MASTERARBEIT

MOBILE COMPUTING
GEFAHREN UND ABSICHERUNG DER MOBILEN GERÄTE IM UNTERNEHMENS-UMFELD

ausgeführt an der

am Studiengang
Informationstechnologien & Wirtschaftsinformatik

Von: Farid Abdelgaffar
Personenkennzeichen: 1910320002

Graz, am 26. März 2021 .....

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

Ich möchte mich bei meiner Familie bedanken, insbesondere meinen Eltern, welche mich bei den oft schwierigen Phasen dieser Masterarbeit und dem damit verbundenen Semester unterstützt und aufgebaut haben. Ebenfalls bedanke ich mich für die hervorragende Zusammenarbeit und Unterstützung bei der Ressourcenfindung bei dem Unternehmen ACP TEKAEF GmbH.
Weiteren Dank haben meine Kollegen und Freunde Patrick Gollner, Patrick Ulz, Patrick Posch, Christopher Wastl, Gerwin Passer und Zlatko Knežević, die geschlossenen Freundschaften sehe ich als meinen größten Gewinn des Studiums an.
Abschließend möchte ich mich noch bei meinem Betreuer, Herrn Dipl.-Ing. Dr. techn. Selver Softic, BSc für die durchgehende Betreuung für fachliche und organisatorische Fragen bei dieser Masterarbeit bedanken.

KURZFASSUNG

Die folgende Masterarbeit behandelt das Thema der Sicherheit im Umgang mit mobilen Geräten und welche Gefahren für diese bestehen und welche Maßnahmen getroffen werden können, um Schäden im Unternehmensumfeld zu vermeiden.
Dabei wird ein großer Fokus auf mögliche Angriffsvektoren gelegt, diese evaluiert und betrachtet, wie ein Schaden auf den Angriffsvektor bestmöglich vermieden werden kann.
Des Weiteren werden Penetration Tests von Geräten näher erleuchtet, da diese für das IT-Personal eine wichtige Möglichkeit darstellt, um die Sicherheit der Geräte und des Netzwerkes zu testen.
Das Hauptaugenmerk der ersteren Kapitel bezieht sich auf die Verwendung von Notebooks für den mobilen Arbeitsgebrauch. Im letzten Kapitel des theoretischen Teiles werden Mobiltelefone nochmals genauer erörtert, da diese heutzutage zum Standardequipment von vielen Angestellten gehört.
Schlussendlich werden für den praktischen Teil dieser Arbeit mehrere Experten zum Thema der mobilen Sicherheit im Unternehmen befragt, um zu erörtern welchen Stand diese derzeit und welche Maßnahmen diese anwenden, um deren Unternehmen abzusichern.
Die Ergebnisse zeigen, dass von allen befragten Experten valide Standards eingesetzt werden, um die Sicherheit der Mobilgeräte zu garantieren. Dabei versuchen diese sowohl die Sicherheit der Geräte, aber auch der Daten zu garantieren.

ABSTRACT

This thesis explores IT security on mobile devices, both the dangers and the available countermeasures. A major focus is on evaluating potential attack vectors to learn how best to avoid or mitigate damage. Furthermore, penetration tests of mobile devices are performed, as these tests are an important tool to assess hardware, software, and network security. The first chapters consider notebooks for mobile work and their possible dangers. The theoretical section closes with a detailed discussion of mobile telephones, as these are standard equipment for many employees. Several experts are interviewed for the practical section of this thesis. These interviews concern corporate mobile security and the applied measures to secure their workplace.

The results show that all the surveyed experts use valid standards to guarantee the security of hardware and stored data of their mobile devices.

INHALTSVERZEICHNIS

1 EINLEITUNG

Ultimately, the pace at which mobile is evolving in the enterprise is completely unique, changing how businesses have to think about security. Companies need to establish trust and security in a world where they have less and less control—over devices, over apps and their users. The only way to do this effectively moving forward is to truly understand how people work and interact on mobile while knowing that threats are present. We know that attackers follow users and the popularity of mobile apps in conjunction with the emergence of their security flaws means that mobile is prime to be the next attack vector that threatens corporate data and user privacy.
(Ely, 2020)

Mobile Geräte verändern die Welt auf rasante weise. Waren diese vor 20 Jahren aufgrund ihrer Schwerfälligkeit und Unhandlichkeit noch selten anzutreffen, so sind diese heutzutage allgegenwärtig. Selbst Personen, welche nicht technikaffin sind, besitzen zumeist mindestens ein Mobiltelefon.

Diese Mobilität in der Technik bietet eine große Anzahl an Vorteilen, aber mit diesen kommen auch viele neue Gefahren. Potenzielle Angreifer und Angreiferinnen erhalten durch die große Anzahl an Geräten, Applikationen und Situationen, welche durch die Mobilität gegeben ist, eine Reihe von neuen Angriffsvektoren.

1.1 Ziel der Arbeit

Diese Arbeit nimmt sich die Beantwortung der Frage zum Ziel, welche Möglichkeiten zur Absicherung der mobilen Geräte in der Informationstechnik (IT) existieren und welche das IT-Fachpersonal am geeignetsten ansieht. Dabei muss zusätzlich auch erörtert werden, welche einzigartigen Gefahren es im Bereich Mobile Computing gibt. Im Vorfeld werden daher Hypothesen aufgestellt, wie sich das IT-Personal auf diese Problemstellung vorbereiten kann. Für die Beantwortung dieser Hypothesen werden Experten und Expertinnen aus dem Bereich der IT befragt und die daraus folgenden Resultate anschließend ausgewertet.

1.2 Motivation

Die berufliche Tätigkeit des Autors im Bereich der IT-Sicherheit und ein zusätzliches privates Interesse sind die Hauptmotivationsfaktoren für die Themenwahl dieser Masterarbeit. Mit der immer häufigeren Möglichkeit, die Arbeit im Homeoffice zu verrichten oder aufgrund der steigenden

Globalisierung eine Dienstreise durchzuführen, werden Mitarbeiter und Mitarbeiterinnen, sowie das IT-Fachpersonal auf neue Proben gestellt. Wichtig ist hierbei vor allem, aufgrund Verordnungen wie der Datenschutz-Grundverordnung (DSGVO), die Sicherheit aller sensiblen oder anderweitig vertraulichen Daten eines Unternehmens sicherzustellen.

1.3 Aufbau und Methodik der Arbeit

Die folgende Arbeit besteht zur ersten Hälfte aus einer Recherche von Fachliteratur, welche sich mit präventiven und reaktiven Aktionen für die Sicherheit im Bereich des Mobile Computings beschäftigt. Hierbei wird ein zusätzliches Augenmerk auf den Einbezug von möglichen Angriffsvektoren gelegt, welche es aufgrund der Unterschiedlichkeit der eingesetzten Geräte und Applikationen im Unternehmensumfeld gibt.

Der zweite Teil der Arbeit beinhaltet das Aufstellen von Hypothesen und die anschließende Beantwortung dieser. Die Beantwortung wird mithilfe von Expertengesprächen vorgenommen. Den Experten und Expertinnen werden einige Fragen vorgelegt, welche qualitative Antworten zulassen sollen.

Zusätzlich zur Befragung werden andere Details zu den jeweiligen Experten und Expertinnen erhoben, um eventuelle Korrelationen über berufliche Erfahrungen und der allgemeinen Einstellung zur Daten- und IT-Sicherheit feststellen zu können.

1.4 Hypothesen

Obwohl die Meinung, dass die IT-Sicherheit unabdingbar für das eigene Unternehmen ist, grundsätzlich überall angenommen wird, gibt es sehr unterschiedliche Grade, wie wichtig diese empfunden wird. Die in dieser Masterarbeit vorab aufgestellten Hypothesen werden mithilfe von Expertengesprächen geprüft und anschließend widerlegt oder bestätigt. Falls es aufgrund fehlender oder unzureichender Daten nicht möglich ist, diese zu beweisen, werden diese als „nicht belegbar“ kategorisiert.

> *Hypothese 1: Durch das Eintreten der COVID-Pandemie stieg das Sicherheitsbewusstsein im Bereich des Mobile Computings.*

Die erste Hypothese soll mit Daten beweisen, dass durch das Eintreten der Coronavirus disease (COVID) Pandemie und den damit einhergehenden Homeoffice-Regelungen das Sicherheitsbewusstsein in Unternehmen gestiegen ist.

> *Hypothese 2: Unternehmen sind gut auf den physikalischen Diebstahl von mobilen Geräten vorbereitet, weshalb ein solcher in den meisten Umständen nur wenig Schaden verursacht.*

Die Überlegung für die zweite Hypothese ist es, dass Unternehmen bereits ausreichend auf einen möglichen Diebstahl von mobilen Geräten vorbereitet sind. Der Schaden gegenüber solchen Ereignissen ist aufgrund von branchenüblichen Standards in den meisten Fällen sehr gering.

Hypothese 3: Großunternehmen (> 250 Mitarbeiter) besitzen bereits ein Mobile Device Management System, oder arbeiten derzeit an der Implementierung eines solchen um notwendige Sicherheitsvorschriften auf mobilen Geräten umsetzen zu können.

Hypothese 3 hat die Überlegung, dass Unternehmen ab einer bestimmten Mitarbeiteranzahl, welche der Autor hier mit 250 Personen festgelegt hat, nicht mehr auf ein Mobile Device Management System verzichten können. Ein Mobile Device Management System wird ab diesen Größen notwendig, um die Sicherheit der verschiedenen mobilen Geräte im Unternehmensumfeld sicherstellen zu können.

Hypothese 4: Der Sicherheitsaspekt von Unternehmensfremden Applikationen auf Mobiltelefonen wird derzeit noch unzureichend überwacht, weswegen solche ein mögliches Sicherheitsrisiko darstellen.

Hypothese 4 soll beweisen, dass Applikationen von Drittherstellern, welche auf Mobiltelefonen installiert werden können, derzeit noch ungenügend von Unternehmen überwacht werden. Applikationen mit unzureichender Sicherheit können daher ein Sicherheitsrisiko für das eigene Unternehmen darstellen.

1.5 Kapitelüberblick

Folgend auf die Einleitung in Kapitel 1 werden in Kapitel 2 die Grundlagen der Arbeit näher erläutert. Dabei wird der Begriff des „Mobile Computings“ erörtert und die Datenschutz-Grundverordnung von ihrer rechtlichen Seite betrachtet.

Im dritten Kapitel werden potenzielle Gefahren, aber auch Schutzmaßnahmen für die Unternehmen, näher erläutert. Einige Gefahren wie der Diebstahl des Unternehmenseigentums sind dabei sehr offensichtlich und Unternehmen besitzen eine angemessene Anzahl von Standards, um sich gegen diese vorzubereiten. Die Gefahr, welche von Schadsoftwares ausgeht, ist hierbei schwerer zu generalisieren. Während ein Virus oder eine Ransomware ein einziges Gerät stilllegen kann, kann ein Computerwurm das ganze Unternehmen gefährden.

Kapitel 4 brachtet weitere Angriffsvektoren, welche bei einem Angriff auf die Geräte oder das Netzwerk des Unternehmens verwendet werden können. Eine der Gefahren sind hierbei die unterschiedlichen Schnittstellen, welche durch die Verwendung von bestimmten Geräten wie dem Bash Bunny eine einzigartige Gefahrenquelle darstellen. Das Kapitel betrachtet des Weiteren auch die Kabellosen-Technologien wie Bluetooth und die Angriffsmöglichkeiten, welche über diese existieren. Schlussendlich wird auf die Gefahr, welche durch E-Mails gegeben ist, näher eingegangen.

Kapitel 5 betrachtet kurz, welche Möglichkeiten ein Unternehmen besitzt, externe Assets durch Penetration-Testing abzusichern. Das Unternehmen versucht dabei wie ein Angreifer oder eine Angreiferin die Schwachstellen der Systeme zu erkennen und diese eventuell auszunützen, um den Angriffsweg zu erkennen und schlussendlich absichern zu können.

Das sechste Kapitel betrachtet den Einsatz von Mobiltelefonen im Unternehmen. Dabei werden die Bedrohungen von diesen näher erläutert und der Einsatz von Enterprise Mobility Management betrachtet, um die Mobiltelefone abzusichern.

Kapitel 6 beendet den theoretischen Teil dieser Arbeit, ab Kapitel 7 wird der Fokus auf den praktischen Teil gelegt. Kapitel 7 beginnt daher mit der Überlegung der Experteninterviews, wie die Daten dazu erhoben werden und welche Experten für die Interviews ausgewählt werden. Der Ablauf des Interviews und dessen Abschluss werden an dieser Stelle auch näher definiert, um einen Standard für die folgenden Interviews zu besitzen.

Das achte Kapitel bildet den Leitfaden für die Interviews. Dabei wird der Fokus auf den Aufbau der Fragen und den Einsatz der Methode, in diesem Fall die qualitative Inhaltsanalyse nach Mayring, gesetzt.

Kapitel 9 folgt anschließend mit der Auswertung und Analyse der Interviews. Dabei werden aus den Aussagen der Experten nach Mayrings System Kategorien gebildet, um die Aussagen der Experten zu vergleichen. Im Anschluss wird Schritt für Schritt jede Hypothese mit Mayrings Methode beantwortet.

Die Arbeit endet mit dem zehnten Kapitel. In diesem wird die Conclusio gebildet und der weitere Ausblick dieser Arbeit betrachtet.

2 GRUNDLAGEN

As a result of a single successful cyber-attack a person may lose all data, a critical infrastructure may stop working and even lead to human casualties. In my opinion cybersecurity tolerates no compromises. (Kaspersky, 2017)

Mit steigender Rechenleistung konnten sich Mobilgeräte im letzten Jahrzehnt zur Standardausrüstung im Unternehmensumfeld durchsetzen. In vielen Unternehmen werden aus Gründen der Mobilität, Kostengründen und der Platzersparnis keine Desktop-PCs mehr gekauft. An deren Stelle erhalten Mitarbeiter und Mitarbeiterinnen nun Mobilgeräte, üblicherweise ein Notebook, aber auch je nach Beschäftigungsgrad, ein Mobiltelefon.

Ein Notebook bietet für den Großteil der Mitarbeiter und Mitarbeiterinnen in einem Unternehmen nur Vorteile gegenüber einem Desktop-PC. Nur für Mitarbeiter und Mitarbeiterinnen, welche ihre Arbeit in Bereichen vollrichten, die eine hohe Rechenleistung benötigen, wie Grafik- und Videobearbeitung, reicht die mangelnde Leistung oftmals nicht. Zusätzlich bieten diese oft auch wenigen Möglichkeiten im Bereich der Hardwareverbesserung und müssen daher komplett gegen ein neues Modell ausgetauscht werden.

Mit den Vorteilen von Mobilgeräten kommen entstehen jedoch auch einige einzigartige Gefahren, welche von den IT-Administratoren und IT-Administratorinnen so gut wie möglich gemildert werden müssen. Hierbei muss jedoch auch immer auf den Balanceakt zwischen Datensicherheit und Privatsphäre geachtet werden, da davon ausgegangen werden kann, dass wenn das Personal die Möglichkeit erhält mobile Geräte vom Arbeitsplatz mitnehmen zu können, diese auch vermehrt für private Zwecke verwendet werden.

2.1 Mobile Computing

Bereits im Namen des Begriffes „Mobile Computing“ wird der Sinn dessen schnell klar, hierbei wird von Computern gesprochen, welche den Zweck haben, für den Benutzer leicht transportabel zu sein. Die Zeiten von Desktop-PCs in der Firmenumgebung neigen sich dem Ende zu und diese werden nur noch in Bereichen benötigt, welche eine hohe Rechenleistung erfordern.

Im Gegensatz dazu profitieren die restlichen Mitarbeiter eines Unternehmens nur davon, wenn der eigene Rechner tragbar ist. Mitarbeiter erhalten damit die Möglichkeit, schnell in andere Räume zu wechseln, diesen mit nach Hause zu nehmen oder ihn auf andere Firmenreise mitzunehmen.

Die Nachteile von Mobile Computing dürfen von Unternehmen jedoch nicht vergessen werden. Jeder Mitarbeiter oder jede Mitarbeiterin, welche mit einem Mobiltelefon oder einem Notebook ausgestattet wird, muss sich um dieses besonders kümmern, wenn es vom Arbeitsplatz entfernt wird. Jede IT-Abteilung muss sich darauf vorbereiten, dass die Mitarbeiter oder Mitarbeiterinnen die Geräte verlieren könnten oder diese gestohlen werden.

In vielen Unternehmen wird daher gefordert, dass sensitive Daten nicht auf den Geräten gespeichert werden und diese nur auf Cloud- oder Firmeninternen-Plattformen gespeichert werden dürfen.

Obwohl der Diebstahl eines Gerätes die oft leichteste Variante darstellt, an die Daten eines fremden Unternehmens zu kommen, so gibt es natürlich auch andere und mehr subtile Wege um an Informationen des Unternehmens zu gelangen oder dessen Schwachstellen für anderweitige böswillige Absichten ausnützen zu können. Auf einige Möglichkeiten wird dabei in Punkt 4 näher eingegangen.

2.2 Datenlecks und die Datenschutz-Grundverordnung

Am 25. Mai 2016 trat für die Mitgliedsstaaten der Europäischen Union die Datenschutz-Grundverordnung in Kraft. Zwei Jahre später, am 25. Mai 2018, wurde diese Pflicht und muss von Unternehmen und öffentlichen Einrichtungen eingehalten werden. Das Ziel der Verordnung ist die Regelung und der Schutz der personenbezogenen Daten und auch Unternehmen, welche ihren Sitz außerhalb der Europäischen Union haben, müssen die Richtlinien anwenden, falls Daten von europäischen Bürgern und Bürgerinnen verarbeitet werden.

Mit insgesamt 99 Artikeln stellt die Datenschutz-Grundverordnung ein massives Projekt der Europäischen Union dar und schützt deren Bewohner und Bewohnerinnen im digitalen Zeitalter. Obwohl die Datenschutz-Grundverordnung für die einzelnen Bewohner und Bewohnerinnen der Europäischen Union größtenteils positive Regelungen bietet, so führt diese bei Unternehmen oft zu Kopfzerbrechen.

Mit der Einführung der Datenschutz-Grundverordnung müssen Unternehmen, welche ein Datenleck entdecken, dieses nun innerhalb 72 Stunden an eine zuständige Aufsichtsbehörde melden. Dies wird in Artikel 33 der Datenschutz-Grundverordnung beschrieben:

> *Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 51 zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen. (Art. 33 Datenschutz-Grundverordnung)*

Das Problem für viele Unternehmen an Artikel 33 besteht dabei, dass das IT-Personal einige Zeit benötigt, um das Ausmaß des Datenlecks zu evaluieren. Die IT-Fachkräfte müssen hierbei zuerst evaluieren, ob überhaupt sensible Daten entwendet wurden. Falls keine sensiblen Daten betroffen waren, muss dies nicht weiter gemeldet werden und kann vom Unternehmen intern behandelt werden. Falls es jedoch zu einer Entwendung von sensiblen Daten kam, dann muss schnellstmöglich evaluiert werden, welche Daten betroffen sind und was das Ausmaß des Datenlecks war.

Je nach betroffener Applikation und System kann sich dies als große Herausforderung herausstellen, besonders wenn vom Personal festgestellt wird, dass kein ausreichendes Logging betrieben wurde.

Nachdem die Aufsichtsbehörde laut Artikel 33 informiert wurde, müssen zusätzlich auch die Betroffenen des Datenlecks so schnell wie möglich informiert werden. Dies wird folglich in Artikel 34 der Datenschutz-Grundverordnung festgehalten:

> *Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Verantwortliche die betroffene Person unverzüglich von der Verletzung. (Art. 34 Datenschutz-Grundverordnung)*

Nicht immer muss bei der Auslösung von Artikel 33, die Meldung an die Datenschutzbehörde, auch Artikel 34 vom Unternehmen eingeleitet werden. Ein Beispiel wäre hierbei, dass die entwendeten Daten zwar sensibel sind, aber dank einer zuvor gut gewählten Kryptographie stark verschlüsselt wurden und damit für den Angreifer oder die Angreiferin wertlos sind.

Üblicherweise sollte das Unternehmen anschließend alle Betroffenen direkt kontaktieren. Stellt sich dies aber als zu große Herausforderung dar, da zu viele Personen betroffen wurden, kann dies aber auch durch eine öffentliche Bekanntmachung wie einer Pressekonferenz vom Unternehmen erfolgen.

Von einem Datenleck oder ab und an auch als Datenpanne bekannt, wird dann gesprochen, wenn es zu einem ungewünschten Verlust von Daten kommt. Dabei handelt es sich immer um vertrauliche Daten, wobei sich das Hauptaugenmerk hierbei auf personenbezogene Daten bezieht. (Artikel 29 Datenschutzgruppe, 2017)

Die Gründe, wie es zu einem Datenleck kommen kann, sind vielfältig. Üblicherweise wird angenommen, dass ein Angreifer oder eine Angreiferin eine Schwachstelle im System findet und sich somit Zugang zum gewünschten System verschafft, aber dies ist nicht immer so. Dank einer Studie des Unternehmens Verizon können die potenziellen Angriffsvektoren mit 3950 dokumentierten Datenlecks wie folgt aufgeschlüsselt werden:

Angriffsvektor	**Prozentueller Anteil**
Hacking	45 %
Menschlicher Fehler	22 %
Social Engineering	22 %
Malware	17 %
Unbefugter Zugriff von unternehmensinternen Personen	8 %
Physikalischer Zugriff	4 %

Tabelle 1: Angriffsvektoren (Verizon, 2020)

Es wird schnell erkenntlich, dass normale Hacking-Angriffe nur 45 % der gesamten Angriffe in Anspruch nehmen. Das Hauptaugenmerk dieser Arbeit konzentriert sich aber nicht auf diese 45 %, da es Angreifer und Angreiferinnen üblicherweise bei einer solchen Attacke es nicht auf die mobilen Geräte der Benutzer oder Benutzerinnen absehen, sondern auf Server und Datenbanken, wo eine größere Anzahl von Ressourcen gespeichert werden.

Datenlecks müssen aber nicht zwingend durch Angreifer mit böswilligen Absichten durchgeführt werden. 22 % aller Angriffe geschieht aufgrund von menschlichen Fehlern. Üblicherweise wird darunter verstanden, dass die falschen Dokumente oder Informationen an irrtümliche Personen geschickt oder übergeben wird. Ein weiteres Beispiel wäre es auch, dass bestimmte Daten vom IT-Personal ungeschützt online gestellt werden und jede Person diese problemlos herunterladen kann.

Hand in Hand mit den menschlichen Fehlern geht der unbefugte Zugriff von unternehmensinternen Personen her. Hierbei wird schnell an einen böswilligen Zugriff gedacht, wie unter anderem der Whistleblower Edward Snowden, welcher die Daten von der amerikanischen National Security Agency entwendet hat, aber dies ist nicht zwingend so. Mitarbeiter oder die Mitarbeiterinnen können die Daten unbeabsichtigt erhalten haben, besonders wenn diese zuvor nicht mit wirksamen Zugriffsberechtigungen ausgestattet wurden.

Gleichauf mit den menschlichen Fehlern stehen Social Engineering Angriffe. Warum diese auch für Mitarbeiter und Mitarbeiterinnen mit mobilen Geräten eine große Bedrohung darstellen und welche Möglichkeiten ein Unternehmen hat, gegen diese vorzugehen, wird näher in Kapitel 3 erörtert.

Die Chance von 17 % von Malware sagt klar aus, dass es einige Probleme gibt. Erstens gelangt diese auf den Rechner eines Mitarbeiters oder einer Mitarbeiterin. Hier könnte wieder übereilt angenommen werden, dass diese von böswilligen Hackern und Hackerinnen platziert werden, aber die Realität ist zumeist so, dass Benutzer und Benutzerinnen selbst Schadsoftware herunterladen. Oft, weil sie erwarten, dass diese einen Nutzen haben, aber anschließend in Wirklichkeit einen Schaden am Gerät anrichten. Diese Art der Schadsoftware wird als Trojan Horse bezeichnet.

Zweitens sagt die Malwarechance auch aus, dass es einige Probleme mit Antivirenlösungen gibt. Vom Unternehmen können unzureichende Produkte gewählt worden sein, oder diese wurden zu schwach konfiguriert und lassen zu viel Unbekanntes durch, oder aber es mangelt an Updates bei den Antivirenlösungen und diese erkennen den Schadcode nicht.

Zuletzt bleiben die physikalischen Zugriffe mit 4 % über. Dies ist glücklicherweise ein recht geringer Wert. Angreifern gelingt es also nur in seltensten Fällen einen physikalischen Zugriff auf die Hardware zu erhalten.

3 GEFAHREN UND SCHUTZ

Der Schutz von Mobilgeräten gewinnt immer mehr an Wichtigkeit. Eine gewagte Aussage, hat diese doch bereits einen so hohen Stellenwert in Unternehmen, welche Mobilgeräte an die Mitarbeiter und Mitarbeiterinnen ausgeben. Besonders seit dem Eintreten der DSGVO hat die Empfundene Wichtigkeit aber nochmals spürbar zugenommen. Kein Betrieb möchte, dass ein Notebook eines Mitarbeiters, auf welchen zusätzlich kritische Kundendaten und unternehmensinterne sensible Daten gespeichert waren, verlieren und die Schmach eines solchen Fehlers durchgehen.

Die Frage ist nun nur, wie beginnt ein Unternehmen. Die möglichen Angriffsvektoren von Mobilgeräten sind sehr hoch, besonders daher, da viele verschiedene Geräte in die Kategorie der „mobilen Geräte“ fallen. Das folgende Kapitel versucht eine Vielzahl dieser Gefahren aufzulisten und zu erklären und schlussendlich auch die möglichen Schutzmöglichkeiten dieser zu erörtern. Nicht jede hier aufgelistete Bedrohung ist eine reine Bedrohung für mobile Geräte, viele davon, wie beispielsweise Viren, stellen natürlich auch eine Gefahr für Geräte ohne mobile Komponente dar.

3.1 Bedrohungen und Schutzmöglichkeiten

Im folgenden Unterkapitel werden einige Bedrohungen für mobile Geräte näher erleuchtet.

3.1.1 Diebstahl

Der Diebstahl von mobilen Geräten ist eine der simpelsten, aber oftmals konstantesten Gefahren für Unternehmen. Der Verlust der Hardware kann sich aus mehreren Situationen ergeben. So kann das mobile Gerät einem Benutzer oder einer Benutzerin in einem Café oder Gaststätte am Abend gestohlen werden, oder der Nutzer oder die Nutzerin können dies auch einfach irgendwo verlieren oder vergessen und das Gerät wird nicht bei einer örtlichen Fundstelle gemeldet.

Die Frage für Unternehmen ab einer bestimmten Größe stellt sich nicht, ob so etwas passieren wird, sondern wann. Größere Unternehmen müssen sich jedoch darauf einstellen, dass solche Ereignisse keine Einzelfälle sind und zu hoher Wahrscheinlichkeit monatlich, wenn nicht sogar häufiger, eintreffen werden. Die Wahrscheinlichkeit, dass ein Unternehmen ein Datenleck in den nächsten zwei Jahren haben wird, ist laut einer Studie des Unternehmens IBM bei 29.6 %. Dieser Wert steigt auch ständig mit einer Steigung von 31 % seit dem Jahr 2014. (IBM Security, 2019)

Ohne gut getroffene Sicherheitsmaßnahmen kann der Schaden einer solchen Situation sehr hoch sein. Dabei wird nicht nur der finanzielle Schaden gemeint, sondern auch der Rufschaden, welcher bei einem Unternehmen entstehen kann, bei welchem ein Datenleck auftritt.

Wie schwer sich ein Datenleck eines Unternehmens auswirken kann, kann sehr gut anhand des Unternehmens Equifax betrachtet werden. Der Aktienwert des Unternehmens sank nach dem Bekanntwerden des Skandals in kurzer Zeit um 33 %.

Equifax is down 33%, falling from $143 to $96, since the news broke on September 7 that it had been hacked. Some might say the market has over-reacted. But, the scale of the data breach is breathtaking. Personal data on 143 million consumers has been stolen, putting 44% of America's population and Equifax's future at risk. (Kam, 2017)

Gefahr besteht auch, wenn auf dem Mobilgerät Kundendaten lokal abgespeichert wurden. Bei einem nicht ausreichend geschützten Gerät muss anschließend bei einem Verlust angenommen werden, dass die Daten geleakt wurden. Ein bekannter Fall ist dabei der Verlust eines unverschlüsselten Universal Serial Bus (USB) Sticks des Flughafens Heathrow mit mehr als 1000 Daten. (Morris, 2018)

Hierbei sind unter Mobilgeräten nicht ausschließlich Notebooks gemeint. Auch ein verlorenes Mobiltelefon kann dank eines immer größer werdenden Speichers immer mehr Daten beinhalten. Beispielsweise können alle Kontaktinformationen von Kollegen und Kolleginnen sowie Kunden und Kundinnen automatisch von der Cloud lokal auf das Gerät synchronisiert werden. Ein verlorenes Mobiltelefon mit einem schwachen Bildschirmsperrcode kann somit für einen großen Leak sorgen.

3.1.2 Schadensmilderung von Diebstählen

Diebstähle können mit mobilen Geräten nicht verhindert werden. Sobald die Mitarbeiter und Mitarbeiterinnen des Unternehmens die Erlaubnis erhalten die Geräte vom Arbeitsplatz mit nachhause zu nehmen, werden früher oder später auch einige diesen verloren gehen oder gestohlen werden.

Eine komplette Vermeidung des Problems ist daher nicht möglich und es müssen Wege zur bestmöglichen Schadensminderung getroffen werden. Die bestmögliche Situation wäre daher, dass nur die Hardware verloren oder gestohlen wurde, aber die Sicherheit der Daten ohne jegliche Zweifel garantiert werden kann.

Die beste Möglichkeit dafür ist die Verschlüsselung der mobilen Geräte und der Applikationen. Bestmöglich wird der Schlüssel noch direkt vor dem Start des Betriebssystems vom Benutzer oder von der Benutzerin verlangt, um zu verhindern, dass keine Sicherheitslücken des Betriebssystems selbst von einem potenziellen Angreifer oder einer Angreiferin ausgenützt werden könnten. (Afonin, 2020)

Eine weitere Maßnahme, die von dem IT-Personal getroffen werden kann, ist die Durchführung einer Fern-Löschung. Diese sollte im besten Fall nicht notwendig sein, da der potenzielle Angreifer oder die Angreiferin keine Möglichkeit haben sollten das Gerät, ohne den passenden Schlüssel zu starten. Da mobile Geräte aber aufgrund ihrer immer länger werdenden Batteriekapazität oftmals nicht mehr abgeschaltet werden, besteht die Möglichkeit, dass ein Angreifer oder eine Angreiferin sich diesen Schritt ersparen kann.

Die Initialisierung einer Fernlöschung kann nur mit spezieller Software wie dem Microsoft System Center Configuration Manager oder dem Microsoft Endpoint Manager durchgeführt werden. Sobald dieser das Gerät online findet, wird die umgehende Löschung dieses durchgeführt. Womit ein Angreifer oder eine Angreiferin jeglichen Nutzen für das Gerät verlieren würde. (Microsoft, 2020)

Auch Mobiltelefone können mit Enterprise Mobility Management von der IT-Abteilung eines Unternehmens ausreichend geschützt werden. Verschlüsselungen der Hardware sind gleich wie bei Notebooks heutzutage kein Problem mehr. Der Schutz von Mobiltelefonen wird nochmals genauer in Punkt 6 durchleuchtet.

Zuletzt muss noch kurz die Tatsache erleuchtet werden, dass oftmals andere Dokumente bei einem Diebstahl mit entwendet werden. Ist dies bei dem Diebstahl des Mobiltelefons eher unwahrscheinlich, ist es aber bei einem Notebook meist so, dass dieses nicht für sich allein, sondern mitsamt der Tragetasche entwendet wird.

Die Aufbewahrungstasche für das Notebook kann für Angreifer und Angreiferinnen einen großen Bonus bringen. In dieser sind oftmals zusätzliche Dokumente zu Projekten oder Kunden enthalten und mit etwas Glück für den Angreifer oder die Angreiferin auch Passwörter oder andere Informationen, welche zum Erraten des Passwortes von Nutzen sein könnten.

Um diese Art von Datenlecks, welche in einer Tragetasche mitgeführt werden, vorbeugen zu können, müssen unternehmensweite Regelungen gesetzt werden. Diese müssen zusätzlich den Mitarbeitern näher beigebracht werden durch Trainings oder Meetings mit diesem Thema.

3.1.3 Passwort Rücksetzung

Falls ein Angreifer oder eine Angreiferin Zugriff auf ein Gerät erhält welches nicht durch eine Laufwerksverschlüsselung wie Bitlocker gesperrt ist und damit einhergehend nicht ausgeschalten ist, kann es für einen Angreifer sehr einfach sein, sich den Zugriff zu einem lokalen User zu verschaffen.

Die Passwörter von lokalen Usern können mithilfe von Softwareprodukten von Drittanbietern mit Leichtigkeit zurückgesetzt werden. Angreifer und Angreiferinnen können an dieser Stelle die Privilegien von den Benutzeraccounts erhöhen und diese gleich zu lokalen Administratoren aufstufen.

Mitarbeiter und Mitarbeiterinnen von größeren Unternehmen erhalten meist keine lokalen Benutzer mehr, sondern Active Directory Benutzer und auch im privaten Bereich drängt Windows 10 die Benutzer dazu, dass diese ein Microsoft-Konto anlegen und kein lokales Profil verwenden.

Oftmals ist es jedoch weiterhin so, dass Unternehmen sich dazu entschließen, einige lokale Benutzer im Betriebssystem zu platzieren. Ein Grund dafür wäre beispielsweise jener, dass die Support-Abteilung diese verwenden könnten, um Benutzer zu unterstützten, falls diese unterschiedliche Probleme hätten und sich nicht im Firmennetzwerk befinden.

Dafür müssen Angreifer und Angreiferinnen nicht einmal Geld ausgeben. Tools, mit welchen die Passwörter von lokalen Windows Accounts zurücksetzen kann, gibt es zu Unmengen gratis im Internet.

Ein Beispiel Tool wäre dabei Chntpw, mit welchen jeder, nachdem er eine CD gebrannt hat oder einen USB-Stick damit bespielt hat, dass gewünschte lokale Passwort innerhalb weniger Minuten ändern kann.

Wie bereits vorher erwähnt, ist die beste Lösung gegen dieses Risiko die Einrichtung einer Laufwerksverschlüsselung. Angreifer und Angreiferinnen müssen für die Rücksetzung des Passworts zwingend den Rechner neustarten, da vom USB-Stick oder der CD mit der Drittapplikation gebootet werden muss. An dieser Stelle würden diese anschließend scheitern, die Festplatte mit dem Betriebssystem ohne das benötigte Passwort, zu laden.

3.1.4 Passwort Cracking

Oftmals gibt es für Angreifer und Angreiferinnen je nach Situation keine leichte Möglichkeit, das Kennwort zurückzusetzen oder das System anderweitig auszutricksen, um einen Zugang zu erhalten. Falls diese Möglichkeiten aber fehlschlagen besteht immer noch die Möglichkeit, das Kennwort zu erraten, um Zugang zum System zu erhalten.

Die bekannteste und simpelste Möglichkeit ist ein Brute-Force Angriff auf das Ziel. Brute Force stellt eine absolut sichere Methode dar, dass das Passwort erraten wird. Da bei einem Brute-Force Angriff aber jegliche möglichen Kombinationen versucht werden, kann ein Angriff eine lange Zeit in Anspruch nehmen. Werden simple Passwortkombinationen sehr schnell gebrochen, können lange und komplexe Passwörter mit dieser Methode Jahre in Anspruch nehmen. (Kofler et al., 2018)

Die Anzahl der zu errechnenden Passwortmöglichkeiten bei einem Brute-Force Angriff kann mit der Formel `(Anzahl der Zeichen) ^ Passwortlänge` berechnet werden. Nimmt man nun die 26 Zeichen des deutschen Alphabets ohne Umlaute und ein Kennwort der Länge von 5 Zeichen, so ergibt sich folgende Rechnung:

`26 ^ 5 = 11.881.376` mögliche Kombinationen.

Da mithilfe von modernen Grafikkarten mehrere Millionen Hashes in der Sekunde getestet werden können, zeigt dies schnell, wie anfällig ein zu kurzes Passwort mit geringer Zeichenwahl ist. Üblicherweise ist es nun, dass ein Kennwort mit bestimmter Länge gewählt wird und in dieses Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen enthält, um eine möglichst große Anzahl an Zeichen zu besitzen. Dies würde die Anzahl der möglichen Kombinationen auf das Folgende ändern, wenn die Sonderzeichen ( ) [ ] { } ? ! $ % & / = * + ~ , . ; : < > - _ verwendet werden könnten und das Passwort auf 8 Stellen erhöht wird:

`(26 + 26 + 10 + 24) ^ 8 = 86 ^ 8 = 2.99217927 × 10^15` mögliche Kombinationen.

Bei einem Test von 1 Million Passwörter je Sekunden würde ein solches Passwort daher für die Dauer von 94 Jahren sicher sein. Die Anzahl der Passwortversuche bei einem Brute-Force Angriff hängt jedoch auch sehr stark vom verwendeten Hash-Verfahren ab und manche Hashes sind

schwerer zu berechnen. Als Beispiel wäre hierbei der Unterschied in der Berechnung eines MD5-Hahs-Wertes zu einer SHA-512-Brechnung. Dieser liegt bei einem Faktor von 1:25. (Kofler et al., 2018)

Eine weitere Möglichkeit ist jene der Wörterbuch Angriffes. Da Menschen sich nicht leicht Buchstabenketten ohne bestimmten Zweck merken können, verwenden diese üblicherweise Wörter als Passwörter. Ein Wörterbuchangriff nützt dieses Verhalten aus und testet bei einem Angriff mit großer Geschwindigkeit alle ihn bekannten Wörter, um den Zugriff zum System zu erhalten. Für diese Art des Angriffes gibt es im Internet leicht erhältliche Listen mit Wörtern aller Sprache und Listen der meistverwendeten Kennwörter. (Vigliarolo, 2018)

Die letzte hier beschriebene Möglichkeit ist jene des Rainbow-Table Angriffes. Hierbei werden im Vergleich zum Brute-Force Angriffes, die Hashes bereits im Vorhinein erledigt und das Ergebnis in einer Tabelle so hinterlegt, dass jeder Hash sein dazugehöriges Passwort besitzt. Anschließend werden alle Hashes der Tabelle getestet. Solche Rainbow Tables können selbst erstellt werden, aber kann auch im Internet erhalten werden. Das bekannteste Beispiel dürfte hierbei das RainbowCrack Project darstellen. Auf dieser Seite können fertige Rainbow Tables, mit einer Größe von bis zu 690 Gigabyte, erworben werden. (RainbowCrack Project, 2020)

Eine Möglichkeit sich vor Rainbow Table Angriffen schützen zu können ist der Einsatz eines Salts. Hierbei werden die Passwörter „gesalzen“ und bedeutet damit das bei der Hasherstellung der Passwörter, eine zusätzliche Zeichenkette hinzugerechnet wird und das Ergebnis damit immer ein anderes ist. Diese Zeichenkette muss aber in der Datenbank abgelegt werden, damit immer zurück gerechnet werden kann. (Arias, 2018)

In den folgenden Tabellen wird erklärt, wie die Passwörter gehashed werden und welchen Unterschied es mit einem Salt gibt, das verwendete Kennwort ist dabei „Security“ und das verwendete Hashing-Verfahren SHA1.

Benutzername	**Passwort**	**SHA1-Hash**
User	Security	F25CE1B8A399BD8621A57427A20039B4B13935DB
Admin	Security	F25CE1B8A399BD8621A57427A20039B4B13935DB

Tabelle 2: Hashing ohne Salt (Kofler et al., 2018)

Es wird schnell erkenntlich, dass beide Benutzerkonten dasselbe Passwort besitzen und auch den gleichen Hash. Sobald der Hash für das Kennwort „Security“ in einer Rainbow Table existiert, ist dieses unsicher und das Konto kann innerhalb kürzester Zeit von einem Angreifer oder einer Angreiferin übernommen werden.

Benut-zername	Passwort	Salt	SHA1-Hash
User	Security	34EKXPT	E067526108EE21EDF050128AD8736B68AACDD91F
Admin	Security	43EWKTT	5F590900F607305C769998F4DBB159C8782B6BE3

Tabelle 3: Hashing mit Salt (Kofler et al., 2018)

Dank des Salts besitzen nun beide Benutzerkonten mit demselben Kennwort unterschiedliche Hashes. Ein Rainbow Table Angriff mit einer Liste, die bereits den errechneten Hash für das Kennwort „Security“ besitzt, kann nun nicht mehr mit dieser Information allein diese zwei Benutzerkonten übernehmen.

3.1.5 Eavesdropping

Mit dem englischen Wort Eavesdropping wird veräußert, dass der Datenverkehr des Ziels belauscht wird. Dies ist seit jeher eine bekannte Gefahr für local area networks (LAN) und stellt in Zeiten von mobilen Geräten und Wireless LAN (WLAN) eine besondere Bedrohung dar, da ein potenzieller Angreifer oder eine potenzielle Angreiferin nicht mehr unmittelbaren Zugang zu einem Firmengebäude benötigt. Der Angreifer oder die Angreiferin muss sich nur in Reichweite des WLANs des Unternehmens befinden, um einen Angriff darauf starten zu können.

Um einen Lauschangriff auf ein Netzwerk starten zu können, muss der Angreifer oder die Angreiferin bereits einen Zugang zum besagten Netzwerk haben. Für den Zugang zu einem Passwortgeschützen Netzwerk können aber mehrere Möglichkeiten verwendet werden, welche in Kapitel 4.2 evaluiert werden.

Eine der bekanntesten Applikationen für das Belauschen eines Netzwerkes ist Wireshark. Aufgrund seiner vielseitigen Einsetzbarkeit ist Wireshark ein beliebtes Tool sowohl für Entwickler und Entwicklerinnen sowie Netzwerkadministratoren und Netzwerkadministratorinnen. Schlussendlich kann es auch von Angreifer und Angreiferinnen als nützliches Tool für die Analyse des Netzwerkverkehrs verwendet werden.

Administratoren und Administratorinnen können Wireshark verwenden, um Unregelmäßigkeiten im Netzwerkverkehr zu finden, oder um zu evaluieren, ob ein Gerät unerwünschte Nachrichten versendet. Im Gegensatz dazu ist der Nutzen eines Angreifers oder einer Angreiferin, dass Mitlesen von unverschlüsselten Nachrichten. Hierbei findet die Applikation dann aber auch das Ende seiner Nützlichkeit, da verschlüsselte Nachrichten wie Hypertext Transfer Protocol Secure (HTTPS) oder Secure Shell (SSH) nur als unlesbare Zeichenkette in der Oberfläche angezeigt werden.

Ein möglicher Angriff wäre daher die Platzierung eines Hotspots ohne Kennwort in der gewünschten Zielgegend des Angreifers oder der Angreiferin. Sobald sich nun jemand mit diesem verbindet und ihn verwendet, erhält der Angreifer die Möglichkeit, diesen abzuhorchen. Vorausgesetzt, dass auch hier ein unverschlüsseltes Protokoll von dem Benutzer oder von der Benutzerin verwendet wird. (Kofler et al., 2018)

3.1.6 Schadsoftware

Eine Schadsoftware ist ein Programm, welches auf dem Rechner unerwünschte und schädliche Aktionen durchführt. Schadsoftware kann unterschiedlich kategorisiert werden:

Virus - oft als unscheinbares Programm versteckt und kann beim Ausführen einen Schaden am Gerät wie die Löschung von Daten verursachen. Oftmals wird fälschlicherweise der Begriff „Virus“ als Überbegriff für alle Arten von Schadsoftware verwendet, dies ist aber nicht korrekt, da es sich hierbei um eine eigene Art handelt, die sich von den anderen unterscheidet.

Trojanisches Pferd – getarnt als nützliches Programm, welches bei der Ausführung im Hintergrund den Schaden verursacht.

Computerwurm – ein Computerwurm, ist eine Schadsoftware mit einem sehr hohen Schadenspotenzial für Unternehmen. Die Gefahr besteht darin, dass sich der Wurm über das Netzwerk eines Unternehmens weiterverbreiten und andere Geräte infizieren kann.

Rootkits – ein Rootkit ist eine Softwaresammlung, welche es sich zum Ziel nimmt, so wenige Spuren wie möglich am Zielsystem zu hinterlassen. Wurde dies einmal von einem Angreifer oder einer Angreiferin installiert, wird es für den Benutzer oder die Benutzerin sehr schwer, dieses wieder zu entfernen.

Ransomware – der Einsatz von Ransomware, einer Software, welches sich zum Ziel nimmt ein Opfer zu erpressen, gewann in den letzten Jahren immer mehr an Beliebtheit bei Angreifern und Angreiferinnen. Sobald das Opfer die Schadsoftware auf dem Rechner aktiviert hat, versucht diese die Daten jenes Gerätes zu sperren. Anschließend wird dem Opfer eine Warnung am Bildschirm angezeigt, welches die Details vermittelt wie die Sperrung aufgehoben werden kann, üblicherweise mit einer Zahladresse für die Geldüberweisung. Aufgrund der hohen Anonymität bevorzugen Angreifer und Angreiferinnen für die Überweisung normalerweise eine Bezahlung von Bitcoin. Eine der bekannteren Angriffe dieser Art, die Ransomware WannaCry, verlangte je gesperrten Rechner ein Lösegeld von 300$. Zusätzlich handelte es sich bei WannaCry um einen Computerwurm, welcher im Netzwerk andere Opfer suchen und infizieren konnte.

Abbildung 3-1 WannaCry Erpressungsnotiz (WannaCry, 2017)

Wie in Abbildung 3-1 erkenntlich, erhält ein Benutzer oder eine Benutzerin die Warnung, dass die Daten verschlüsselt wurden. Die Erklärung ist dabei detailliert genug damit auch Personen, welche nur wenig technische Erfahrung haben, den Schritten folgen können. Zusätzlich gibt es eine Zieladresse wohin die Bitcoins überwiesen werden müssen, den genauen Betrag und ein Zeitlimit, welches droht die Daten zu löschen, wenn keine Zahlung erfolgt.

Um die Sicherheit der Mitarbeiter und Mitarbeiterinnen gegen die zuvor genannten möglichen Malwares zu garantieren, gibt es für Administratoren und Administratorinnen mehrere Möglichkeiten.

Die Grundlegendste dabei ist die Verwendung eines Antivirus Programms. Aufgrund der großen Auswahl an Antiviren Software und der verschiedenen Features dieser kann sich die Auswahl auf eine bereits als großes Projekt herausstellen.

Administratoren und Administratorinnen wird die Arbeit aber aufgrund von ausführlichen Tests von unabhängigen Teststellen, wie der AV-Test GmbH, erheblich erleichtert. Mithilfe dieser unabhängigen Teststellen sinkt die Anzahl der möglichen Auswahl für Administratoren und Administratorinnen.

Eine weitere Möglichkeit ist der Einsatz einer Antispam-Lösung. Da früher oder später viele E-Mail-Adressen aufgrund Datenlecks von eigener oder fremder Seite an die Öffentlichkeit gelangen, steigt auch der Einsatz von Spammails in Unternehmensumgebungen. Um dieser steigenden Rate entgegenzukommen, gibt es einige Lösungen am Markt, welche Mails auf schädlichen

Inhalt überprüft. Wird ein solcher schädlicher Inhalt gefunden oder wird das Mail aufgrund anderer Auffälligkeiten vom System erkannt, kann dieses verworfen werden.

Eine weitere Notwendigkeit ist die regelmäßige Aktualisierung des Betriebssystems. Falls die Malware eine bekannte Sicherheitslücke verwendet, besteht die Möglichkeit, dass es bereits ein Update gibt, oder eine andere Möglichkeit zur Absicherung dieser Lücke existiert. Ein Beispiel hierfür ist wieder der WannaCry Wurmangriff. Dieser verwendete den Angriff mit den Namen EternalBlue, welcher wiederum eine Schwachstelle in Microsofts Server Message Block Protokolls ausnützte. (Islam, Oppenheim & Thomas, 2020)

Zuletzt müssen Unternehmen ihre Mitarbeiter und Mitarbeiterinnen regelmäßig Schulen. Die Mitarbeiter und Mitarbeiterinnen müssen über mögliche Gefahren regelmäßig informiert werden und sollten eine Schulung erhalten, damit schädliche Software überhaupt nicht auf das verwendete Gerät gelangt.

Für die Durchführung von Schulungen stehen den Mitarbeitern und Mitarbeiterinnen der IT-Sicherheit mehrere Möglichkeiten zur Verfügung. So bietet ein Präsenzunterricht die Möglichkeit eines aktiven Austausches mit den Mitarbeitern und Mitarbeiterinnen. Der Nachteil ist jedoch, dass bei größeren Unternehmen nicht alle Mitarbeiter und Mitarbeiterinnen anwesend sein werden.

Anders hierbei ist die Möglichkeit eines Onlinekurses, welcher direkt am eigenen Rechner abgeschlossen werden kann. Dieser steht für Mitarbeiter und Mitarbeiterinnen immer zur Verfügung, aber hat den Nachteil, dass Mitarbeiter und Mitarbeiterinnen nicht sofort nachfragen können oder den Kurs nicht die volle Aufmerksamkeit schenken und diesen so schnell wie möglich beenden.

3.1.7 Sicherheitslücken in der Firmware

> *Fehler auf Hardware- oder Firmware-Ebene werden immer häufiger, und ihre Tragweite ist enorm – zum einen sind solche Fehler betriebssystemunabhängig auszunutzen, zum anderen ist eine Behebung per Update besonders schwierig: Zwar sind bei den meisten Chips Firmware-Updates möglich, deren Durchführung ist aber bei vielen Betriebssystemen kompliziert, bei anderen gar nicht vorgesehen. Für Mitarbeiter, die für die Sicherheit einer Firma oder Organisation verantwortlich sind, ist das ein Alptraum: Müssen nun alle PCs ausgemustert werden, für die kein Firmware-Update verfügbar ist? Wer übernimmt bzw. rechtfertigt die damit verbundenen Kosten? (Kofler et al., 2018)*

Unter dem Begriff Firmware wird jene Software verstanden, welche auf der Hardware eines Gerätes eingebettet wurde. Gespeichert wird diese üblicherweise auf Flash-Speicher, wie dem Electrically Erasable Programmable Read-Only Memory (EEPROM) und stellt damit eine Zwischenschicht zwischen der Hardware und Software her.

Da Firmware so stark mit der Hardware verknüpft ist, haben Benutzer und Benutzerinnen nur wenige Möglichkeiten, auf diese einzuwirken. Dies stellt vor allem dann ein Problem dar, wenn eine Sicherheitslücke für die Firmware oder Hardware auf einem Gerät gefunden wird.

Um die Arbeit für das IT-Personal zu vereinfachen und einen Standard im Unternehmen zu haben, versuchen die meisten Unternehmen so viele Geräte eines Modells zu besitzen wie möglich. Der Nachteil dieser Standardisierung von Client und Server Hardware ist jedoch die Möglichkeit eines entstehenden Problems für die Hardware. Wird ein Fehler wie eine Sicherheitslücke in der Firmware gefunden, müssen alle verwendeten Geräte entweder auf eine fehlerfreie Version aktualisiert oder ganz ausgetauscht werden.

Die Wellen, die solche Hardware- oder Firmwarefehler schlagen können, zeigt die Entdeckung der Meltdown oder Specter Sicherheitslücken, welche im Jahr 2018 veröffentlicht wurden. Bei Meltdown handelte es sich um eine Hardware-Sicherheitslücke in Mikroprozessoren des Unternehmens Intel und ermöglichte den unautorisierten Zugriff auf den Speicher fremder Prozesse. Obwohl neuere Modelle von Intel Prozessoren diesen Fehler nicht mehr besitzen, konnte dieser auf älteren Generationen nicht vollständig behoben werden. Als Lösung gegen den Fehler für die älteren Generationen wurde von Intel ein Update veröffentlicht, welches diesen Fehler mildert und auf der Softwareebene deaktiviert. Dies hatte jedoch den Nachteil, dass Geräte mit Intel-CPUs mit Geschwindigkeitseinbußen von 5 % bis 30 % rechnen mussten. (Metz & Perlroth, 2018)

4 ANGRIFFSVEKTOREN

Ein Angriffsvektor beschreibt einen möglichen Angriffsweg im Bereich der IT-Sicherheit. Angreifer und Angreiferinnen haben den Vorteil, nur eine Schwachstelle bei einem Unternehmen finden zu müssen. Die IT-Mitarbeiter und IT-Mitarbeiterinnen eines Unternehmens müssen jedoch alle möglichen Bereiche schützen und verhindern, dass eine Schwachstelle ausgenutzt werden kann. Das folgende Kapitel betrachtet einige mögliche Angriffsvektoren näher, welche vor allem bei mobilen Geräten ausgenützt werden können.

4.1 USB-Schnittstellen

In diesem Unterkapitel werden die potenziellen Gefahren der USB-Schnittstelle näher erleuchtet. USB-Sticks bieten Benutzer und Benutzerinnen eine leichte Möglichkeit des Datentransfers und werden auch in Unternehmensumgebungen gerne verwendet. Aufgrund der Gefahren haben einige Unternehmen jedoch bereits beschlossen, die erlaubten USB-Geräte, welche an einen Rechner angeschlossen werden dürfen, stark zu limitieren. Um sicherzustellen, dass Mitarbeiter und Mitarbeiterinnen das Unternehmensnetzwerk und deren Geräte nicht in Gefahr bringen, können nur bestimmte Modellversionen von zugelassenen USB-Sticks auf den Unternehmensrechnern freigegeben werden.

Um sicherzustellen, dass ein Benutzer oder eine Benutzerin ein schädliches Gerät mit USB am Gerät verbinden, haben Angreifer und Angreiferinnen mehrere Möglichkeiten. Eine bekannte Art ist dabei der beabsichtigte Verlust eines USB-Sticks des Angreifers oder der Angreiferin. Dabei platziert der Angreifer oder die Angreiferin einen USB-Stick an einen unscheinbaren Ort in der Nähe des Zielunternehmens. Beispiele hierfür wären der Unternehmensparkplatz, ein öffentlich zugänglicher Front-Desk, oder beim Eingang des Unternehmens.

Für die Konfiguration eines schädlichen USB-Stick gibt es mehrere Möglichkeiten für Angreifer oder eine Angreiferin, welche im Folgenden kurz evaluiert werden.

4.1.1 Rubber Ducky

Ein Rubber Ducky ist ein von dem Unternehmen Hak5 erstelltes Hacking-Gerät. Sobald jenes Gerät zu einem Host angeschlossen wurde, gibt sich der Rubber Ducky, welcher von außen wie ein normaler USB-Stick wirkt, als Tastatur aus und führt anschließend vorkonfigurierte Skripte am Zielsystem aus.

Dafür wurde von dem Unternehmen Hak5 eine simple Skriptsprache konzipiert, um Payloads, ein schädliches Programm am Zielsystem auszuführen. Dank dem bereitgestellten Regelwerk der Skriptsprache, welche das DuckyScript bezeichnet wird, können Benutzer diese auch schnell selbst konfigurieren. Zusätzlich werden viele Skripte von Hak5 oder der Community öffentlich geteilt und müssen somit nur noch minimal vom Angreifer für das Ziel vorbereitet werden. (Kofler et al., 2018)

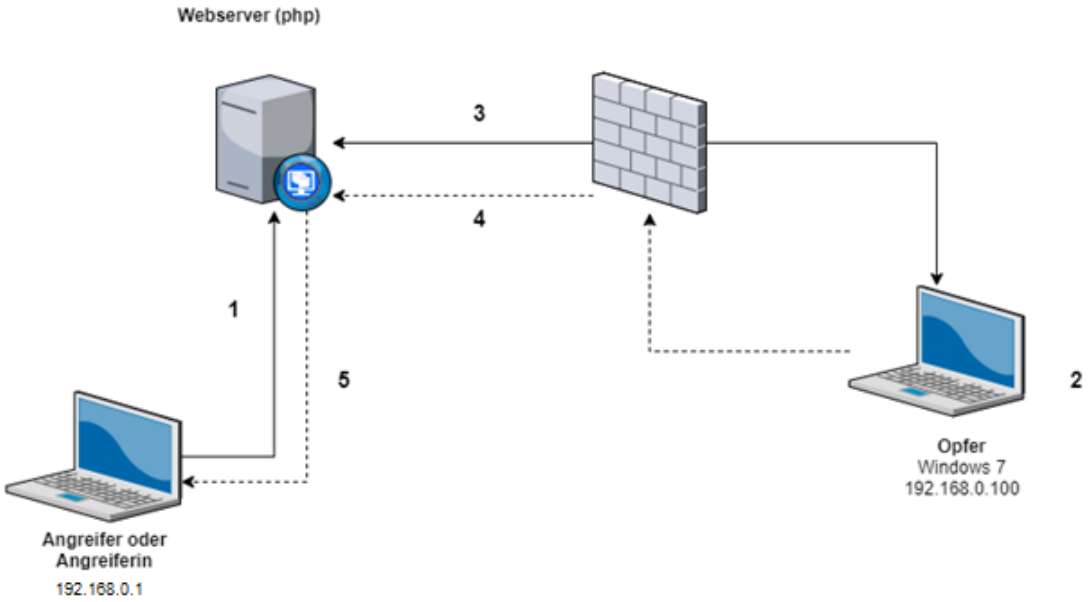

Abbildung 4-1 Passwortdiebstahl mit Rubber Ducky (Kofler et al., 2018)

Die Einsatzmöglichkeit eines Rubber Ducky und die damit verbundene Gefahr für einen Endbenutzer oder einer Endbenutzerin sind bei Anschluss des Gerätes sehr hoch. Im harmlosesten Fall für den Benutzer oder die Benutzerin plant der Angreifer oder die Angreiferin nur einen Streich, welche den Hintergrund des Benutzers oder der Benutzerin ändert oder ein Youtube-Video öffnet. Da ein Rubber Ducky aber je Stück einen hohen Anschaffungspreis besitzt, kann angenommen werden, dass ein Angreifer oder eine Angreiferin einen Rubber Ducky nicht für einen kurzweiligen Spaß verwenden würde.

Beispiele für schädliche Payloads welche zum öffentlichen Download bereitstehen, wären die Deaktivierung des Windows Defenders, das Kopieren und Ausführen von schädlichen Dateien, das Löschen von Daten oder die die Erstellung eines Backdoors.

Abbildung 4-1 zeigt, dass auch der Passwortdiebstahl mit einem zuvor konfigurierten Rubber Ducky möglich ist. Sobald der Rubber Ducky mit dem Rechner verbunden wird, führt dieser folgende Schritte aus:

1. Angreifer oder Angreiferin legt die benötigten Daten auf einem Webserver ab
2. Ruber Ducky wird am Zielsystem angesteckt
3. Mithilfe eines Skripts werden die benötigten Daten vom Webserver heruntergeladen
4. Passwörter werden ausgelesen und an den Webserver übertragen
5. Angreifer oder Angreiferin kann Passwörter im Klartext vom Webserver abrufen

Dabei wird von der Community folgender mimikatz Code zur freien Verfügbarkeit bereitgestellt: https://github.com/hak5darren/USB-Rubber-Ducky/wiki/Payload---mimikatz-payload

```
REM mimikatz
DELAY 3000
CONTROL ESCAPE
DELAY 1000
STRING cmd
DELAY 1000
CTRL-SHIFT ENTER
DELAY 1000
ALT y
DELAY 300
ENTER
STRING powershell (new-object System.Net.WebClient).DownloadFile('http://<re-
place me with webserver ip/host>/mimikatz.exe','%TEMP%\mimikatz.exe')
DELAY 300
ENTER
DELAY 3000
STRING %TEMP%\mimikatz.exe
DELAY 300
ENTER
DELAY 3000
STRING privilege::debug
DELAY 300
ENTER
DELAY 1000
STRING sekurlsa::logonPasswords full
DELAY 300
ENTER
DELAY 1000
STRING exit
DELAY 300
ENTER
DELAY 100
STRING del %TEMP%\mimikatz.exe
DELAY 300
ENTER
```

Abbildung 4-2: Mimikatz Code

Mithilfe dieses öffentlich verfügbaren Codes erhält jeder potenzielle Angreifer oder Angreiferin ein Startpaket für die Verwendung eines Rubber Duckys. Durch die einfache Art des Einsatzes und der hohen Anzahl an fertigen Skripten ist die Einstiegsbarriere für die Verwendung eines Rubber Duckys sehr gering, womit auch Angreifer und Angreiferinnen ohne großes Fachwissen diese Art des Angriffes verwenden können.

4.1.2 Bash Bunny

Der Bash Bunny ist eine Weiterentwicklung des Unternehmens Hak5 zum Vorgängermodell Rubber Ducky. Nicht zuletzt durch Vorschläge und Einbringungen der Community und von Entwicklern erhielt der Bash Bunny einige sehr nützliche neue Features. So kann der Bash Bunny, im Gegensatz zum Vorgängermodell Rubber Ducky, sich nicht nur als programmierbare Tastatur

ausgeben, sondern auch als USB-Massenspeicher, serielle Schnittstelle oder Gigabit-Ethernet-Adapter.

Mithilfe eines Hardwareschalters kann der Angreifer oder die Angreiferin zusätzlich mehrere Payloads für den Angriff vorbereiten, womit dieser oder diese flexibler auf unterschiedliche Situationen reagieren kann.

Der Bash Bunny besitzt trotz seiner kompakten und USB ähnlichen Größe eine für den Nutzen sehr gute Hardware. Ausgestattet mit einem Quad-Core Prozessor, 512 Megabyte (MB) Random-Access-Memory (RAM) und einer 8 Gigabyte (GB) Solid-State-Drive (SSD) sollten selbst längere Arbeiten für diesen kein Problem darstellen. (Hak5, 2020)

Wie der Rubber Ducky bereits zuvor versucht das Unternehmen Hak5 die Skriptsprache für den Bash Bunny so simpel wie möglich zu halten. Für die Shell-Programmierung wird dabei Bash verwendet, da das Betriebssystem des Bash Bunnys auf einer Linux-Distribution aufsetzt.

Benutzer von Rubber Ducky können die für diesen erstellten Skripts mit nur wenigen Einstellungen auf den Bash Bunny übernehmen. Dies bietet dem Bash Bunny eine sehr hohe Anzahl an fertigen Skripts für dessen Verwendung.

Zum Zeitpunkt der Erstellung dieser Arbeit ist der Bash Bunny weiterhin in aktiver Entwicklung. Aus diesem Grund besitzen die Käufer und Käuferinnen des Bash Bunnys die Möglichkeit, diesen regelmäßig zu aktualisieren. Dafür wird vom Unternehmen Hak5 der Bunny Updater angeboten, dieser erlaubt es, zügig den Bash Bunny auf die neueste Version zu updaten. (Hak5, 2020)

4.1.3 Digispark

Der Digispark ist ein weiteres Hacking-Gerät, welches ein hohes Schadenspotenzial verursachen könnte. Da der Digispark nur etwa so groß wie eine 1-Cent-Münze ist, besitzt das Gerät etwas weniger Leistung als der zuvor genannte Bash Bunny oder Rubber Ducky. Der verfügbare Speicherplatz am Gerät beträgt für den Digispark nur 6 Kilobyte (KB), aber diese Größe des Speicherplatzes ist ausreichend für einige Skripte. (Digistump, 2020)

Anders als bei dem zuvor genannten Rubber Ducky können nicht einfach neue Skripts in einem Texteditor erstellt werden, da der Digispark an die Arduino Entwicklungsumgebung gebunden ist.

Aufgrund der geringen Größe des Digispark kann dieser sehr unauffällig an Hardware angebracht werden. Erhält ein Angreifer oder eine Angreiferin Zugriff auf ein Gerät, so kann dieser oder diese den Digispark leicht am USB-Port des Gerätes angesteckt werden. Aufgrund anderer Kabel im Gerät sollte der Digispark so gut wie unsichtbar sein für das Opfer. (Kofler et al., 2018)

Ein Beispiel eines möglichen Angriffes findet sich in Abbildung 4-3. Der Digispark muss an das Gerät des Opfers angeschlossen werden, um bei diesen ein Backdoor zu schaffen. Auch dieser Angriff wird erlaubt, da der Digispark als programmierbare Tastatur vom System erkannt wird.

Der Angriff läuft anschließend mit den folgenden Schritten ab:

1. Payload wird generiert und auf dem Webserver abgespeichert, diese soll anschließend eine reverse Verbindung auf das Zielsystem durchführen
2. Das auf dem Digispark gespeicherte Skript wird ausgeführt, sobald dieser angeschlossen wird und wiederholt sich in einer Schleife.
3. Backdoor wird auf das Zielsystem heruntergeladen
4. Eine permanente Verbindung zum Zielsystem wurde aufgebaut

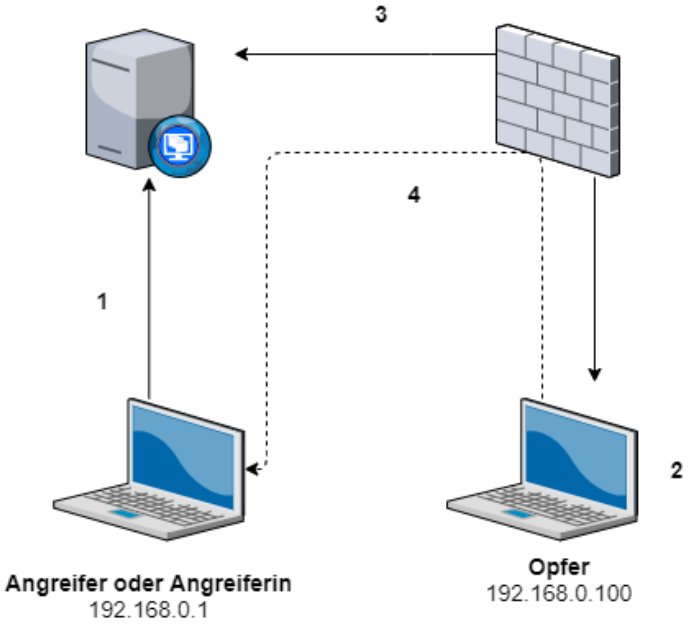

Abbildung 4-3: Linux-Backdoor mit Digispark

Aufgrund der unscheinbaren Größe und des niedrigen Preises, im Gegensatz zum Bash Bunny und Rubber Ducky, bietet der Digispark eine alternative für Angreifer und Angreiferinnen, um einen Angriff auf ein Zielsystem durchzuführen. (Kofler et al., 2018)

4.1.4 Gegenmaßnahmen

Während die vorherigen Kapitel sich damit beschäftigten, wie der Angriffsvektor USB ausgenützt werden könnte, betrachtet dieses Kapitel kurz mögliche Gegenmaßnahmen gegen solche Angriffe. Angriffe auf die USB-Schnittstelle sind jene, wo der Angreifer oder die Angreiferin beim Angriff physikalisch anwesend sein muss. Dies besitzt einige Nachteile für den Angreifer oder die Angreiferin, besonders da diese sich dem Ziel nähern müssen und somit deren Anonymität riskieren.

Es ist daher von höchster Wichtigkeit die Mitarbeiter und Mitarbeiterinnen des Unternehmens mithilfe von Schulungen auf solche Gegebenheiten vorzubereiten. Können kleinere Unternehmen diese Schulung noch durch eine physikalische Präsentation nutzen, so müssen größere Unternehmen wahrscheinlich auf Onlinekurse ausweichen.

In diesen Kursen sollte an die Mitarbeiter des Unternehmens die Gefahr von nicht vertrauenswürdigen USB-Geräten mitgegeben werden und wo solche USB-Geräte von Angreifern und Angreiferinnen platziert werden. (Kofler et al., 2018)

IT-Administratoren und IT-Administratorinnen sollten jedoch trotz ausreichender Schulung weitere Schutzmöglichkeiten aufbauen, um die Unternehmenshardware und Netzwerk zu schützen. Mit aktuellen Softwareprogrammen und Betriebssystemen besitzen Administratoren und Administratorinnen die Möglichkeit, dieses Problem von Hardware- oder Softwareseite zu lösen.

Beim Wunsch einer hardwareseitigen Lösung können IT-Administratoren und IT-Administratorinnen die nicht verwendeten USB-Ports sperren. Diese sind anschließend von niemanden mehr verwendbar. Diese Möglichkeit kann jedoch für Mitarbeiter und Mitarbeiterinnen sehr beschränkend sein und sollte daher nur verwendet werden, wenn eine sehr hohe Sicherheit für das Gerät notwendig erscheint.

Im Falle einer softwareseitigen Lösung besitzen IT-Administratoren und IT-Administratorinnen mehr Möglichkeiten, das Zielsystem anzupassen. Bei Geräten mit einem Windows Betriebssystem kann die Installation von zusätzlichen neuen Geräten unterbunden werden. Zusätzlich können nur Geräte mit einer bestimmten Hardware-ID für die Installation zugelassen und alle anderen unterbunden werden. Somit können Unternehmen alle Mitarbeiter mit der gleichen Serie von USB-Sticks ausrüsten, welche anschließend von allen Mitarbeitern und Mitarbeiterinnen auf den Firmengeräten verwendet werden könnten. (Kofler et al., 2018)

4.2 WLAN

Ein WLAN bietet für Benutzer und Benutzerinnen sowie Administratoren und Administratorinnen viele Vorteile. Nicht jede Einrichtung ermöglicht die einfache Verlegung eines Ethernet Kabels. Aufgrund der hohen Verwendung von Notebooks und Mobiltelefonen sind Nutzer und Nutzerinnen auch mehr mobil mit diesen und können die Geräte in andere Büros, Konferenzräume oder den Aufenthaltsraum bringen. Für Angreifer und Angreiferinnen bietet dies jedoch hingegen einen weiteren Angriffsvektor, welcher angewendet werden kann, um sich Zugang zum Ziel zu verschaffen.

Falls das Wired Equivalent Privacy (WEP) Verschlüsselungsprotokoll verwendet wird, ist es möglich, den Schlüssel innerhalb von wenigen Minuten zu entschlüsseln. Aufgrund einer Schwachstelle im Authentifizierungsverfahren kann innerhalb weniger Sekunden der Schlüssel von einem Angreifer oder einer Angreiferin ermittelt werden. Aufgrund dieser kritischen Schwachstelle im Protokoll wird dieses aber kaum noch verwendet und stattdessen das sichere Wi-Fi Protected Access (WPA) oder Wi-Fi Protected Access II (WPA2) Protokoll eingesetzt.

Da der WPA und WPA2 Standard derzeit als sicher gelten, stellt sich der Angriff auf ein WLAN mit diesem Protokoll als sehr aufwendig dar. Anders als beim WEP-Protokoll kann das Kennwort nicht direkt berechnet werden. Eine Möglichkeit ist die Verwendung eines Wörterbuchangriffes auf das Netzwerk. Falls ein übliches Wort, welches im Wörterbuch zu finden ist, als Kennwort gesetzt wurde, kann der Schlüssel auf diese Art erörtert werden. Im Gegensatz zu den üblichen

Brute-Force-Angriffen, welche mehrere Millionen Passwortversuche je Sekunde durchführen können, ist der Angriff auf WPA und WPA2 mit etwa 2300 Passwörter je Sekunde stark begrenzt. Da die Mindestlänge des Kennwortes zusätzlich 8 Zeichen beträgt, bedeutet dies, dass ein Kennwort mit Großbuchstaben, Kleinbuchstaben sowie Ziffern mehr als 200 Billionen mögliche Kombinationen aufweisen würde. Mit einem Durchsatz von 2300 Passwörtern die Sekunde würde sich der Angriff daher für Angreifer und Angreiferinnen als nutzlos erweisen, da dieser um die 3500 Jahre dauern würde.

Wireless Protected Setup (WPS) ist ein Standard, welcher es Benutzer und Benutzerinnen den Konfigurationsschritt beim Aufbau einer Wireless-Verbindung erleichtern soll. Dabei wird am Access-Point ein Passwort mit hoher Komplexität und Länge generiert, um diesen abzusichern. Benutzer müssen dieses Kennwort jedoch nicht verwenden und erhalten stattdessen eine 8-stellige Persönliche Identifikationsnummer (PIN), einen sogenannten WPS-PIN, welcher stattdessen eingegeben werden kann. Anschließend tauschen Client und Access-Point das komplexe WPA2 Passwort und verwenden dieses für die weitere Kommunikation. Für die Sicherheit bedeutet dies aber auch, dass das Netzwerk von einer 8-stelligen Zahl gesichert wird, welche bis zu 100 Millionen mögliche Kombinationen annehmen kann. Da der Test einer Zahl ungefähr 1 bis 2 Sekunden in Anspruch nehmen würde dies bedeuten, dass ein vollständiger Brute-Force-Angriff mehrere Jahre in Anspruch nehmen könnte. (Kofler et al., 2018)

Das WPS-Protokoll hat jedoch auch starke Nachteile, welche aufgrund des Protokolldesigns gegeben sind. Wenn das WPS-Protokoll verwendet wird, dann bestätigt der Access-Point bei einem Anmeldeversuch, ob die ersten vier Zahlen des PIN-Codes korrekt sind oder nicht. Dies bedeutet, dass im ersten Schritt nur eine vierstellige Zahl, für welche es 10.000 mögliche Kombinationen gibt, ermittelt werden muss. Anschließend müssen nur noch die folgenden drei Zahlen, ermittelt werden, da die letzte Zahl eine Prüfziffer ist welche automatisch berechnet wird. Die folgenden drei Zahlen können mit um die 1.000 Möglichkeiten ermittelt werden. Dies bedeutet, dass ein Angreifer mit insgesamt 11.000 Brute-Force-Versuchen den WPS-PIN Code ermitteln kann. (Kofler et al., 2018)

Eine Möglichkeit der Hersteller, diese Lücke abzusichern, ist die Einführung von Limitationen beim Login. Dabei erhält jede Person, welche es versucht, zu oft mit den falschen Daten anzumelden, eine zeitliche Sperre vom System.

4.3 Bluetooth

Mit einem Alter von über 30 Jahren gehört der Bluetooth Standard noch immer zu einem der meistverwendeten Technologien im Bereich der drahtlosen Übertragung und findet weiterhin ausreichend Verwendung in jeglicher mobilen Technologie wie Notebooks, Mobiltelefone und Peripheriegeräten. Bluetooth besitzt Standardgemäß eine Reichweite von 10 bis 200 Meter, aber dies könnte durch zusätzliche Komponenten wie Antennen erweitert werden.

Konkret handelt es sich bei Bluetooth um eine Netzwerktechnologie respektive Schnittstelle, mithilfe derer mobile Gerätschaften miteinander kommunizieren können. Die Übertragung von Daten erfolgt dabei über das sogenannte ISM-Band (kurz für Industrial, Scientific and Medical

Band). Es wird von Hochfrequenz-Geräten – also die Übertragung von Frequenzen über hörbare Schallwellen – genutzt. Bei Bluetooth erfolgt dies über das 2,48-GHz- und 2,4-GHz-Band. Da auch andere Funkstandards, wie zum Beispiel WLAN oder Mikrowellenherde, diese Frequenzbänder nutzen, kann es teilweise zu gegenseitigen Störungen kommen. Was dann der Unterschied zwischen WLAN und Bluetooth ist? Die grundlegende Differenz zwischen den Funkstandards stellt bei der Datenübertragung über WLAN der Mittler dar: der Router. Bluetooth kommt ohne ihn aus. Damit ein Gerät Bluetooth-fähig wird, ist ein entsprechender Chip mit Sender und Empfänger vonnöten sowie passende Software, die den Datenaustausch regelt. Der Standard ist weltweit verfügbar und kostenlos nutzbar. (Warnke, 2020)

Aufgrund seiner hohen Verfügbarkeit und der weiterhin stetigen Verwendung des Standards hat sich dieser jedoch auch als attraktiver Angriffsvektor für Angreifer und Angreiferinnen ergeben.

Eine erste Schutzmöglichkeit für jede Person wäre es, dass das Gerät, welches als Bluetooth verwenden soll, nicht sichtbar ist. Dies kann bei einigen Geräten wie PCs und Notebooks konfiguriert werden, aber diese Funktion ist nicht garantiert und oftmals nicht verfügbar für Peripheriegeräte. Angreifer und Angreiferinnen haben hingegen die Möglichkeit, auch diese unsichtbaren Geräte mit etwas Zeit und Aufwand zu identifizieren. Ein Beispiel hierfür ist das Ubertooth Projekt. Das Ubertooth Projekt ist ein Open Source Projekt und bietet verbesserte Analysemöglichkeiten für Bluetooth. (Ossmann, 2020)

Ein möglicher Angriff auf Bluetooth wäre der Crackle Exploit. Dieser nützt eine Schwachstelle im Bluetooth-Verbindungsaufbauprozess und versucht dabei den Temporary Key mithilfe eines Brute-Force-Angriffes zu ermitteln. Mithilfe des Temporary Keys kann in Folge auch der Short-Term-Key und anschließend auch der Long-Term-Key ermittelt werden welches eine komplette Entschlüsselung der Verbindung zweier Geräte erlauben würde. (Ryan, 2018)

Da der Crackle Exploit jedoch auf Basis einer Schwachstelle basiert, welche beim Verbindungsaufbau existiert, bedeutet dies auch, dass diese Schwachstelle nur beim erstmaligen Verbindungsaufbau ausgenutzt werden kann. Die Wahrscheinlichkeit für einen Angreifer oder eine Angreiferin genau jene Situation abzuwarten, um eine gewünschte Kommunikation zu entschlüsseln stellt sich in der Praxis daher als sehr schwierig dar.

4.4 Internet

Das Internet als Angriffsvektor kann als Sammelbegriff angesehen werden für jegliche Angriffe, welche online durchgeführt werden. Auch der folgende Punkt 4.5, der Angriff über Mails, stellt eine Gefahr dar welche durchgeführt werden kann, wenn das Gerät des Benutzers oder der Benutzerin online ist. Da der Angriff über Mail jedoch einen so große Gefahr darstellt, wurde es in einen eigenen Punkt ausgelagert, um die Gefahr mehr im Detail zu beschreiben.

Eine der großen Gefahren über das Internet ist der potenzielle Download von Schadsoftware für das Gerät. Die Schadsoftware kann aus den unterschiedlichsten Gründen heruntergeladen werden und nicht jede Schadsoftware verursacht sofortige Probleme am Zielsystem. Ein Beispiel

wäre hierbei Spyware verursachen andere Malwareklassifikationen einen direkten schaden, ist das Ziel einer Spyware die wie bereits im Namen erkenntliche Spionage des Opfers.

Auch die restlichen Malwareklassifikationen, welchen sehr voneinander ab und Benutzer und Benutzerinnen laden unter Umständen eine legitime wirkende Software herunter, welche sich anschließend als trojanisches Pferd herausstellt. Die genaue Definition der unterschiedlichen Arten findet sich unter Punkt 3.1.6.

Eine weitere Gefahr für Benutzer ist die häufige Wiederverwendung von Kennwörtern. Benutzer und Benutzerinnen verwenden oftmals für Accounts dieselben Kennwörter oder ändern diese nur minimal. Sobald eine Datenpanne eines Unternehmens die Passwörter der Benutzer und Benutzerinnen veröffentlicht und diese zusätzlich nicht verschlüsselt waren, dann erhalten Angreifer und Angreiferinnen die Möglichkeit, dieselben Anmeldeinformationen des Benutzers oder der Benutzerin auch auf anderen Webseiten zu testen. Dies geschieht üblicherweise automatisch, sodass Angreifer und Angreiferinnen, wenn überhaupt, nur über erfolgreiche Accountübernahmen informiert werden.

Einige Webseiten reagieren auf diese Gefahr mit spezifischen Passwortregeln, um Benutzer und Benutzerinnen zu einzigartigen Kennwörtern hinzuführen. Eine andere und mittlerweile immer beliebtere Möglichkeit ist der Einsatz von Multi-Faktor-Authentifizierung (MFA), welche den Nutzer oder die Nutzerin mindestens auf einen zweiten Faktor überprüft. Dabei gibt es mehrere unterschiedliche Möglichkeiten, um die gewünschte Person zu verifizieren, wie das Verwenden eines zusätzlichen Gerätes, ein Mobiltelefon, welches einen zusätzlichen Code erhält, oder eine biometrische Überprüfung wie ein Retinascan, Handflächenscan, oder Fingerabdruck für die Anmeldung.

Direkte Gefahren durch das Internet sind vielfältig und würden den Rahmen dieser Arbeit überschreiten. Die Absicherung vor jenen wird Benutzern und Benutzerinnen jedoch auch leichter gemacht. Dank kompetenter Antivirenprodukte, welche selbst auf privaten Geräten durch das Betriebssystem zumeist vorinstalliert wurden, werden Benutzer und Benutzerinnen oftmals vor den schlimmsten Folgen eines gefährlichen Downloads abgesichert.

Der Schutz eines Identitätsdiebstahles erfordert andererseits etwas mehr Aufwand von jeder Person. Jedoch erhalten Nutzer und Nutzerinnen auch hier Unterstützung durch die Verwendung von Passwortmanagern und modernen Browsern, welche zufällige Kennwörter anbieten und diese anschließend am Gerät speichern. Wenn ein Benutzer oder eine Benutzerin genügend unterschiedliche Kennwörter verwendet und eines dabei aufgrund eines Datenlecks öffentlich gemacht wird, dann werden jegliche Folgeschäden des Datenlecks um ein Vielfaches minimalisiert.

4.5 Mail

Aufgrund der Tatsache, dass alle Mitarbeiter und Mitarbeiterinnen, welche am Computer arbeiten, E-Mails verwenden, bietet dieser Vektor für Angreifer und Angreiferinnen eine beliebte Möglichkeit, um Zugang in das Unternehmensnetzwerk zu erhalten. Phishing-Angriffe stellen dabei eine

der größten Gefahren für Unternehmen dar, da selbst mit der besten aktuellen Antispam-Technologie weiterhin einige Spam- und Phishing-Mails den Endbenutzer oder die Endbenutzerin erreichen.

Ein Phishing-Angriff kann dabei in die Kategorien des normalen Phishing und des viel präziseren Spear-Phishing unterschieden werden. Ein Angreifer oder eine Angreiferin, welcher einen normalen Phishing-Angriff durchführt, zielt diesen nicht auf eine bestimmte Person oder ein Unternehmen ab. Vielmehr werden hier Hunderte von tausend E-Mails ausgesandt und der Angreifer oder die Angreiferin hofft dabei auf das „throw against the wall and hope that it sticks“ Prinzip. Auch wenn nur eine kleine Menge der Opfer der Phishing-Attacke auf den Angriff hereinfallen würde, wäre dies für den Angreifer oder die Angreiferin bereits ein Gewinn, da diese Art des Angriffs wenig Vorbereitung verlangt.

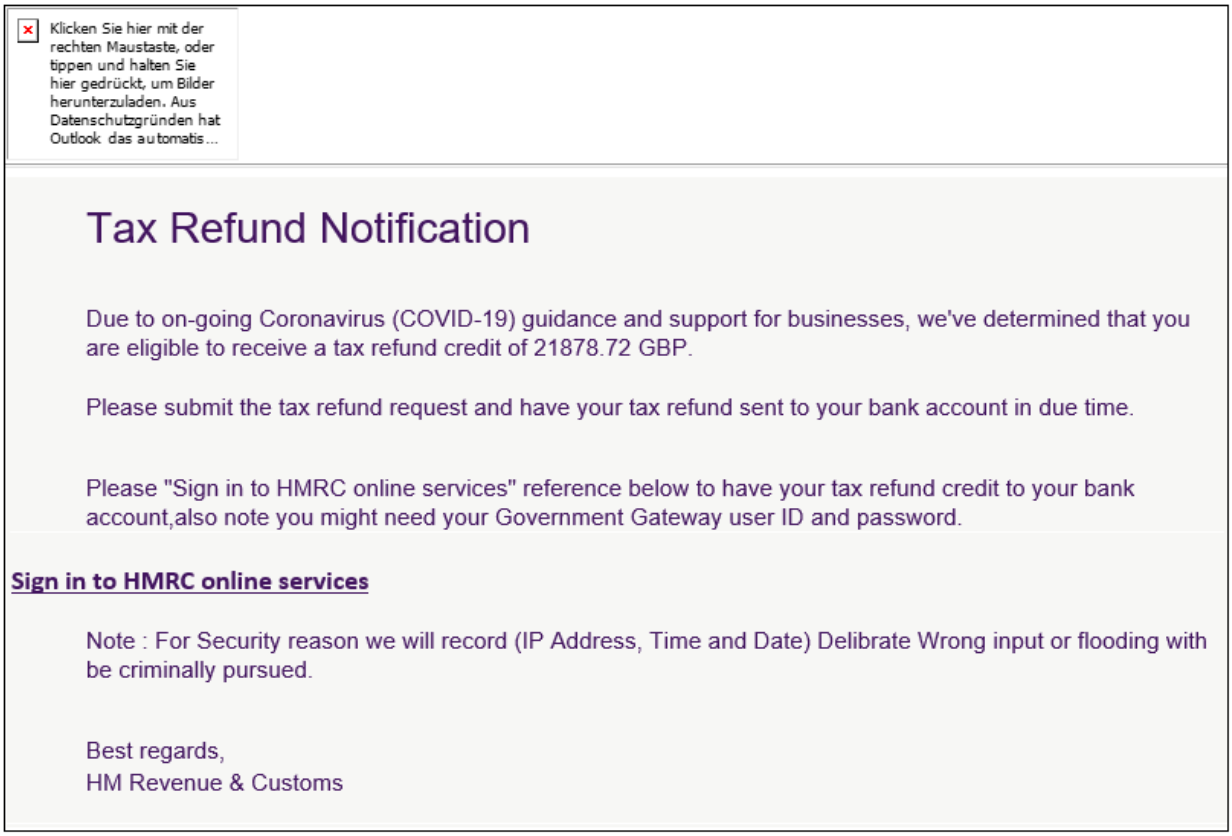

Abbildung 4-4: Phishing-Mail Beispiel

Aufgrund des fehlenden persönlichen Aspekts bei normalen Phishing-Mails versuchen Angreifer und Angreiferinnen anderweitig die Aufmerksamkeit ihrer Opfer zu erhalten. Beliebte Methoden sind hierbei der Erhalt eines Preises, eine entgeltlichen Auszahlung oder die nicht verschiebbare Dringlichkeit des Mails, wie zum Beispiel die Deaktivierung des eines Bank- oder Mailkontos.

Ähnlich, aber um einiges Gefährlicher ist jedoch ein Spear-Phishing Angriff auf eine Person oder ein Unternehmen. Anders als ein normaler Phishing-Angriff investieren die Angreifer und Angreiferinnen bei dieser Methode Zeit in die Evaluierung ihres Zieles. Die E-Mail-Adressen werden

spezifisch an das Unternehmen angepasst, um den Mitarbeitern und Mitarbeiterinnen ein Gefühl der Vertraulichkeit zu geben. Wenn ein E-Mail nicht fremd und unbekannt auf das Opfer wirkt, dann bemerkt dieser unter Umständen nicht die kleineren Fehler, welche das Phishing-Mail erkennbar machen. Je nach Unternehmensgröße kann es auch für einige Mitarbeiter und Mitarbeiterinnen schwer feststellbar sein, welches Format von anderen Abteilungen des Unternehmens eingesetzt werden.

Eine bekannte Methode, welche Angreifer und Angreiferinnen beim Spear-Phishing verwenden, ist die Erscheinung als IT-Support oder IT-Administration. Dabei werden im Mail die vom Unternehmen verwendeten Banner, Farben und Formate des Unternehmens verwendet, um den Schein der Legitimität zu erhalten.

Abbildung 4-5: Spear-Phishing Beispiel

Wie in Abbildung 4-5 ersichtlich, wird der Benutzer oder die Benutzerin des Unternehmens dazu gedrängt, den eigenen Benutzeraccount zu bestätigen oder den Zugang zu diesen zu verlieren. Obwohl der Angreifer oder die Angreiferin keine spezifischen Banner oder anderweitig verwendeten Unternehmensfarben verwendet hat, versucht dieser mit der falschen Zeile „From a trusted sender“ das Vertrauen des Opfers zu gewinnen. Da es sich hierbei um einen Spear-Phishing-Angriff handelt, wurden die persönlichen Daten des Empfängers oder der Empfängerin unkenntlich gemacht.

Die Gefahr von Phishing darf von Unternehmen auf keinen Fall übersehen werden. Laut einer Studie des Unternehmens Verizon ist Phishing für 22% der Datenlecks verantwortlich. Dabei ist das Hauptziel der Erhalt der Anmeldeinformationen eines Benutzers oder einer Benutzerin, um Zugriff auf den Account zu erhalten. (Verizon, 2020)

Eine weitere Gefahr mit der Verwendung von E-Mails ist der Empfang von Mails mit schädlichen Anhängen. Dabei ist der Text-Inhalt des Mails meist nur ein Vorwand, um eine Öffnung des Anhangs zu erreichen. Sobald der Benutzer oder die Benutzerin dieses öffnet, wird ein Schadcode ausgeführt. Die Effektivität des Angriffes hängt anschließend von einigen Faktoren wie dem verwendeten Betriebssystem, Patchlevel und der Sicherheitskonfiguration des Gerätes ab.

Da diese Art des Angriffes in den letzten Jahren aufgrund von Ransomware-Angriffen einiges an Bekanntheit gewonnen hat, verwenden Angreifer und Angreiferinnen auch hier wie bei Spear-Phishing-Angriffen verschiedenste Methoden, um das Vertrauen der Opfer zu gewinnen und diese dazu zu bewegen, den Anhang zu öffnen.

Eine weitere Methode, welche in den letzten Jahren an Häufigkeit zugenommen hat, ist der Einsatz von Erpressungsmails. Angreifer oder Angreiferinnen kontaktieren dabei Benutzer und Benutzerinnen welche Opfer eines Datenlecks wurden und versuchen diese davon zu überzeugen, dass diese peinlichen oder privaten Informationen der Person besitzen. Durch alte Passwörter von vorherigen Datenlecks versuchen Angreifer oder Angreiferinnen dabei, ihre Drohung zu unterstreichen und das Opfer davon zu überzeugen, dass diese das Gerät des Opfers gehackt hätten.

Hi, stranger!

I hacked your device, because I sent you this message from your account.
If you have already changed your password, my malware will be intercepts it every time.

You may not know me, and you are most likely wondering why you are receiving this email, right?
In fact, I posted a malicious program on adults (pornography) of some websites, and you know that you visited these websites to enjoy (you know what I mean).

While you were watching video clips,
my trojan started working as a RDP (remote desktop) with a keylogger that gave me access to your screen as well as a webcam.

Immediately after this, my program gathered all your contacts from messenger, social networks, and also by e-mail.

What I've done?
I made a double screen video.
The first part shows the video you watched (you have good taste, yes ... but strange for me and other normal people),
and the second part shows the recording of your webcam.

What should you do?

Well, I think $565 (USD dollars) is a fair price for our little secret.
You will make a bitcoin payment (if you don't know, look for "how to buy bitcoins" on Google).

BTC Address: [redacted]
(This is CASE sensitive, please copy and paste it)

Remarks:
You have 2 days (48 hours) to pay. (I have a special code, and at the moment I know that you have read this email).

If I don't get bitcoins, I will send your video to all your contacts, including family members, colleagues, etc.
However, if I am paid, I will immediately destroy the video, and my trojan will be destruct someself.

If you want to get proof, answer "Yes!" and resend this letter to youself.
And I will definitely send your video to your any 19 contacts.

This is a non-negotiable offer, so please do not waste my personal and other people's time by replying to this email.

Bye!

Abbildung 4-6: Erpressungsmail Beispiel

Diese Art des Angriffes entwickelte sich erst durch die steigende Beliebtheit von Bitcoins. Angreifer und Angreiferinnen erhalten dabei die Möglichkeit, den Zahlungsfluss bestmöglich zu anonymisieren. Da jede Bitcoin Transaktion öffentlich einsehbar ist, kann schnell ermittelt werden, dass diese Art des Angriffes leider sehr erfolgreich ist. Folgt man der Bitcoin Adresse eines solchen Mails, welches wie ein normales Phishing-Mail an Tausende von Empfänger und Empfängerinnen versandt wird, kann schnell ermittelt werden, dass oftmals bereits Tausende von Euro darauf eingezahlt wurden.

Die Anzahl der bereits geleakten E-Mail-Adressen ist enorm. Laut Troy Hunt, dem Betreiber der Website haveibeenpwned.com sind der Website derzeit mehr als 10 Milliarden geleakter Accounts bekannt. (Hunt, 2020) Da zumeist eine E-Mail-Adresse als Accountlogin verwendet wird, kann an die meisten dieser geleakten Accounts daher auch eine Mail geschrieben werden. Jedoch können auch Angreifer und Angreiferinnen nicht einfach an eine solche Menge an Empfängern eine Mail aussenden. Um sicherzugehen, dass die echten Phishing-Mails daher das Ziel erreichen, versuchen Angreifer und Angreiferinnen daher auch durchgehend die Anzahl an inaktiven Mailkonten anzupassen.

Benutzer und Benutzerinnen als auch Administratoren und Administratorinnen bemerken diese Versuche anhand von leeren E-Mails, welche keinerlei Inhalt besitzen. Bekommt ein Angreifer oder eine Angreiferin nach einer solchen Mail keine Information vom Mailsystem, dass diese Adresse nicht mehr funktioniert, dann kann davon ausgegangen werden, dass diese noch gültig ist und Spam oder Phishing an diese Adresse versendet werden kann.

Das Kapitel um Mails weist einige große Gefahren für Unternehmen auf und trotz besten Maßnahmen können Unternehmen trotzdem nicht sichergehen, dass alle E-Mails mit bösartigem Inhalt korrekt von der Antispam-Lösung des Unternehmens abgefangen werden kann.

Jeder Benutzer und jede Benutzerin erhält früher oder später Phishing- oder Spammails. Unternehmen müssen daher ihre Mitarbeiter und Mitarbeiterinnen auf diese Umstände vorbereiten und Schulungen für diese anbieten. In diesen Schulungen sollten die Teilnehmer und Teilnehmerinnen erlernen, wie verdächtige Mails erkannt werden können oder welche Teams im Unternehmensumfeld zur Verfügung stehen, um bei der Erkennung helfen zu können. Zusätzlich muss diesen auch die Gefahr des Phishings beigebracht werden und die Tatsache, dass die Zugangsdaten nicht auf suspekten Seiten eingetragen werden dürfen.

Die Betreiber und Betreiberinnen der Kurse dürfen jedoch auch andere Themen nicht vergessen bei dem Angebot einer Sicherheitsschulungen. Die Gefahren, welche von Software oder Hardware ausgeht, ein potenzieller Social Engineering Angriff und einige andere Gefahren müssen in den Schulungen auch bearbeitet werden. Es muss daher eine Balance zwischen den Unterschiedlichen Angriffsvektoren gefunden werden und Unternehmen müssen sich spezifisch auf Bedrohungen, welche sich je nach Unternehmensgröße und Branche ändern kann, auf Angriffe vorbereiten.

5 PENETRATION-TESTING

Um sicher zu stellen, dass die Geräte eines Unternehmens sicher sind, werden von den Mitarbeitern und Mitarbeiterinnen von IT-Abteilungen sogenannte Penetration-Tests durchgeführt. Diese simulieren einen Angriff auf das Netzwerk und der Geräte darin und versuchen die vorhandenen Schwachstellen aufzudecken.

5.1 Vulnerability Scan

Angreifer und Angreiferinnen hacken sich nicht wie in Hollywood Filmen schnell in Firmennetzwerke und extrahieren die Informationen, die sie brauchen. Üblicherweise sind diese wochenlang, wenn nicht monatelang im Netzwerk und sammeln Informationen.

Die Angreifer und Angreiferinnen müssen zuerst eine mögliche Schwachstelle im System des Ziels finden. Dazu können die im Punkt 4 beschriebenen Angriffsvektoren verwendet werden, aber der hier beschriebene Vulnerability-Scan wird üblicherweise direkt über das Internet verwendet. Dabei werden alle im Internet verfügbaren Ressourcen eines Unternehmens gescannt und auf eventuelle Schwachstelle überprüft.

Mitarbeiter und Mitarbeiterinnen der IT-Abteilungen machen dies nicht anders. Um sicherzustellen, dass Angreifer und Angreiferinnen keine Schwachstelle finden, führen die Mitarbeiter und Mitarbeiterinnen von IT-Abteilungen die gleichen Schritte durch.

Dafür gibt es für die Mitarbeiter und Mitarbeiterinnen der IT auch eine große Anzahl an Tools, welche dies leicht möglich machen. Bekannte Produkte sind hierbei unter anderem OpenVas und Nessus. Zusätzlich gibt es noch das Kali-Betriebssystem, welches viele gratis Hackingtools beinhaltet. (Said, 2020)

Alle diese Produkte funktionieren aber praktisch gleich und bieten dem Benutzer und der Benutzerin die Schritte, welche in Abbildung 5-1: Schritte des Vulnerability Scannings (in Anlehnung an Mona Mangat, 2020) sichtbar sind, an.

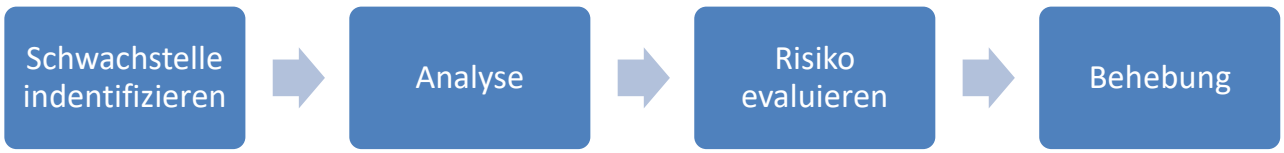

Abbildung 5-1: Schritte des Vulnerability Scannings (in Anlehnung an Mona Mangat, 2020)

Im ersten Schritt müssen hierbei Schwachstellen gefunden werden. Bei einem Tool mit graphischer Oberfläche wie Nessus oder OpenVas, trägt man hierzu ein einzelnes Ziel, eine Reihe verschiedener Ziele oder ein Netzwerk ein und startet den Scan. Je nach Ziel verwendeten Tool

und Ausmaß des gewählten Scans kann dies von wenigen Minuten bis zu mehreren Stunden dauern. Anschließend sollte dem Benutzer oder der Benutzerin jedoch eine Liste der vorhandenen Schwachstellen ausgegeben werden.

In den folgenden Schritten wird die Analyse des Outputs durchgeführt. Vulnerability-Scanner liefern üblicherweise eine große Anzahl an Informationen über das Zielsystem, wovon aber nicht alle nützlich sind. Benutzern und Benutzerinnen wird diesen Schritten jedoch erleichtert, indem der Scan bei den meisten Tools die Analyse automatisch ausführt und die gefundenen Schwachstellen nach dem Risikofaktor anordnet. (WhiteSource, 2019)

Für die Bewertung wird dafür üblicherweise das Common Vulnerability Scoring System (CVSS), ein offener Industriestandard für die Bewertung der Schwere von Sicherheitslücken verwendet.

Mithilfe der CVSS Bewertung einer Schwachstelle können IT-Administratoren und IT-Administratorinnen anschließend die Entscheidung treffen, ob diese behoben werden muss oder ob das Risiko der Schwachstelle akzeptiert werden kann.

Die CVSS Wertung der Version 3.0 beinhaltet dabei folgende Schweregrade:

SCHWEREGRAD	WERTUNGSBEREICH
NONE	0.0
LOW	0.1 – 3.9
MEDIUM	4.0 – 6.9
HIGH	7.0 – 8.9
CRITICAL	9.0 – 10.0

Tabelle 4: Wertungsbeschreibung CVSS

Um die Sicherheit der unternehmenseigenen Systeme und des Netzwerks garantieren zu können sollten Sicherheitslücken mit dem Schweregrad „Critical“ und „High“ so schnell wie möglich behoben werden. Fehler mit diesem Schweregrad deuten darauf hin, dass das betroffene System, von einem Angreifer oder einer Angreiferin übernommen werden könnte oder durch einen gezielten Angriff der Arbeitsbetrieb unterbrochen werden könnte.
Bei Fehler mit dem Schweregrad Medium und geringer kann abgewogen werden, ob es für das Unternehmen von Wert ist diese Vorzubeugen. Diese Fehler können unter normalen Umständen entweder nur schwer ausgenützt werden, oder besitzen nur ein überschaubares potenzielles Schadensausmaß. Ein Beispiel hierfür wäre eine nicht aktuelle Verschlüsselung in der verwendeten Kommunikation.

5.2 Exploitation

Sobald durch einen Vulnerability-Scan festgestellt wurde, dass eine Schwachstelle auf dem Zielsystem besteht, besteht für einen Angreifer oder einer Angreiferin die Möglichkeit, diese auszunützen. Jedoch bedeutet nicht jede gefundene Schwachstelle, dass eine Gefahr besteht. Nur weil eine Schwachstelle in der Theorie bekannt ist, heißt dies nicht, dass bereits ein praktisch funktionierender Exploit, ein Code, welcher diese Sicherheitslücke ausnützt, existiert.
Für die Linux Distribution Kali gibt es dabei das Metasploit Framework, dieses Bündelt eine umfassende Sammlung von Exploits von bekannten Schwachstellen, die Möglichkeit, diese vorzubereiten und auf einem Zielsystem auszuführen. (Porup, 2019)

6 MOBILTELEFONE

Der Einsatz von Mobiltelefonen im Arbeitsleben wurde in den letzten zwei Jahrzehnten zum Standard. Unternehmen fördern dies, indem den Mitarbeitern und Mitarbeiterinnen ein Mobiltelefon oftmals kostenfrei oder zumindest vergünstigt angeboten wird.

Da viele Menschen nur ungern zwei Mobiltelefone mit sich tragen, eines für private Zwecke und eines für geschäftliche, erlauben Unternehmen oftmals zusätzlich die private Verwendung des Gerätes. Dies hat für Mitarbeiter und Mitarbeiterinnen einige Vorteile, so sparen diese Platz beim Tragen des Geräts, besitzen alle notwendigen Informationen auf einem Gerät und sparen generell Zeit, wenn nur ein Mobiltelefon verwendet werden muss.

Mit den Vorteilen kommen aber auch Nachteile, welche sowohl von den Mitarbeitern und Mitarbeiterinnen als auch von der Geschäftsführung und Administration bedacht werden sollten.

Ein wichtiger Aspekt, der nur indirekt mit der Sicherheit des Mobiltelefons in Verbindung steht, ist die allgegenwärtige Erreichbarkeit der Person mit einem Mobiltelefon. Diese durchgehende Erreichbarkeit kann die Work-Life-Balance eines Mitarbeiters oder einer Mitarbeiterin negativ beeinflussen und dafür sorgen, dass die Person sich in der Ruhezeit nicht ideal erholt.

Wie auch das Notebook besitzt das Mobiltelefon als Mobilgerät eine hohe Anzahl an gleichen Bedrohungen, welche im folgenden Punkt näher erörtert werden.

6.1 Betriebssystemsicherheit, mögliche Bedrohungen und Schutzmaßnahmen

Wie bei anderen Geräten ändern sich auch die möglichen Bedrohungen von Mobiltelefonen je nach verwendetem Betriebssystem. Hierbei gibt es üblicherweise zwei Möglichkeiten für Mobiltelefon Nutzer und Nutzerinnen, dass Android-Betriebssystem von Google und das iOS (iPhone Operating System) von Apple. Weitere Betriebssysteme für Mobiltelefone wären unter anderem auch die Blackberry und Windows Mobile Serie, welche aber aufgrund des geringen Marktanteiles und einer künftigen Einstellung der Entwicklung in dieser Arbeit nicht beachtet werden.

Gleich wie ein Notebook kann auch ein Mobiltelefon der es tragenden Person überall mitgenommen werden. Anders als ein Notebook ist ein Mobiltelefon jedoch durch seine kleine Größe handlicher und wird daher üblicherweise immer vom Besitzer oder der Besitzerin mitgetragen.

Dies erhöht die Gefahr eines Diebstahls des Geräts. Anders ein Notebook findet sich in einem Mobiltelefon ein für Angreifer und Angreiferinnen kleines und unauffälliges Ziel, welches in einem kurzen Moment von dem Besitzer oder der Besitzerin entwendet werden kann.

Obwohl durch Cloud-Lösungen und Weiterentwicklung der Mobiltelefon-Betriebssysteme und Hardware das Mobiltelefon immer mehr Funktionen eines Notebooks oder PCs durchführen kann, besitzt ein Mobiltelefon aufgrund seiner einzigartigen Funktionen für einen Angreifer oder eine

Angreiferin ein sehr verlockendes Ziel. Dank der Synchronisation von Kontakten kann ein ungeschütztes Mobiltelefon sehr schnell alle Kontaktmöglichkeiten des Unternehmens preisgeben. Die Gefahr erhöht sich umso mehr, wenn am Mobiltelefon auch Kundenkontakte gespeichert wurden, in diesem Fall kann das betroffene Unternehmen mit den Regelungen der DSGVO in Konflikt kommen.

In den letzten Jahren boten Unternehmen vermehrt ihren Gästen die Möglichkeit eines Gast-Hotspots an. Dies wird von vielen Kunden und Kundinnen für bestimmte Unternehmen wie in der Hotellerie-Industrie sogar als Standard angesehen.

Solche Hotspots bieten für Gäste einen großen Vorteil, besonders um die Datenrate des Mobilfunkvertrages gering zu halten. Hauptproblem an Hotspots ist jedoch die Undurchsichtigkeit der angebotenen Gastnetzwerke. Benutzer und Benutzerinnen von jenen Hotspots wissen nicht welche Route der eigene Datenverkehr verwendet, über welche Server und Geräte die Daten geschleust werden und wer eventuell zuhören könnte.

Ein unbekannter Hotspot sollte aus diesen Gründen nur bei gegebener Dringlichkeit verwendet werden und selbst dann nur mit größter Vorsicht. Sehr von Nutzen wäre hierbei die Verwendung eines Virtual Private Network (VPN), welcher den kompletten Datentransfer des Benutzers oder der Benutzerin verschlüsselt zum Ziel tunnelt. (Kofler et al., 2018)

Um die Gefahr von unerwünschten Zuhörern und Zuhörerinnen zu limitieren, sollte ausnahmslos mit verschlüsselten Protokollen gearbeitet werden. Das bekannteste Beispiel ist hierbei das Hypertext Transfer Protocol (HTTP), welche seine Daten im Klartext überträgt. Um die Sicherheit der Daten vor unerwünschten Lesen auf dem Transportweg zu garantieren, sollte aus diesem Grund ausschließlich die HTTPS-Variante verendet werden.

Nicht zwingend muss die Bedrohung jedoch von einem Angreifer oder einer Angreiferin ausgehen. Auch normal erhältliche Applikationen (Apps) können unerwünscht viele Daten beanspruchen obwohl diese gar nicht für gewünschte Arbeit benötigt werden sollten. Moderne Betriebssysteme auf Mobiltelefonen geben dem Benutzer oder der Benutzerin die Möglichkeit, hierbei die gewünschte Berechtigung zu verwalten. Die gründliche Absicherung für den Datenzugriff ist vor allem für Firmengeräte aufgrund der DSGVO essenziell.

Dabei gibt es mehrere Berechtigungen, welche von Benutzer oder der Benutzerinnen gesetzt werden können, aber zugleich aufgrund der Sensibilität der Daten gut überlegt werden sollten: (Kofler et al., 2018)

GPS-Tracking: *Der Zugriff auf die Lokationsdaten ist für einige Apps notwendig, um die beabsichtigte Funktion der App erfüllen zu können. Beispielsweise braucht eine Navigations-App den permanenten Zugriff auf den physikalischen Standort des Geräts, oder eine Wetter-App benötigt Ihren Standort, um Sie rechtzeitig vor Unwettern zu warnen (auch wenn die App nur im Hintergrund aktiv ist). Der aktuelle Standort stellt aber gleichzeitig ein sensibles Datum des Benutzers dar und kann je nach Handhabung einen tiefen Einschnitt in die Privatsphäre des Benutzers darstellen. So können Apps mit Berechtigung zur Erfassung der Lokationsdaten relativ mühelos ein präzises Bewegungsprofil des Benutzers anfertigen.*

Audioaufnahme (Wanze): *Auch die Audioaufnahme ist eine durchaus sensible Berechtigung, wenn sie missbräuchlich von Apps verwendet wird. Mit dieser Berechtigung kann eine bösartige App das Endgerät praktisch in eine Wanze verwandeln. Während eine laufende Kamera in den meisten Fällen durch eine leuchtende LED signalisiert wird, bekommt der Benutzer von der heimlichen Aktivierung des Mikrofons nichts mit.*

Adressbuch/Kalender: *Die Kontaktliste und die Kalendereinträge können wertvolle Daten enthalten. Spionage-Apps erfragen in der Regel die Berechtigung, auf das Adressbuch oder den Kalender zuzugreifen. Mehrheitlich steht die Spionage im Vordergrund, das heißt, die Einträge werden ausgelesen und übertragen, in manchen Fällen greifen Apps aber auch schreibend zu, um neue Einträge einzufügen oder vorhandene zu löschen.*

6.2 Enterprise Mobility Management

Beim Enterprise Mobility Management geht es um das Sicherheitsmanagement der Mobilgeräte, um das Mobile Device Management (MDM), dessen Zielsetzung die durch die Bring Your Own Device (BYOD) Strategie beeinträchtigte IT-Sicherheit ist. Es geht um den Schutz der Unternehmensdaten, die durch Schnüffel-Apps beeinträchtigt sein könnten. Eine weitere Technologie ist die Verwaltung und der Zugriff auf Anwendungsprogramme, Apps, die vom Mobile Application Management (MAM) verwaltet und überwacht werden. Und die dritte Technologie des Enterprise Mobility Management ist das Mobile Information Management (MIM). (DATACOM Buchverlag GmbH, 2020)

Ab einer bestimmten Unternehmensgröße werden die verschiedenen Arten der Management-Systeme immer notwendiger. Ein Unternehmen und dessen IT-Administratoren und IT-Administratorinnen können die Mobilgeräte eines Kleinunternehmens noch manuell konfigurieren, aber ab einer bestimmten Unternehmensgröße wird diese Aufgabe zu zeitaufwendig.

Die Lösung dafür ist die Einführung eines Management-Systems, welches alle Mobilgeräte verwalten sollte. Dabei sollten, wenn möglich, von der ersten Konfiguration eines neuen Mobilgerätes, bis zur Verwaltung von Applikationen und des Betriebssystems, so viele Aufgaben wie möglich über das Management-System abgenommen werden.

Dies ist jedoch keine leichte Aufgabe. Verschiedene Betriebssysteme im Fall von Mobiltelefonen wären hierbei iOS und Android zu nennen, Hardware und Applikationen verlangen für das Ausrollen von Konfigurationen ein ausführliches Testen, um sicherzugehen, dass die gewünschte Konfiguration auf allen Geräten funktioniert. Oftmals erleichtern sich Unternehmen hierbei die Arbeit und stellen dem Mitarbeiter oder der Mitarbeiterin nur ein bis zwei Mobiltelefonarten zur Wahl.

Die meisten der in Punkt 6.1 genannten Gefahren können durch ein Enterprise Mobility Management minimiert werden. Das Mobilgerät kann dementsprechend konfiguriert werden, dass dieses immer zu automatischen Software-Updates gezwungen wird, wobei bereits ein großer Teil der Gefahren für jenes Gerät entfallen würden.

Die Installation eines Enterprise Mobility Management Systems kann aufgrund der großen Konfigurationsmöglichkeiten zu rechtlich heiklen Situationen führen. Um starke Eingriffe in die Privatsphäre eines jeden Mitarbeiters und einer jeden Mitarbeiterin zu vermeiden, sollte das System ausschließlich auf Firmengeräten installiert werden. Üblicherweise bieten Unternehmen ihren Mitarbeitern und Mitarbeiterinnen im Anschluss an, dieses Gerät auch für private Zwecke nutzen zu können.

Erhalten Mitarbeiter und Mitarbeiterinnen diese Möglichkeit, dann besitzen diese die Möglichkeit, auf das Tragen von mehreren Mobiltelefonen verzichten zu können. Mit der privaten Verwendung eines Mobiltelefons steigt andererseits wieder die Wahrscheinlichkeit, dass Mitarbeiter und Mitarbeiterinnen sich unsichere oder unerwünschte Applikationen herunterladen oder anderweitige Schadsoftware erhalten. Zusätzlich verarbeiten viele Applikationen mehr Daten als diese benötigen sollten und die Gefahr besteht, dass Kontaktinformationen von Kollegen und Kolleginnen sowie Kunden und Kundinnen entwendet werden könnten.

Besitzer und Besitzerinnen von Mobiltelefonen müssen aus diesem Grund bei jeder Applikation gut überlegen, ob diese auf bestimmte Daten zugreifen darf und sollte. Aktuelle Mobiltelefone fragen den Benutzer bei der Erstverwendung der Applikation oder bei einer zusätzlich benötigten Freigabe nach dessen Genehmigung.

Mobiltelefone mit dem Android Betriebssystem besitzen die Möglichkeit jenen Aspekt der Privat- und Geschäftsnutzung sicherer zu gestalten mit der Funktion „Android for Work“. Dabei wird ein zweites Arbeitsprofil am Mobiltelefon erstellt, für welches eigene Regeln, Applikationen und Funktionen gelten.

Applikationen, welche aufgrund von Android for Work ein zweites Profil besitzen sind aufgrund eines kleinen Aktenkoffer-Symbols, welches sich wiederum am Symbol der Applikation befindet, leicht für den Benutzer oder die Benutzerin erkenntlich. Das Mobiltelefon kann, sobald Android for Work aktiv ist, immer zwischen Arbeits- oder Privatmodus wechseln. Die Sicherheit des Wechsels in den Arbeitsmodus kann zusätzlich durch eine notwendige Authentifizierung verbessert werden. (Google, 2021)

Die iPhone Serie von Apple hat in dieser Hinsicht kein Äquivalenzprodukt zu bieten. Dies heißt jedoch nicht, dass das Unternehmen Apple keinen Wert auf Sicherheit legt. Das Unternehmen verteidigt seit Jahren die Sicherheit, deren Produkte gegenüber staatlichen Organisationen und deren Wunsch für eine Hintertür in das Betriebssystem.

The iPhone was locked with a four-digit passcode that the FBI had been unable to crack. The FBI wanted Apple to create a special version of iOS that would accept an unlimited combination of passwords electronically, until the right one was found. The new iOS could be side-loaded onto the iPhone, leaving the data intact.

But Apple had refused. Cook and his team were convinced that a new unlocked version of iOS would be very, very dangerous. It could be misused, leaked, or stolen, and once in the wild, it could never be retrieved. It could potentially undermine the security of hundreds of millions of Apple users. (Kahney, 2019)

7 GRUNDÜBERLEGUNG FÜR DIE EXPERTENINTERVIEWS

Wie in Kapitel 1.3 erwähnt, werden Experteninterviews in dieser Arbeit durchgeführt welche vordefinierten Fragen beantworten. Der geplante Umfang der Interviews soll 3 Experten und Expertinnen im Bereich der IT beinhalten, welche sich mit der Sicherheit des Unternehmens beschäftigen. Die geplante Dauer der Interviews soll, um den Rahmen der Arbeit nicht zu überschreiten, nicht die 40 Minuten je Person überschreiten. Anschließend werden die Interviews in Punkt 9 ausgewertet und analysiert.

7.1 Erhebung der Daten

Die Daten werden schriftlich vom Ersteller dieser Arbeit bei dem Experteninterview mitgeführt. Das Protokoll dieser Experteninterviews wird aufgrund des Datenschutzes anonymisiert und anschließend mit der restlichen Arbeit der Kommission vorgelegt. Eine Ausnahme gegen die Anonymisierung wäre die schriftliche Zusage des Experten oder der Expertin für eine namentliche Veröffentlichung. (Abdelgaffar, 2019)

Aus empirischen Zwecken sollen zusätzlich zu den Fragen, welche die vorher erstellten Hypothesen beantworten, folgende Daten von den Experten und Expertinnen erhoben werden:

- Name der Person, diese wird jedoch im weiteren Verlauf anonymisiert
- Derzeitige Position der Person in deren Unternehmen
- Personalanzahl des Unternehmens
- Sicherheitsempfinden des Unternehmens

7.2 Expertenauswahl

Um die beste mögliche Auswertung zu garantieren und die zuvor erwähnten Hypothesen bestmöglich und empirisch zu beantworten, muss die Auswahl der Experten und Expertinnen gut erwogen werden.

Laut Gläser und Laudel können die Experten und Expertinnen zusätzlich in drei Kategorien unterteilt werden: (Gläser & Laudel, 2012)

- Auswahl typischer Fälle: Die ausgewählten Fälle sind typisch für das Spektrum. Diese Fälle repräsentieren das Untersuchungsfeld besonders gut und stellen den größten und üblichen Teil der ausgewählten Experten und Expertinnen dar.
- Auswahl von Extremfällen: Die ausgewählten Fälle sind untypisch für das Spektrum und stellen das direkte Gegenteil der typischen Fälle dar. Dies bedeutet, dass Extremfälle in bestimmten Bereichen besonders stark oder besonders schwach ausgeprägt sind. Ob-

wohl es nur wenige Extremfälle geben kann, da eine hohe Anzahl dieser wiederum bedeuten würde, dass diese typischen Fälle sind, ist die Analyse von Extremfällen jedoch sehr interessant und gibt interessante Einblicke in die Studie und mögliche Fälle.

- Suche nach empirischen Gegenspielern: Diese Fälle widersprechen den bislang entwickelten Interpretationen. Bei dem Fund solcher Fälle müssen diese einbezogen werden und versucht werden, die theoretischen Erklärungen für diese zu finden.

In dieser Arbeit wird versucht, alle Strategien anwenden zu können und solche Experten und Expertinnen zu finden, dass alle Möglichkeiten abgedeckt werden können. Da viele der befragten Experten und Expertinnen dem Autor jedoch im Vorfeld nicht persönlich bekannt sind, kann nicht garantiert werden, dass Extremfälle oder empirische Gegenspieler gefunden werden können. (Abdelgaffar, 2019)

Bei der Auswahl der Experten und Expertinnen wird auf folgende Merkmale geachtet: (Gläser & Laudel, 2012)

- Der Experte oder die Expertin tätigt seine Arbeit im Bereich der IT-Sicherheit, der Compliance Abteilung, Leitung einer IT oder Compliance Abteilung oder der täglichen Arbeit in der IT-Abteilung mit häufigen Tätigkeiten im Bereich der IT-Sicherheit.
- Der Experte oder die Expertin besitzt ein gewisses Maß an Berufserfahrung in diesem Bereich.

Extrempositionen werden anhand folgender Merkmale erkannt: (Gläser & Laudel, 2012)

- Der Experte oder die Expertin hat abweichend stark negative Erfahrungen mit dem Thema Security gemacht und sieht dies als nicht wichtig an.

Obwohl es bereits während des Interviews leicht ersichtlich sein kann, dass der Experte oder die Expertin eine Extremposition vertritt, kann dies erst in der anschließenden Auswertung des Interviews tatsächlich festgestellt werden.

Die gewählten Experten waren, ohne dies im Vorhinein zu beabsichtigen, alle von männlichem Geschlecht. Aus diesem Grund werden diese in der Auswertung der Fragen und Hypothesen nicht weiter gegendert. (Gläser & Laudel, 2012)

7.3 Interviewablauf

Der Experte oder die Expertin wird bei Beginn des Interviews darauf aufmerksam gemacht, dass das Interview dokumentiert wird und anschließend ausgewertet. Dies dient zur rechtlichen Absicherung des Autors und zur Informierung des Experten oder der Expertin.

Während der Dauer des Interviews wird vom Autor darauf geachtet, dass dieses dem vorbereiteten Leitfaden entspricht und beantwortet. Obwohl kurze Abschweifungen und Gespräche über die Materie in Ordnung sind, wird darauf geachtet, dass die Dauer von 40 Minuten je Expertengespräch nicht überschritten wird. (Abdelgaffar, 2019)

Falls der Autor empfindet, dass das Gespräch, aus welchen Gründen auch immer, keinen sinnvollen Beitrag in dieser Arbeit leisten kann, behält sich dieser das Recht vor, diese Interviews nicht auszuwerten und damit für diese Arbeit zu verwerfen.

Der Beginn des Interviews startet mit einer Klarstellung des Namens des Experten oder der Expertin. Im Anschluss darauf wird dieser, wie bereits vorher erwähnt, darauf aufmerksam gemacht, dass dieses Interview dokumentiert wird. (Abdelgaffar, 2019)

Falls der gewählte Experte oder die Expertin dieser Voraussetzung nicht zustimmt, dann wird das Interview beendet. Im Falle einer Zustimmung wird das Interview mit der Befragung der allgemeinen Fragen, siehe Punkt 8.2, fortgeführt.

Im Anschluss auf die allgemeinen Fragen wird begonnen über die essenziellen Fragen zu sprechen. Jene Fragen sind notwendig um die in Punkt 1.4 aufgestellten Hypothesen zu beantworten. (Abdelgaffar, 2019)

7.4 Interviewabschluss und Nachbereitung

Aus Dokumentationsgründen und für Nachweiszwecke wird eine Nachbereitung der Interviews durchgeführt. Dies dient dem Zweck, dass während des Interviews die Informationen in Echtzeit vom Autor dokumentiert werden und eventuelle Lücken, welche aus Gründen der Zeitersparnis entstanden, geschlossen werden.

Die Nachbereitung beinhaltet aus diesen Gründen folgendes:

- schriftliche Fixierung und Fehlerbehebung des Gesprächs
- entstandener Eindruck des Gesprächs
- paraphrasieren des Gespräches
- Kategorienbildung

Auf Wunsch des Experten oder der Expertin wird diesem zum Abschluss der Nachbearbeitung diesem oder dieser eine Kopie zugesandt. (Abdelgaffar, 2019)

8 LEITFADENBILDUNG FÜR DIE INTERVIEWS

Im folgenden Kapitel wird auf die Interviews, welche mit den Experten oder den Expertinnen durchgeführt wurden, näher eingegangen. Alle Fragen nehmen es sich zum Ziel, die in Punkt 1.4 erstellten Hypothesen zu beantworten.

Um den Rahmen dieser Arbeit nicht zu überschreiten, wurde vom Autor entschieden, dass es vier Hypothesen gibt. Die dazu erstellten Fragen sollen einen hohen qualitativen Standard besitzen, über den die Experten oder Expertinnen diskutieren und Ihre Ansicht erläutern können.

Die an die Experten oder Expertinnen gestellte Fragen besitzen zum Teil aus Gründen der Klassifizierung und um mögliche Korrelationen zu veranschaulichen, einen quantitativen Wert. Folgende Fragen können somit gestellt werden:

Für wie wichtig halten Sie die IT-Sicherheit auf einer Skala von 1 (unwichtig) bis 10 (sehr wichtig), im Allgemeinen?

1	2	3	4	5	6	7	8	9	10

Tabelle 5: Beispiel Antwortmöglichkeiten 1

Diese Zwischenfrage stellt eine der allgemeinen Fragen, welche zum Beginn des Interviews an den Experten oder die Expertin gestellt wird, dar. Der Experte oder die Expertin erhalten zum Beginn des Interviews einfachere Fragen, welche einen sanften Einstieg in das Gespräch ermöglichen. Zusätzlich soll hierbei die Grundstimmung des Experten oder der Expertin zum Punkt IT-Sicherheit gezeigt werden. Falls dieser oder diese die IT-Sicherheit an diesem Punkt als nicht relevant bezeichnen würde, dann müsste vom Autor überlegt werden, ob die Person geeignet ist für die Fortführung des Interviews.

Die Skala besitzt dabei den Wertebereich von 0 – 10, wobei der Wert 0 die niedrigste oder eine höchst negative Zustimmung ausdrückt und der Wert 10 die höchste oder positivste gegebene Zustimmung. Anhand des zuvor genannten Beispiels könnte daher eventuell gesagt werden, dass Experte oder Expertin 1 mit der Wertung 8 antworten könnte und Experte oder Expertin 2 mit der Wertung 6. (Abdelgaffar, 2019)

Die Wertungen spiegeln darüber hinaus nicht das schulische Wertungssystem wider, welches erst ab einer Wertung über der Hälfte als positiv gewertet wird, sondern versuchen, die ganze Skala zu verwenden. Eine Wertung von 5 stellt daher eine durchschnittliche Wertung dar. Diese Information wird den Experten und Expertinnen vor der ersten Bewertung der ersten qualitativen Frage nähergebracht. (Abdelgaffar, 2019)

Da Skalen von 1-10 jedoch nicht bei allen Fragen einen Sinn ergeben oder als Antwort nützlich sind, gibt es auch Fragen, welche als Skala bereits vordefinierte Antworten enthalten. Diese Antworten wurden so gesetzt, dass diese die möglichen Spektren der Antworten vollständig abdecken sollten. Ein Beispiel wäre hierbei die Frage, wie die Ausgaben des Unternehmens im Bereich der IT-Sicherheit sind. (Abdelgaffar, 2019) Auf diese Frage werden folgende Antwortmöglichkeiten geboten:

Sehr gering	Gering	Angemessen	Hoch	Sehr hoch

Tabelle 6: Beispiel Antwortmöglichkeiten 2

Die restlichen Fragen besitzen eine offene Antwortmöglichkeit. Mit der Methode der qualitativen Inhaltsanalyse werden. Dabei wird die induktive Kategorienbildung angewandt, um die Auswertung der Interviews zu kategorisieren und analysieren.

Da die Expertengespräche in einem Videoanruf durchgeführt werden, kann es während eines für beide Parteien interessanten Themas durchaus dazu kommen, dass von der Hauptthematik abgewichen wird und andere Ursachen für die Themenproblematik gefunden oder besprochen werden. Da es dies zu vermeiden gilt, sollte dies bereits mit einer eindeutigen Fragestellung verhindert werden. (Abdelgaffar, 2019)

8.1 Qualitative Inhaltsanalyse mit induktive Kategorienbildung

Um die offenen Antworten der Experten und Expertinnen auswerten zu können, wird die Methode der qualitativen Inhaltsanalyse von Mayring angewandt. Dabei werden die Aussagen der Experten und Expertinnen paraphrasiert und abstrahiert, um diese in Kategorien einordnen zu können. Für diese Kategorisierung wird die von Mayring bekannte induktive Kategorienbildung verwendet, welche es erlaubt, im Anschluss der Interviews eigene, vom Autor gewählte Kategorien passend zu den Aussagen zu bilden. (Mayring, 2015)

Nachdem in den ersten Schritten der Analyse das Material genau beschrieben und durch die Fragestellung festgelegt wurde, was zusammengefasst werden soll, müssen also die Analyseeinheiten bestimmt werden. Die einzelnen Kodiereinheiten werden nun in eine knappe, nur auf den Inhalt beschränkte, beschreibende Form umgeschrieben (Paraphrasierung). Dabei werden bereits nicht inhaltstragende (ausschmückende) Textbestandteile fallen gelassen. Die Paraphrasen sollen auf einer einheitlichen Sprachebene formuliert sein, was vor allem bei mehreren Sprechern (z. B. Gruppendiskussion) wichtig ist. Schließlich sollen sie in einer grammatikalischen Kurzform stehen (z.B. »Ja wissen Sie, ich hab' ja eigentlich keine Belastung im Großen und Ganzen damals gespürt.« wird zu »keine Belastung gespürt«). Handelt es sich um überschaubare Materialmengen, so werden diese Paraphrasen herausgeschrieben; wäre das zu aufwendig, so werden die nächsten beiden Analyseschritte gleich mit vollzogen. (Mayring, 2015)

Der genaue Ablauf für die Bildung einer solchen Inhaltsanalyse mit einer induktiven Kategorienbildung kann anschließend wie in Abbildung 8-1 durchgeführt werden.

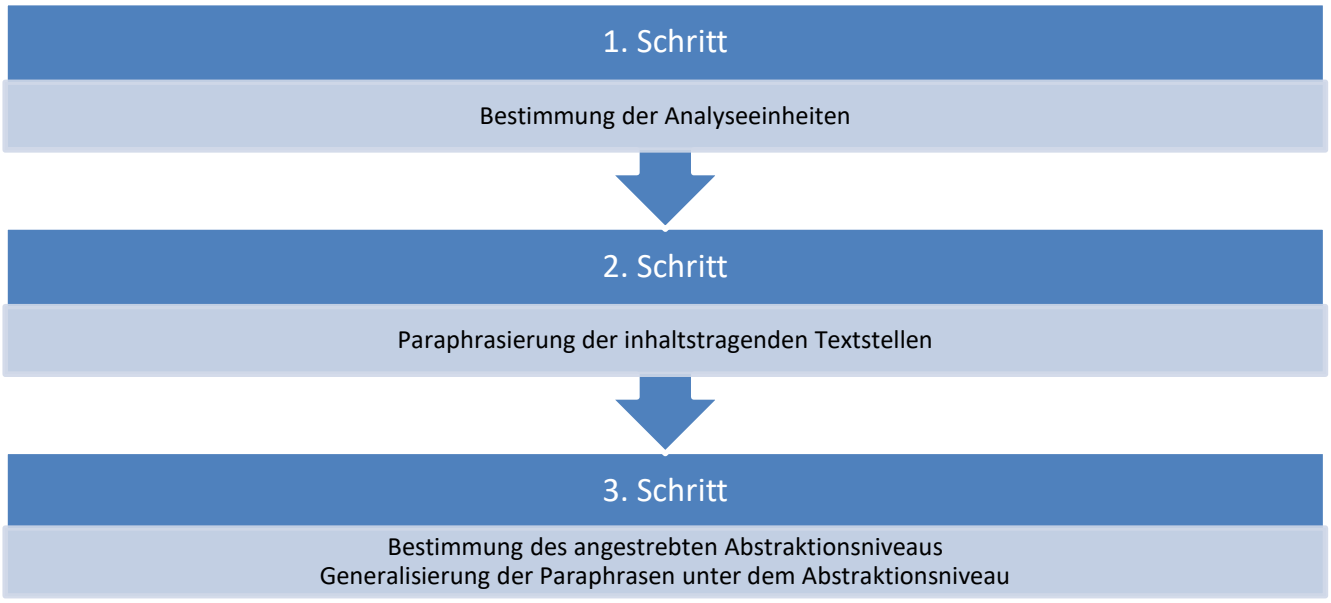

Abbildung 8-1 Ablaufmodell zusammenfassende Inhaltsanalyse 1 (in Anlehnung an Mayring, 2015)

Der erste Schritt, die Bestimmung der Analyseeinheit, muss überlegt werden, was als Analyseeinheit der Inhaltsanalyse fungieren wird. In dieser Arbeit sind Analyseeinheiten jedes vollständige Interview mit einem Experten oder einer Expertin.

Im zweiten Schritt werden die Aussagen der Experten und Expertinnen paraphrasiert, was bedeutet, dass die Aussagen der Experten und Expertinnen von überflüssigen Aussagen bereinigt werden und auf das Wesentlichste reduziert werden. Dabei gibt Mayring folgende Regeln für die Paraphrasierung: (Mayring, 2015)

- *Streiche alle nicht (oder wenig) inhaltstragenden Textbestandteile wie ausschmückende, wiederholende, verdeutlichende Wendungen!*
- *Übersetze die inhaltstragenden Textstellen auf eine einheitliche Sprachebene!*
- *Transformiere sie auf eine grammatikalische Kurzform!*

In den Schritten drei, vier und fünf wird anschließend das Abstraktionsniveau festgelegt und die zuvor paraphrasierten Sätze einer weiteren Reduktion unterzogen.

Das Ziel der Reduktion ist die Kürzung der kompletten Aussagen auf jede Frage zu ein bis zwei Wörter.

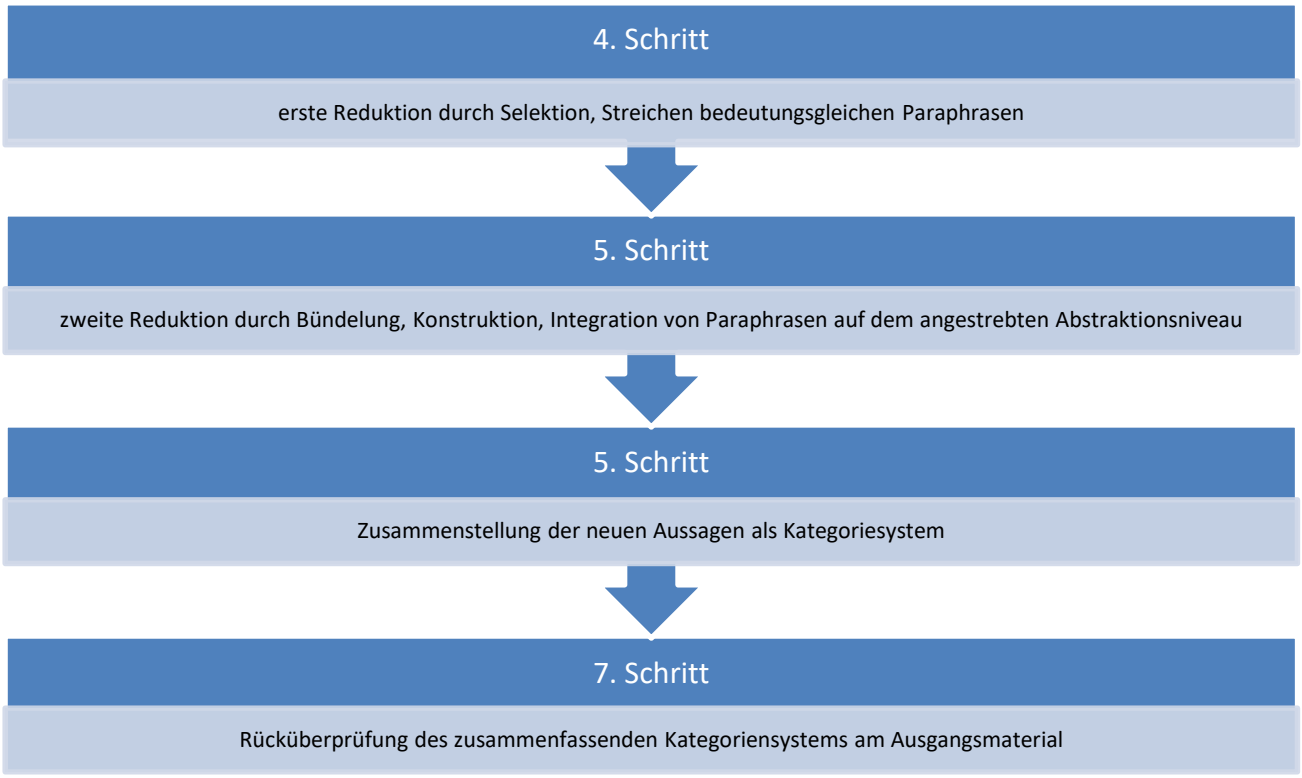

Abbildung 8-2 Ablaufmodell zusammenfassende Inhaltsanalyse 2 (in Anlehnung an Mayring, 2015)

Es muss jedoch angemerkt werden, dass dem in Abbildung 8-1 gezeigten Ablaufmodell nicht zwangsweise gefolgt werden muss. Je nach Aussage der Experten und Expertinnen müssen unter Umständen nicht zwei Reduktionen durchgeführt werden, sondern nur eine aufgrund einer kurzen Antwort des Experten oder der Expertin. Dass dem Autor bei diesem Ablaufmodell etwas Freiraum eingeräumt wird, wird auch von Mayring so verdeutlicht:

Die Inhaltsanalyse ist kein Standardinstrument, das immer gleich aussieht; sie muss an den konkreten Gegenstand, das Material angepasst sein und auf die spezifische Fragestellung hin konstruiert werden. Dies wird vorab in einem Ablaufmodell festgelegt (Beispiele für solche Modelle finden sich beim Durchblättern dieses Buches in großer Anzahl), die die einzelnen Analyseschritte definieren und in ihrer Reihenfolge festlegen. (Mayring, 2015)

Im Schritt sechs werden in Folge die paraphrasierten und reduzierten Aussagen zu Kategorien zugeordnet. Dabei werden, wenn notwendig, neue Kategorien für Aussagen erstellt oder diese zu vorhandenen Kategorien hinzugefügt.

Im letzten Schritt der Rücküberprüfung wird der vorhandene Kategorienpool nochmals überprüft. Hierbei gilt es festzustellen, ob es zu viele Kategorien gibt, diese sich ähneln und zusammengefügt werden können. Zusätzlich ist hierbei zu überprüfen, ob die Aussagen der Experten und Expertinnen sich in den erstellten Kategorien angemessen widerspiegeln oder die erstellten Kategorien nochmals überarbeitet werden müssen.

8.2 Allgemeine Fragen

Die allgemeinen Fragen zum Beginn des Interviews haben einen großen und übergreifenden Nutzen für das folgende Gespräch. So wird bei diesen Fragen zu Beginn versucht, ein angenehmes Klima für das restliche Gespräch herzustellen.

Zusätzlich ist es das Ziel dieser Fragen, die Basisinformationen des Unternehmens, in welchem der Experte oder die Expertin arbeitet, zu erhalten und die grundlegende Einstellung des Experten oder der Expertin zum Thema IT-Sicherheit.

Auch kann in diesem Abschnitt bereits erkannt werden, ob die gewählten Experten und Expertinnen sich tatsächlich für das folgende Interview eigenen. Falls ein potenzieller Experte oder eine potenzielle Expertin trotz der zuvor ermittelten Beschäftigung von diesem keinen Zugang zum Thema IT-Sicherheit besitzt, kann an dieser Stelle das Gespräch beendet werden.

Folgende Fragen werden in der Einleitung des Gespräches gestellt:

1. Welche Position nehmen Sie in Ihrem Unternehmen ein?
2. Welche Mitarbeiteranzahl weißt Ihr Unternehmen auf?
3. Für wie wichtig halten Sie die IT-Sicherheit auf einer Skala von 0 (unwichtig) bis 10 (sehr wichtig) im Allgemeinen?
4. Beschreiben Sie die Maßnahmen, welche Sie derzeit treffen und in naher Zukunft geplant haben, um Ihre Sicherheit für mobile Geräte (Notebooks und Mobiltelefone) zu erhöhen.
5. Haben Sie ein Mobile Device Management System? Falls nicht, bitte geben Sie einen Grund an wieso nicht und ob ein solches System, in naher Zukunft, noch für Ihr Unternehmen geplant ist.
6. Wie hoch, auf einer Skala von 0 (überhaupt nicht) bis 10 (sehr hoch), empfinden Sie das Risiko eines Angriffes auf Ihre mobilen Geräte, welcher es auf sensible/DSGVO relevante Daten des Unternehmens abgesehen hat.

   Bitte begründen Sie, wieso diese Wertung vergeben wurde und eine solche Gefahr für das Unternehmen besteht.

Wie ersichtlich verfolgt hierbei nicht jede Frage einer qualitativen Antwort. So ist beispielsweise keine Begründung für die zweite Frage, die Mitarbeiteranzahl des Unternehmens von Nöten. Diese Frage ist jedoch von größter Notwendigkeit für die Analyse der folgenden Hypothesen.

8.3 Überlegungen und Erstellung von Hypothese 1

> *Hypothese 1: Durch das Eintreten der COVID-Pandemie stieg das Sicherheitsbewusstsein im Bereich des Mobile Computings.*

Das Ziel der ersten Hypothese ist die Beantwortung der Frage, ob das Sicherheitsbewusstsein von Unternehmen durch das Eintreten der COVID-Pandemie stieg. Aufgrund der COVID-Pande-

mie wurden einige Unternehmen dazu gezwungen, den Hauptarbeitsplatz von dem Firmengebäude in das Homeoffice zu versetzen. Dies versichert, dass Mitarbeiter und Mitarbeiterinnen vor dem Virus geschützt werden, da die Infizierungsrate aufgrund des verringerten körperlichen Kontaktes reduziert wird.

Aufgrund einer zu schnellen und starken Ausrichtung auf den Homeoffice-Arbeitsplatz riskieren Unternehmen jedoch einige arbeits- und sicherheitsrelevante Risiken. Unternehmen können eventuell unzureichend auf diese schnelle Änderung reagieren, was zu Netzwerkproblemen führen könnte und die VPN-Verbindungen der Mitarbeiter und Mitarbeiterinnen unterbrechen würde.

Zusätzlich entstehen auch neue sicherheitsrelevante Gefahren, auf welche von Unternehmen zuvor nicht eingegangen werden konnte.

Für die Beantwortung dieser Hypothese werden dem Experten oder der Expertin im Laufe des Interviews folgende Fragen gestellt:

- Beschreiben Sie die derzeitigen Maßnahmen Ihres Unternehmens für die Schulung der Mitarbeiter im Umgang mit Mobile Security.
- Gab es bereits vor dem Eintreten der COVID Pandemie regelmäßige Schulungen für die Mitarbeiter, welche einen Fokus auf den Umgang mit mobile Security legten?
- Konnten Sie die mobile Sicherheit Ihrer Geräte seit dem Eintreten der COVID-Pandemie nennenswert verbessern?
    - Falls ja, welche Möglichkeit konnten Sie dazu anwenden

8.4 Überlegungen und Erstellung von Hypothese 2

Hypothese 2: Unternehmen sind gut auf den physikalischen Diebstahl von mobilen Geräten vorbereitet, weshalb ein solcher in den meisten Umständen nur wenig Schaden verursacht.

Mobile Geräte bieten für die meisten Arbeitnehmer und Arbeitnehmerinnen, aber auch Arbeitgeber und Arbeitgeberinnen eine große Anzahl von Vorteilen. Das mobile Gerät ist für Arbeitnehmer und Arbeitnehmerinnen üblicherweise leicht zu transportieren und bietet diesen eine erhöhte Flexibilität für die Durchführung von deren Bestreben.

Der Nachteil von mobilen Geräten ist jedoch, dass diese seit jeher leichter von dem Besitzer oder der Besitzerin verloren werden können. Der Diebstahl eines Notebooks oder eines Mobiltelefons kann sich für einen Angreifer oder eine Angreiferin als wahre Goldgrube erweisen. Je nach gefundenen Dokumenten kann das betroffene Unternehmen, je nach dem Wert der Daten, schweren Image- oder Finanzschäden davontragen.

Aufgrund der potenziell hohen Strafen, welche seit der Einführung der DSGVO von Möglichkeit sind, ist es die Annahme des Autors, dass Unternehmen ausreichend gut auf einen Diebstahl der mobilen Geräte vorbereitet sind.

Für die Beantwortung der zweiten Hypothese werden dem Experten oder der Expertin im Laufe des Interviews folgende Fragen gestellt:

- Wurden innerhalb der letzten sechs Monate mobile Geräte von Mitarbeitern gestohlen oder als verloren angegeben, wenn ja, welche?
- Bitte beschrieben Sie, welchen Schaden ein gestohlenes Notebook für Ihr Unternehmen bedeuten kann.
- Welche Methoden verwenden Sie, um die Anzahl von gestohlenen Mobilgeräten zu verringern.

8.5 Überlegungen und Erstellung von Hypothese 3

Hypothese 3: Großunternehmen (> 250 Mitarbeiter) besitzen bereits ein Mobile Device Management System, oder arbeiten derzeit an der Implementierung eines solchen, um notwendige Sicherheitsvorschriften auf mobilen Geräten umsetzen zu können.

Mit der dritten Hypothese wird überlegt, dass größere Unternehmen bereits Mobile Device Management Systeme durch deren IT-Abteilungen umsetzen konnten. Mobile Device Management Systeme können sich, aufgrund ihrer Komplexität und des benötigten Fachwissens im Umgang mit diesen, als sehr kostspielig für das Unternehmen erweisen. Kleinere Unternehmen besitzen daher, unter Umständen, nicht die Möglichkeit ein solches System einzuführen.

Mobile Device Management Systeme können der IT-Abteilung eines Unternehmens jedoch eine große Arbeitslast abnehmen. Viele Aufgaben, welche manuell auszuführen wären, können automatisiert werden. Ab einer bestimmten Unternehmensgröße würde ein komplett manuelles System, bei welchen die Installation, Erstkonfiguration, Regelsetzung und laufende Updates verwaltet werden müssten, sich als zu zeitaufwendig auszeichnen.

Für die Beantwortung der dritten Hypothese werden dem Experten oder der Expertin im Laufe des Interviews folgende Fragen gestellt:

- Besitzen Sie ein Mobile Device Management System?
    - Falls nicht, bitte geben Sie einen Grund an wieso nicht und ob ein solches System, in naher Zukunft, noch für Ihr Unternehmen geplant ist und wie Sie das System derzeit absichern.
- Welche Aspekte Ihres Mobile Device Management System wird für die Sicherheit Ihrer Mobiltelefone verwendet?
    - Welche zukünftigen Funktionen planen Sie für die Sicherheit Ihrer Mobiltelefone?

8.6 Überlegungen und Erstellung von Hypothese 4

Hypothese 4: Der Sicherheitsaspekt von unternehmensfremden Applikationen auf Mobiltelefonen wird derzeit noch unzureichend überwacht, weswegen solche ein mögliches Sicherheitsrisiko darstellen.

Hypothese 4 stellt die Frage, ob die von Benutzer und Benutzerinnen installierten Applikationen auf Unternehmensmobiltelefonen eine Gefahr für Unternehmen darstellen kann.

Die Verwendung von privaten Applikationen kann bei Administratoren und Administratorinnen einiges an Kopfzerbrechen verursachen. Viele Unternehmen erlauben die Verwendung privater Applikationen auf Firmengeräten und auch Dienstnehmer und Dienstnehmerinnen nehmen dieses Angebot oftmals an, da diese somit kein zweites Gerät für rein private Zwecke erwerben müssen.

Die Erlaubnis, dass Benutzer und Benutzerinnen unternehmensfremde Applikationen auf dem Firmengerät verwenden dürfen, kann sich daher als nennenswerten Comfort-Faktor herausstellen. Jedoch dürfen auch nicht die Gefahren, welche damit einhergehen, vergessen werden. Jede Applikation kann, aufgrund von Sicherheitslücken in der Applikation selbst oder eines Datenlecks des Herstellers, sich als kritische Sicherheitslücke erweisen.

Von Unternehmensseite ist es daher wichtig abzuwägen, welche Freiheiten den Benutzern oder Benutzerinnen am Firmengerät erlaubt werden und welche Applikationen, aufgrund der potenziellen Gefahren, konkret verboten werden müssen.

Für die Beantwortung der vierten Hypothese werden dem Experten oder der Expertin im Laufe des Interviews folgende Fragen gestellt:

- Wie bewerten Sie die getroffenen Schutzmaßnahmen für Ihre Notebooks in Ihrem Unternehmen?
- Wie bewerten Sie die getroffenen Schutzmaßnahmen für Mobiltelefone in Ihrem Unternehmen?
- Besitzen Mobiltelefone Limitierungen, welche es aus Sicherheitsgründen nicht ohne weiteres ermöglichen unternehmensfremde Applikationen zu verwenden?

8.7 Abschluss des Interviews

Zum Abschluss des Interviews wird mit dem Experten oder der Expertin über das vergangene Interview nochmals gesprochen und wie dieses empfunden wurde. Wurden einzelne Gesprächspunkte während des Interviews zugunsten des Leitfadens unterdrückt, dann ist es an dieser Stelle möglich, die gewünschte Diskussion wieder aufzunehmen, um somit neue Erkenntnisse zu erhalten.

Das große Ziel des Abschlusses ist es jedoch, einen freundlichen, natürlichen und professionellen Ausklang für das Gespräch zu ermöglichen. Falls der Experte oder die Expertin an dieser Stelle weitere Fragen besitzen, dann kann auf diese im Abschluss eingegangen werden ohne die zeitliche Agenda des Interviews nennenswert zu verletzten.

9 AUSWERTUNG UND ANALYSE DER INTERVIEWS

Die Interviews, welche mit den Experten und Expertinnen durchgeführt wurden, können als großer Erfolg gewertet werden. Alle Interviews konnten ohne vorzeitige Abbrechung problemlos durchgeführt werden. Die Interviews mit den Experten und Expertinnen verlief geregelt und nach Plan ab, es gab von keiner Seite längere Ausschweifungen zu einem Thema. Zusätzlich wurde kein Thema, welches gänzlich außerhalb des Rahmens des Leitfadens wäre, von den Experten und Expertinnen angeschnitten. Aus diesem Grund konnten alle Gespräche innerhalb der gesetzten zeitlichen Frist beendet werden.

Unter den Experten und Expertinnen fanden sich zudem keine empirischen Gegenspieler der Thematik. Alle befragten Experten und Expertinnen waren sich über den hohen Stellenwert der IT-Sicherheit bewusst und haben dies kundgetan.

Der Sinn der gestellten Fragen wurde von den Experten und Expertinnen schnell verstanden und zügig beantwortet. Dies resultierte aus dem hohen Fachwissen der befragten Personen zum Thema und deren derzeitigen Arbeitsstatus im Bereich IT-Management oder IT-Sicherheit.

Die Experten und Expertinnen waren des Weiteren sehr kommunikativ zu den gestellten Fragen und konnten großzügige Aussagen über deren Sicherheitsstatus angeben. Der Autor musste aus diesen Gründen nur sehr selten zu bestimmten Fragen nachfragen, um eine genauere Antwort des Befragten oder der Befragten zu erhalten.

Aufgrund der derzeitigen Pandemie mussten die Gespräche mit den Experten und Expertinnen online durchgeführt werden. Als Gesprächssoftware wurde Microsoft Teams verwendet. Aufgrund der Sicherheitsrichtlinien der einzelnen Unternehmen konnten die Gespräche jedoch nicht in diesem aufgenommen werden. Für die Aufnahme war aus diesen Gründen eine zusätzliche Software notwendig. Der Autor entschied sich hierbei für Open Broadcaster Software (OBS), einer freien open source Software, welche ihren Schwerpunkt auf Streaming und Aufnahmen setzt. (Edwards, 2012)

Die Aufnahmen verliefen problemlos und die Endaufnahmen waren von zufriedenstellender Qualität.

Zum Anschluss mussten die Gespräche für das anschließende Paraphrasieren und die Kategorienbildung, transkribiert werden. Da es sich hierbei bei längeren Gesprächen um einen großen Zeitlichen Aufwand handelt, wurde hierfür die auf Künstliche Intelligenz (KI) basierte Gesprächs-zu-Text Software rev.ai verwendet. (Chicola, 2019)

Der Einsatz der Software rev.ai stellte sich ebenfalls als gute Entscheidung heraus. Mit der Software konnte einiges an Zeit für die Transkription gespart werden. Obwohl die Umsetzung der Software nicht perfekt war und einige Fehler in die Transkription gelangten, konnten diese schnell bei einer manuellen Kontrolle behoben werden.

Zusätzlich wurden bei dieser manuellen Kontrolle jegliche in den Gesprächen genannten Personen und Unternehmen anonymisiert. Dieser Wunsch wurde von mehreren der Experten und Expertinnen im Laufe des Gesprächs geäußert.

Das weitere Ziel dieses Kapitels ist nun die Aufschlüsselung der Interviews, der Vergleich der Kategorien und die Auswertung dieser. An dieser Stelle werden die Zusammenhänge der Experten und Expertinnen gesucht, um Korrelationen in den gegebenen Antworten zu finden. Der Autor nimmt es sich zusätzlich vor, die Aussagen der Experten nicht direkt zu zitieren, sondern diese zusammenzufassen, bevor diese wiederum zu Kategorien zusammengefasst werden. Der Autor nimmt verständlicherweise größte Rücksicht darauf, die Aussagen der Experten unter keinen Umständen zu verändern.

9.1 Kategorienbildung

Die anschließende Kategorisierung der paraphrasierten Antworten der Expertengesprächen stellte aufgrund des zeitlichen Aufwandes eine große Herausforderung dar. Die von Mayring empfohlenen zwei Reduktionen der paraphrasierten Antwort konnte innerhalb einer Reduktion durchgeführt werden. Die darauffolgende Kategorisierung der reduzierten Antworten ergab eine Gesamtanzahl von 45 Kategorien.

Diese 45 Kategorien wurden im Anschluss überprüft und auf ihre Sinnhaftigkeit, Aussagekraft und Einzigartigkeit überprüft und bewertet. Kategorien, welche sich zu sehr ähnelten, wurden zusammengefügt, um eine sinnvollere Korrelation darstellen zu können.

Der komplette Prozess der Expertengespräche, Paraphrasierung, Reduktion und Kategorisierung kann im beigefügten Dokument am Ende dieser Arbeit genauer betrachtet werden. Hier werden folglich nur die Schlüsselkategorien und die Zusammenfügung der Kategorien näher erklärt.

Von den anfangs vorhandenen 45 Kategorien wurden diese durch eine Zusammenfügung auf 22 einzigartige Kategorien reduziert. Eine weitere Reduktion dieser wäre nur schwer möglich, da die gegenwärtigen Aussagen der Experten und Expertinnen dadurch verwässert werden könnte.

Die größten Kategorien, hierbei bezeichnet als Schlüsselkategorien, sind die Kategorie Schulung und Sicherheitsrichtlinien. Diese Kategorien wuchsen auf ihre Größe aus jenem Grund der ähnlichen Vorgehensweisen der Experten in einer Situation und der Zusammenfügung von ähnlichen Kategorien, welche durch die Aussage der Experten und Expertinnen gewonnen wurde.

Für die Kategorie „Schulung“ wurden dabei folgende Kategorien zusammengefügt:

Jährliche-Schulung, Führungskraft-Schulung, Security Information Mails, interaktive Schulung und Einzelschulungen.

All jene Kategorien und Aussagen können dabei in der Schlüsselkategorie „Schulung“ aufgefangen werden, da alle dieselbe Aussage beinhalten. Die jährlichen Schulungen sind aufgrund Ihrer Notwendigkeit für bestimmte Zertifizierungen ein Standard der meisten Betriebe. Die Kategorie „Führungskraft-Schulung“ lässt darauf schließen, dass es hierbei Abweichungen von normalen Schulungen gibt und die Führungskräfte eine gänzlich unterschiedliche Schulung zu den normalen Mitarbeitern und Mitarbeiterinnen enthält. Das Gespräch mit dem für diese Kategorie verantwortlichen Experten lässt aber darauf schließen, dass dieser im Gesundheitsbereich arbeitet und das übliche Personal des Unternehmens keine Computerhardware verwendet für deren tägliche

Arbeit im Gesundheitsbereich. Erst Führungskräfte des Unternehmens erhalten ausnahmslos ein Arbeitsgerät und damit auch eine verpflichtende Schulung.

Nr.	Kategorie	Anzahl
1	Anschaffung Ersatzgerät	2
2	Budget angemessen	3
3	Budgeterhöhung erwünscht	3
4	Cyberkriminalität	4
5	Datenschutz	4
6	Hardware Security	4
7	kein vorhandenes MDM	2
8	keine Diebstähle	2
9	keine Vorbeugemaßnahmen	3
10	Phishing	3
11	Ransomware	2
12	Reduktion Diebstähle	1
13	remote Gerätelöschung	2
14	restliche Malware	2
15	Schulung	11
16	Schulung vor COVID	3
17	Sicherheit ist angemessen	6
18	Sicherheitsrichtlinien	31
19	Software Security	5
20	Stagnation	3
21	Verbesserungspotenzial vorhanden	2
22	vorhandenes MDM	1

Tabelle 7: gebildete Kategorien

Jährliche-Schulung, Führungskraft-Schulung, Security Information Mails, interaktive Schulung und Einzelschulungen.

All jene Kategorien und Aussagen können dabei in der Schlüsselkategorie „Schulung“ aufgefangen werden, da alle dieselbe Aussage beinhalten. Die jährlichen Schulungen sind aufgrund Ihrer Notwendigkeit für bestimmte Zertifizierungen ein Standard der meisten Betriebe. Die Kategorie „Führungskraft-Schulung“ lässt darauf schließen, dass es hierbei Abweichungen von normalen

Schulungen gibt und die Führungskräfte eine gänzlich unterschiedliche Schulung zu den normalen Mitarbeitern und Mitarbeiterinnen enthält. Das Gespräch mit dem für diese Kategorie verantwortlichen Experten lässt aber darauf schließen, dass dieser im Gesundheitsbereich arbeitet und die meisten üblichen Mitarbeiter des Unternehmens keine Computerhardware verwendet für deren tägliche Arbeit im Gesundheitsbereich. Erst die Führungskräfte des Unternehmens erhalten ausnahmslos ein Arbeitsgerät und damit auch eine verpflichtende Schulung.

Der Sinn der Kategorie „Security Information Mails“ wirkt weit entfernt von den anderen Schulungskategorien, aber auch hier muss wieder auf den Kontext geachtet werden. Der Experte gibt an, diese Mails, wenn benötigt, an die Mitarbeiter und Mitarbeiterinnen des Unternehmens auszusenden, um diese vor einer aktuellen Gefahr zu warnen. Obwohl die Mitarbeiter und Mitarbeiterinnen bereits durch Schulungen eine bestimmte Gefahr erkennen sollten, so riskieren die IT-Experten des Unternehmens nicht, die Mitarbeiter abermals vor einer akuten Gefahr zu warnen, wenn diese gefunden wurde.

Die Kategorien „interaktive Schulung“ und „Einzelschulungen“ können indessen leicht zur Schlüsselkategorie hinzugefügt werden. Eine interaktive Schulung, meist live, wo Mitarbeiter und Mitarbeiterinnen den Experten einige Fragen stellen können, ändert die Schulungsagenda nicht weitgehend von nicht interaktiven Schulungen. Gleichfalls wird bei Einzelschulungen der gleiche Inhalt vermittelt wie in normalen Schulungen, weswegen auch diese Kategorie ohne Probleme an die Schlüsselkategorie hinzugefügt werden kann.

Eine ähnliche Situation ergibt sich bei der Schlüsselkategorie „Sicherheitsrichtlinien“, welche aus den folgenden Kategorien zusammengelegt wurde:

Datenseparation, Verschlüsselung, Unternehmensrichtlinien, Access Control, Multi-Faktor-Authentifizierung, Applikationssperre, Updates, Privatgebrauch, nicht lokale Datensicherung und länderspezifische Unterschiede

Die meisten Kategorien können ohne große Bedenken in die Schlüsselkategorie übernommen werden. Bei nicht lokale Datensicherung, Verschlüsselung, Access Control, Multi-Faktor-Authentifizierungen, Applikationssperren, Updates und länderspezifische Unterschiede handelt es sich vom Unternehmen eingesetzte Policies welche die Sicherheit des Unternehmensnetzwerkes und der Infrastruktur erhöhen sollen. Auf länderspezifische Unterschiede muss aus jenem Grund geachtet werden, da je nach Land eine ganz andere notwendige Sicherheitssituation vonnöten ist. Je nach Land muss die Sicherheit entweder erhöht oder verringert werden, da diese zu stark in die Privatsphäre der Mitarbeiter oder Mitarbeiterinnen eingreifen würde.

Die Kategorie Unternehmensrichtlinien ist gleichzusetzen mit der Schlüsselkategorie. Die Kategorie wurde dennoch der Schlüsselkategorie untergeordnet, da in den Unternehmensrichtlinien jegliche Vorgehensweisen beinhaltet werden, wie zum Beispiel Multi-Faktor-Authentifizierung oder Verschlüsselung, welche auch in die Sicherheitsrichtlinien fallen würden.

Die Kategorien „Privatgebrauch“ und „Datenseparation“ ergeben praktisch die gleiche Aussage. In beiden Kategorien verwenden Benutzer und Benutzerinnen ihr mobiles Gerät auch für private Zwecke. Hierbei wird jedoch geachtet, dass die Unternehmensdaten weiterhin sicher am Gerät sind und bestenfalls von den Privatdaten getrennt wurden.

Eine weitere gebildete Kategorie, welche jedoch aufgrund des geringen Vorkommens jedoch keine Schlüsselkategorie ist, ist die Kategorie „Cyberkriminalität“. Hierbei wurden die folgenden Kategorien zusammengefügt: Accountübernahme, Datendiebstahl und Auftragsverlust.

Sowohl die Kategorien Accountübernahme und Datendiebstahl können schnell und problemlos zu dieser Kategorie hinzugefügt werden. Die Kategorie Auftragsverlust hingegen erfordert etwas Kontext, um den Grund der Zusammenfügung nachvollziehen zu können. Der Kontext des Experten hinter dieser Aussage ist jener, dass der Auftragsverlust aufgrund eines Cyberangriffes stattfinden würde und dies die natürlichen Folgen eines solchen Angriffes darstellen. Kunden und Unternehmenspartner verlieren eventuell das Vertrauen zum Unternehmen, wenn diese Datenverluste aufgrund der Cyberkriminalität erfahren.

9.2 Grundfragen

Um den Experten und Expertinnen einen angenehmen Einstieg in das Interview zu ermöglichen, erhalten diese zu Beginn des Gespräches einige sehr allgemeine Fragen.

Begonnen wird dies mit der Position des Experten im Unternehmen. Diese teilen sich wie folgt ein in deren Unternehmen:

Person	**Position**
Experte 1	Head of Security
Experte 2	IT-Consultant
Experte 3	IT-Manager

Tabelle 8: Position der Experten und Expertinnen

Alle befragten Experten können hierbei Erfahrung in der IT und der IT-Security vorweisen. Experte 1 und 3 müssen diese Kenntnisse bei der täglichen Managementarbeit einbeziehen. Experte 2, welcher keine Managementposition besitzt, arbeitet jedoch auch an der IT-Sicherheit des Unternehmens und kann aus diesem Grund die benötigte Expertenmeinung zu dieser Arbeit beitragen.

Die darauffolgende Frage war die derzeitige Mitarbeiteranzahl im Unternehmen. Die Aussage der Experten war wie folgt:

Person	**Anzahl der Mitarbeiter und Mitarbeiterinnen im Unternehmen**
Experte 1	5000
Experte 2	280
Experte 3	310

Tabelle 9: Mitarbeiteranzahl im Unternehmen

Mit einer Mitarbeiterzahl von 5000 Mitarbeitern stellt das Unternehmen des ersten Experten eine große Kluft zu der Mitarbeiteranzahl der anderen Expertenunternehmen dar. Da alle Experten in Unternehmen von zumindest mittlerer Größe arbeiten, gibt es an dieser Stelle keine weitere Berücksichtigung dieser. Ausnahmen hätten überlegt werden müssen, wenn ein Experte oder eine Expertin nur in einem Kleinbetrieb gearbeitet hätte, dies hätte die Sicherheitsstrategie des Experten oder der Expertin eventuell stark von jener Strategie der anderen getrennt.
Auf die Frage, für wie wichtig die Experten die IT-Sicherheit ausmachen, gaben alle Experten an, dass diese für Sie die Wertung 10, sehr wichtig einnehmen würde. Die den Experten angebotene Skala reicht dabei von 1-10, wobei 1 die niedrigste Wertung ist und eine 10 die höchste.
Diese Frage gilt dazu, die generelle Meinung des Experten zum Thema IT-Sicherheit zu erfahren. Hätte ein Experte an dieser Stelle mit einer Wertung von 1 bis 4 geantwortet, dann würde eine solche Antwort einen Zweifel über dessen Interesse und Erfahrung in dem Bereich der IT-Sicherheit werfen und die Verwendung des Experteninterviews für diese Arbeit hätte stark überdacht werden müssen. Glücklicherweise wurde ohne Zögern von allen Experten die höchste Meinung zum Thema IT-Sicherheit eingenommen.
Anschließend wurden die Experten dazu befragt, welche Maßnahmen diese treffen oder in naher Zukunft geplant haben, um die Sicherheit für deren mobile Geräte zu erhöhen.
Experte 1 liefert hierbei eine kurze und prägnante Antwort:
„Unabhängig davon, wo die Daten liegen, müssen sie immer gleich geschützt sein.“
Mit einer solchen Aussage räumt Experte 1 schnell ein, dass egal wo Firmendaten gesichert werden, wie zum Beispiel auf Mobiltelefone, Notebooks, Server oder in der Cloud. Alle verwendeten Produkte müssen gleichermaßen vom Unternehmen geschützt werden. Nicht jedes Gerät oder Speicher erlaubt den gleichen Schutz, aber trotz alledem müssen alle Daten auf das gleiche oder zumindest ähnliche Level gesichert werden.
Um diesen Standard an Sicherheit zu erreichen, verwenden die Experten eine Ansammlung von Software- und Hardware-Lösungen und kombinieren diese mit sicheren Policies, welche alle Personen im Unternehmen zur Umsetzung der sicherheitsrelevanten Richtlinien bewegen.
Experte B plant für die weitere Verbesserung der Sicherheit die Akquirierung von Zertifizierungen. Im Zuge dieser Akquirierung muss das Unternehmen Sicherheitsanforderungen erfüllen, um die gewünschte Zertifizierung zu erhalten. Diese Sicherheit setzt einen passablen Standard in der Branche.
Experte C plant für die nächste Zeit die Einführung eines Mobile Device Management Systems. Der Einsatz von Mobile Device Management Systemen findet seine Wichtigkeit auch in den kommenden Hypothesen wieder und wird aus diesem Grund dort weiter erörtert.

Die nächste Frage, welche den Experten gestellt wurde, ist, wie hoch diese das Risiko eines Angriffes auf deren mobile Geräte empfinden. Wie bei der vorherigen Frage erhielten die Experten die Möglichkeit, auf einer Skala von 1 bis 10 zu antworten, wobei eine 10 die höchste Antwort darstellt.
Die Experten geben hier abermals stark ähnliche Aussagen und zwei Experten geben deren Einschätzung nach die Wertung 7 und einer die Wertung 8. Als Gründe für diese hohe Wertung wird die Gefahr, welche von Phishing ausgeht, von den Experten klargemacht.
Experte 1 gibt hierbei auch an, welche besondere Bedrohung von Mobiltelefonen ausgehen kann: „*Natürlich auf den kleineren Displays von Mobilgeräten. Es wird alles verkürzt. Dadurch ist es einfach schwerer zu erkennen, ob die App, die E-Mail oder diese Phishing E-Mails z.B. von der von einer validen Adresse kommen oder gespooft sind.“* Obwohl für den Experten eine erhöhte Gefahr für Mobilgeräte besteht, vermeidet dieser mit seiner Folgeaussage die gänzliche Unsicherheit von Mobiltelefonen: *„…heißt aber nicht, dass per se Mobilgeräte unsicher sind, denn die das möchte ich vermeiden, dass das mit Mund gelegt wird.“*. Auch Experte C erklärt dessen Respekt vor der Gefahr von Phishing-Mails. Nicht nur der Datendiebstahl bei Phishing stellt eine Gefahr für diesen dar, auch ein möglicher Download von Malware, besonders Crypto-Viren, welche das Gerät und dessen Daten verschlüsseln, stellen eine besondere Gefahr dar. Experte B teilt diese Meinung und fügt hinzu das keine Person so vorsichtig arbeitet, dass diese von sich behaupten kann zu 100% geschützt zu sein.
Die letzte allgemeine Frage, welche den Experten gestellt wurde, ist die Frage zu den finanziellen Ausgaben im Bereich der IT-Sicherheit. Auch hier haben alle ausgewählten Experten eine überraschend ähnliche Meinung. Alle Experten sind der Meinung, dass die derzeitigen Ausgaben für die IT-Sicherheit als angemessen zu bezeichnen sind. Alle Experten sind jedoch der Meinung, dass zusätzliche Ressourcen aber gerne erwünscht werden. Nur im Unternehmen von Experten A, gibt es eine dedizierte IT-Security Abteilung, welche sich um den Sicherheitsbereich kümmert. In den Unternehmen der anderen Experten werden diese Aufgaben vom IT-Team und IT-Management übernommen. Dies überrascht kurzweilig, aber mit dem Vergleich der Mitarbeiteranzahl macht dies bereits mehr Sinn. Das Unternehmen von Experte A ist um ein Vielfaches größer als jene der anderen zwei Experten, eine dedizierte IT-Security Abteilung ist notwendig und wird sogar von einigen Kunden vertraglich gefordert. Die Unternehmen der anderen zwei Experten sind derzeit noch auf einer Firmengröße, wo diese Arbeit vom normalen IT-Team vollbracht werden kann.

Kategorie	Anzahl
Datenschutz	4
Sicherheitsrichtlinien	11
Software Security	3
Hardware Security	4
Schulungen	2
Phishing	3
restliche Malware	2
Ransomware	2
Budget angemessen	3
Budgeterhöhung erwünscht	3

Tabelle 10: Kategorien allgemeine Fragen

Die Kategorien, welche für die Grundfragen erstellt wurden, zeigen ein eindeutiges Bild. Sicherheitsrichtlinien sind die Hauptverteidigung der Experten. Die Experten separieren ihre Daten und versuchen die Mitarbeiter und Mitarbeiterinnen so zu schulen, dass diese keine kritischen Daten lokal am mobilen Gerät belassen. Zusätzlich verschlüsseln zwei der drei Experten ihre Geräte mit der Bitlocker Laufwerksverschlüsselung.

Die Unternehmen der Experten verwenden auch die anderen Standardmaßnahmen, welche im IT-Bereich verwendet werden. Voran die Verwendung von Firewalls und Anti-Spam-Lösungen, welche das Unternehmensnetzwerk an dessen Grenze zum Internet schützen. Diese Maßnahmen stellen aber einen solchen Standard in der IT dar, dass diese von den Experten nicht großflächig erwähnt werden. Oftmals werden diese Lösungen zusätzlich von einem eigenen Team, dem Netzwerkteam, durchgeführt. Ähnlich ist die Situation mit Security-Software. Programme, mit welchen die Sicherheit des Betriebssystems vor Malware gewährleistet wird, wie ein Antivirensystem, gehören zu einem solchen Standard in der Industrie, dass ein Gerät ohne aktiven Virenschutz, aufgrund von Würmer und Crypto-Viren, eine Bedrohung für das ganze Unternehmen darstellen könnte.

Die Experten gaben zudem alle an, dass diese der Meinung sind, dass das Budget, welche diese für die IT-Sicherheit aufweisen können, als angemessen betrachtet werden kann. Interessanterweise gaben alle Experten im Anschluss auf diese Aussage an, dass das Budget durchaus höher sein könnte, aber derzeit angemessen ist. Dies ergibt Sinn, die Experten besitzen die Möglichkeiten das Unternehmensnetzwerk und dessen Geräte darin abzusichern, aber die Einführung von so mancher Software konnte aufgrund finanzieller Möglichkeiten nicht abgeschlossen werden. Zwei der drei Experten besitzen derzeit kein MDM-System im betriebsbereiten Status. Beide planen aber die Einführung eines solchen Systems für die Absicherung der mobilen Geräte.

Zusätzlich besaßen dieselben zwei Experten der kleinen Unternehmen auch keine dedizierte Stelle für einen IT-Security verantwortlichen. Wie bereits zuvor kurz erwähnt, kann diese Stelle

bei Klein- und Mittelunternehmen noch vom Management und der IT-Abteilung durchgeführt werden, ab einer bestimmten Größe empfiehlt es sich jedoch, eine dedizierte Person für diese Arbeit anzustellen.

9.3 Erkenntnisgewinnung für Hypothese 1

Hypothese 1: Durch das Eintreten der COVID-Pandemie stieg das Sicherheitsbewusstsein im Bereich des Mobile Computings.

Kategorie	Anzahl
Schulung	6
Software Security	1
Schulung vor COVID	3
Stagnation	3

Tabelle 11: Kategorien Hypothese 1

Das Sicherheitsbewusstsein der Experten im Bereich der Sicherheit von mobilen Geräten war bereits vor dem Eintreten der COVID-Pandemie hoch. Alle drei Experten gaben an, dass deren Mitarbeiter und Mitarbeiterinnen bereits vor dem Beginn der Pandemie bereits regelmäßige Schulungen zum Thema IT-Sicherheit besaßen.
Der Standard ist hierbei eine jährliche Schulung. Um den Groll von Mitarbeitern oder dem Management aufgrund zu langer oder vieler Trainings zu vermeiden, kombinieren die Experten die vorhandenen Sicherheitstrainings zu einzelnen Schulungen, welche einen möglichst umfassenden Überblick über IT-Sicherheit und Compliance bieten soll. Ein Teil dieser Schulung sind der Umgang mit den mobilen Geräten und Aktionen, welche es zu vermeiden gilt oder Maßnahmen, welche zu treffen sind, wenn das Gerät gestohlen werden würde. Teil dieser Schulungen ist das Erkennen von E-Mails mit gefahrvollen Absichten. Bereits bei den allgemeinen Fragen gaben die Experten an, dass die Gefahr, welche von E-Mails ausgehen kann, eine der größten für die jeweiligen Unternehmen sei. Die Gefahr von Phishing ist dermaßen hoch und allgegenwärtig, dass dies von den Experten beinahe so oft erwähnt wurde als jegliche restliche Malware inklusive Ransomware.
Moderne Phishing-Webseiten sind nur schwer von ihren originalen zu unterscheiden. Der größte Hinweis ist zumeist ein falscher Uniform Resource Locator (URL), welcher die Absichten der Website bekannt macht. Wie von Experten 1 jedoch erwähnt, ist eine solche URL schwer auf Mobiltelefonen zu erkennen, wodurch diese ein größere Anfälligkeit für solche Angriffe darstellen können.
Auch die Gefahr von Ransomware wird von den Experten nicht ignoriert. Im Gegensatz zu Phishing besitzen Experten jedoch Möglichkeiten, sich gegen Ransomware abzusichern. Moderne Antivirensysteme haben oftmals die Möglichkeit, die Schadsoftware zu erkennen und diese

an der Ausführung ihrer Arbeit zu verhindern. Obwohl ein Benutzer die Schadsoftware heruntergeladen und ausgeführt hat, so schützt das Antivirenprogramm das Gerät vor den negativen Konsequenzen.
Diesen Schutz gibt es jedoch nicht für die meisten Phishing-Angriffe. Individuelle Phishing-Webseiten nutzen deren Domain nur für eine jeweils kurze Zeit, bevor diese an andere Webseiten und Dienste gemeldet wird und auf einer Blacklist landet. Dieser kurze Zeitraum reicht oftmals aus, um das Opfer dazu zu bringen, sich auf der Zielseite anzumelden und damit seine Login-Informationen kundzutun.
Aus diesem Grund ist die beste Lösung gegenüber Phishing-Angriffen die konstante Schulung der Mitarbeiter und Mitarbeiterinnen eines Unternehmens. Jede einzelne Person, wird diese nicht ausreichend geschult, stellt ein mögliches Einfallstor gegen Angriffe dieser Art. Dies zwang die Experten bereits vor dem Aufkommen der COVID-Pandemie ein aktuelles und sich wiederholendes Schulungsprogramm für deren Mitarbeiter und Mitarbeiterinnen aufzubauen.
Die Experten gaben zusätzlich jedoch auch an, dass in der Zeit seit dem Beginn der Pandemie auch keine eindeutigen Verbesserungen durchgeführt wurden. Dies hat mehrere Gründe, da zu einem das Sicherheitsbewusstsein der Experten bereits sehr hoch war und diese Schulungen bereits anboten. Zusätzlich darf nicht die schlechte wirtschaftliche Lage, welche seit dem Eintritt der COVID-Pandemie existiert, vergessen werden. Viele Unternehmen vermeiden derzeitige Investitionen in Projekte und pausieren diese auf einen späteren Zeitpunkt. Andere Punkte, wie Beispielsweise die Last auf die Hardware und VPN-Dienste des Unternehmens aufgrund der Home-Office Policy rückten in den Vordergrund.
Für den Autor kann aus diesen Gründen Hypothese 1 als widerlegt angesehen werden. Das Sicherheitsbewusstsein im Bereich des Mobile Computings erlebte keinen plötzlichen Anstieg seit dem Eintreten der COVID-Pandemie. Experten waren bereits davor auf eine solche Situation, wenngleich auch nicht in diesem Ausmaß vorbereitet und konnten die IT ohne große Hindernisse auf den Homeoffice-Betrieb umstellen.

9.4 Erkenntnisgewinnung für Hypothese 2

Hypothese 2: Unternehmen sind gut auf den physikalischen Diebstahl von mobilen Geräten vorbereitet, weshalb ein solcher in den meisten Umständen nur wenig Schaden verursacht.

Kategorie	Anzahl
Reduktion Diebstähle	1
keine Diebstähle	2
Sicherheitsrichtlinien	7
Anschaffung Ersatzgerät	2
keine Vorbeugemaßnahmen	2
Schulungen	3
Cyberkriminalität	4

Tabelle 12: Kategorien Hypothese 2

Anhand der erstellten Kategorien kann schnell erkannt werden, dass die befragten Experten und damit auch deren Unternehmen keine größeren Probleme mit Diebstählen besitzen. Zwei der Experten merken hierbei an, dass es keine Diebstähle in der letzten Zeit gab, bei einem der befragten Experten konnte dieser Zeitraum überraschenderweise auf drei Jahre erweitert werden: *„Ich bin sehr froh darüber, dass ich es sagen kann, und ich kann es sogar ausweiten auf die letzten drei Jahre, es ist noch nie etwas verloren gegangen oder gestohlen worden. Kein Gerät, nicht einmal ein Handy."*

Die Tatsache, dass die Unternehmen eine solch geringe Verlustrate besitzen, beantwortet aber nicht die aufgebaute Hypothese, in dieser wird angenommen, dass diese auf einen eventuellen Diebstahl gut vorbereitet sind. Ein Teil kann hierbei der Pandemie zugeschrieben werden und den damit einhergehenden verringerten Freizeit- und Reisemöglichkeiten. Die Tatsache, dass die Unternehmen der Experten jedoch nur eine solch geringe Verlustrate aufweisen können, zeigt, dass von den Unternehmen und deren Experten verschiedene Methoden angewandt werden, welche die Diebstahlrate senkt. Experte A gibt dabei folgende Aussage zur Prävention von Diebstählen: *„Crime Prevention ist immer etwas Schönes. Natürlich, man gibt seinen Mitarbeitern Schulungen, wo man sagt, tragt der eure Tasche richtig, wenn ihr euch in der Metro befindet und dergleichen. Damit reduziert man es natürlich, aber man beseitigt es nicht. Wenn eine Stadt von Haus aus. Nehmen wir einfach Paris her, welches eine hoher Diebstahl Rate hat und man setzt dort viele Mitarbeiter hin, dann ist es automatisch vorhersehbar, dass es Diebstähle gibt. Das heißt, man kann mitregierende Maßnahmen treffen."*

Experte A, welcher von den vorhandenen Experten in dem mit 5000 Mitarbeitern größten Unternehmen arbeitet, gibt an, dass deren Diebstahlrate starke Schwankungen in unterschiedlichen Ländern aufweist und für diese Länder spezielle Maßnahmen getroffen werden können, um die Diebstahlrate zu verringern. Experte B erläutert auf diese Frage, dass die Konsequenzen, wie der persönliche Datenverlust der Mitarbeiter und Mitarbeiterinnen an diese hervorgehoben wird:

„Immer wieder die Konsequenzen darlegen, das bedeutet, wenn sowas verloren wird. Das ist deshalb immer der Vergleich, denn wenn die privaten Daten von jemanden auf dem Gerät gespeichert werden, ob es gemocht wird, dass diese verloren gehen. Und da muss ich sagen, das fruchtet und die Leute passen sehr gut drauf.“

Somit kann gesagt werden, dass die Experten ihr bestmögliches geben, um den generellen Diebstahl von Geräten auf das Minimum zu reduzieren. Es soll für diese nicht zu dem Moment kommen, wenn das Gerät gestohlen wird und die getroffenen Schutzmöglichkeiten notwendig werden.

Mit dem Vorkommen eines Diebstahls muss aber gerechnet werden. Auch jene Experten, bei welchen es seit einiger Zeit keinen Diebstahl gab, gaben trotzdem an, dass deren Geräte einen adäquaten Schutz aufweisen können. Von Experte A wird dabei folgende Gefahr angegeben:

„Der Schaden geht vom Wert die des Gerätes selbst hat im Optimalfall. Bis im schlimmsten Fall, wenn jemand seine Zugangsdaten aufgeschrieben hat, um auf den Terminal Server zu kommen oder ein sehr leichtes Passwort vergeben hat, dann kann der Schaden enorm sein. Es ist schwer abschätzbar.“

Jeder Diebstahl besitzt damit den Mindestschaden des verlorenen Gerätes. Besitzen Unternehmen an dieser Stelle eine aktuelle Festplattenverschlüsselung und ist das Gerät deaktiviert, dann kann davon ausgegangen werden, dass die Daten am Gerät unantastbar sind und somit vor Fremdzugriff ausreichend geschützt sind. Ein Angreifer oder eine Angreiferin, welche nicht zu den Daten gelangen kann, kann bestenfalls je nach Art der Verschlüsselung nur die Festplatte tauschen oder im schlimmsten Fall das ganze Gerät nicht verwenden.

Experte A gab dabei folgende Aussage zu der Gefahr eines verlorenen Gerätes an: *„Natürlich ist es eine absolute Gefahr. Am Ende vom Tag ist das Mobilgerät auch wieder nur ein Gateway ins Netz der der Firma und in dieser Welt, in der wir derzeit leben, wo jeder connected sein möchte, immer Zugriff auf Daten haben möchte, egal wo er sich befindet. Bedeutet dies auch, dass das Mobilgeräte Zugriff auf diese Daten hatte. Das heißt, wenn man nicht im Vorfeld Schritte unternommen hat wie PIN-Code, two factor authentication, womöglich, wenn gewünschtes oder erforderlich ist oder eben Verschlüsselung, ganz klar, dann kann ein gestohlenes Gerät relativ schnell zu großen Problemen führen. Wenn sich auf dem Gerät Daten befinden oder wenn das Gerät entsperrt in die Hände von einem Angreifer fällt, der dann gemütlich auf das E-Mail-System oder die Dateien Ablage zugreift. Aber es kommt auch auf die Maßnahmen an, die getroffen werden, um nachts schlafen zu können.“*

Experte A lässt hierbei erkennen, dass dieser eine Reihe von Methoden einsetzt, um die Sicherheit der Geräte zu garantieren. Sicherheitsvorkehrungen wie Verschlüsselung, PIN-Codes, Two-Factor-Authentication verringern die Chance, dass Angreifer einen Zugriff auf die Daten im Unternehmensnetzwerk erhalten können. Interessanterweise gibt dieser jedoch auch an, dass der

Balanceakt, welcher zwischen der Sicherheit und der Usability existiert, immer in Betracht gezogen werden muss. Werden Benutzer mit zu vielen Sicherheitsvorkehrungen bei deren Arbeit belästigt, so finden diese eventuell Möglichkeiten, welche die getroffenen Vorkehrungen aushebeln könnten. Ein bekanntes Beispiel dafür sind Personen, welche aufgrund eines zu häufigen Passwortwechsels deren Kennwörter auf den Monitor oder unter die Tastatur kleben. Der häufige Wechsel eines Kennwortes wird aus diesen Gründen von vielen Experten und Unternehmen nicht weiterempfohlen.

Auch Experte B teilt unwissentlich die gleiche Meinung der anderen Experten: *„Also grundsätzlich ist das so wie gesagt, dass wir schon auch sehr auf Sicherheit achten. Aus diesem Grund sind TPM Chips im Einsatz. Bitlocker Verschlüsselung bei den mobilen Geräten. Es wird auf sichere Passwörter geachtet. Auf sinnvolle Passwort Richtlinien. Und unsere Mitarbeiter werden natürlich auch darauf hingewiesen, wo und wie sie Daten ablegen sollen oder müssen. Und unter anderem aber sag ich mal, kann der Schaden durch ein verlorenes Gerät sehr hoch sein. Das kann bis zum Verlust von Aufträgen und viel mehr führen. Aber grundsätzlich aufgrund der Verschlüsselung und Absicherunsmechanismen, die wir im Einsatz haben ist der Schaden bei korrekter Einhaltung der Richtlinien und Umsetzung unserer technischen Maßnahmen eher der Zeitaufwand, den welche unsere Mitarbeiter haben, wenn sie ihre Geräte wieder neu einrichten, bis sie dann das neue Gerät haben und so weiter. Das in dem Sinne aufgrund bestimmter Richtlinien und Maßnahmen sag ich mal, sollte sich der Schaden in Grenzen halten.“*

Zwei der drei Experten, welche eine Geräteverschlüsselung besitzen, wirken damit sehr überschaubar auf die maximale Gefahr, welche durch einen Datendiebstahl verursacht werden kann. Das Ärgernis über den Verlust des Gerätes und den damit verbundenen Prozess der Neuanschaffung, Installation und Konfiguration wirkt dabei fast größer an diese als der Diebstahl selbst. Lediglich Experte C, in dessen Unternehmen keine Verschlüsselung verwendet wird, gibt sich unsicher über den maximalen Schaden, welcher bei einem Diebstahl eintreten kann. Dieser führt jedoch aufgrund der fehlenden Diebstahlrate in den letzten drei Jahren andere präventive Maßnahmen durch, damit es nie zu einem solchen Schaden kommt.

Diese Aussagen spiegeln sich auch in den erstellten Kategorien wider. Die Kategorie „Sicherheitsrichtlinien“ ist erneut die häufigste Kategorie. Dies zeigt schnell das Vertrauen, welches Experten in deren Vorkehrungen getroffen haben und zurecht, da es sich hierbei um Industriestandards handelt, welche von den meisten Unternehmen getroffen werden.

Hypothese 2 wird aus diesem Grund vom Autor als korrekt angesehen. Die befragten Experten gaben alle an, dass der Diebstahl von Geräten als Gefahr bekannt ist und unterschiedlichste Sicherheitsrichtlinien verwendet werden, um den Schutz der Geräte zu garantieren. Dieser Schutz weitet sich dahingehend aus, dass zwei der drei Experten alle Geräte im Unternehmen verschlüsseln, sodass diese für potenzielle Angreifer oder Angreiferinnen praktisch unverwertbar werden, falls ein Gerät in deren Hände fällt.

9.5 Erkenntnisgewinnung für Hypothese 3

Hypothese 3: Großunternehmen (> 250 Mitarbeiter) besitzen bereits ein Mobile Device Management System, oder arbeiten derzeit an der Implementierung eines solchen, um notwendige Sicherheitsvorschriften auf mobilen Geräten umsetzen zu können.

Kategorie	Anzahl
vorhandenes MDM	1
Sicherheitsrichtlinien	5
remote Gerätelöschung	2
Software Security	1
kein vorhandenes MDM	2

Tabelle 13: Kategorien Hypothese 3

Wie in Tabelle 9 ersichtlich, erreichen alle Experten die von der Hypothese gewünschten Mindestgröße von 250 Mitarbeitern, damit ist keinerlei Anpassung an der gegebenen Hypothese notwendig, auch wenn das Unternehmen von Experten A um ein Vielfaches größer ist als jenes der anderen Experten.

Anhand der gesetzten Kategorien ist schnell ersichtlich, dass nur einer der drei Experten ein betriebsfunktionales Mobile Device Management System vorweisen kann. Dies erscheint logisch, da das Unternehmen von Experten A bereits eine so hohe Mitarbeiteranzahl aufweist, dass ein Mobile Device Management System für das Unternehmen notwendig ist. Auch Experte A vertritt diese Meinung mit folgender Aussage: *„Absolut. Wir besitzen ein Mobile Device Managementsystem. Also ich weiß, Ihre Frage hat gerade damit begonnen, ob bei mehr als 250 Mitarbeiter. Selbst bei 200 Mitarbeitern würde ich es brauchten. Wobei das Mobile Device Managementsystem dann am Ende vom Tag, und wir hatten es ja ein oder zwei Fragen vorher, ein Gateway zu den Daten ist, das können Kundendaten, oder Internetdaten sein. Am Ende vom Tage ist es egal, was für Daten es sind. Aber es muss klar sein, dass die Daten geschützt werden, wenn ich ohne Mobile Device Management Diensthandys betreibe, die aber dann Zugriff auf Daten gebe, dann kann das relativ schnell in die Fahrlässigkeit führen. Das heißt kleine Investitionen in Mobility Device Management selbst bei einer großen Anzahl an Mitarbeitern schlägt das wenig ins Geld und ist in den Schutzmechanismus, den es bietet, definitiv wert.“*

Durch die Aussage von Experte A wird schnell ersichtlich, dass ein Mobile Device Management zur absoluten Grundausstattung für eine erfolgreiche Mobilgeräteverwendung von Nöten ist. Dies wirft im weiteren Sinne die Frage auf, wieso die restlichen Experten derzeit kein vorhandenes Mobile Device Management System aufweisen können. Experte B konnte zu dessen fehlenden MDM-System folgende Aussage geben:

„Wir sind gerade in der Pilotphase. Wir schauen uns gerade verschiedene Lösungen an. Wir sind da leider ein wenig hinten nach, weil aber zwischendurch Ressourcen technisch einfach bestimmte andere Themen mehr in den Vordergrund gerutscht sind, wodurch das Thema Mobile

Device Management leider ein wenig vernachlässigt wurde. Aber aufgrund der Corona Pandemie ist jetzt recht schnell wieder geändert und wir sind gerade daran eine sinnvolle Mobile Device Management Lösung zu evaluieren und einzuführen.“

Die Aussage von Experten C ist hierbei sehr ähnlich, auch dieser plant die Einführung für das aktuelle Jahr.

Es wird daher schnell ersichtlich, dass alle Experten sich ein Mobile Device Management System wünschen und versuchen, dieses so schnell wie möglich in deren Unternehmen einzuführen. Die Vorteile, welche das System für das Unternehmen bieten kann, sind vielfältig. Experte A gibt hierbei folgende Aussage zu den verwendeten Funktionen von dessen MDM-System*: „Natürlich ganz klar Policies. Wir geben die Security-Policies vor. Sei das jetzt Passcode, damit ein Standard Pattern nicht verwendet werden kann. Wir hatten hierbei iPhones, wo wir kein Work Profil erstellen können. Auf Wunsch des Herstellers haben wir trotzdem die Möglichkeit, dass wir sagen "Okay, der Hersteller weigert sich, aber wir verwenden Applikationen, die sich selber schützen können". Damit gemeint sind die Office 365 Applikationen und wir verwenden hier ebenfalls Device Policies, wo wir sagen „okay, jemand kann WhatsApp verwenden. Das ist okay.“ Aber WhatsApp, als Beispiel, kann dann nicht auf die Outlook Daten zugreifen, da sich die Outlook Applikation dann selbst schützen würde und im Verlustfall können wir auch sagen „ok, destroy the data“ und können so unsere Firmendaten schützen, falls das Gerät gestohlen wird.“*

Auch diese Aussage spiegelt sich in den vorhandenen Kategorien wider. Es wird sofort ersichtlich, dass die Experten bei der Verwendung eines Mobile Device Management Systems stark auf den Einsatz von Sicherheitsrichtlinien setzen. Obwohl das MDM-System auch für die Installation und Konfiguration der Geräte verwendet werden kann, wird dies von den Experten nicht häufig erwähnt und diese Funktion wirkt daher für diese wie ein optionales Feature, welches verwendet werden kann, aber im Gegensatz zum Einsatz von Sicherheitsrichtlinien nicht die höchste Priorität einnimmt. Die Zusammenfügung der Kategorie „Sicherheitsrichtlinien“ erfolgte an dieser Stelle aus den vorhandenen Kategorien „Datenseparation“, „Applikationssperre“ und „Unternehmensrichtlinien“. Der Wunsch der Datenseparation wird vor allem von Experten A häufig erwähnt und der Nachteil, dass Mobiltelefone von Apple diese Funktion nicht anbieten, ist erkennbar. Aufgrund des hohen Marktanteiles und anderen unternehmensinternen Gründen kann dieser jedoch auch nicht einfach auf eine reine Verwendung von Android-Geräten umsteigen. Die Kategorie „Unternehmensrichtlinien“ spiegelt vor allem Standardrichtlinien wider, welche von den Experten gesetzt werden. Ein bekanntes und häufig erwähntes Beispiel wäre hierbei der Einsatz einer Kennwort- oder PIN-Policy, welche den Benutzer oder die Benutzerin dazu zwingt, das Gerät abzusichern.

Die Kategorie Applikationssperre ist die letzte Kategorie, welche in die Schlüsselkategorie „Sicherheitsrichtlinien“ einverleibt wurde. Der genaue Aspekt der Applikationssperren wird in Hypo-

these 4 näher betrachtet, aber es ist ersichtlich, dass die Experten eine Notwendigkeit darin erkennen, dass bestimmte Applikationen nicht vertrauenswürdig sind und nicht auf Firmengeräte gelangen sollten.
Zuletzt erhält die Kategorie „remote Gerätelöschung“ Erwähnungen. Vom Autor wurde hierbei überlegt diese Kategorie zur bestehenden Schlüsselkategorie „Sicherheitsrichtlinien“ hinzuzufügen, aber schlussendlich wurde sich dagegen entschieden, da diese Funktion von den Experten besonders hervorgehoben wurde. Die remote Gerätelöschung stellt für Experten die letzte Möglichkeit dar ein Gerät, nachdem es verloren oder gestohlen wurde, zu löschen und damit die absolute Sicherheit der Daten zu garantieren.
Auch Hypothese 3 kann aus diesem Grund vom Autor als korrekt angesehen werden. Obwohl nur einer der Experten ein einsatzfähiges Mobile Device Management System vorweisen kann, arbeiten die restlichen Experten bereits an der Einführung eines solchen. Alle Experten haben das mögliche Risiko von mobilen Geräten und den potenziellen Nutzen eines Mobile Device Management Systems erkannt und versuchen diese Vorteile für sich zu verwenden.

9.6 Erkenntnisgewinnung für Hypothese 4

Hypothese 4: Der Sicherheitsaspekt von Unternehmensfremden Applikationen auf Mobiltelefonen wird derzeit noch unzureichend überwacht, weswegen solche ein mögliches Sicherheitsrisiko darstellen.

Kategorie	Anzahl
Sicherheitsrichtlinien	8
Sicherheit ist angemessen	6
Verbesserungspotenzial vorhanden	2

Tabelle 14: Kategorien Hypothese 4

Es wird schnell ersichtlich, dass Tabelle 14 mit nur drei Kategorien die kleinste Kategorientabelle von allen vier Hypothesen darstellt. Die Erklärung findet sich hierbei in der Schlüsselkategorie „Sicherheitsrichtlinien“, welche aus 4 einzelnen Kategorien zusammengefügt wurde.
Den Experten wurde separat die Frage gestellt, wie diese die getroffenen Schutzmaßnahmen sowohl für Notebooks als auch für deren Mobiltelefone bewerten würden. Alle drei Experten gaben dazu an, dass die getroffenen Sicherheitsrichtlinien und Schutzmaßnahmen für die Geräte angemessen seien. Zwei der drei Experten gaben jedoch zusätzlich auch an, dass Verbesserungspotenziale weiterhin ausnutzbar seien und es laufende Verbesserungen in deren Unternehmen in der Zukunft geben werde.
Experte A gibt hierbei folgende Aussage: „*Es gibt sowas wie zu viel Sicherheit. Das wird gerne übersehen. Aber am Ende von Tag kann man es auch übertreiben. Und wenn man es übertreibt,*

dann schränkt man die Mitarbeiter ein. Das muss man immer im Hinterkopf behalten. Ist die Sicherheit Adäquat für die Daten? Definitiv. Sonst könnte ich nachts nicht schlafen. Und ich muss es ja am Ende vom Tag verantworten. Das heißt, ich muss das Mindestmaß zusichern, um sagen zu können Ich habe mein Bestes getan. Sehe ich aber definitiv Technologien am Markt, wo ich sage, ja, das wäre klasse, wenn wir sie hätten, oder das könnte Dinge verbessern. Definitiv."

Experte A spricht erneut über den feinen Grad zwischen der IT-Sicherheit und Verwendbarkeit von Geräten und Applikationen. Die Sicherheit kann weiter erhöht werden, aber Benutzer und Benutzerinnen könnten dann aufgrund der hohen Sicherheitsrichtlinien mit Groll auf die hohen Sicherheitsanforderungen reagieren. Benutzer und Benutzerinnen werden oftmals bei vielen Sicherheitsanforderungen zu längeren Prozeduren für deren Authentifizierungen gezwungen.

Im Unternehmen von Experten C wird dies etwas anders versucht. Dieser versucht eine generelle Vermeidung von Datenverlust durch das Fehlen von diesen auf den lokalen Geräten der Benutzer und Benutzerinnen. Stattdessen müssen Mitarbeiter und Mitarbeiterinnen, welche im gleichen Unternehmen wie Experte C arbeiten, auf einen Terminalserver zugreifen, um ihre weitere Arbeit zu verrichten. Die genaue Aussage von diesem ist dabei folgende: „*Durch die Abtrennung, dass auf den lokalen Geräten keine Daten oben sind, ist das schon ein sehr guter Weg, und dass man sie ihm zweimal authentifizieren muss. Zum einen auf dem lokalen Gerät selbst und dann am Terminal Server noch einmal mit unterschiedlichen Zugängen und dann um an die Daten, die gearbeitet wird, muss man sich nochmal anmelden. Ich denke, dass der Schutz durchaus angemessen ist.“*

Die letzte Frage, welche den Experten während dem Interview gestellt wurde, ist die Frage, welche Limitierungen für Applikationen auf Mobiltelefonen bestehen. Aufgrund der vorherigen Information, dass nur einer der drei Experten ein funktionierendes Mobile Device Management System vorweisen kann, könnte angenommen werden, dass auch nur im Unternehmen von Experten A bestimmte Applikationen aus Sicherheitsgründen gesperrt wurden. Dem ist jedoch nicht so und auch Experte C, bei welchem ein MDM-System noch in Planung steht, fand hierbei eine Möglichkeit, unerwünschte Applikationen auf den Mobiltelefonen der Mitarbeiter und Mitarbeiterinnen zu sperren: „*Ja, es mit einer App-Blocker-App, die heißt App-Block wird limitiert, dass überhaupt nichts installiert werden kann. Es kann nicht mal der App-Store aufgemacht werden ohne Passwort.“*

Experte A, welcher ein MDM-System im Unternehmen aufweisen kann und in dem größten Unternehmen von den drei Experten arbeitet, gibt hierbei an, dass es hierbei, je nach Land, unterschiedliche Richtlinien gibt: „*Hier muss man ganz stark differenzieren. Denn dies ist Land zu Land leicht unterschiedlich. Aber in den meisten Fällen darf das Mobiltelefon von den Mitarbeitern auch zu privaten Zwecken verwendet werden. Aus solcher Sicht muss ich natürlich dann auch sagen, sie dürfen private Applikationen installieren und das schließt im Grunde den Kreis wieder zurück*

zum Android Enterprise oder diesem Work Profil. Denn hier haben wir dieses fantastische, perfekte Beispiel, wo wir sagen können, Im Standardprofil kann der Mitarbeiter mit dem Gerät machen, was immer sein Herz danach sehnt. Aber im Work-Profil ist es dann ganz klar restriktiv, was sich installieren lässt und worauf diese Applikationen dann Zugriff haben. Das sorgt natürlich für Unmut, weil dann viele Dinge nicht funktionieren, die die Leute gerne hätten. Und dann braucht es einer sicheren Überprüfung, bevor die Applikation freigegeben wird. Aber wir versuchen trotzdem, diese Balance zu schlagen."

Je nach Land müssen mussten solche Richtlinien von Experte A daher angepasst werden, aber die Funktion des Work-Profils auf Android-Geräten bietet eine gute Möglichkeit zur Datentrennung auf dem Gerät. Apple, hierbei etwas restriktiver in der Funktion, bietet diese Möglichkeit noch nicht, aber bietet im Gegenzug auch andere Vorteile wie jene, dass diese deren Mobiltelefone auch nicht für Geheimdienste entsperren würden.

Mit diesen Informationen ist es die Meinung des Autors, dass Hypothese 4 als widerlegt angesehen werden. Zwei der drei Experten besitzen eine Möglichkeit, die Applikationen auf den Mobiltelefonen der Mitarbeiter und Mitarbeiterinnen einzuschränken. Lediglich Experte B, welcher erst an der Einführung des Mobile Device Management Systems arbeitet, besitzt dazu keine Möglichkeit. Dieser plant die Einführung jedoch noch im Jahr 2021 und sieht die potenzielle Gefahr, welche von unkontrollierten Applikationen existieren könnte.

10 CONCLUSION UND AUSBLICK

Das folgende Kapitel betrachtet die gewonnen Erkenntnisse der Arbeit und gibt einen Ausblick auf zukünftige Forschungen, welche mithilfe dieser Arbeit weiter untersucht werden könnten.

10.1 Conclusio

In den Interviews, welche mit den Experten durchgeführt wurde, konnte ein großer Einblick in die Arbeitsweise, Maßnahmen und Standards der Experten beobachtet werden. Die Sicherheitsexperten reagierten, obwohl diese keine Bekanntschaft untereinander aufweisen konnten, auf viele Sicherheitsrisiken auf dieselbe Art. Dies ist nachzuvollziehen, da bestimmte Standards sich in der Industrie durchgesetzt haben. Es sind jedoch trotz alledem eindeutige Unterschiede ausmachbar, welche die Möglichkeit bietet, die Forschungsfrage zu beantworten, welche Möglichkeiten zur Absicherung der mobilen Geräte im Home-Office-Einsatz die Sicherheitsexperten am geeignetsten ansehen.

Die erste angefertigte Hypothese stellt die Frage, ob aufgrund des erhöhten Homeoffice-Einsatzes das Sicherheitsbewusstsein im Bereich des Mobile Computings einen plötzlichen Anstieg erlebte. Diese Hypothese konnte vom Autor als widerlegt angesehen werden. Experten wurden durch den hohen Andrang in das Homeoffice nicht überrascht und mussten maximal kleinere Probleme wie die Erweiterung der vorhandenen VPN-Lizenzen beheben.

Hypothese 2 wird vom Autor hingegen als korrekt angesehen und befasste sich mit der Frage, ob die Experten sich auf den physikalischen Diebstahl von Mobilgeräten ausreichend gut vorbereitet haben, um die möglichen hohen Schäden eines solchen Ereignisses abzuschwächen. Dies wurde von den Experten definitiv erfüllt. Die Experten überraschten an dieser Stelle mit einer sehr geringen Diebstahlrate im Unternehmensumfeld, aber auch wenn ein solcher Diebstahl stattfinden würde, wäre der übliche Schaden sehr gering da Aufgrund von Standards wie Verschlüsselung und durch die Trennung der Daten vom Gerät nur wenig von einem potenziellen Angreifer oder einer potenziellen Angreiferin gewonnen werden könnte.

Auch Hypothese 3 konnte vom Autor als korrekt betrachtet werden. Alle befragten Experten gaben an, dass diese ein Mobile Device Management System besitzen oder derzeit an der Einführung eines solchen arbeiten. Aufgrund der beim Schreiben dieser Arbeit aktuellen COVID-Situation, mussten Experten die Einführung eines solchen Systems einigermaßen verschieben, aber zielen eine Einführung weiterhin für dieses Jahr an. Dies bestätigt die Forschungsfrage dahingehend, dass der Einsatz eines Mobile Device Management Systems von allen Experten als essenziell angesehen wird und in den folgenden Jahren zu einem Standardtool der Branche werden wird.

Die vierte und letzte Hypothese konnte nach Meinung des Autors auch widerlegt werden. Zwei der drei Experten bieten die Möglichkeit an gewünschte Applikationen auf Mobiltelefonen zu blo-

ckieren. Dies schützt das Unternehmen vor eventuell gefährlichen Applikationen, welche Sicherheitslücken aufweisen oder selbst zu viele Daten der Nutzer und Nutzerinnen entwenden. Lediglich einer der Experten konnte ein solches System noch nicht aufweisen, aber dieser arbeitet jedoch an der derzeitigen Einführung eines MDM-Systems, welches sich derzeit in der Testphase befindet, um diesen Gefahrenvektor abzusichern. Hypothese 4 greift auf Hypothese 3 auf und betrachtet eine wichtige Eigenschaft des MDM-Systems. Die Experten verstehen die Gefahr, welche durch eine uneingeschränkt Applikations-Policy ausgehen könnte und versuchen auch diesen Gefahrenvektor zum Schutz der Unternehmenshardware und -informationen abzusichern.
Schlussendlich konnten mit dem Experten alle aufgestellten Hypothesen beantwortet werden. Hypothese 1 und 4 konnten vom Autor widerlegt werden. Die Experten zeigten sich zur Überraschung des Autors besser vorbereitet als erwartet und boten ähnliche Maßnahmen zur Absicherung der Geräte und Daten. Standards, welche zum derzeitigen Zeitpunkt noch nicht erfüllt werden konnten, werden von diesen nicht ignoriert und versucht in das Unternehmen einzuführen.
Die Hypothesen 2 und 3 konnten im Gegensatz als korrekt betrachtet werden. Die Gefahr eines Diebstahls und die damit einhergehende größere Gefahr eines Datenlecks wird von den Experten ernst genommen und mit bestem Wissen und Gewissen gemildert, um die Sicherheit der Unternehmensdaten zu garantieren.

10.2 Ausblick

Die verwendeten Methoden der Experten zur Absicherung der mobilen Geräte wirkt einheitlich und die befragten Experten verwenden dieselben oder zumindest ähnliche Maßnahmen, welche einen Standard in der Industrie darstellen. Aufgrund des schnellen technologischen Fortschrittes in der Security-Branche müssen diese Methoden jedoch wiederholt erfragt werden, um den aktuellen Status der Industrie zu ermitteln.
Bei den befragten Betrieben handelte es sich ausschließlich um Betriebe von deutschem oder österreichischem Ursprung. Es wäre daher im weiteren Zuge interessant zu ermitteln, ob diese Maßnahmen auch in unterschiedlichen Ländern, vor allem außerhalb Europas, durchgeführt werden. Eine mögliche Fortsetzung dieser Forschung fände sich in der generellen Erhöhung der befragten Experten für die Festigung der hier ermittelten Expertenmeinungen. Zusätzlich gäbe es weiter Gefahrenvektoren wie die Verwendung von Wearables wie Smartwatches oder anderen Internet of Things (IoT) Geräten, welche bei einer fortsetzenden Forschung dieser Arbeit ermittelt werden könnten.

11 ABKÜRZUNGSVERZEICHNIS

A

Applikationen ..... *App*

B

Bring Your Own Device ..... *BYOD*

C

Common Vulnerability Scoring System ..... *CVSS*

coronavirus disease ..... *COVID*

D

Datenschutz-Grundverordnung ..... *DSGVO*

E

Electrically Erasable Programmable Read-Only Memory ..... *EEPROM*

G

Gigabyte ..... *GB*

H

Hypertext Transfer Protocol ..... *HTTP*

Hypertext Transfer Protocol Secure ..... *HTTPS*

I

Internet of Things ..... *IoT*

iPhone Operating System ..... *iOS*

K

Kilobyte ..... *KB*

Künstliche Intelligenz ..... *KI*

M

Megabyte ..... *MB*

Mobile Application Management ..... *MAM*

Mobile Device Management ..... *MDM*

Mobile Information Management ..... *MIM*

Multi-Faktor-Authentifizierung ..... *MFA*

O

Open Broadcaster Software ..... *OBS*

P

Persönliche Identifikationsnummer ..... *PIN*

R

Random-access memory ..... RAM

S

Secure Shell ..... *SSH*

Solid-State-Drive ..... *SSD*

U

Uniform Resource Locator ..... *URL*

Universal Serial Bus ..... USB

V

Virtual Private Network ..... *VPN*

W

Wi-Fi Protected Access ..... *WPA*

Wi-Fi Protected Access II *WPA2*

Wired Equivalent Privacy ..... *WEP*

Wireless LAN ..... *WLAN*

Wireless Protected Setup ..... *WPS*

12 ABBILDUNGSVERZEICHNIS

13 TABELLENVERZEICHNIS

14 LITERATURVERZEICHNIS

Abdelgaffar, F. (2019). *Reaktionsanalyse von Unternehmen beim Eintritt eines Datenlecks*.

Afonin, O. (2020). *Introduction to BitLocker: Protecting Your System Disk*. Zugriff am 14.10.2020. Verfügbar unter: https://blog.elcomsoft.com/2020/01/introduction-to-bitlocker-protecting-your-system-disk/

Arias, D. (2018). *Adding Salt to Hashing: A Better Way to Store Passwords*. Zugriff am 14.10.2020. Verfügbar unter: https://auth0.com/blog/adding-salt-to-hashing-a-better-way-to-store-passwords/

Art. 33 Datenschutz-Grundverordnung.. Verfügbar unter: https://dsgvo-gesetz.de/art-33-dsgvo/

Art. 34 Datenschutz-Grundverordnung.. Verfügbar unter: https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

Artikel 29 Datenschutzgruppe. (2017). *Guidelines on Personal data breach notification under Regulation 2016/679* (Europäische Kommission, Hrsg.). Brüssel.

Chicola, J. (2019). *About Rev.ai*. Verfügbar unter: https://www.rev.ai/about

DATACOM Buchverlag GmbH. (2020). *Enterprise Mobility Management,* DATACOM Buchverlag GmbH. Zugriff am 01.02.2021. Verfügbar unter: https://www.itwissen.info/EMM-enterprise-mobility-management-Enterprise-Mobility-Management.html

Digistump. (2020, 12. November). *Digispark USB Development Board*. Zugriff am 12.11.2020. Verfügbar unter: http://digistump.com/products/1

Edwards, C. (2012). *OBS Studio*. Verfügbar unter: https://github.com/obsproject/obs-studio/blob/master/README.rst

Ely, A. (2020, 9. Oktober). *Rethinking Mobile Security - Why Apps Come First*. Zugriff am 11.10.2020. Verfügbar unter: https://www.securityweek.com/rethinking-mobile-security-why-apps-come-first

Gläser, J. & Laudel, G. (2012). *Experteninterviews und qualitative Inhaltsanalyse als Instrumente rekonstruierender Untersuchungen* (Lehrbuch). Wiesbaden: VS, Verl. für Sozialwiss.

Google. (2021). *What is a work profile? - Android Enterprise,* Google. Zugriff am 04.02.2021. Verfügbar unter: https://support.google.com/work/android/answer/6191949?hl=en&ref_topic=6151012

Hak5. (2020, 12. November). *Bash Bunny*. Zugriff am 12.11.2020. Verfügbar unter: https://shop.hak5.org/products/bash-bunny

Hunt, T. (2020). 10 Billion. *Troy Hunt*. Zugriff am 18.01.2021. Verfügbar unter: https://www.troyhunt.com/10b/

IBM Security (Hrsg.). (2019). *Cost of a Data Breach Report 2019*. Verfügbar unter: https://www.ibm.com/downloads/cas/ZBZLY7KL

Islam, A., Oppenheim, N. & Thomas, W. (2020). *SMB Exploited: WannaCry Use of EternalBlue*. Accessed 22.10.2020. Retrieved from https://www.fireeye.com/blog/threat-research/2017/05/smb-exploited-wannacry-use-of-eternalblue.html

Kahney, L. (2019). The FBI Wanted a Backdoor to the iPhone. Tim Cook Said No. *WIRED*. Zugriff am 04.02.2021. Verfügbar unter: https://www.wired.com/story/the-time-tim-cook-stood-his-ground-against-fbi/

Kam, K. (Forbes, Hrsg.). (2017). *After Falling 33%, Equifax Is Still Overvalued*. Zugriff am 07.01.2019. Verfügbar unter: https://www.forbes.com/sites/kenkam/2017/09/21/after-falling-33-equifax-is-still-overvalued/#70ae79722b88

Kaspersky, E. (2017, 26. Oktober). NSA contractor leaked US hacking tools by mistake, Kaspersky says. Verfügbar unter: https://www.theguardian.com/technology/2017/oct/26/kaspersky-russia-nsa-contractor-leaked-us-hacking-tools-by-mistake-pirating-microsoft-office

Kofler, M., Zingsheim, A., Gebeshuber, K., Widl, M., Aigner, R., Hackner, T. et al. (2018). *Hacking & Security. Das umfassende Handbuch* (1. Auflage). Bonn: Rheinwerk Verlag; Rheinwerk Computing.

Mayring, P. (2015). *Qualitative Inhaltsanalyse. Grundlagen und Techniken* (12., überarb. Aufl.). Weinheim, Basel: Beltz Verlag.

Metz, C. & Perlroth, N. (2018, 3. Januar). Researchers Discover Two Major Flaws in the World's Computers. *The New York Times*. Zugriff am 20.10.2020. Verfügbar unter: https://www.nytimes.com/2018/01/03/business/computer-flaws.html

Microsoft. (2020, 14. Oktober). *Retire or wipe devices using Microsoft Intune*. Zugriff am 14.10.2020. Verfügbar unter: https://docs.microsoft.com/en-us/mem/intune/remote-actions/devices-wipe

Mona Mangat. (2020). *17 Best Vulnerability Assessment Scanning Tools*. Zugriff am 02.10.2020. Verfügbar unter: https://phoenixnap.com/blog/vulnerability-assessment-scanning-tools

Morris, J. (EveningStandard, Hrsg.). (2018). *Heathrow Airport fined £120k over lost USB stick data breach,* 165348596842143. Zugriff am 19.12.2018. Verfügbar unter: https://www.standard.co.uk/news/uk/heathrow-airport-fined-120000-over-lost-usb-stick-data-breach-a3956631.html

Ossmann, M. (2020, 25. November). *Ubertooth*. Zugriff am 25.11.2020. Verfügbar unter: https://github.com/greatscottgadgets/ubertooth

Porup, J. M. (2019). *What is Metasploit? And how to use this popular hacking tool*. Zugriff am 14.10.2020. Verfügbar unter: https://www.csoonline.com/article/3379117/what-is-metasploit-and-how-to-use-this-popular-hacking-tool.html

RainbowCrack Project. (2020, 9. September). *RainbowCrack - Crack Hashes with Rainbow Tables*. Zugriff am 13.10.2020. Verfügbar unter: https://project-rainbowcrack.com/index.htm

Ryan, M. (2018). *mikeryan/crackle*. Zugriff am 25.11.2020. Verfügbar unter: https://github.com/mikeryan/crackle

Said, Y. (2020). *Exploitation Tools in Kali Linux 2020.1 – Linux Hint*. Zugriff am 14.10.2020. Verfügbar unter: https://linuxhint.com/exploitation_tools_kali_linux/

Verizon. (2020). *2020 Data Breach Investigations Report*.

Vigliarolo, B. (2018). *Brute force and dictionary attacks: A cheat sheet*. Zugriff am 14.10.2020. Verfügbar unter: https://www.techrepublic.com/article/brute-force-and-dictionary-attacks-a-cheat-sheet/

WannaCry. (2017, 13. Mai). Zugriff am 19.10.2020.

Warnke, S. (2020, 20. Mai). *Was ist Bluetooth? Alles rund um Funktion, Pairing, Sicherheit*. Zugriff am 25.11.2020. Verfügbar unter: https://www.inside-digital.de/ratgeber/bluetooth-erklaert

WhiteSource. (2019). *Understanding CVSS v3.1 - Security Boulevard*. Zugriff am 14.10.2020. Verfügbar unter: https://securityboulevard.com/2019/11/understanding-cvss-v3-1/

15 ANHANG A - INTERVIEWLEITFADEN

Forschungsfrage:

Welche Möglichkeiten zur Absicherung der Mobilen Geräte im Home-Office Einsatz sehen Sicherheitsexperten als am geeignetsten?

Allgemeine Fragen

1. Welche Position nehmen Sie in Ihrem Unternehmen ein?

2. Welche Mitarbeiteranzahl weist Ihr Unternehmen im Moment auf?

3. Für wie wichtig halten Sie die IT-Sicherheit, auf einer Skala von 0 (unwichtig) bis 10 (sehr wichtig), im Allgemeinen?

0	1	2	3	4	5	6	7	8	9	10

4. Beschreiben Sie die Maßnahmen, welche Sie derzeit treffen und in naher Zukunft geplant haben, um Ihre Sicherheit für mobile Geräte (Notebooks und Mobiltelefone) zu erhöhen.

5. Wie hoch, auf einer Skala von 0 (überhaupt nicht) bis 10 (sehr hoch), empfinden Sie das Risiko eines Angriffes auf Ihre mobilen Geräte?

0	1	2	3	4	5	6	7	8	9	10

   Bitte begründen Sie wieso diese Wertung vergeben wurde und eine solche Gefahr für das Unternehmen besteht:

6. Bitte bewerten und beschreiben Sie Ihre derzeitigen Ausgaben im Bereich der IT-Sicherheit.

Sehr gering	Gering	Angemessen	Hoch	Sehr hoch

Hypothese 1: Durch das Eintreten der COVID-Pandemie stieg das Sicherheitsbewusstsein im Bereich des Mobile Computings.

7. Beschreiben Sie die derzeitigen Maßnahmen Ihres Unternehmens für die Schulung der Mitarbeiter im Umgang mit Mobile Security.

8. Gab es bereits vor dem Eintreten der COVID Pandemie regelmäßige Schulungen für die Mitarbeiter, welche einen Fokus auf den Umgang mit mobile Security legten?

9. Konnten Sie die mobile Sicherheit Ihrer Geräte seit dem Eintreten der COVID Pandemie nennenswert verbessern?

    a. Falls ja, welche Möglichkeit konnten Sie dazu anwenden

Hypothese 2: Unternehmen sind gut auf den physikalischen Diebstahl von mobilen Geräten vorbereitet, weshalb ein solcher in den meisten Umständen nur wenig Schaden verursacht

.

10. Wurden innerhalb der letzten sechs Monate mobile Geräte von Mitarbeitern gestohlen oder als verloren angegeben, wenn ja, welche?

11. Bitte beschrieben Sie welchen Schaden ein gestohlenes Notebook für Ihr Unternehmen bedeuten kann.

12. Welche Methoden verwenden Sie, um die Anzahl von gestohlenen Mobilgeräten zu verringern.

Hypothese 3: Großunternehmen (> 250 Mitarbeiter) besitzen bereits ein Mobile Device Management System, oder arbeiten derzeit an der Implementierung eines solchen um notwendige Sicherheitsvorschriften auf mobilen Geräten umsetzen zu können.

13. Besitzen Sie ein Mobile Device Management System?

    a. Falls nicht, bitte geben Sie einen Grund an wieso nicht und ob ein solches System, in naher Zukunft, noch für Ihr Unternehmen geplant ist und wie Sie das System derzeit absichern.

14. Welche Aspekte Ihres Mobile Device Management System wird für die Sicherheit Ihrer Mobiltelefone verwendet?

    a. Welche zukünftigen Funktionen planen Sie für die Sicherheit Ihrer Mobiltelefone?

Hypothese 4: Der Sicherheitsaspekt von Unternehmensfremden Applikationen auf Mobiltelefonen wird derzeit noch unzureichend überwacht, weswegen solche ein mögliches Sicherheitsrisiko darstellen.

15. Wie bewerten Sie die getroffenen Schutzmaßnahmen für Ihre Notebooks in Ihrem Unternehmen?

16. Wie bewerten Sie die getroffenen Schutzmaßnahmen für Mobiltelefone in Ihrem Unternehmen?

17. Besitzen Mobiltelefone Limitierungen, welche es aus Sicherheitsgründen nicht ohne weiteres ermöglichen unternehmensfremde Applikationen zu verwenden?