollte nicht nur der Server gehärtet werden, sondern alle eingesetzten Systeme. Durch das Härten wird die Angriffsfläche minimiert, da nur die tatsächlich benötigten Funktionen und Protokolle aktiv sind und der Rest deaktiviert wird. Bei der Einrichtung neuer Anwendungen ist es jedoch mühsamer, da die benötigten Funktionen und Ports eingeschaltet werden müssen. Ein IT-Administrator sollte die Aktivitäten seines Netzwerkes kennen und regelmäßig analysieren. Dazu kann ein SIEM verwendet werden, welches ihn dabei unterstützt. Damit die Systeme tatsächlich am neuesten Stand sind, sollte regelmäßig nach Updates gesucht werden. Updates schließen Sicherheitslücken und müssen daher zeitgerecht installiert werden, dass wurde durch Beschreiben des WannaCry Angriffs zusätzlich verdeutlicht.

Eine Erhöhung der Sicherheit der IT-Systeme ist zum Teil mit hohem Aufwand verbunden, denn nicht immer sind die Maßnahmen in einer bestehenden Infrastruktur einfach umzusetzen. Besonders beim Härten des Servers kommt es meistens zu Funktionsausfällen, da Ports in der Firewall gesperrt werden, die für bestehende Applikationen verwendet werden. Auch kann es zu Problemen kommen, da Abhängigkeiten von anderen Programmen notwendig sind, die beim Härten deinstalliert wurden. Der Konfigurationsaufwand ist nur ein Teil der benötigten Ressourcen, denn wenn ein IDS und IPS im Betrieb sind, kann es häufig zu Fehlalarmen

kommen. Auf diese sollte unmittelbar reagiert werden, da es sich um einen realen Hackangriff handeln könnte. Eine Hardware, die nicht mehr den aktuellen Sicherheitsstandards entspricht (verwendet alte Protokolle oder unterstützt nur bereits gebrochene Verschlüsselungsalgorithmen) sollte ersetzt werden, was oft hohe Kosten verursachen kann.

Für die AnwenderInnen sind die Sicherheitsmaßnahmen mit deutlichem Mehraufwand verbunden. Daher sollte sorgfältig abgewogen werden, welche Bereiche kritisch sind und nur diese müssen dann speziell abgesichert werden. Ein gutes Beispiel ist die Anmeldung der BenutzerInnen an einem Computer. Zuerst muss ein BIOS Passwort eingegeben werden. Anschließend erfolgt die Eingabe des Passwortes für die Festplattenentschlüsselung (PIN für Bitlocker) und dann kommt die Abfrage von Benutzername und Passwort. Das Anmeldeverfahren kann durch Gesichtserkennung, Fingerabdruck oder Hardwaretoken zwar vereinfacht werden, bleibt aber immer noch aufwendig. Dieser zusätzliche Aufwand dürfte wohl der Grund sein, wieso Unternehmen IT-Sicherheit nur teilweise oder überhaupt nicht umsetzen.

6.2 Aufgetretene Probleme

Folgend werden Probleme beschrieben, die im Zuge dieser Arbeit entstanden sind. Zunächst mussten Gruppenrichtlinien angepasst werden, um die Bitlocker Verschlüsslung durchzuführen, da die verwendete Hardware kein TPM verbaut hatte. Diese Maßnahme sollte, wie bereits beschrieben, mit neuerer Hardware umgesetzt werden, die ein TPM besitzt.

Bei dem Programm Gpg4Win kam es vermehrt zu Abstürzen der Kleopatra Oberfläche und es musste diese des Öfteren neu gestartet werden. Ein Grund hierfür könnte auch die Kombination von Gpg4Win und dem neuen Windows Build gewesen sein. In der PowerShell funktionierte das Programm problemlos.

Dem OSSIM-Server wurden 2GB Arbeitsspeicher zugewiesen, was zu Problemen beim Starten des Servers führte, da er versuchte auf die Festplatte auszulagern und dadurch das ganze System verlangsamte. Nach vergrößern des Arbeitsspeichers auf 7GB funktionierte der Server ordnungsgemäß. Für die Clients wird der gleiche Agent verwendet wie für OSSEC, daher sollte zuerst überlegt werden, ob ein SIEM benötigt wird, denn dann kann OSSIM den Bereich von OSSEC für ein HIDS abdecken.

6.3 Weiterführende Forschungen

Dieses Themengebiet bietet noch Potenzial für weiterführende Forschungen, die an diese Arbeit anknüpfen könnten. Ein an diese Arbeit anknüpfendes Forschungsgebiet, könnte eine Bewertung der einzelnen Maßnahmen sein, wie viel Sicherheit diese tatsächlich bringen und ob sich eine Umsetzung auch für nicht kritische Infrastrukturen lohnt. Außerdem könnten Maßnahmen für weitere Betriebssysteme erforscht werden oder Maßnahmen zur Absicherung von beispielsweise mobilen Geräten, Clouddiensten und Webanwendungen ausgearbeitet werden. Es könnte auch gezielt auf eine kritische Infrastruktur eingegangen werden und für

diese, Sicherheitsmaßnahmen ausgearbeitet oder bestehende Maßnahmen, angepasst werden. Hierfür wäre eine Zusammenarbeit mit einem Betrieb, der in den Bereich einer kritischen Infrastruktur fällt, notwendig. Organisatorische Maßnahmen wurden in dieser Arbeit nicht behandelt und bieten ebenso weitere Forschungsmöglichkeiten.

In den nächsten Jahren wird sich noch vieles in der IT-Sicherheit für kritische Infrastrukturen ändern, da die NIS-Richtlinie dann von allen EU-Mitgliedstaaten umgesetzt werden muss und der erste Bericht am 09. Mai 2021 vorzulegen ist. Dies bietet dann weiteres Potenzial für Forschungen.

7 SCHLUSSFOLGERUNG

Die Forschungsfrage, ob kritische Infrastrukturen mittels Härten der IT-Systeme abgesichert werden können, konnte durch die Masterarbeit verifiziert werden. Hierfür wurden zunächst kritische Infrastrukturen und Angriffe der Vergangenheit beschrieben und mögliche Sicherheitsmaßnahmen ausgearbeitet und in einer Testumgebung umgesetzt. Die Maßnahmen sind allgemein gehalten, damit sie von möglichst vielen kritischen Infrastrukturen anwendbar sind. Aufgrund dessen wurde der Rahmen der Masterarbeit auf derzeit aktuelle Windows Betriebssysteme eingeschränkt. Ebenso ist es bei der Absicherung der IT-Systeme von enormer Bedeutung die Ziele der AngreiferInnen zu kennen, um entsprechende Maßnahmen zu setzen.

Die Untersuchung des Einflusses der Vernetzung auf kritische Infrastrukturen ergab, dass diese einen großen Einfluss auf die IT-Sicherheit hat. Jedoch ist ein Voranschreiten der Vernetzung im vollem Gange und aus vielen Bereichen nicht mehr wegzudenken. Durch die Vernetzung können Unternehmen den Überblick behalten (Monitoring) und Kosten sparen, da wie bereits beschrieben, beispielsweise bei der Verwaltung von Kraftwerken nur eine zentrale Steuerungszentrale errichtet werden muss und dadurch Personal eingespart wird. Da die Vernetzung nicht zu stoppen ist, müssen kritische Infrastrukturen mit entsprechenden Sicherheitsmaßnahmen bestmöglich abgesichert werden, um sie vor möglichen Angriffen zu schützen.

Ein vollständiger Schutz der kritischen Infrastrukturen wird nicht umsetzbar sein, jedoch wird anhand der Masterarbeit gezeigt, dass eine deutliche Erhöhung der IT-Sicherheit möglich ist. IT-Sicherheit bedarf eines laufenden Prozesses zur Weiterentwicklung, denn die Maßnahmen müssen immer an den aktuellen Stand der Technik angepasst werden, um auch den neuesten Angriffen standzuhalten.

ABKÜRZUNGSVERZEICHNIS

AD	Active Directory
AES	Advanced Encryption Standard
APCIP	Österreichisches Programm zum Schutz kritischer Infrastrukturen (Austrian Program for Critical Infrastructure Protection)
ASCII	American Standard Code for Information Interchange
ASLR	Address Space Layout Randomization
BSI	Bundesamt für Sicherheit in der Informationstechnik
D-A-CH	Deutschland, Österreich, Schweiz
DDoS	Distributed Denial-of-Service
DEP	Data Execution Prevention
EPCIP	Europäisches Programm zum Schutz kritischer Infrastruktur (European Program for Critical Infrastructure Protection)
EU	Europäische Union
FIDO	Fast IDentity Online
HIPS	Host Based Intrusion Protection Systems
HOTP	HMAC-based One-Time-Passwort
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IEC	International Electrotechnical Commission
IKT	Informations- und Kommunikationstechnologie
IP	Internet Protocol
IPS	Intrusion Protection System
ISO	International Organization of Standardization
IT	Information Technology
LAN	Local Area Network
MFA	Multi-Faktor Authentifizierung
NIPS	Network Intrusion Protection Systems
NIS	Netzwerk- und Informationssicherheit
NHS	National Health Service
NSA	National Security Agency
OTP	One-time password
PGP	Pretty Good Privacy
PKI	Public Key Infrastructure
RAM	Random Access Memory
RFID	Radio Frequency Identification
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Information and Event Management

SKI	Schutz kritischer Infrastrukturen
SMB	Server Message Block
SPS	speicherprogrammierbare Steuerung
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOM	Technische und Organisatorische Maßnahmen
TOTP	Time-based One-Time-Passwort
TPM	Trusted Platform Module
USB	Universal Serial Bus
USM	Unified Security Management
USV	unterbrechungsfreie Stromversorgung
VM	virtuelle Maschine
VPN	Virtual Private Network
IDS	Intrusion Detection System

ABBILDUNGSVERZEICHNIS

LITERATURVERZEICHNIS

Anderson, R. J. (2010). *Security Engineering: A Guide to Building Dependable Distributed Systems* (2nd ed.). John Wiley & Sons Inc. http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=343359

Andreas, P. (25. Mai 2020). DSGVO & NIS-Richtlinie: Doppelte Aufsicht, einfache Sicherheitslösung. *IT Finanzmagazin*. https://www.it-finanzmagazin.de/dsgvo-nis-richtlinie-doppelte-aufsicht-einfache-sicherheitsloesung-106806/

Augsten, S. (26. Juli 2019). 10 Vorteile der Open-Source-Nutzung. *Dev-Insider*. https://www.dev-insider.de/10-vorteile-der-open-source-nutzung-a-849395/

AV-Test (Hg.). (2020). *Test Sophos Intercept X Advanced 10.8 für Windows 10*. https://www.av-test.org/de/antivirus/unternehmen-windows-client/windows-10/august-2020/sophos-intercept-x-advanced-10.8-203220/

Bartels, K. U. (28. Juni 2017). Der Stand der Technik in der IT-Sicherheit: komplexe technische und rechtliche Anforderungen. *Heise*. https://www.heise.de/select/ix/2017/7/1499358051209829

Bartels, K. U., Dehning, O., Dominkovic, D., Dubbel, S., Falkenthal, O., Fischer, M., Gehrmann, M., Gora, S., Heyde, S., Kerbl, T., Kippert, T., Kolmhofer, R., Lawicki, T., Liedke-Deutscher, B., Maier, J., Menge, S., Mühlbauer, H., Müller, S., Robin, M. & Wüpper, W. (2020). *IT-Sicherheitsgesetz und Datenschutz-Grundverordnung: Handreichung zum "Stand der Technik" technischer und organisatorischer Maßnahmen*. https://www.teletrust.de/fileadmin/docs/fachgruppen/ag-stand-der-technik/2020-02_TeleTrusT_Handreichung_Stand_der_Technik_in_der_IT-Sicherheit_DE.pdf

Beiersmann, S. (16. April 2020). Studie: Coronakrise treibt Homeoffice in Deutschland voran. *ZDNet.de*. https://www.zdnet.de/88378877/studie-coronakrise-treibt-homeoffice-in-deutschland-voran/

Bendel, O. (16. August 2018). Cybersecurity. *Springer Fachmedien Wiesbaden GmbH*. https://wirtschaftslexikon.gabler.de/definition/cybersecurity-99856/version-331724

Bertram, A. (5. April 2019). Find weak Active Directory passwords with PowerShell. *4sysops*. https://4sysops.com/archives/find-weak-active-directory-passwords-with-powershell/

Birari, S. (6. Juni 2018). *OSSEC-HIDS Installation & Configuration on Amazon EC2 Instance*. https://blog.e-zest.com/ossec-hids-installation-and-configuration-on-amazon-ec2-instance

Briegleb, V. (13. Mai 2017). WannaCry: Was wir bisher über die Ransomware-Attacke wissen. *heise Online*. https://www.heise.de/newsticker/meldung/WannaCry-Was-wir-bisher-ueber-die-Ransomware-Attacke-wissen-3713502.html

BSI (Hg.). (2020a). *BSI – Technische Richtlinie: Kryptographische Verfahren: Empfehlungen und Schlüssellängen.* BSI. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile

BSI. (18. November 2020b). *BSI für Bürger - Verschlüsselung mit Software*. https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Verschluesselung/Datenverschluesselung/Software/software_node.html

Bundesamt für Bevölkerungsschutz BABS (Hg.). (2017). *Nationale Strategie Zum Schutz Kritischer Infrastrukturen*. https://www.babs.admin.ch/content/babs-internet/de/aufgabenbabs/ski/nationalestrategie/_jcr_content/contentPar/tabs/items/downloads/tabPar/downloadlist/downloadItems/73_1460987489220.download/natstratski2018-2022_de.pdf

Bürki, P. (2019). *Über Gewissheiten, Vermutungen und juristische Unwahrheiten.* www.svgw.ch, svgw. https://www.aquaetgas.ch/energie/gas/20190506_ag5_%C3%BCber-gewissheiten-vermutungen-und-juristische-unwahrheiten/

Cherepanov, A. & Lipovsky, R. (2016). *BlackEnergy – what we really know about the notorious cyber attacks.* Virus Bulletin. https://www.virusbulletin.com/virusbulletin/2017/07/vb2016-paper-blackenergy-what-we-really-know-about-notorious-cyber-attacks/

Cyber Security Austria - Verein zur Förderung der Sicherheit Österreichs strategischer Infrastruktur (Hg.). *Cyber Security Austria.* Landespolizeidirektion Wien, Referat Vereins-, Versammlungs- und Medienrechtsangelegenheiten. https://www.cybersecurityaustria.at/index.php/home/kritische-infrastrukturen

Dännart, Diefenbach, Hofmeier, Lechner & Rieb. (2018). *IT-Sicherheit in Kritischen Infrastrukturen–eine Fallstudien-basierte Analyse von Praxisbeispielen*. http://mkwi2018.leuphana.de/wp-content/uploads/mkwi_64.pdf

Dirscherl, H.-C. & Arne, A. (2020). *So gefährlich falsch werden Passwörter benutzt.* IDG Tech Media GmbH. https://www.pcwelt.de/news/So-gefaehrlich-falsch-werden-Passwoerter-benutzt-10807537.html

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE (Hg.). (2020). *IEC 62443: Die internationale Normenreihe für Cybersecurity in der Industrieautomatisierung.* DKE Deutsche Kommission Elektrotechnik Elektronik. https://www.dke.de/de/arbeitsfelder/industry/iec-62443-cybersecurity-industrieautomatisierung

DNSstuff (Hg.). (2019). *10 Best Free and Open-Source SIEM Tools in 2020*. https://www.dnsstuff.com/free-siem-tools#ossim

Dunn Cavelty. (2010). *Cyberwar: concept, status quo, and limitations*. https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/23217/1/eth-1580-01.pdf

Fekete, A. (2013). *Schlüsselbegriffe im Bevölkerungsschutz zur Untersuchung der Bedeutsamkeit von Infrastrukturen–von Gefährdung und Kritikalität zu Resilienz und persönlichen Infrastrukturen.* https://www.researchgate.net/profile/Alexander_Fekete/publication/331230861_Schlusselbegriffe_im_Bevolkerungsschutz_zur_Untersuchung_der_Bedeutsamkeit_von_Infrastrukturen_-_von_Gefahrdung_und_Kritikalitat_zu_Resilienz_personlichen_Infrastrukturen/links/5c6d57fc4585156b570be34b/Schluesselbegriffe-im-Bevoelkerungsschutz-zur-Untersuchung-der-

Bedeutsamkeit-von-Infrastrukturen-von-Gefaehrdung-und-Kritikalitaet-zu-Resilienz-persoenlichen-Infrastrukturen.pdf

FIDO2: Der neue Standard für den sicheren Web-Log-in: Was ist FIDO2? (4. Oktober 2019). *1&1 IONOS SE*. https://www.ionos.de/digitalguide/server/sicherheit/was-ist-fido2/

Gaycken, S. (2011). *Entnetzung statt Vernetzung: Paradigmenwechsel bei der IT-Sicherheit*. http://www.it-rechts-praxis.de/files/entnetzung_gaycken_karger_mmr_2011.pdf

Glenk, T. (2020). *WireGuard: Was kann der VPN-Newcomer?* https://www.computerbild.de/artikel/cb-Tipps-VPN-WireGuard-Was-kann-der-VPN-Newcomer-29268697.html

Grassi, P. A., Newton, E. M., Perlner, R. A., Regenscheid, A. R., Burr, W. E. & Richer, J. P. (2017). *Nist special publication 800-63b. digital identity guidelines: Authentication and lifecycle management: Authentication and Lifecycle Management*. https://pages.nist.gov/800-63-3/sp800-63b.html

Heise (Hg.). (2020). *VeraCrypt*. https://www.heise.de/download/product/veracrypt-95747

Kersten, H., Klett, G., Reuter, J. & Schröder, K.-W. (2016). *IT-Sicherheitsmanagement nach der neuen ISO 27001: ISMS, Risiken, Kennziffern, Controls*. *Edition <kes>*. Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-14694-8

Klein, E. (2020). *Top 5 open-source HIDS systems*. https://logz.io/blog/open-source-hids/

Kuhn, J. (2005). *Der Schutz kritischer Infrastrukturen. Unter besonderer Berücksichtigung von kritischen Informationsinfrastrukturen*. http://edoc.vifapol.de/opus/volltexte/2008/590/pdf/wp5.pdf

Lauterschlag, E. (15. Dezember 2017). Verschlüsselung: Definition, Ziele, Funktionsweise und Verfahren. *Enrico Lauterschlag*. http://www.was-ist-malware.de/it-sicherheit/verschluesselung-definition-ziele-funktionsweise-und-verfahren/

Long, H. (13. Juni 2020). *WireGuard vs OpenVPN: In-Depth Analysis and Test Results*. https://restoreprivacy.com/vpn/wireguard-vs-openvpn/

Maduz, L. & Roth, F. (2018). Vierter Trilateraler Workshop D-A-CH Schutz kritischer Infrastrukturen 4.-6. Juni 2018 in Bonn. *ETH Zurich.* Vorab-Onlinepublikation. https://doi.org/10.3929/ethz-b-000315459

Marwan, P. (15. März 2018). Darum geht es bei Endpoint Detection and Response (EDR). *ChannelPartner*. https://www.channelpartner.de/a/darum-geht-es-bei-endpoint-detection-and-response-edr,3333456

Meixner, W. (2016). *Die Gefahr der totalen Vernetzung*. http://wwwmayr.informatik.tu-muenchen.de/personen/meixner/gefahrtotalervernetzung_mannheim.pdf

Metcalf, S. (6. November 2014). How Attackers Extract Credentials (Hashes) From LSASS. *Active Directory Security*. https://adsecurity.org/?p=462

Mierke, M. (21. Oktober 2019). Thunderbird: PGP-Verschlüsselung für E-Mails einrichten. *heise Online*. https://www.heise.de/tipps-tricks/Thunderbird-PGP-Verschluesselung-fuer-E-Mails-einrichten-4561551.html

Mierke, M. (5. August 2020). BitLocker auf Windows 10: Festplatte richtig verschlüsseln. *heise Online*. https://www.heise.de/tipps-tricks/BitLocker-auf-Windows-10-Festplatte-richtig-verschluesseln-4325375.html

Minnich, S. (2016). *Malware, Viren und Trojaner – Das Schädlings-ABC*. https://www.heise.de/download/blog/Malware-Viren-und-Trojaner-Das-Schaedlings-ABC-3356219

Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie) (17. Juni 2009). *Bundesministerium des Innern, für Bau und Heimat*. https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/kritis.html

Niedermeier, T. (3. September 2019). OPNsense WireGuard VPN für Road Warrior einrichten. *Thomas-Krenn.AG*. https://www.thomas-krenn.com/de/wiki/OPNsense_WireGuard_VPN_f%C3%BCr_Road_Warrior_einrichten

Österreichisches Programm zum Schutz kritischer Infrastrukturen (APCIP). (2014). https://www.bundeskanzleramt.gv.at/dam/jcr:bb6a1a41-eb1d-4552-96da-9b460bbc5c0b/%C3%96sterreichisches%20Programm%20zum%20Schutz%20kritischer%20Infrastrukturen%20(APCIP).pdf

Pössneck, L. (6. März 2008). Kostenloser BSI-Leitfaden zur Festplattenverschlüsselung. *silicon.de*. https://www.silicon.de/39188048/kostenloser-bsi-leitfaden-zur-festplattenverschluesselung

Rentrop, C. & Will, M. (20. Mai 2020). E-Mails verschlüsseln - lohnt sich das? *heise Online*. https://www.heise.de/tipps-tricks/E-Mails-verschluesseln-lohnt-sich-das-3900717.html

Robles, R. J., Choi, M.-k., Cho, E.-s., Kim, S.-s., Park, G.-c. & Yeo, S.-S. (2008). *Vulnerabilities in SCADA and critical infrastructure systems* (Bd. 2008). http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.176.5665&rep=rep1&type=pdf

Rosenthal, S. & Schmitz, P. (17. Februar 2017). NIS-Richtlinie, IT-Sicherheitsgesetz und die Folgen. *Security-Insider*. https://www.security-insider.de/nis-richtlinie-it-sicherheitsgesetz-und-die-folgen-a-581850/

Rouse, M. (30. April 2020). Security Information and Event Management (SIEM). *ComputerWeekly.com/de*. https://www.computerweekly.com/de/definition/Security-Information-and-Event-Management-SIEM

Saxena, V. (25. November 2020). *Description of the Difference Between HIDs & NIDs*. https://www.techwalla.com/articles/description-of-the-difference-between-hids-nids

Schmidt, J. (4. Februar 2020). Passwörter: BSI verabschiedet sich vom präventiven, regelmäßigen Passwort-Wechsel. *heise Online*.

Schmitz, P. (20. August 2013). Mit SIEM IT-Gefahren erkennen. *Security-Insider*. https://www.security-insider.de/mit-siem-it-gefahren-erkennen-a-415029/?p=3

Schmitz, P. (4. August 2017a). Was ist Multi-Faktor-Authentifizierung (MFA)? *Security-Insider*. https://www.security-insider.de/was-ist-multi-faktor-authentifizierung-mfa-a-631486/

Schmitz, P. (29. Dezember 2017b). Was ist Zugangskontrolle? *Security-Insider*. https://www.security-insider.de/was-ist-zugangskontrolle-a-673084/

Schmitz, P. (14. August 2018). Intrusion-Detection und -Prevention-Systeme. *Security-Insider*. https://www.security-insider.de/intrusion-detection-und-prevention-systeme-a-735825/

Schmitz, P. (24. Oktober 2019). Was ist TOTP? *Security-Insider*. https://www.security-insider.de/was-ist-totp-a-875708/

Schneier, B. (2015). *Secrets and Lies: DIGITAL SECuRITy IN A NETWORkED WORLD* (15th Anniversary Edition). Wiley.

Selinger, M. (2019). *Sophos Intercept X Endpoint im Test*. https://www.com-magazin.de/praxis/test/sophos-intercept-x-endpoint-im-test-2403557.html?page=1_gute-schutzwirkung-mit-last

Singh, M. (20. Juni 2020). 15 Password Cracking Techniques Used By Hackers in 2020. *Tech Viral*. https://techviral.net/top-password-cracking-techniques-used-by-hackers/

Siriu, S. (12. Februar 2019). Schutzziele der Informationssicherheit. *Haufe-Lexware GmbH & Co. KG*. https://www.haufe.de/compliance/management-praxis/informationssicherheit/schutzziele-der-informationssicherheit_230130_483172.html

Steinmann, C. (2018). *IT-Sicherheit in Unternehmen–State of the Art, Gefahren und Trends: Informatics Inside connect (IT)*. https://www.hhz.de/fileadmin/user_upload/Fakultaet_INF/Bilder/Aktuelles/News/2018/010_Informatics_Inside/Tagungsband_InformaticsInside2018_digital_final_inhalt.pdf#page=57

Stubbig, M. (2019). *Practical OPNsense: Building Enterprise Firewalls with Open Source*. BoD - Books on Demand GmbH.

Sullivan, J., Loffler, J. & Gordon, Y. (2019). *Complaint in the United States District Court for the Southern District of New York.* https://nsarchive2.gwu.edu/dc.html?doc=5736655-National-Security-Archive-Bangladesh-Bank-vs

Symantec. (2015). *Security Response: Regin: Top-tier espionage tool enables stealthy surveillance.* Symantec Security Response. https://docs.broadcom.com/doc/regin-top-tier-espionage-tool-15-en

Thabet, A. (2011). *Stuxnet malware analysis paper*. http://itdesigns.net/wp-content/uploads/reports/stuxnet%20malware%20analysis%20paper%20.pdf

Tischer, M., Durumeric, Z., Foster, S., Duan, S., Mori, A., Bursztein, E. & Bailey, M. (2016). Users Really Do Plug in USB Drives They Find. In *2016 IEEE Symposium on Security and Privacy: SP 2016 : 23-25 May 2016, San Jose, California, USA : proceedings.* IEEE. https://doi.org/10.1109/sp.2016.26

Tunggal, A. T. (6. Februar 2020). What is Defense in Depth? *UpGuard*. https://www.upguard.com/blog/defense-in-depth

Unterfingher, V. (2020). *Ten Open-Source EDR Tools to Enhance Your Cyber-Resilience Factor*. https://heimdalsecurity.com/blog/open-source-edr-tools/

Vetter, J. *Gesetzeslücken bei der Internetkriminalität: Gesetzeslücken bei der Internetkriminalität*. kops.uni-konstanz.de. http://kops.uni-konstanz.de/handle/123456789/3376

Wakolbinger, Fickert, Malleck & Aigner. (2012). *SMART emergency -Ein Konzept Für die Versorgung von kritischer Infrastruktur*. http://www.tugraz.at/fileadmin/user_upload/events/eninnov2012/files/lf/lf_wakolbinger.pdf