MASTERARBEIT

GEWÄHRLEISTUNG DER INFORMATIONSSICHERHEIT IM KONTEXT SOCIAL-ENGINEERING

ausgeführt am

Studiengang

Informationstechnologien und Wirtschaftsinformatik

Von: Mario Gollob

Personenkennzeichen: 2010320004

Graz, am 14. März 2022 .....

Unterschrift

EHRENWÖRTLICHE ERKLÄRUNG

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

.....

Unterschrift

DANKSAGUNG

An dieser Stelle möchte ich mich bei all denjenigen bedanken, die mich während der Zeit des Schreibens dieser Masterarbeit unterstützt und motiviert haben. In erster Linie möchte ich den Expertinnen und Experten für die Interviews und den Personen, die sich die Zeit genommen haben, die Umfrage der vorliegenden Arbeit auszufüllen, meinen Dank aussprechen. Dadurch konnten qualitativ und quantitativ hochwertige Daten im Kontext Social Engineering für eine qualitative Inhaltsanalyse gefunden werden. Ein großes Dankeschön gebührt auch meinem Betreuer Herrn DI (FH) Günther Zwetti, der die vorliegende Masterarbeit bestens betreut und begutachtet hat. Für all die hilfreichen Anregungen und die konstruktive Kritik bei der Erstellung möchte ich mich recht herzlich bedanken.

Des Weiteren bin ich meiner Familie dankbar, die mir stets Unterstützung geboten und mich während des Schreibprozesses immer ermutigt hat. Ich bedanke mich bei meinen Arbeitskolleginnen und -kollegen und meinen Vorgesetzten, die stets Verständnis für die Arbeit aufgebracht haben, sodass ich zu Besprechungsterminen mit den Expertinnen und Experten erscheinen konnte.

Ebenfalls möchte ich mich bei meinen Studienkolleginnen und -kollegen bedanken, die mir mit viel Geduld, Interesse und Hilfsbereitschaft zur Seite standen. Danke für die zahlreichen Ideen und die Hilfestellungen bei diversen Formatierungen, die maßgeblich dazu beigetragen haben, dass diese Masterarbeit in ihrer jetzigen Form vorliegt.

Herzlich danken möchte ich außerdem meiner Freundin Julia für die aufgebrachte Geduld während des Schreibens dieser Masterarbeit.

Da meine Mutter Elisabeth, die mich immer in jeglicher Hinsicht unterstützt hat, im Jahr 2021 den Kampf gegen das Coronavirus leider verloren hat und deswegen verstorben ist, möchte ich ihr diese Arbeit widmen.

KURZFASSUNG

Diese Masterarbeit behandelt die Informationssicherheit im Kontext des Social Engineerings von Unternehmen. Das Ziel ist es, Initiativen zu definieren, die Unternehmen kritischer Infrastruktur einsetzen müssen, um die Informationssicherheit in diesem Kontext zu gewährleisten.

Im Bereich der Theorie wurde eine Literaturrecherche über das Thema ‚Social Engineering' durchgeführt. Es ließ sich herausfinden, welche Möglichkeiten es gibt, Unternehmen zu attackieren. Des Weiteren bedeutet Social Engineering nicht, dass immer eine illegale Aktivität dahinter steckt, sondern dass hier lediglich mithilfe von Psychologie ein Mehrwert für die Angreiferin oder den Angreifer generiert wird.

Für den empirischen Teil der Arbeit wurde eine Umfrage an Personen gesendet, die in ihrer Arbeit mit Informationssystemen zu tun haben. Diese Befragung hat ergeben, dass Personen wissen, wie bedeutsam Informationssicherheit ist, und es wurde kein signifikanter Unterschied zwischen IT-affinen und nicht IT-affinen Personen festgestellt. IT-affine Personen wissen lediglich besser über die Auswirkungen Bescheid.

Des Weiteren wurden Interviews mit Expertinnen und Experten aus dem Bereich der Informationssicherheit durchgeführt. Deren Zweck war es, herauszufinden, welche Maßnahmen es gibt, die Informationssicherheit im Kontext von Social Engineering zu gewährleisten bzw. zu erhöhen. Es hat sich herausgestellt, dass Security-Awareness-Schulungen sehr sinnvoll sind. Unternehmen kritischer Infrastruktur sollten sich auf Vor-Ort-Schulungen fokussieren, da diese ein höheres Informationssicherheitsempfinden beim Personal auslösen. In Relation zu den Kosten, die ein Social-Engineering-Angriff verursachen kann, zahlt sich für ein Unternehmen kritischer Infrastruktur eine Security-Awareness-Schulung mit großer Wahrscheinlichkeit aus.

Es wird auch empfohlen, technische und physische Maßnahmen einzusetzen, um einen Social-Engineering-Angriff zu erschweren. Jedoch ist zu erwähnen, dass technische Maßnahmen nicht ausschließlich darauf ausgelegt sind, Social-Engineering-Angriffe zu verhindern. Das ist lediglich ein Teil davon. technische Maßnahmen schützen die Allgemeinheit vor Social-Engineering-Angriffen, jedoch nicht einzelne Personen.

Für Unternehmen kritischer Infrastruktur sollten wiederkehrende Security-Awareness-Schulungen und technische Maßnahmen eingesetzt werden, um die Informationssicherheit im Kontext des Social Engineerings zu gewährleisten. Diese Vorkehrungen haben nämlich keinen erheblich negativen Einfluss auf die Arbeitstätigkeiten der Mitarbeiterinnen und Mitarbeiter im Allgemeinen. Auf der anderen Seite stellen sie jedoch sicher, dass die Angestellten ein entsprechendes Bewusstsein für diese Gefahr entwickeln und es stetig erweitern.

ABSTRACT

This thesis investigates information security in the context of social engineering of companies. The aim is to define initiatives that critical infrastructure companies need to implement to ensure information security in the context of social engineering. A literature review was conducted on social engineering, highlighting potential attack vectors. Furthermore, social engineering does not mean that there is always an illegal activity behind it, but that an added value is generated for the attacker with the help of psychology. A survey was sent out to information-systems user. This survey shows a clear awareness of the importance of information security, and no significant difference was found between IT-savvy and non-IT-savvy people. IT-savvy people are more aware of the implications. Furthermore, interviews were conducted with experts to find out what measures are available to ensure or increase information security in the context of social engineering. It turned out that security awareness training is very useful. In the case of companies with critical infrastructure, on-site training should be used, as this triggers a greater sense of information security among the staff. Concerning the costs that a social engineering attack can cause security awareness training always pays off for a critical infrastructure company. It is also recommended to use technical and physical measures to make a social engineering attack more difficult. However, it is worth mentioning that technical measures are not exclusively designed to prevent social engineering attacks. Technical measures protect the public from social engineering attacks, but not individuals. For critical infrastructure companies, recurrent security awareness training and technical measures should be used to ensure information security in the context of social engineering, as these do not have a significant negative impact on the work activities of employees in general, but on the other hand, ensure that employees develop and continuously expand their awareness of this threat. Further research can review these deployed initiatives and measure how much they bring to a company's information security

INHALTSVERZEICHNIS

1 EINLEITUNG

„Es existieren zahlreiche technische Schutzmechanismen, die IT-Systeme vor unberechtigten Zugriffen schützen sollen: Proxys, Firewalls, Schutzprogramme gegen Malware oder schlicht Benutzername und dazugehöriges Passwort lassen sich beispielhaft ins Feld führen. Häufig wird bei der Absicherung von IT-Systemen und anderer für Unternehmen bedeutsamer Informationsquellen eine ganz entscheidende Komponente vollständig außer Acht gelassen oder zu wenig Bedeutung beigemessen: der Mensch als Sicherheitsrisiko.“ (Hoss, 2015, S. 54)

Hoss (2015) beschreibt mit diesem Zitat, dass Personen allgemein im Bereich der Informationssicherheit vernachlässigt werden. Deswegen ist der Mensch ein beliebtes Angriffsziel, um an Informationen von Unternehmen zu kommen bzw. den Unternehmen Schaden zuzufügen. Folgende Grafik zeigt eine Statistik über die Verteilung der verschiedenen Angriffsarten, ausgeführt an weltweit 254 Institutionen.

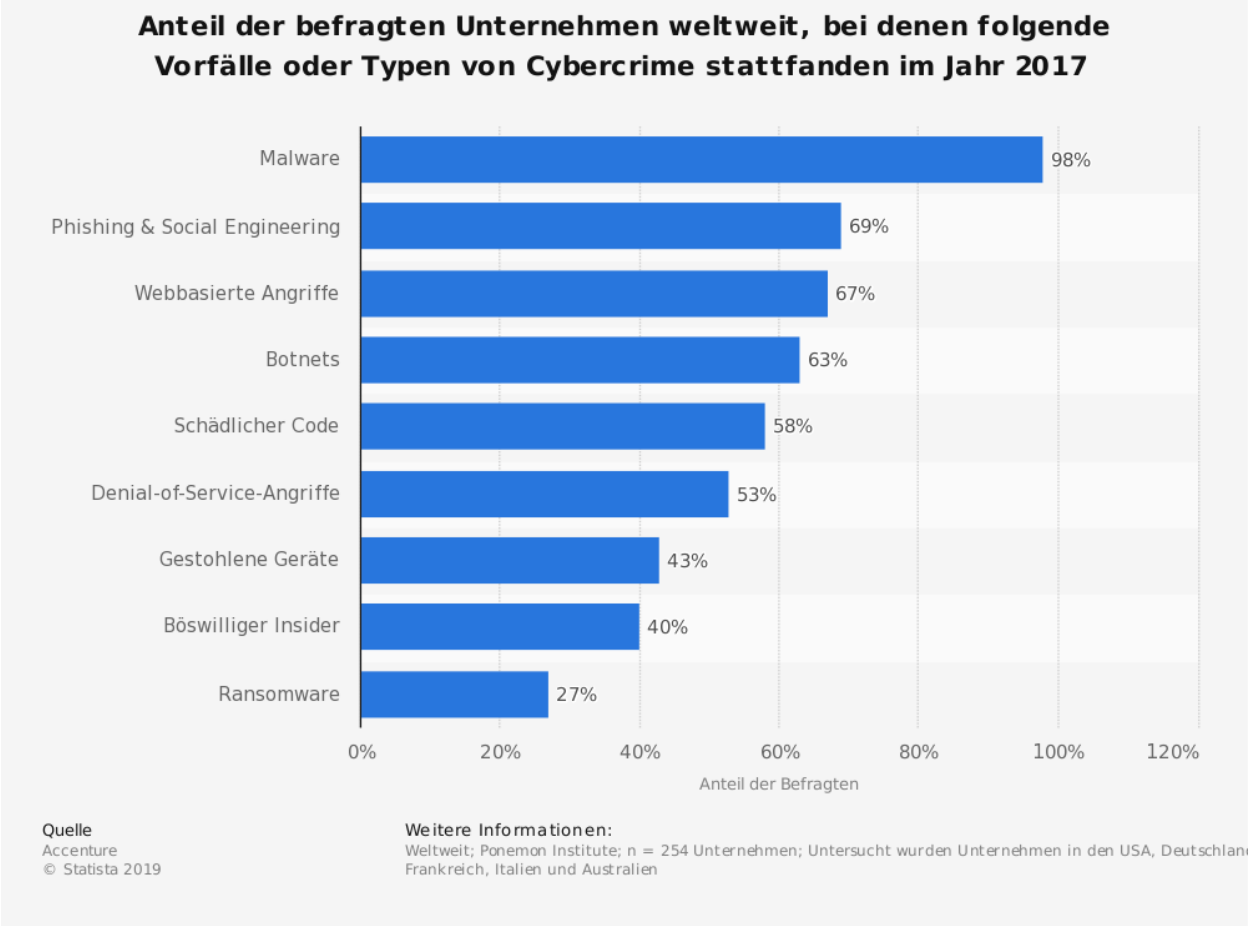

Abbildung 1: Statistik für die Typen von Cybercrime (Accenture, 2017)

In dieser Statistik ist ersichtlich, dass 69 % der befragten Unternehmen angaben, im Jahr 2017 Opfer eines versuchten Phishings oder Social-Engineering-Angriffs gewesen zu sein. Somit belegt dieses Angriffsszenario Platz zwei der Statistik. Da der Mensch hier selbst die größte Sicherheitslücke darstellt, werden Implementationen von Equipment oder Software, die die Informationssicherheit gewährleisten soll, keinen Mehrwert bringen. (Lipski, 2009)

1.1 Problemstellung

Das Sprichwort, dass keine Kette stärker als ihr schwächstes Glied ist, gewinnt im Bereich der Informationssicherheit an Bedeutung. Jede Implementation eines Sicherheitskonzepts lässt sich mit wenig Aufwand umgehen, wenn die Mitarbeiterinnen und Mitarbeiter freiwillig sensible Daten wie Passwörter oder Zutrittscodes zur Verfügung stellen. (Lipski, 2009)

Hoss (2015) stellte im Kontext zu Social Engineering folgende Kernthesen auf:

- Bei einem Angriff in Form von Social Engineering sind die psychologischen Faktoren ein wesentlicher Bestandteil.
- Ein behutsamer Angriff auf ein Unternehmen, um an Informationen zu gelangen, wird von ungeschulten Mitarbeiterinnen und Mitarbeitern kaum erkannt.
- Alleinig die Einführung von Compliance-Regelungen bietet keinen ausreichenden Schutz.

Diese Thesen sagen aus, dass das Personal geschult werden muss, um die Chance eines Gewinns sensibler Informationen durch einen Angriff auf die Psyche des Menschen gering zu halten.

Des Weiteren wird schon seit dem Kalten Krieg versucht, die Sicherheit von Unternehmen kritischer Infrastruktur zu gewährleisten, denn diese stellen oft ein beliebtes Ziel für einen Angriff dar. (Fischer, 2007, S. 23)

Folgende Statistik zeigt, welcher Anteil der Unternehmen kritischer Infrastrukturen in den Jahren 2013 und 2014 einen Datendiebstahl in Form eines Angriffs hatte:

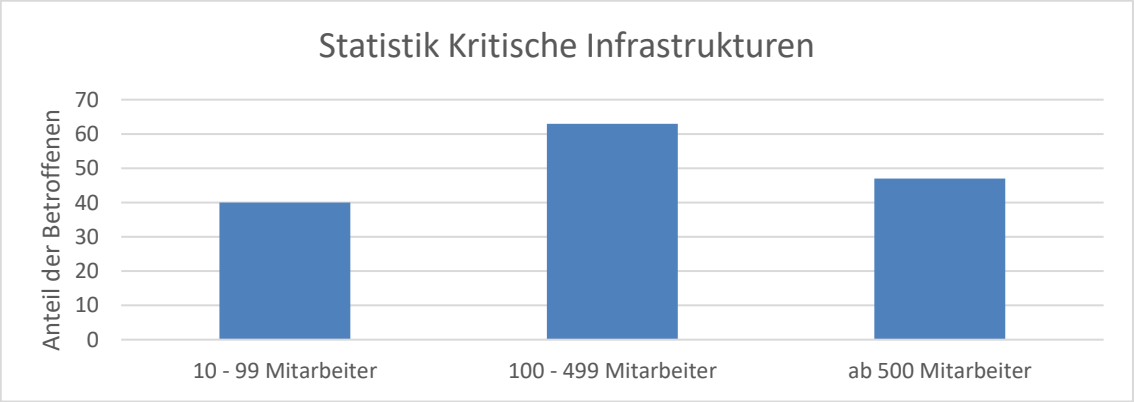

Abbildung 2: Angriff auf kritische Infrastrukturen (Statista Research Department, 2015)

Diese Statistik zeigt, dass Unternehmen kritischer Infrastrukturen von Datendiebstahl etc. betroffen sind, wobei die Größe der Betriebe unerheblich ist. Deswegen herrscht hier großes Potential, einen Schritt Richtung Gewährleistung der Informationssicherheit im Kontext von Social Engineering zu setzen.

1.2 Ziele dieser Arbeit

Ziel dieser Arbeit ist es, Initiativen zu finden, denen Unternehmen kritischer Infrastruktur folgen können, um die Informationssicherheit im Bereich Social Engineering zu gewährleisten.

Ebenfalls Ziel dieser Arbeit ist es, dass diese Initiativen nicht zu kompliziert sind. Sie sollen einfach formuliert werden, damit auch Personen, die keine Kompetenzen in den Bereichen Datenschutz etc. aufweisen, sie verstehen und anwenden können.

Diese Initiativen sollen ohne Änderungen von jeder Mitarbeiterin und von jedem Mitarbeiter, unabhängig von dem jeweiligen Tätigkeitsbereich, ausgeübt werden.

Zum Erreichen dieses Zieles werden Umfragen an Mitarbeiterinnen und Mitarbeiter gesendet, um herauszufinden, welche Sicherheitsmaßnahmen den Einfluss der Arbeit erheblich beeinflussen. Im Anschluss werden mit diesen Informationen Interviews mit Expertinnen und Experten im Bereich Datenschutz durchgeführt, um damit im nächsten Schritt den Leitfaden zu erstellen.

Ein weiteres Ziel dieser Arbeit besteht darin, vergangene, erfolgreich durchgeführte Angriffe mithilfe von Social Engineering zu analysieren und anschließend zu bewerten, warum es zu dem entstandenen Schaden gekommen ist.

Kein Ziel dieser Thesis ist es, eine Langzeitstudie durchzuführen, wie erfolgreich diese Initiativen sind. Diese werden lediglich mit Hilfe von Expertinnen und Experten herausgefunden und spezialisiert in Unternehmen kritischer Infrastrukturen eingesetzt werden können. Eine Studie über den langfristigen Erfolg dieser Initiativen ist in einer neuen Arbeit zu definieren.

1.3 Forschungsfrage und Hypothesen

In der Masterarbeit soll somit folgende Forschungsfrage vollständig beantwortet werden:

„Welche Initiativen müssen gesetzt werden, um die Informationssicherheit von Unternehmen kritischer Infrastruktur im Kontext Social Engineering zu gewährleisten, ohne einen beträchtlichen Mehraufwand für Mitarbeiterinnen und Mitarbeiter zu verursachen?“

In der verfassten Masterarbeit werden die folgenden Hypothesen mithilfe wissenschaftlicher Kriterien analysiert:

Hypothese 1:

H0: Jährliche Schulungen für Mitarbeiterinnen und Mitarbeiter im Kontext des Social Engineerings haben einen positiven Einfluss auf die Informationssicherheit von kritischen Infrastrukturen.

H1: Ein positiver Einfluss auf die Informationssicherheit von kritischen Infrastrukturen durch jährliche Schulungen für Mitarbeiterinnen und Mitarbeiter im Kontext des Social Engineerings kann nicht festgestellt werden.

Hypothese 2:

H0: Jährliche Schulungen für Mitarbeiterinnen und Mitarbeiter können als Investition für die Informationssicherheit kritischer Infrastruktur gesehen werden und sparen im Allgemeinen Kosten, wenn die Ausgaben für die Schulung mit jenen infolge eines Vorfalles verglichen werden.

H1: Jährliche Schulungen für Mitarbeiterinnen und Mitarbeiter verursachen Mehrkosten für Unternehmen und stehen in keiner Relation zu den Kosten eines Vorfalles.

Hypothese 3:

H0: Mitarbeiterinnen und Mitarbeiter, die keine hohe IT-Affinität haben, kennen die Auswirkungen eines Social-Engineering-Angriffs und der daraus entstehenden Nebenwirkungen nicht.

H1: Mitarbeiterinnen und Mitarbeiter, die keine hohe IT-Affinität haben, kennen die Auswirkungen eines Social-Engineering-Angriffs und der daraus entstehenden Nebenwirkungen.

Hypothese 4:

H0: Mitarbeiterinnen und Mitarbeiter halten Einführungen von Regeln, die Social-Engineering-Angriffe verhindern sollen (zum Beispiel, dass ein Telefongespräch nicht weitergeleitet werden darf oder das Ändern des Passwortes in zyklischen Abständen) für einen Mehraufwand und unpraktisch.

H1: Mitarbeiterinnen und Mitarbeiter finden Einführungen von Regeln, die Social-Engineering-Angriffe verhindern sollen (zum Beispiel, dass ein Telefongespräch nicht weitergeleitet werden darf oder das Ändern des Passwortes in zyklischen Abständen) für sinnvoll und unbedingt notwendig.

2 KRITISCHE INFRASTRUKTUR

Die Definition von kritischen Infrastrukturen in Österreich hat sich seit dem 2. April 2008 verändert. Anfangs war die Definition stark durch Ideen, die aus dem European Program for Critical Infrastructure Protection (EPCIP) stammen, beeinflusst. Dieses Programm wurde unter Berücksichtigung des Terroranschlags, der am 11. September 2001 in den USA stattfand, entwickelt. In Österreich wird der Begriff der umfassenden Sicherheit verwendet. Dies bedeutet, dass äußere und innere Sicherheit eng miteinander verbunden sein müssen. Anders betrachtet, sagt das aus, dass das gesamte soziale und ökonomische Netzwerk gefordert ist, um die Sicherheit zu gewährleisten.

Das Ganze bedeutet, dass es sich bei Unternehmen kritischer Infrastruktur um Unternehmen handelt, die Dienstleistungen an der Bevölkerung, beispielsweise Wasser-, Gesundheits-, Elektrizitätsversorgung etc., durchführen. Insofern ergibt sich daraus, dass diese Unternehmen eine vital bedeutende Rolle für die Daseinsvorsorge spielen. Politisch werden Betriebe kritischer Infrastruktur als strategisch wichtige Unternehmen eingestuft. Das Ziel der Definition von kritischen Infrastrukturen in Österreich besteht darin, diese Unternehmen zu kennzeichnen und aufgrund von präventiven Maßnahmen bzw. durch Maßnahmen einer Schadensbehebung den Schaden möglichst gering zu halten. (Czerni, 2012)

Birkmann (2010) definiert Unternehmen kritischer Infrastrukturen als Organisationen, die eine bedeutsame Rolle für die Bevölkerung spielen. Deren Ausfall hätte gemäß dem Autor nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere nicht vorhersehbare Auswirkungen zur Folge. Diese Definition wird für die vorliegende Arbeit verwendet, da das Beschriebene von Czerni (2012) darin treffend zusammenfasst ist.

Des Weiteren gilt zu erwähnen, dass schon seit einigen Jahren die Informationstechnologie (IT) eine große Rolle für die heutige Weltbevölkerung spielt. Zum einen hat die IT einen Vorteil, da viele Aufgaben des Alltags vereinfacht werden, jedoch bringt sie auch einen Nachteil, da zahlreiche Firmen darüber miteinander vernetzt sind. Aufgrund von steigenden Angriffen könnten ohne ausreichende Sicherheitsmaßnahmen schwerwiegende Katastrophen entstehen. (Holznagel, 2001) Wie bereits in Kapitel 1.1 erwähnt, liegt der Anteil an bemerkten Social-Engineering-Angriffen auf Unternehmen kritischer Infrastruktur bei mindestens 40 %. Aus diesem Grund sollen Initiativen aufgezeigt werden, die die Sicherheit dieser Unternehmen und aufgrund dessen auch die Sicherheit der Bevölkerung gewährleistet.

3 SOCIAL ENGINEERING

In der heutigen Zeit wird der Informationssicherheit eine wichtige Rolle zugewiesen. Um sich vor unautorisierten und unberechtigten Zugriffen auf die interne IT-Infrastruktur zu schützen, werden zahlreiche technische Schutzmaßnahmen wie Firewalls, Proxys, Schutzprogramme gegen Malware etc. eingeführt. Unternehmen investieren für solche Implementationen große Summen an Geld, jedoch lassen sie eine entscheidende Komponente meistens außer Acht: Der Mensch stellt häufig die größte Sicherheitslücke in einem System dar. (Hoss, 2015)

In der IT ist die Metapher, dass eine Kette nur so stark wie ihr schwächstes Glied ist, häufig zu hören. Diese Aussage ist sehr treffend, da sich in jedes IT-System, so professionell und raffiniert es implementiert wurde, mit wenig Aufwand eindringen lässt, wenn Mitarbeiterinnen und Mitarbeiter Passwörter herausgeben. Oftmals passiert es, dass Personen ihre Passwörter freiwillig verraten. (Lipski, 2009)

Mann (2008) definierte den Begriff ‚Social Engineering' dabei wie folgt: „Menschen durch Täuschung zu manipulieren, damit sie Informationen herausgeben oder eine Handlung ausführen." In dieser Definition wird beschrieben, dass Personen infolge von Manipulation durch eine Angreiferin oder einen Angreifer gewünschte Aktionen ausführen oder direkt Informationen weitergeben. (Mann, 2008)

Auf der anderen Seite wird ‚Social Engineering' von Hoss (2015), S. 2, wie folgt definiert:

> *„Unter den Begriff Social Engineering sind sämtliche Techniken zur Beeinflussung von Menschen zu fassen, die primär dazu genutzt werden, unberechtigt an Daten oder Informationen zu gelangen oder ein regelwidriges Verhalten auszulösen."*

Werden diese beiden Definitionen verglichen, fällt auf, dass sie sehr ähnlich ausfallen. Mann (2008) und Hoss (2015) beschreiben in erster Linie, dass die Angreiferin oder der Angreifer Menschen manipuliert, um an Informationen zu kommen. Die zweite Definition unterscheidet sich jedoch von der ersten darin, dass sie detailreicher formuliert ist, was wiederum zu Problemen führen kann. Es gibt Beispiele, in denen Menschen manipuliert worden sind, wobei jedoch kein regelwidriges Verhalten ausgelöst wurde, oder in denen Menschen unberechtigt Informationen weitergegeben haben. Ein Beispiel hierfür sind Personen, die im Verkauf tätig sind und die Fähigkeit der Beeinflussung und Überredung besitzen. (Mitnick & Simon, 2003) Hier werden Personen ebenfalls getäuscht und führen möglicherweise die gewünschte Handlung der Verkäuferin oder des Verkäufers aus, nämlich den Kauf des Produktes.

Die Definition von Social Engineering für die Masterarbeit soll ein breites Spektrum der Manipulation von Menschen abdecken. Daraus wird ein Prozess erstellt, der dieser Manipulation so effektiv wie möglich entgegenwirkt. Somit lässt sich die Informationssicherheit von Unternehmen kritischer Infrastruktur gewährleisten.

Die relevante Definition für diese Masterarbeit lautet daher wie folgt:

> *„Social Engineering ist die Manipulation von Menschen, damit diese mit freiwillig gegebenen Informationen oder mittels von ihnen durchgeführten Aktionen einen Mehrwert für die Interessen der Angreiferin oder des Angreifers liefern."* (Eigendefinition zusammengefasst aus Hoss (2015); Mann (2008); Mitnick & Simon (2003))

3.1 Methoden

Es gibt unzählige Techniken, die bei Social-Engineering-Angriffen verwendet werden können. Des Weiteren ist ein Angriff auf keine Weise beschränkt und kann so weit gehen, wie es die Vorstellungskraft der Angreiferin bzw. des Angreifers zulässt. (Manske, 2000) Das grundlegende Ziel eines Social Engineers besteht darin, dass Informationen entweder physisch oder digital gewonnen werden. (Thornburgh, 2004) Das Ganze bedeutet, dass ein Social Engineer von seinen sozialen und interaktiven Begabungen abhängig ist und nicht wie bei den herkömmlichen Hackingmethoden von technischen Fähigkeiten. (Bhagyavati, 2007)

Bhagyavati (2007) beschreibt, dass es drei grundlegende Phasen gibt, die bei einem Social-Engineering-Angriff durchlaufen werden müssen.

- Vorbereitungsphase
- Phase des Angriffs
- Phase nach dem Angriff

In der Literatur wird oft von Shoulder-Surfing oder Dumpster-Diving als möglicher Technik für einen Social-Engineering-Angriff gesprochen. Diese Methoden sind der Vorbereitungsphase zuzuordnen, da es hier keinerlei Interaktion mit dem Opfer gibt. Dabei werden lediglich Informationen für den nachfolgenden Angriff gesammelt. (Janczewski & Colarik, 2007)

In der Phase des Angriffs beschreiben Janczewski & Colarik (2007), dass es die folgenden Möglichkeiten gibt:

- Person zu Person
- Person zu Person via Media

3.1.1 Person zu Person

Bei der Methode von Person zu Person herrscht grundsätzlich eine direkte oder persönliche Kommunikation mit dem Opfer. Der oder die Betroffene gibt hier Informationen an die Angreiferin oder den Angreifer weiter, ohne zu wissen, dass er oder sie Opfer eines Betruges geworden ist. (Kamal & Crews, 2008)

Pretexting

Beim Pretexting wird versucht, unter einem Vorwand an Informationen zu kommen. Der Vorwand ist glaubwürdig darzustellen und muss der Überprüfung der Zielperson standhalten. (Mouton et al., 2014) Diese Technik erfordert sehr viel Vorbereitung, da vor dem Angriff auch Nachforschungen über das Opfer durchgeführt werden müssen, damit der erläuterte Vorwand glaubwürdig mitgegeben wird. (Ivaturi & Janczewski, 2011)

Ein Vorfall, der auf diese Technik zurückgeht, ist der Hewlett-Packard-Skandal. Sicherheitsexperten wollten die Spur eines Datenlecks der Unternehmensstrategie analysieren. Sie nahmen die Identität eines Vorstandmitgliedes an, um den Zugang zu Telefonaufzeichnungen zu erhalten. (Baer, 2008) Dieses Szenario wurde in den Medien oft wiederholt und erregte großes Aufsehen. Schlussendlich führte es zu einem neuen Gesetz, dass es verbietet, solche Techniken einzusetzen, um Informationen unter falschem Vorwand zu bekommen. (Ivaturi & Janczewski, 2011)

Reverse Social Engineering

Anstatt ein potentielles Opfer direkt zu kontaktieren, kann eine angreifende Person versuchen, es glauben zu machen, dass er oder sie vertrauenswürdig ist. Das Ziel ist es, potentielle Opfer dazu zu bringen, sich ihm zu nähern, um zum Beispiel um Hilfe zu bitten. Dieser indirekte Ansatz wird als ‚Reverse Social Engineering' bezeichnet und besteht aus drei Phasen: Sabotage, Werbung und Unterstützung. (Granger, 2001)

In folgender Grafik sind die drei Phasen eines Reverse-Social-Engineering-Angriffs ersichtlich:

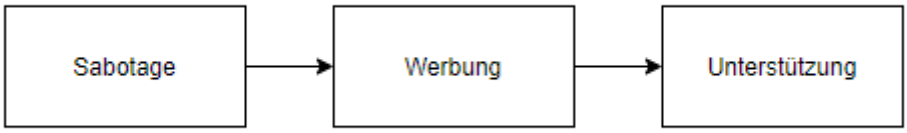

Abbildung 3: Drei Phasen des Reverse Social Engineering (in Anlehnung an Granger, 2001)

Diese drei Phasen durchläuft ein Social Engineer, um an sein Ziel zu kommen. Beispielsweise wird in der ersten Phase das Netzwerk sabotiert. In der zweiten Phase bewirbt die Angreiferin bzw. der Angreifer die Lösung und versucht, sich dadurch als richtige Person für die Problemlösung darzustellen. Im Anschluss behebt er oder sie das Problem mit Hilfe des Opfers. In der letzten Phase versucht der Social Engineer unter einem Vorwand, eine Mitarbeiterin oder einen Mitarbeiter dazu zu bringen, sich im Netzwerk einzuloggen. Damit wird ein Mehrwert für die Angreiferin oder den Angreifer generiert. Diese Technik wird als besonders effektiv eingestuft, weil sie dem Opfer ein Glücksgefühl gibt, da das Problem gelöst wird. Deswegen schöpft niemand Verdacht. Die Angreiferin oder der Angreifer schaffen hier für das Opfer einen Anreiz, diese Informationen preiszugeben, die es sonst geheim halten würde. (Ivaturi & Janczewski, 2011)

Tailgating

Unter Tailgating ist im Allgemeinen zu verstehen, dass einer Person, die eine Autorisierung hat, einen sicheren Bereich zu betreten, gefolgt wird. (Long, 2011) Bei einem Social-Engineering-Angriff muss die Angreiferin oder der Angreifer gut vorbereitet sein, um gegebenenfalls Fragen zu beantworten. (Ivaturi & Janczewski, 2011) Thompson (2006) beschreibt, dass es normalerweise zwei Werkzeuge gibt, um die Glaubwürdigkeit einer Geschichte zu erhöhen. Diese sind:

- Verwendung der Firmensprache in einer Geschichte
- Es müssen Wissenspersonal und -richtlinien bereitgestellt werden

In einem typischen Szenario gibt es eine Figur und einen Kontext. Die Angreiferin oder der Angreifer wird hier als Vektor verwendet. Der Charakter kann entweder gefälscht, d. h. ausgedacht, oder eine echte Person sein, deren Identität missbraucht wird. Eine große Hilfe bei solchen Angriffen bieten öffentliche Datenbanken wie LinkedIn und XING. Hier werden oftmals Organisationsstrukturen mit Namen von Personen und Positionen bekannt gegeben. (Huber et al., 2009)

Ivaturi & Janczewski (2011) kategorisieren Person-Person-Angriffe in zwei Kategorien:

- Identitätswechsel durch Aufbau einer gefälschten Person
- Identitätswechsel einer echten Person

Diese beiden Kategorien umfassen alle vorhin erwähnten Techniken wie Pretexting und Reverse Social Engineering. Es gilt ebenfalls zu beachten, dass diese Aspekte nicht nur mittels persönlicher Kommunikation zum Einsatz kommen können. Diese lassen sich ebenso durch andere Medien nutzen. (Ivaturi & Janczewski, 2011) Im Folgenden werden Techniken dargestellt, die einen Angriff über Medien ermöglichen.

3.1.2 Person zu Person via Media

Jegliche Angriffsvektoren, die keine psychische Anwesenheit einer Angreiferin oder eines Angreifers voraussetzen, werden als Social-Engineering-Angriff von Person zu Person via Media kategorisiert. Die Verwendung von Computern und Mobiltelefonen kann viele Vorteile besitzen, denn dadurch kann der Social Engineer oftmals anonymisiert werden. Außerdem lässt sich der Angriff besser skalieren als jener, der von einer persönlichen Kommunikation abhängig ist. (Ivaturi & Janczewski, 2011)

Person zu Person via Text

Jegliche Angriffe, für die Text als Kommunikationsmedium verwendet wird, ob E-Mail, Surfen, Chatten, soziale Netzwerke oder Kurznachrichten via SMS oder Postsendung, lassen sich dieser Kategorie zuzuordnen. (Ivaturi & Janczewski, 2011) Verschiedene Techniken eines solchen Angriffs werden im Folgenden erörtert.

Phishing

Wird der Ansatz des Phishings ausgewählt, so hat der Angreifer oder die Angreiferin die Absicht, sich sensible und persönliche Information zu beschaffen, indem er oder sie sich als eine vertraute Entität ausgibt. Das bei solchen Angriffen meistens verwendete Kommunikationsmittel sind E-Mails. Es werden realistisch aussehende Nachrichten mit der Aufforderung zum Klicken auf einen Link, der das Opfer auf eine schädliche Website weiterleitet, auf der dessen Eingaben gespeichert werden, versendet. Dafür werden Hunderte E-Mails an generierte E-Mail-Adressen in der Hoffnung geschickt, dass ein kleiner Teil der Adressaten auf den Link klickt und dadurch Informationen preisgibt. Mit dieser Angriffsmethode wird das Opfer auf trügerische Weise beeinflusst, sensible Informationen weiterzugeben und damit einen Mehrwert für die Angreiferin oder den Angreifer zu bringen. (Ivaturi & Janczewski, 2011)

Lee et al. (2007) beschreiben, dass in den letzten Jahren das Problem an Umfang und an Komplexität zugenommen hat.

Smishing

Ähnlich wie bei Phishing-Angriffen werden beim Smishing betrügerische Nachrichten und SMS über Mobiltelefone an Opfer gesendet, um bei diesen eine Handlung auszulösen. Der Unterschied zu Phishing-Angriffen liegt darin, dass die Effizienz um einiges höher ist, da die Opfer ihre Handys meist bei sich haben. (Yeboah-Boateng & Amanor, 2014)

Ein weiterer Vorteil für die Angreiferin oder den Angreifer besteht darin, dass empfangene Nachrichten auf einem Smartphone Malware enthalten können, selbst wenn diese von einer vertrauenswürdigen Stelle gesendet wurden. Wird eine solche Malware geöffnet, arbeitet sie als Hintergrundprozess und installiert Programme, die eine Zugriffsmöglichkeit für die Angreiferin oder den Angreifer schaffen. Damit ist der Abruf von Informationen wie Kontaktlisten, Nachrichten etc. gewährleistet. Ebenso könnte ein Rootkit installiert werden, damit der Social Engineer vollständige Kontrolle über das Smartphone erlangen kann. (Yeboah-Boateng & Amanor, 2014)

Cross-Site-Request-Forgery (CSRF)

Mittels CSRF wird ein Endbenutzer gezwungen, erwünschte oder unerwünschte Aktionen in einer Webanwendung auszuführen, unter der Voraussetzung, dass das Opfer bei einem Onlinedienst authentifiziert ist. Mit der Hilfe von Social Engineering bzw. durch die Technik des Phishings kann ein Link per E-Mail versendet werden, über den im Anschluss das Opfer unbewusst dazu gezwungen wird, Geldüberweisungen oder eine Änderung der eigenen E-Mail-Adresse etc. durchzuführen. (KirstenS)

Malware

Dieser Angriff wird als der effektivste und erfolgreichste aller Social-Engineering-Angriffe deklariert, da er oft zur Anwendung kommt und widerstandsfähig ist. In der Regel werden damit Tausende von ahnungslosen Durchschnittsbenutzerinnen und -benutzern mit einer Kombination von psychologischen und technischen Tricks angegriffen. (Abraham & Chengalur-Smith, 2010) Ivaturi & Janczewski (2011) beschreiben, dass sich durch die verbesserten Abwehrtechnologien gegen Malware auch die Malware-Angriffe weiterentwickelt haben. Ebenso haben sich die psychologischen Taktiken der Angreiferinnen und Angreifer verbessert. Ausschlaggebend für einen erfolgreichen Malware-Angriff sind heutzutage auch die zahlreichen Möglichkeiten und Plattformen für die Durchführung. Grundsätzlich ist jedes Gerät mit einem Betriebssystem anfällig für Malware. (Lehle & Reutter, 1997)

Abgesehen von den eingesetzten Geräten, dem genutzten Betriebssystem oder der verwendeten Plattform ist ein Malware-Angriff aus dem folgenden Grund so widerstandsfähig: Die Angreiferinnen und Angreifer können oftmals eine Expertise in sozialen Fähigkeiten aufweisen und nutzen diese, um durch einen Angriff einen Mehrwert für sich selbst zu generieren. Jegliche Art, mit der das Opfer angesprochen wird, wie Neugierde, Angst oder Gier, kann als Taktik eingesetzt werden. (Ivaturi & Janczewski, 2011)

Ivaturi & Janczewski (2011) listen Beispiele für solche Angriffe unter Angabe der jeweils verwendeten Taktik auf:

- **E-Mail:**
  Hier wird angestrebt, dass das Opfer eine E-Mail und bestenfalls den zusätzlichen Anhang öffnet. Das Ganze kann durch die Neugierde, Angst oder Gier des Opfers erfolgen. Ein Beispiel, das in der Literatur genannt wird, ist der ‚Lovebug'-Wurm aus dem Jahr 2000. Der Betreff der E-Mail war hier „ILOVEYOU" und die Mail war mit einem Anhang ausgestattet, der wie eine Textdatei aussah. Die ahnungslosen Opfer öffneten dieses File und im Anschluss war der Computer mit einem Skript infiziert, das eine Kopie vom E-Mail-Konto des Opfers selbst an alle Personen im Adressbuch schickte. (Ivaturi & Janczewski, 2011)

- **Pop-ups:**
  Pop-ups sind zufällige Warnmeldungen, die sich in einem neuen Fenster öffnen und in der Regel als Mittel der Onlinewerbung eingesetzt werden. Die Angreiferinnen und Angreifer nutzen diese Methode, um eine Angst oder die Gier eines Opfers anzusprechen, damit diese die aufgeforderte Meldung des Pop-ups ausführen. (Ivaturi & Janczewski, 2011) Ein bekanntes Beispiel hierfür ist das Auftauchen von ‚Scareware', bei der Pop-ups mit einer falschen Aufforderung erscheinen. Diese besagt, dass auf dem Computer des Opfers ein Virus entdeckt worden sei und deswegen ein bestimmtes Antivirus-Programm heruntergeladen werden müsse, um es zu entfernen (FBI, 2010). Die typischen Benutzerinnen und Benutzer, die wenig vertiefte Kompetenz im Bereich der Security aufweisen, werden diese Software herunterladen und damit versuchen, den Computer zu reparieren. Dabei bemerken sie oft nicht, dass sich durch diesen Download der Computer mit einem Virus infizieren wird. (Ivaturi & Janczewski, 2011)

- **Search-Engine-Poisoning:**
  Search-Engine-Poisoning (SEP) liegt vor, wenn die Angreiferin oder der Angreifer mit unethischen Techniken Menschen auf eine schädliche Website lockt. Wenn das Opfer auf das Ergebnis der Suche im Internet klickt, weil es relevant erscheint, wird es auf eine andere Website umgeleitet. Dort wird versucht, den Benutzer oder die Benutzerin zum Herunterladen einer bestimmten Malware zu bewegen. (Ivaturi & Janczewski, 2011)

  Diese Art von Angriff wird besonders dann ausgeübt, wenn es ein bedeutendes globales Ereignis gibt. Solche Ereignisse werden meist im Internet recherchiert. Mithilfe von Google Trends können solche Phänomene als Trend erkannt werden. Aufgrund dessen erstellen Angreiferinnen und Angreifer falsche Websites, die mit einer Malware bestückt sind. (Townsend et al., 2010)

  Janczewski & Colarik (2007) beschreiben, dass der Social-Engineering-Ansatz bei dieser Form des Angriffs auf dem folgenden Sachverhalt basiert: Die Angreiferin oder der Angreifer profitiert vom Vertrauen der Nutzerinnen und Nutzer in die von den Suchmaschinen gelieferten Suchergebnisse, um den Malware-Angriff zu starten. Ebenfalls beschreiben Janczewski & Colarik (2007), dass SEP zunehmend beliebter wird, da es nicht einmal die für einen typischen Social-Engineering-Angriff erforderlichen menschlichen Emotionen hervorrufen muss. Diese werden nämlich bereits durch das Auftreten von globalen Ereignissen erzeugt.

- **Social Networking:**
  Heutzutage werden viele Social-Engineering-Angriffe über soziale Netzwerke verübt. (Janczewski & Colarik, 2007) Zu betrachten sind hier große Plattformen wie Facebook mit ca. 2,9 Milliarden Nutzerinnen und Nutzern (Statista Research Department, 2022) oder Instagram, das 1,18 Milliarden Nutzerinnen und Nutzer für das Jahr 2023 prognostiziert (Rabe, 2020). Angesichts dieser hohen Nutzerzahlen wären hier potentiell viele Opfer mit wenig Aufwand zu erreichen. Auch beim sozialen Netzwerk Twitter wurden bereits zahlreiche Social-Engineering-Angriffe durchgeführt. Der Prozess eines typischen Social-Networking-Angriffs beginnt mit der Erstellung eines gefälschten Profils. Von diesem Account aus werden Nachrichten an Kontaktpersonen im sozialen Netzwerk gesendet. Diese Nachrichten beinhalten einen verkürzten, mit Hilfe von tinyurl.com generierten Link, der auf eine schädliche Website weiterleitet. Hier wird im Hintergrund unerlaubt Malware auf dem Computer installiert. (Naraine, 2008)

Person zu Person via Voice

Ivaturi & Janczewski (2011) sagen, dass jeder Angriff, bei dem die Angreiferin oder der Angreifer nicht physisch anwesend ist und stattdessen das Sprechen als Kommunikationsmedium nutzt, dieser Kategorie zugeordnet wird.

Diese Art von Angriffen kann beispielsweise über Mobiltelefone oder über das Internet mit der sogenannten Voice-over-IP-Technologie durchgeführt werden. (Ivaturi & Janczewski, 2011)

Einige dieser Arten sind im Folgenden aufgelistet und werden erläutert.

Vishing

Vishing ist ein sehr erfolgreicher Bedrohungsvektor. Die Opfer werden oftmals mit Identitätsdiebstahl und/oder Finanzbetrug konfrontiert. (Griffin & Rackley, 2008)

Es ist den zuvor erörterten Angriffsmethoden Phishing und Smishing sehr ähnlich. Der Unterschied besteht darin, dass die Angreiferin oder der Angreifer hierbei die Sprache benutzen, um dem Opfer zu schaden und für sich selbst einen Mehrwert zu generieren. (Ivaturi & Janczewski, 2011)

Ivaturi & Janczewski (2011) beschreiben einen typischen Vishing-Angriff mit folgenden Schritten:

- Das Opfer wird angerufen und mit einer auf die Mailbox gesprochenen Nachricht aufgefordert, zurückzurufen, um beispielsweise die Glaubwürdigkeit seiner Bankdaten zu überprüfen.
- Das Opfer ruft zurück und wird mittels eines Sprachdialogsystems aufgefordert, eine Option auszuwählen.
- Das Opfer wählt eine Option aus und wird unabhängig von der Auswahl aufgefordert, sich mit seiner Kontonummer und PIN (Personal-Identification-Number) zu authentifizieren.
- Nach Eingabe der Kontonummer und PIN wird entweder der Anruf von der Angreiferin bzw. dem Angreifer beendet oder direkt an den echten Kundendienst weitergeleitet.

Person zu Person via Video

Bei dieser Art von Delikt kann der Angreifer das Video als Kommunikationsmedium nutzen, um Social-Engineering-Angriffe zu inszenieren. Die rapide Zunahme der Internetnutzung und die zunehmende Verbreitung von Breitbandanschlüssen auf der Welt haben zum Erfolg von Websites wie YouTube beigetragen, die es den Menschen ermöglichen, Wissen zu teilen und über Videos zu kommunizieren. Bei einem solchen Angriff kann ein Video in Umlauf gebracht werden, dass sich als eine Art ‚Anleitung' ausgibt und eine Reihe von Anweisungen für ein vom Angreifer erstelltes Problem enthält. Wenn ein ahnungsloses Opfer, das von dem zuvor geschaffenen Problem betroffen ist, online auf dieses Video stößt, wird es bereitwillig den Anweisungen folgen und auf die Täuschung hereinfallen. Diese Art von Angriff ähnelt der bereits erwähnten Reverse-Engineering-Technik, bei der die angreifende Person das Opfer mit der

Behauptung hereinlegt, er oder sie habe eine Lösung für ein zuvor erstelltes Problem. Obwohl in den Medien keine Berichte über derartige Angriffe zu finden sind, ist dies angesichts der Anzahl der Menschen, die sich heutzutage Videos online ansehen und sich darüber austauschen, ein potentiell nutzbarer Weg für Hacker. (Ivaturi & Janczewski, 2011)

In folgender Grafik ist eine Übersicht zur Zuordnung der einzelnen Social-Engineering-Angriffsmethoden ersichtlich:

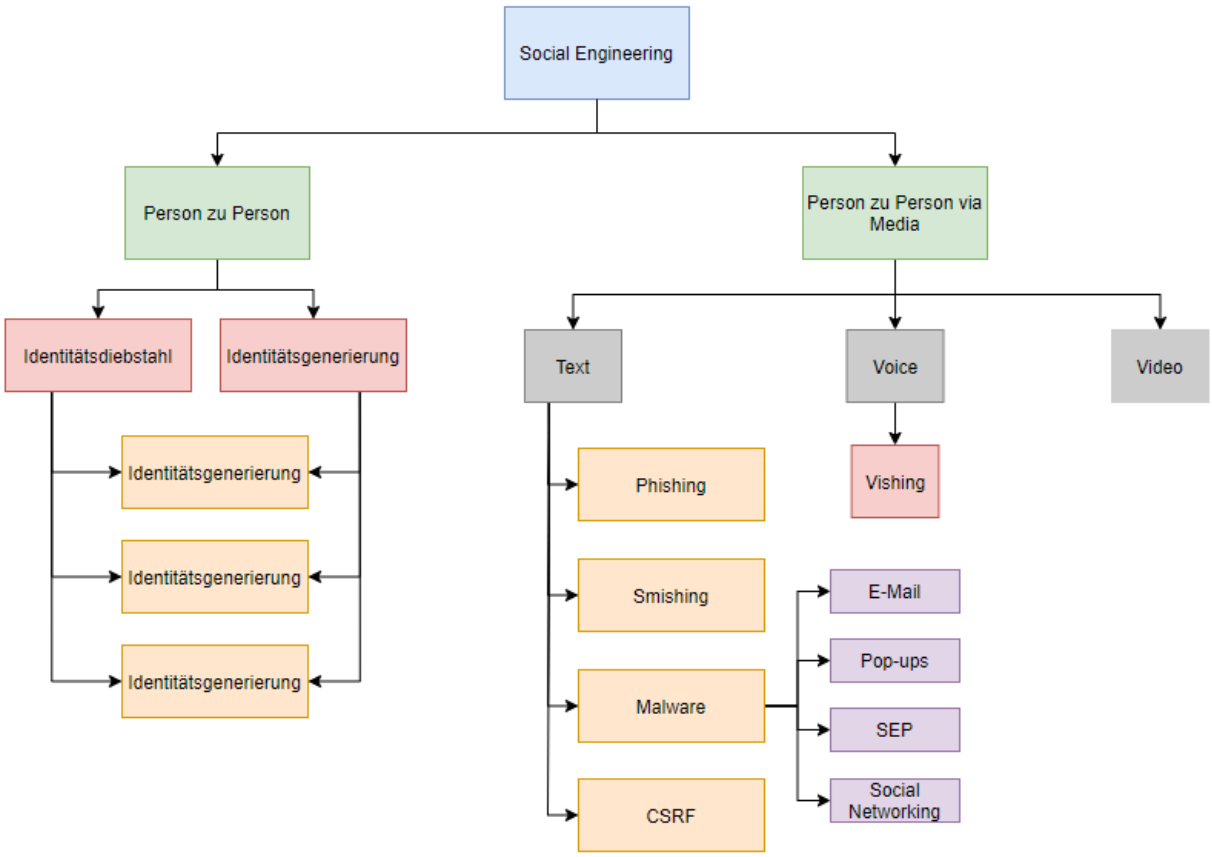

Abbildung 4: Taxonomie von Social-Engineering-Attacken (vgl. Ivaturi & Janczewski, 2011)

Bei genauerer Betrachtung der oben genannten Möglichkeiten ist ersichtlich, dass die meisten Methoden sehr ähnlich aufgebaut sind. Es wird immer das Vertrauen und die Konfliktscheue des Menschen ausgenutzt, um für sich selbst einen Mehrwert zu generieren. Allgemein betrachtet, wird hier die Gewährleistung der Sicherheit im Kontext des Social Engineerings hauptsächlich durch psychologische Schulungen der Mitarbeiterinnen und Mitarbeiter erreicht werden können und nicht durch das Implementieren weiterer Sicherheitssoftware.

3.2 Verschiedene Typen von Social Engineers

Wie in Kapitel 3 ersichtlich, erfolgt die Generierung eines Mehrwertes für einen selbst laut der Definition von Social Engineering nicht immer ausschließlich durch illegale Aktivitäten. Das bedeutet, dass es vielerlei Formen von Social Engineering gibt. Social Engineers können freundlich oder böswillig sein mit der Absicht, etwas aufzubauen oder etwas zu zerstören (Hadnagy, 2012).

Es gibt verschiedene Arten der Social Engineers und auf diese wird im folgenden Abschnitt eingegangen. (Hadnagy, 2012)

- **Hacker**
  Da die Programmiererinnen und Programmierer von Software heutzutage stets bessere Arbeit leisten, wird es für Personen immer schwieriger, das entstandene Programm zu knacken. Aus diesem Grund widmen sich die klassischen Hacker vermehrt dem Social Engineering. Oftmals wird eine Mischung aus Hardware, beispielsweise einem Keylogger, und verbalen Skills angewendet, um einen Mehrwert für eine einzelne Person oder eine Gemeinschaft zu generieren. Schimmer (2008) erwähnt ebenso, dass vermehrt technische Hilfsmittel in einem Social-Engineering-Angriff Verwendung finden. Mittlerweile wird Social Engineering bei fast jedem Angriff beliebiger Größe eingesetzt. Das ist auch ersichtlich, denn viele Unternehmen investieren heutzutage in sogenannte Awareness-Programme. Diese sollen der Mitarbeiterin oder dem Mitarbeiter das Bewusstsein für Informationsschutz näherbringen. (Schimmer, 2008)

- **Penetrationstesterinnen und -tester**
  Penetrationstesterinnen oder -tester, auch bekannt als Pentester, besitzen die gleichen Skills wie böswillige Hacker. Sie werden meistens beauftragt, um die Sicherheit eines Konzerns zu überprüfen. Damit diese Sicherheitsüberprüfung alle Punkte abdeckt, müssen sich Penetrationstesterinnen und -tester mit Social Engineering auseinandersetzen. Penetrationstesterinnen und -tester generieren hier zwar keinen Mehrwert für sich selbst, aber für das Unternehmen.

- **Spione**
  Spione sind spezialisiert auf Social-Engineering-Angriffe. Sie besitzen weniger technisches Wissen, jedoch sind sie Expertinnen und Experten im Bereich der Manipulation. Sie vermitteln Opfern erfundene, aber glaubhafte Geschichten, damit jene vertrauliche Informationen freiwillig preisgeben. Spione setzen hier hauptsächlich auf die eigene Glaubwürdigkeit. Ihre Aussagen können plausibel vermittelt werden, wenn viel Wissen oder wenn wenig Wissen im Business verbreitet ist. Beides kann einen Mehrwert generieren. Wichtig ist die erfundene Geschichte, warum gewisse Informationen benötigt werden. Becker (2015) beschreibt, dass es bei der Spionage auf die Kommunikationsfähigkeit ankommt, um die Opfer zu manipulieren.

- **Identitätsdiebe**
  Allgemein gesagt, erfinden Identitätsdiebe eine glaubhafte Identität oder stehlen diese, um damit einen Mehrwert zu generieren. Oftmals werden ohne Wissen des Eigentümers

persönliche Daten wie Name, Adresse, Kontonummer etc. entwendet. Damit lässt sich bereits ein enormer Schaden anrichten. Es reicht aber oft, sich zum Beispiel mit der Uniform eines Polizisten einzukleiden und so Strafzettel zu vergeben. Auch im Internet werden oft Daten gesammelt. Aus diesem Grund werden Personen zunehmend vorsichtiger bei der Preisgabe persönlicher Informationen. Der Staat oder eine höhere Instanz ist ebenso dafür verantwortlich, dass nicht unberechtigt Daten gesammelt werden dürfen. Das ist in der Datenschutzgrundverordnung geregelt. (Schalbruch, 2009)

- **Verärgerte Angestellte**
  Oftmals kommen Mitarbeiterinnen oder Mitarbeiter in die Situation, dass sie sich unangemessen von der Arbeitgeberin oder dem Arbeitgeber behandelt fühlen. Meistens besteht dieser Konflikt nur für die Mitarbeiterinnen oder die Mitarbeiter, da diese ihre momentane Laune verbergen wollen, um das Arbeitsverhältnis nicht zu gefährden. Im Endeffekt führt es dazu, dass die Angestellten immer verärgerter werden und deswegen Handlungen wie Diebstahl von Papier etc. rechtfertigen.

- **Trickbetrügerinnen oder -betrüger**
  Trickbetrügerinnen oder -betrüger weisen eine enorme Expertise in der Anwendung von Betrugsmaschen auf. Sie analysieren das Opfer unbemerkt und erkennen bei diesen, ob eine Fortführung des Betruges sinnvoll ist und funktionieren wird. Ebenfalls werden Situationen geschaffen, die dem Opfer einen vermeintlichen Mehrwert bieten. Hierzu gibt es eine Studie, in der vermittelt wird, dass Personen mit zunehmendem Alter nicht leichtgläubiger sind als Jüngere. In der Regressionsanalyse wurde herausgefunden, dass Personen um die 50 Jahre das Ganze kritischer betrachten. (Schmidt et al.)

- **Personalvermittlerinnen oder -vermittler**
  Auch bei solchen Personen wird auf die Techniken des Social Engineerings zurückgegriffen. Oftmals müssen unbemerkt Informationen entlockt werden, um zu wissen, ob das Personal den Herausforderungen gewachsen ist. Es werden die psychologischen Prinzipien des Social Engineerings eingesetzt. Diese Personen sind sehr gut darin, Menschen zu verstehen und zu durchschauen. Ebenfalls ist es wichtig, nicht nur den Jobsuchenden zufriedenzustellen, sondern auch den zukünftigen Arbeitgeber.

- **Verkaufspersonal**
  Verkäuferinnen und Verkäufer wollen im Allgemeinen etwas verkaufen. Damit dies funktioniert, muss die Kundin oder der Kunde durchschaut werden, damit die Verkaufsperson herausfindet, welches Produkt sie verkaufen kann. Beim Prozess des Verkaufens werden ebenso Techniken des Social Engineerings angewandt. Es beginnt mit der Informationssammlung. Des Weiteren werden persönliche Informationen entlockt, um die Kundin oder den Kunden mittels psychologischer Prinzipien zu beeinflussen, damit ein Produkt gekauft wird. Der Kundin oder dem Kunden wird das Gefühl vermittelt, dass dieses Produkt essentiell für die Ausübung ihrer oder seiner Tätigkeit ist. Schumacher (2014) beschreibt, je wichtiger einem Menschen eine gewisse Sache ist, desto weniger

wird er oder sie sein Verhalten kontrollieren können. Dies stellt für Verkaufspersonal ein hohes Potential dar.

- **Regierungen**
  Einige Regierungen arbeiten mit Social Proof, Autorität und Verknappung. Damit versuchen sie, die Menschen unter Kontrolle zu halten. Es bedeutet hier nicht, dass Regierungen böswillig und negativ handeln, sondern dass sie damit versuchen, das Gemeinwohl aller zu steigern. Social Engineering wird hier indirekt eingesetzt, damit die ausgegebenen Botschaften ansprechender und allgemein akzeptiert werden.
- **Ärztinnen und Ärzte, Psychologinnen und Psychologen und Rechtsanwältinnen und Rechtsanwälte**
  Es scheint, als ob diese Personen keinen Bezug zu Social Engineering hätten. Ruft man sich jedoch die in dieser Arbeit gültige Definition von Social Engineering in Erinnerung, klingt es plausibler. Demnach muss die Anwendung von Social Engineering nicht immer mit illegalen Aktivitäten zu tun haben. Diese Personengruppe wendet keine illegalen Aktivitäten wie das Aussenden einer Phishing-Mail an. Jedoch werden die rhetorischen Fähigkeiten genutzt, um gegebenenfalls Patientinnen und Patienten oder Klientinnen und Klienten Informationen zu entlocken und mit diesen einen beidseitigen Mehrwert zu schaffen.

Werden die oben genannten Personengruppen beachtet, dann ist zu erkennen, dass Social Engineering oder zumindest einige Aspekte davon in vielen Tätigkeitsfeldern, oftmals unbewusst, eingesetzt werden. Die verschiedenen Elemente, die beim Social Engineering zur Verfügung stehen, können als einzelne Bausteine in einer Gleichung je nach Anwendungsgebiet ‚addiert' werden. (Hadnagy, 2012) Es gibt ein Beispiel, wie es bei einem Trickbetrüger aussehen könnte, und das lautet wie folgt:

Pretexting + Manipulation + die Neigung zur Gier = für Social Engineering geeignete Zielperson.
(Hadnagy, 2012, S. 41)

3.3 Vorgehensweise eines Angriffs

Hoss (2015) entwickelte eine Grafik, die die verschiedenen Muster in der Verhaltenspsychologie darstellt, infolge derer sich Menschen am wahrscheinlichsten erfolgsversprechend manipulieren lassen. Die bedeutendsten psychologischen Manipulationsmöglichkeiten für den Menschen wurden von Cialdini (2013) beschrieben und sind in folgender Grafik ersichtlich:

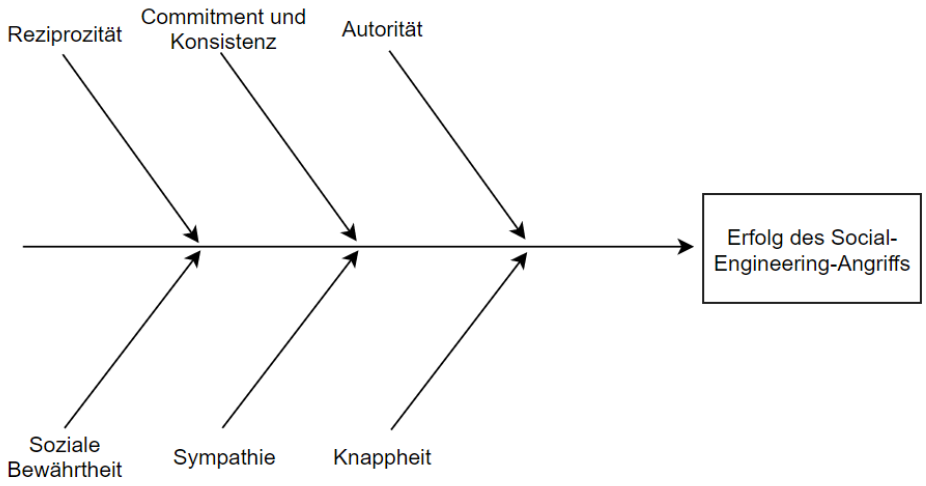

Abbildung 5: Überblick über Angriffsvektoren (vgl. Hoss, 2015)

3.3.1 Reziprozität

Reziprozität steht für Gegenseitigkeit. Das bedeutet, dass Menschen sich verpflichtet fühlen, etwas zurückzugeben, wenn sie etwas erhalten haben. Es gibt auch Personen, die nur nehmen und sich nie für erhaltene Gefälligkeiten revanchieren. Diese Arten von Personen werden Egoistinnen und Egoisten genannt. Sie werden jedoch langfristig ausgegrenzt. (Cialdini, 2013)

Bei der Reziprozität wird das Gefühl, etwas schuldig zu sein, ausgenutzt. Erstaunlich ist, dass jemand oftmals eine höherwertige Gegenleistung im Vergleich zu jener, die er oder sie erhalten hat, erbringt. Das Ganze lässt sich anhand eines Restaurantbesuches veranschaulichen. Hierbei ist die Frage zu stellen, warum am Ende oftmals ein Schnaps kostenlos vergeben oder warum die Rechnung mit Zuckerl serviert wird. Die Bereitschaft, ein höheres Trinkgeld zu geben, steigt damit enorm. Genau diese verhaltenspsychologische Regel lässt sich in vielen anderen Situationen anwenden und ebenso, wenn ein böswilliger Social-Engineering-Angriff geplant ist. (Cialdini, 2013)

3.3.2 Commitment und Konsistenz

Commitment bedeutet, dass sich eine Person durch eine Äußerung auf etwas Bestimmtes festlegt. Ein Beispiel dafür ist, wenn eine Person verspricht, eine gewisse Handlung durchzuführen. Dieses Commitment gewinnt an Bedeutung bzw. die Wirkung wird stärker, wenn es aktiv, freiwillig und öffentlich abgegeben wurde. (Schumacher, 2014) Auf der anderen Seite bedeutet Konsistenz Verlässlichkeit im eigenen Verhalten. (Cialdini, 2013)

Hoss (2015) zitiert eine nicht mehr erreichbare Website, laut der Personen, die einen Social-Engineering-Angriff ausführen, Menschen dazu bringen, sich konsistent zu früheren Versprechen zu verhalten. Die Abgabe eines Commitments ist durch geschickte Rhetorik, Verhandlungs- und Überzeugungskünste zu erreichen. Wurde ein Commitment von der angegriffenen Person abgegeben, war die Manipulation bereits teilweise erfolgreich, denn durch das Konsistenzbestreben der Menschen wird für die Angreiferin oder den Angreifer Arbeit verrichtet.

3.3.3 Autorität

Es gibt eine Regel, die besagt, dass Menschen, die autoritär wirken, was durch Uniform und Titel verstärkt werden kann, Einfluss auf Personen haben. (Cialdini, 2013)

Laut einer Studie kamen Personen einer Bitte von einem Menschen mit Straßenkleidung lediglich zu 42 % nach. Bei Personen in Wachdienstuniform lag die Bereitschaft, eine Bitte zu erfüllen, bei 92 %. (Schumacher, 2014)

Hier können Angreifer gezielt durch das Erstellen von Identitäten, beispielsweise als Systemadministratorin oder Systemadministrator, der bzw. die Zugangsdaten verlangt, an Daten kommen. (Cialdini, 2013)

3.3.4 Soziale Bewährtheit

Oftmals orientieren sich Menschen an anderen Personen, wenn sie eine Entscheidung treffen müssen. Es hat sich Folgendes bewährt und herausgestellt: Ist ein Handeln erforderlich, werden weniger Fehler begangen, wenn man gewissen Mustern folgt. (Cialdini, 2013)

Aus diesem Grund stellt die soziale Bewährtheit eine Angriffsmethode im Social Engineering dar. Hier wird versucht, eine Person gefügig zu machen, indem sie überzeugt wird, dass dieses Handeln schon viele Menschen durchgeführt haben. Als Beispiel ist hier zu nennen, dass Kunden und Kundinnen in Ladengeschäften oft Sätze wie „Der Artikel ist sehr beliebt und wird oft gekauft“ oder „Diesen Artikel müssen wir ständig nachbestellen“ zu hören bekommen. Dabei handelt es sich ebenfalls um den Versuch, einen Mehrwert zu generieren, und somit um Social Engineering. (Cialdini, 2013)

3.3.5 Sympathie

Die Regel der Sympathie besagt, dass Menschen sich von Personen, die ihnen sympathischer sind, leichter von etwas überzeugen bzw. zu etwas verleiten lassen. Verkäuferinnen und Verkäufer wenden das oftmals an, indem sie Gemeinsamkeiten betonen. Diese steigern dann die Erfolgschance, einen Mehrwert zu generieren. Ebenfalls kann die Überzeugungskraft durch Merkmale erhöht werden. (Cialdini, 2013) Cialdini (2013) beschreibt, dass es folgende Merkmale sind:

- Körperliche Attraktivität (wird auch mit Intelligenz und Freundlichkeit assoziiert)
- Ähnlichkeit
- Lob und Anerkennung (sollte nicht zu offensichtlich dargestellt werden, denn sonst ließe sich die Manipulation erkennen)
- Regelmäßiger Kontakt
- Assoziation mit einer positiven Sache

3.3.6 Knappheit

Das Gesetz der Knappheit besagt, dass knappe Produkte oder Leistungen attraktiver sind. Grundlage für dieses Gesetz ist, dass die Verfügbarkeit einer Sache Qualität indiziert. Deswegen wird oft die Taktik verfolgt, nur kleine Mengen zu verkaufen oder eine zeitliche Abgrenzung beizufügen. (Cialdini, 2013)

Dies lässt sich auch in Social Engineering anwenden. Wird eine Verknappung vorgetäuscht, handeln viele Menschen nicht mehr rational und denken nicht über Alternativen bzw. Folgen nach. (Hoss, 2015)

3.3.7 Typischer Prozess bei einem Angriff

Abraham & Chengalur-Smith (2010) beschreiben, dass es viele Kanäle gibt, die hauptsächlich bei einem Social-Engineering-Angriff mit der Absicht, Malware zu verbreiten, genutzt werden.

In folgender Grafik ist dargestellt, wie ein typischer erfolgreicher Angriff aussieht, wenn die Absicht besteht, Malware zu verteilen.

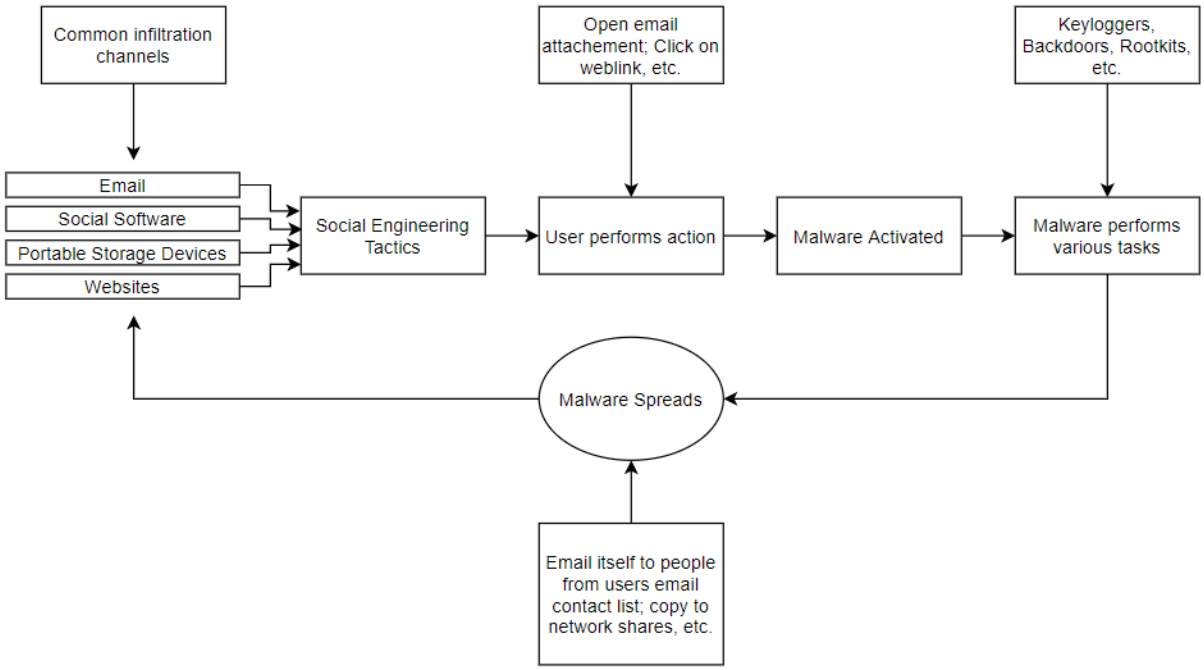

Abbildung 6: Steps taken by malware to infiltrate a system (vgl. Abraham & Chengalur-Smith, 2010)

Bei jeder Art von Social Engineering gibt es vier Stadien, die durchlaufen werden. Sie beginnen mit der Vorbereitung. Es ist Domänenwissen aufzubauen, damit der nächste Punkt erfolgreich durchgeführt werden kann. Hier geht es darum, ein Vertrauensverhältnis zum bzw. eine Autorität gegenüber dem Opfer zu schaffen. Im nächsten Schritt wird das entstandene Vertrauen ausgenutzt und danach wird es wieder in Anspruch genommen, bis ein Mehrwert entsteht. (Mitnick & Simon, 2003)

In folgender Grafik sind die vier Säulen als Prozess dargestellt:

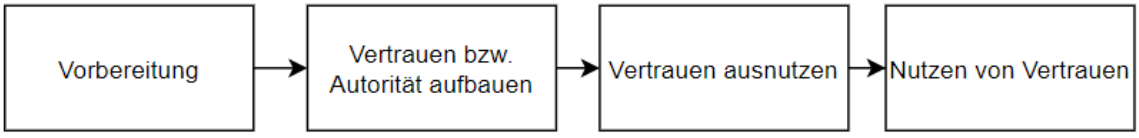

Abbildung 7: Vier Stadien eines Social-Engineering-Angriffs (vgl. Mitnick & Simon, 2003)

Wie in Kapitel 3.1 ersichtlich, beschreibt Bhagyavati (2007), dass es einen Zyklus beim Social Engineering gibt. Dieser besteht aus folgenden Phasen:

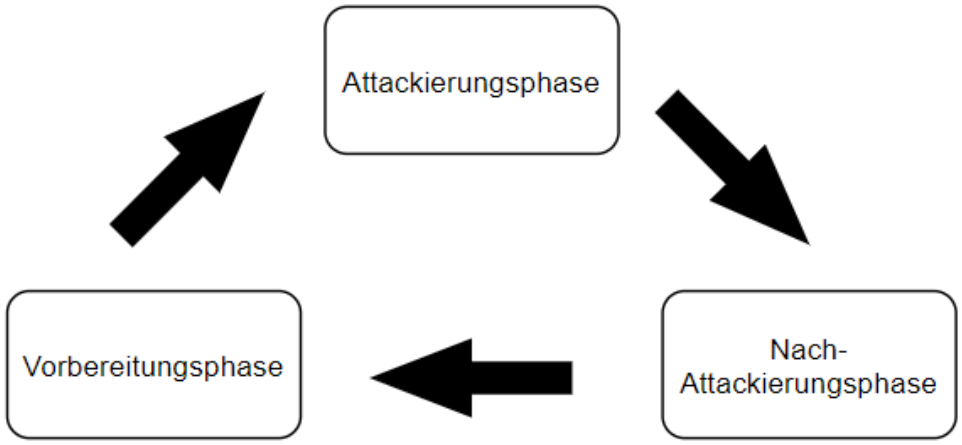

Abbildung 8: Zyklus eines Social-Engineering-Angriffs (vgl. Bhagyavati, 2007)

Beachtet man die Literatur, dann beginnt jeder Social-Engineering-Angriff mit einer Vorbereitungsphase, wo Informationen über das Unternehmen selbst, wie hierarchische Strukturen etc., herausgefunden werden. Mit diesen Daten wird dann der eigentliche Angriff geplant bzw. durchgeführt. Nicht zu vergessen ist die von Bhagyavati (2007) genannte Nachattackierungsphase bzw. das von Mitnick & Simon (2003) genannte „Nutzen von Vertrauen". Hier geht es darum, wie das Verhalten nach einem erfolgreichen Angriff aussieht.

3.4 Auswirkungen

Rund 97 % aller Security-Professionals und etwa 86 % aller IT-Professionals schenken dem Social Engineering sehr viel Beachtung, denn sie wissen, welcher Schaden dadurch entstehen kann. Ungefähr 43 % gaben an, dass sie durch einen Social-Engineering-Angriff attackiert worden sind, und nur 16 % waren sich sicher, nie Opfer eines solchen Angriffs gewesen zu sein. Hingegen wissen 41 % der Befragten nicht, ob sie jemals Opfer eines Angriffs waren. (Dimensional Research, 2011)

Es wurde herausgefunden, dass rund 51 % aller Social-Engineering-Angriffe mit der Motivation, einen monetären Mehrwert zu generieren, stattfinden. Lediglich in 14 % der Angriffe steckt die Motivation, sich zu rächen. (Dimensional Research, 2011)

Dimensional Research (2011) nennen die folgenden Werte für monetäre Schäden bei Unternehmen nach einem erfolgreichen Social-Engineering-Angriff:

- 48 % der Großunternehmen und 32 % der Unternehmen insgesamt gaben an, in den letzten zwei Jahren mehr als 25 Social-Engineering-Angriffe erlebt zu haben.
- Ebenfalls 48 % Prozent der Teilnehmerinnen oder Teilnehmer gaben an, dass sie pro Angriff durchschnittliche Kosten von über 25.000 $ hatten.
- Rund 30 % der Großunternehmen gaben an, durchschnittliche Kosten von über 100.000 $ pro Angriff gehabt zu haben.

3.5 Schützen vor einem Angriff

Dimensional Research (2011) nennt folgende Personen, die von Social-Engineering-Techniken besonders gefährdet sind:

- Rund 60 % aller neuen Mitarbeiterinnen oder Mitarbeiter
- Rund 44 % aller Auftragnehmerinnen oder Auftragnehmer
- Rund 38 % aller Assistentinnen oder Assistenten der Geschäftsführung

Des Weiteren führten rund 26 % der Befragten laufende Schulungen zum Thema Social Engineering durch. Auf der anderen Seite unternahmen 34 % keinerlei Anstrengungen in Bezug auf dieses Thema, obwohl 19 % von ihnen dies bereits planten. (Dimensional Research, 2011)

Eine Weitergabe von datenschutzrelevanten Informationen ist nur erlaubt, wenn ein begründetes Vertrauen zur Adressatin oder zum Adressaten besteht. Ein Unternehmen lässt sich nicht vollständig gegen Social-Engineering-Angriffe schützen, jedoch kann der Bedrohung entgegengewirkt werden. Das Ganze ist durch unkomplizierte Verhaltensregeln der Mitarbeiterinnen und Mitarbeiter und Aufklärung zu erreichen. In der Praxis wird Social Engineering damit erheblich erschwert. (Lardschneider, 2008)

Auch andere Maßnahmen des Informationsschutzes helfen dabei, erfolgreiche Social-Engineering-Angriffe zu reduzieren. Gemeint sind damit zum Beispiel der Gebäudezugang, Vergabe und Entzug von Zugriffsberechtigungen, Umgang mit externen Mitarbeiterinnen und Mitarbeitern etc. (Lardschneider, 2008)

Ein weiterer wichtiger Aspekt ist, dass auch beim Entwurf bzw. bei der Gestaltung von Web-Anwendungen die Gefahr durch Social Engineering berücksichtigt werden muss. Denn eine gefälschte Anwendung, die dem Original sehr ähnelt, kann mittels Man in the Browser der Benutzerin oder dem Benutzer vortäuschen, dass dies die richtige Anwendung ist. Hier müssen die Angriffsflächen der Anwendungen verringert werden, zum Beispiel mit einer Transaction-Authentication-Number (TAN). (Fox, 2013)

Lipski (2009) beschreibt, dass ein Social Engineer versuchen wird, entweder Informationen zu bekommen oder das Opfer zu einer Handlung zu überreden. Beide Angriffsweisen sind für ein Unternehmen gefährlich. Lipski (2009) entwickelte für beide Angriffsweisen ein Flussdiagramm.

Dieses zeigt in folgender Abbildung, wie man datenschutzrelevante Informationen nicht unautorisiert weitergibt:

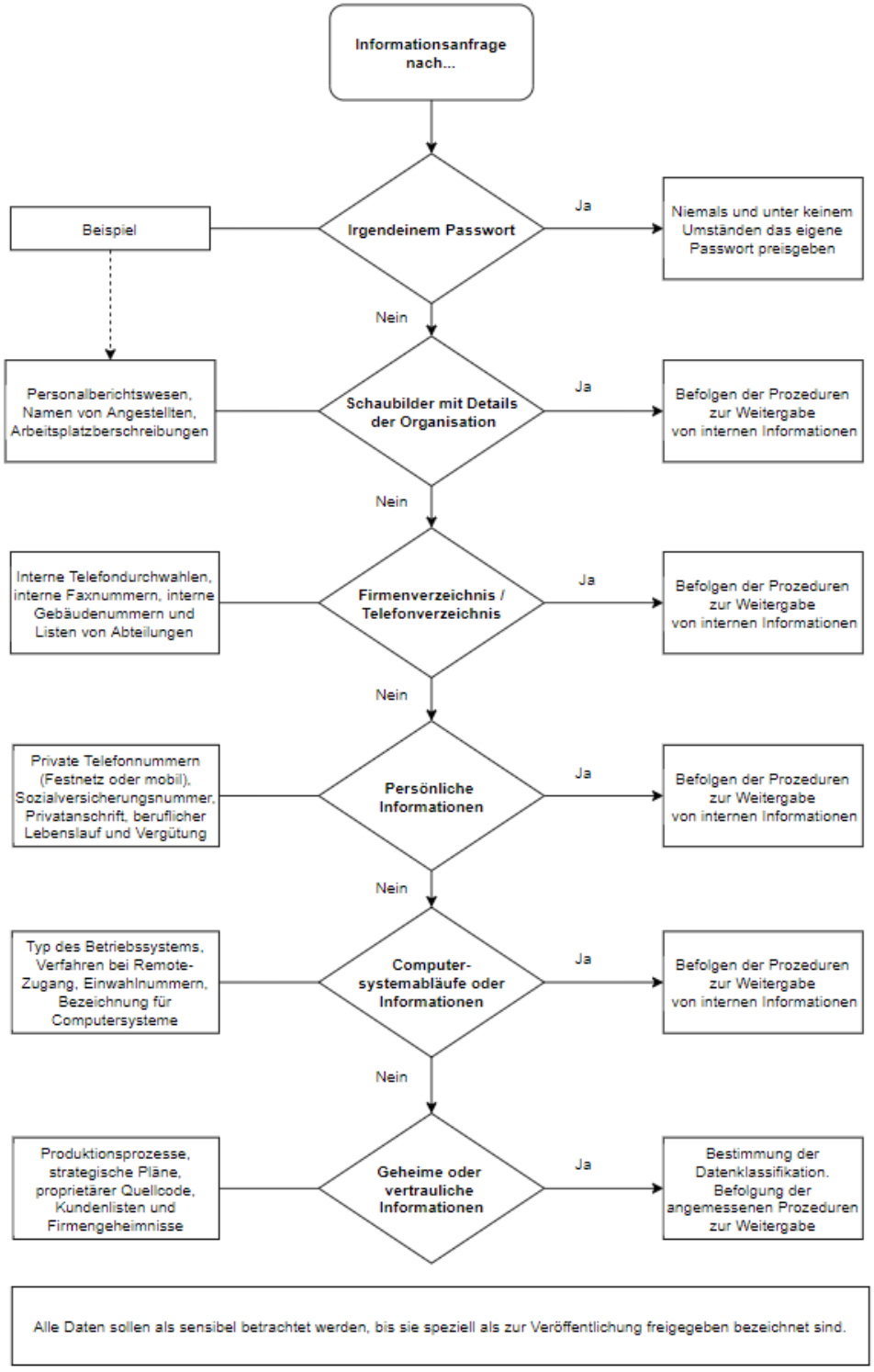

Abbildung 9: Bearbeitung einer Anfrage nach Informationen (vgl. Lipski, 2009)

Im unten stehenden Flussdiagramm ist ersichtlich, wie man nicht zu einer unberechtigten Handlung aufgefordert werden kann:

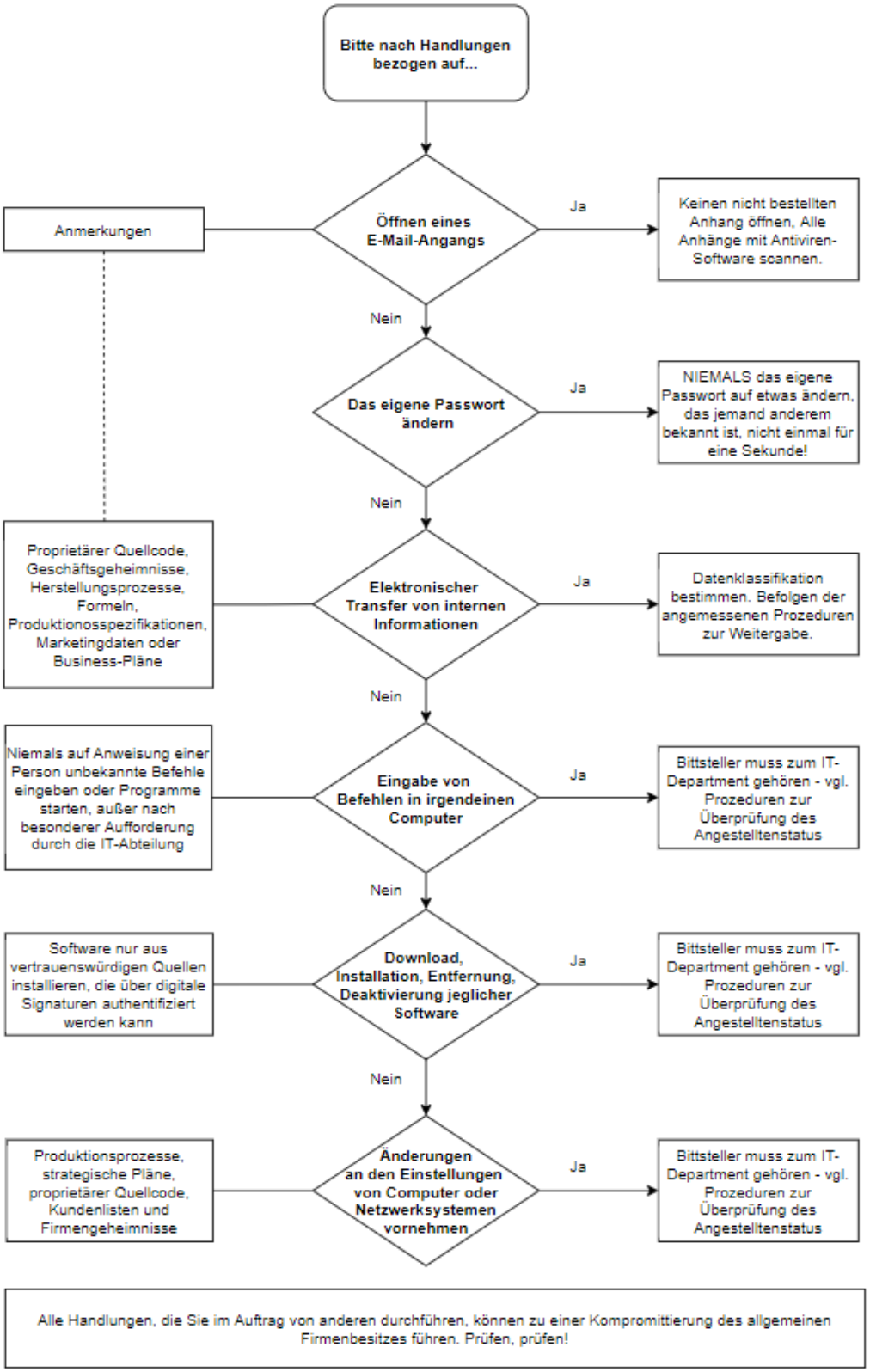

Abbildung 10: Bearbeitung einer Anfrage nach Handlungen (vgl. Lipski, 2009)

3.6 Fallbeispiele

Im Anschluss sind Fallbeispiele mit jeweils unterschiedlichen Methoden erläutert.

3.6.1 Phishing

Social-Engineer-Personen versuchen oftmals, Bankwebsites zu fälschen und diese mit einem leicht abgeänderten Link hochzuladen. Es werden dann viele Personen per Mail mit dem Link zur falschen Bankwebsite kontaktiert und gebeten, ihre Daten für eine Sicherheitsüberprüfung einzugeben. Diese Spam-Mails lassen sich aber oft ohne Aufwand identifizieren, denn diese enthalten in meisten Fällen keine persönliche Anrede. Bei genauer Betrachtung des Links fällt zudem auf, dass der Name der Bank falsch geschrieben ist, zum Beispiel „raifeisenbank.at“ anstatt „raiffeisenbank.at“. Es ist auch möglich, dass die Top-Level-Domain eine andere ist, aber der vordere Teil des Links ist derselbe wie beim Original. (BSI)

3.6.2 Tailgating

Eine häufige Form einer Tailgating-Attacke besteht darin, dass eine Person sich als Fahrer einer Lieferfirma ausgibt und so den Unternehmensstandort betreten kann. Häufig geschieht es, dass eine Mitarbeiterin oder ein Mitarbeiter die Sicherheitsfreigabe erteilt und die Angreiferin oder der Angreifer Zugang zum Unternehmen bekommt. Tailgating funktioniert jedoch nicht bei allen Betrieben. Viele große Unternehmen teilen personalisierte Zutrittskarten an die einzelnen Mitarbeiterinnen und Mitarbeiter aus. Das heißt, wenn es jemandem gelingt, sich Zutritt zum Firmengelände zu verschaffen, hat derjenige im Anschluss dennoch nicht die Möglichkeit, in einzelne Bereiche eines Objektes zu gelangen. Hier müsste die Person sich mit einem anderen Vorwand weiterhelfen. (Grohmann, 2018)

3.6.3 Reverse Social Engineering

Jemand gibt sich als Mitarbeiterin oder Mitarbeiter der IT-Abteilung aus und ruft die Beschäftigten des Konzerns an. Es wird berichtet, dass es einen neuen Virus gibt, der auf einigen Firmencomputern installiert ist, und dass das Antivirenprogramm diesen nicht erkennt. Der Social Engineer nimmt sich Zeit für die Erklärung und bietet dem Opfer die Hilfe an, nachzusehen, ob der Computer des Opfers vom Virus betroffen ist. Die angebliche Mitarbeiterin oder der angebliche Mitarbeiter von der IT-Abteilung leitet das Opfer durch einige Schritte. Zum Schluss wird gebeten, ein Programm zu installieren, das solche Viren besser erkennen sollte. Dieses Programm sendet im Hintergrund Informationen, die auf dem Computer gespeichert sind, an den Social Engineer. (Merten, 2009)

3.6.4 Malware

Der Social Engineer beschafft USB-Sticks mit dem Firmenlogo. Darauf wird eine Malware gespielt und anschließend auf dem Firmengelände in Bereichen verteilt, wo üblicherweise Personen USB-

Sticks ablegen. Viele Angestellte sind neugierig, stecken den USB-Stick in den Computer und wollen nachsehen, welche Daten dort gespeichert sind. Es installiert sich jedoch die Malware. (Merten, 2009)

4 METHODIK

Der empirische Teil dieser Arbeit umfasst eine Umfrage. Diese wird von Personen ausgefüllt, die in einem Unternehmen angestellt sind und mit ihrer Tätigkeit Einfluss auf die Informationssicherheit haben. Ziel dieser Umfrage ist es, herauszufinden, wie einzelne Maßnahmen zur Gewährleistung der Informationssicherheit beitragen und ob sich diese auf die die Effizienz des Arbeitsflusses vom Personal auswirken.

Raithel (2008) stellt den Forschungsablauf einer quantitativen Analyse wie folgt dar:

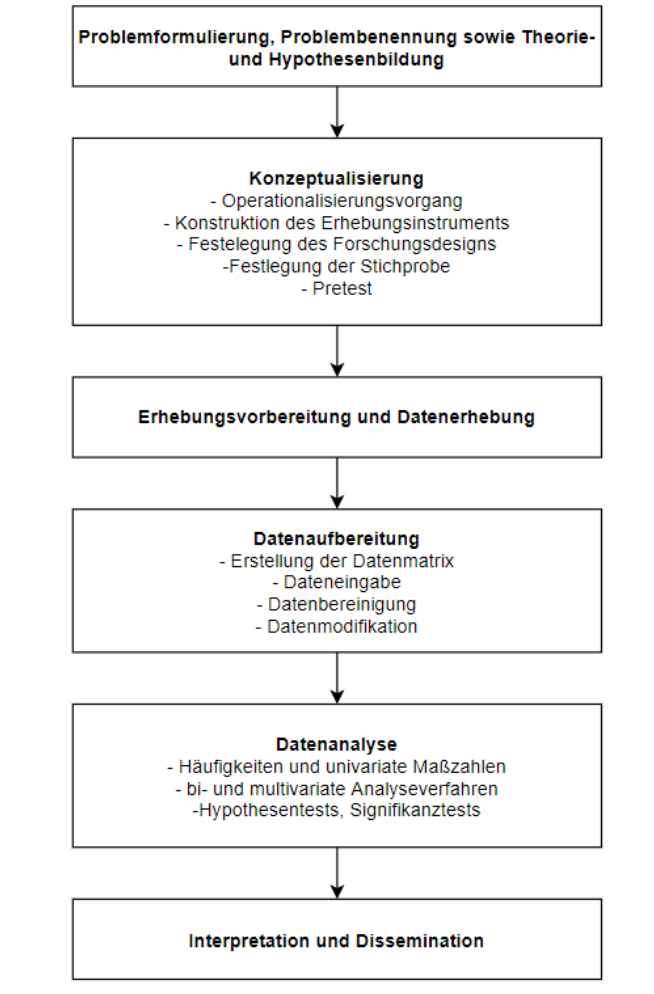

Abbildung 11: Phasen des Forschungsablaufs (vgl. Raithel, 2008)

Im Rahmen dieser Masterarbeit werden bei der Umfrage die oben genannten Phasen durchlaufen.

Im Anschluss wird eine qualitative Inhaltsanalyse nach Mayring durchgeführt. Mit den gewonnenen Erkenntnissen aus den Interviews wird daraufhin ein Konzept mit Initiativen entwickelt, die ergriffen werden müssen, um die Informationssicherheit eines Unternehmens mit kritischer Infrastruktur gewährleisten zu können.

4.1 Sicht von Mitarbeiterinnen und Mitarbeitern, die in ihrer Tätigkeit Einfluss auf die Informationssicherheit haben

In einem Unternehmen gibt es neben der IT auch andere Abteilungen, die in ihrer Tätigkeit sensible Informationen bearbeiten, deren Weitergabe an unbefugte Dritte der Informationssicherheit eines Unternehmens gegebenenfalls schadet.

Es ist bis dato nicht gelungen, durch ein Assessment das Sicherheitsbewusstsein der einzelnen Mitarbeiterinnen und Mitarbeiter zu messen. Aber durch kontrollierte Sicherheitsvorfälle wurde das Risiko, welches Ausmaß ein Social-Engineering-Angriff annehmen kann, vor Augen geführt und war somit greifbar. (Lardschneider, 2008)

4.1.1 Fragebogen

In diesem Teil wird ein Fragebogen erstellt, der dann als Umfrage an verschiedene Personen ausgesendet wird. Mithilfe dieses Fragebogens sollen im Anschluss die Hypothesen 3 und 4, die in Kapitel 1.3 beschrieben sind, überprüft werden.

Auf die Hypothesen 1 und 2 wird in Kapitel 4.2 eingegangen.

Im Folgenden wird die Gliederung des Fragebogens präsentiert.

Einleitung

In der Einleitung werden allgemeine Informationen der befragten Personen erhoben. Unter anderem wird das Alter der Teilnehmerinnen und Teilnehmer abgefragt, damit ersichtlich ist, ob Personen verschiedener Alterskategorien ein unterschiedliches Sicherheitsgefühl aufweisen.

Des Weiteren soll gefragt werden, welche Größe das Unternehmen hat, in dem die Befragten beschäftigt sind. Damit kann herausgefunden werden, ob eine Beschäftigung in einem großen oder kleinen Unternehmen ebenso Einfluss auf das Sicherheitsgefühl hat.

Es soll ebenso erhoben werden, ob das Unternehmen, in dem die teilnehmenden Personen beschäftigt sind, als kritische Infrastruktur gekennzeichnet ist. Damit kann eine Aussage dazu getroffen werden, ob es einen Einfluss auf das Empfinden der Informationssicherheit hat, wenn das Unternehmen zur kritischen Infrastruktur zu zählen ist.

Im nächsten Schritt soll gefragt werden, ob die Teilnehmenden in der IT arbeiten oder in einer anderen Abteilung angestellt sind. Hiermit wird überprüft, ob Personen mit einer IT-Affinität ein höheres Sicherheitsbewusstsein haben als andere Personen.

Eine weitere zentrale Frage besteht darin, ob die Teilnehmerin oder der Teilnehmer als Führungskraft agiert. Damit wird geklärt, ob Personen mit höherer Verantwortung ein stärkeres Empfinden für die Informationssicherheit aufweisen.

Ferner gilt es, herauszufinden, ob die teilnehmenden Personen in ihrer Tätigkeit mit sicherheitsrelevanten Informationen, wie personenbezogenen Daten, arbeiten. Als Abschluss der

Einleitung wird gefragt, ob es im Unternehmen bereits Security-Awareness-Schulungen gegeben hat und ob diese zyklisch stattfinden.

Fragen zur Hypothese 3

In diesem Bereich soll herausgefunden werden, ob Personen mit einer IT-Affinität ein höheres Sicherheitsempfinden haben als Personen ohne IT-Affinität. Dabei wird mit einer Selbsteinschätzung begonnen. Die teilnehmenden Personen können zwischen den folgenden vorgegebenen Antwortmöglichkeiten wählen: „keine IT-Affinität (Standardbenutzer; Office-Anwendungen, Internet-Surfing“, „mittlere IT-Affinität (fortgeschrittener Benutzer, Bau von kleineren Lösungen im Heimnetzwerk, geringe Scripting Kenntnisse und der Umgang mit dem Betriebssystem Linux)“ und „hohe IT-Affinität (Expertin oder Experte in der IT, Bau von großen Lösungen, Hacking, Programmiererinnen und Programmierer).“

Im Anschluss wird gefragt, woher die IT-Kenntnisse stammen, d. h., ob diese durch eigenständiges Lernen angeeignet wurden oder im Rahmen einer Ausbildung. Hiermit soll herausgefunden werden, ob das Sicherheitsbewusstsein durch die Ausbildungsform beeinflusst wird.

Daraufhin sollen die Teilnehmerinnen und Teilnehmer eine weitere Selbsteinschätzungsfrage beantworten. Dabei geht es darum, ob die Befragten eher der Sicherheit oder eher der Effizienz Beachtung schenken. Schutzmaßnahmen wie eine Zwei-Faktor-Authentifizierung schützen vor Angriffen, wenn ein Passwort in falsche Hände gelangt (EUROPOL, 2018).

In diesem Zusammenhang muss jedoch die Frage beantwortet werden, ob solche Maßnahmen für einzelne Personen als sinnvoll und notwendig erachtet werden. Zum Abschluss sollen die befragten Personen angeben, ob sie eine Vorstellung vom Ausmaß der Nebenwirkungen eines Social-Engineerings-Angriffs haben.

Fragen zur Hypothese 4

In diesem Bereich des Fragebogens soll geklärt werden, ob der Arbeitsfluss der teilnehmenden Personen durch den Einsatz von Maßnahmen zur Gewährleistung der Informationssicherheit gestört wird. Da Social-Engineering-Angriffe oftmals auf psychologischen Mechanismen beruhen (Hoss, 2015), werden Security-Awareness-Programme empfohlen (Mitnick & Simon, 2003).

Solche Schulungen werden von diversen Unternehmen angeboten und im Regelfall auch zyklisch durchgeführt. Es soll herausgefunden werden, ob solche Schulungen zyklisch stattfinden und wie lange sie dauern bzw. welchen Aufwand sie für eine einzelne Person verursachen. Des Weiteren wird gefragt, ob die Security-Awareness-Schulungen, falls diese zyklisch durchgeführt werden, immer gleich, d. h. ohne Anpassungen, abgehalten werden oder ob nach einer erfolgreich absolvierten Schulung nur die zentralen Punkte aufgefrischt werden. Neben solchen Schulungen werden von Unternehmen auch technische Maßnahmen, wie die Zwei-Faktor-Authentifizierung oder zyklische Passwortänderungen, ergriffen, um einen Social-Engineering-Angriff zu erschweren. (EUROPOL, 2018)

Solche Maßnahmen können zu einem nicht verständlichen Aufwand für einzelne Personen führen. Auf dem Onlineportal it-daily.net (2020) werden folgende fünf Maßnahmen beschrieben, die einen Angriff verhindern sollen:

- **Awareness-Aufbau**
  Mitarbeiterinnen und Mitarbeiter sollen kontinuierlich geschult werden, damit keine sicherheitsrelevanten Informationen an nicht autorisierte Personen weitergegeben werden.
- **Nutzung von Privileged Access-Management**
  Durch proaktive Planung werden die Zugriffsrechte von Benutzerinnen und Benutzern auf ein Minimum beschränkt.
- **Einsatz einer Multi-Faktor-Authentifizierung**
  Ohne Multi-Faktor-Authentifizierung reicht ein einzelnes Passwort, um Zugriff auf kritische Informationssysteme zu erhalten. Das ist als kritisch anzusehen, denn ein Passwort kann durch eine Social-Engineering-Attacke, wie durch Phishing, schnell herausgefunden werden. Mit einer Multi-Faktor-Authentifizierung bleibt ein Angriff auch bei gestohlenem Kennwort erfolglos.
- **Verwendung dualer Kontrollsysteme**
  Sind vertrauliche Informationen betroffen, sollte zumindest ein Vier-Augen-Prinzip herrschen, damit eine einzelne Mitarbeiterin oder ein einzelner Mitarbeiter keinen alleinigen Zugriff auf die vertraulichen Informationen bekommt.
- **Überwachung privilegierter Aktivitäten**
  Der Zugriff zu sicherheitsrelevanten Informationen sollte kontinuierlich durch den Einsatz diverser Analyse-Tools überwacht werden, damit bei einem Angriff schnell reagiert werden kann.

Die Umfrage beinhaltet Fragen zu den fünf genannten Sicherheitsmechanismen, um herauszufinden, welche davon für Mitarbeiterinnen und Mitarbeiter einen erheblichen Mehraufwand im Arbeitsfluss darstellen.

Abschluss

Am Schluss des Fragebogens soll geklärt werden, ob die teilnehmenden Personen diesen verstanden und selbst ausgefüllt haben. Wurde der Fragebogen von einzelnen Teilnehmerinnen und Teilnehmern nicht verstanden oder wurden die Fragen von gewissen Personen zufällig ausgefüllt, so müssen diese Daten für die weitere Analyse entfernt werden, um Verfälschungen entgegenzuwirken.

4.1.2 Befragte Personen

Die Umfrage richtet sich an Personen, die ein aktives Beschäftigungsverhältnis in einem Unternehmen haben und sicherheitskritische Informationen verarbeiten. Damit das Ergebnis der Umfrage nicht verfälscht wird, wurden entsprechende Überprüfungsfragen eingebaut, um die Stichprobe gegebenenfalls anpassen zu können.

Diese Umfrage wurde an mehrere Unternehmen kritischer Infrastruktur ausgesendet und von einem Teil der Mitarbeiterinnen und Mitarbeiter ausgefüllt. Ebenfalls wurde die Umfrage an weitere Unternehmen, die nicht den Status einer kritischen Infrastruktur haben, geschickt, um einen Vergleich zu erhalten. Des Weiteren wurde die Umfrage über diverse soziale Medien verteilt.

4.1.3 Durchführungszeitraum

Die Umfrage wurde am 22.12.2021 online gestellt und war 26 Tage über den Link, der an die Unternehmen ausgesendet wurde, öffentlich zugänglich. Ein längerer Zeitraum hätte eventuell zu einer größeren Grundgesamtheit, jedoch zu keiner großen Veränderung der Ergebnisse geführt, da viele die Umfrage bereits nach Erhalt der E-Mail ausgefüllt haben.

4.1.4 Verwendete Tool

Die Umfrage wurde mittels Microsoft Word vorgefertigt. Nachdem die einzelnen Fragen formuliert waren, wurde der Fragebogen über die Homepage https://www.umfrageonline.com/ verteilt. Hier haben Studierende die Möglichkeit, kostenlos eine Umfrage zu erstellen und automatisierte statistische Auswertungen zu nutzen. Es wird auf eine schriftliche Befragung gesetzt, denn beim Thema des Social Engineerings überwiegen die Vorteile dieses Ansatzes gegenüber einer mündlichen Befragung. So ist es vorteilhaft, dass durch eine schriftliche Befragung im Verhältnis zu telefonischen Interviews, die aufwändiger sind, eine größere Grundgesamtheit zu Stande kommt.

Schriftliche Befragungen haben gegenüber anderen Varianten folgende Vorteile (Raithel, 2008):

- geringer Zeitaufwand
- geringe Kosten
- Beantwortung ist zeitunabhängig
- Mögliche Einflussfaktoren, wie das Verhalten der befragten Person, werden ausgeschaltet.

Schriftliche Befragungen haben gegenüber anderen Varianten folgende Nachteile (Raithel, 2008):

- Situation der Befragung nicht kontrollierbar
- Beeinflussung der Antworten durch andere Personen
- keine Hilfe bei Verständnisproblemen

4.1.5 Pretest und Pilot-Studie

Das entwickelte Erhebungsinstrument sollte vor der Hauptuntersuchung geprüft werden. Es wird ein sogenannter Pretest durchgeführt, um das Instrument auf Anwendbarkeit, Vollständigkeit, Verständlichkeit und Qualität zu prüfen. (Friedrichs, 1990)

Der entwickelte Fragebogen wird an eine kleine Stichprobe gesendet. Diese Personen füllen ihn aus und markieren unklare Fragen, die im Anschluss angepasst werden.

Im Rahmen dieser Masterarbeit wurde eine Stichprobe von 20 Leuten ausgewählt, die alle im selben Unternehmen angestellt sind und direkt Kontakt zu informationskritischen Systemen haben. Die Pilot-Studie mit der ersten Fassung hat ergeben, dass bei gewissen Fragen ein Grundverständnis der IT erforderlich ist. Das wurde abgeändert und es wurde versucht, bei den Formulierungen kein IT-Wissen vorauszusetzen. Nach dieser Änderung wurde der Fragebogen wieder an die Stichprobe ausgesendet und dieses Mal gab es keine Missverständnisse mehr.

4.2 Sicht von Expertinnen und Experten für Informationssicherheit

Damit eine Hypothesenüberprüfung stattfinden kann, müssen in erster Linie Theorien vorliegen. Ist dies der Fall und lassen sich Annahmen formulieren, dann ist eine empirische Überprüfung möglich. (Raithel, 2008)

In der Grafik unten ist der Prozess zur empirischen Testung ersichtlich.

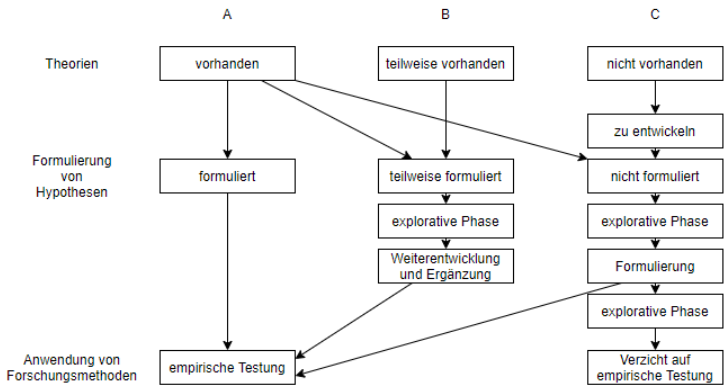

Abbildung 12: Theorien- und Hypothesenbildung (vgl. ATTESLANDER et al., 2003)

Neben der quantitativen Forschungsposition gibt es auch eine qualitative Forschungsposition. Das Ziel bei der qualitativen Forschungsposition ist das Verstehen des menschlichen Verhaltens. Um hier einen Prozess zu rekonstruieren, werden Daten mit einem interpretativen Verfahren verarbeitet. Es können hermeneutische, phänomenologische und dialektische Methoden angewandt werden. (Raithel, 2008)

Als Standardinstrument für eine qualitative Analyse wird die Befragung genannt. (Schnell et al., 1999)

> *„Die Befragung ist ein systematisch geplanter Kommunikationsprozess zwischen mindestens zwei Personen.“* (Raithel, 2008)

Der Unterschied zwischen der wissenschaftlichen Befragung und einer alltäglichen Kommunikation besteht darin, dass die wissenschaftliche Befragung systematisch vorbereitet und zielgerichtet ist. (ATTESLANDER et al., 2003)

Raithel (2008) beschreibt, dass eine Befragung grundsätzlich mündlich oder schriftlich erfolgen werden kann, wobei es folgende Kommunikationsformen gibt:

- wenig strukturiert – Es wird ein narratives Interview durchgeführt.
- teilstrukturiert – Es gibt einen Leitfaden, jedoch kann von diesem leicht abgewichen werden.
- stark strukturiert – Es ist eine standardisierte Befragung, so dass von den Fragen nicht abgewichen werden soll.

Im Rahmen dieser Masterarbeit soll eine teilstrukturierte Befragung durchgeführt werden. Es wurde ein Leitfaden erstellt. Von diesem kann jedoch kurzzeitig abgewichen werden, wenn sich im Experteninterview neue Erkenntnisse auftun.

4.2.1 Qualitative Inhaltsanalyse nach Mayring

Es gibt heutzutage eine Vielzahl an Definitionen der Inhaltsanalyse. Jedoch gibt es keine eindeutige, denn die Begriffsbestimmungen haben immer einen Bezug zur jeweiligen Autorin oder zum jeweiligen Autor. (Mayring, 2015)

Eine beispielhafte Definition stammt von Berelson (1952) und lautet:

„Inhaltsanalyse ist eine Forschungstechnik für die objektive, systematische und quantitative Beschreibung des manifesten Inhalts von Kommunikation."

Mayring selbst fügte keine eigene Definition der Inhaltsanalyse an. Es wurden aber Spezifikationen als sozialwissenschaftliche Methode aufgewiesen. Damit eine Kommunikation analysiert werden kann, muss bei der Inhaltsanalyse systematisch, d. h. regel- und theoriegeleitet, vorgegangen werden. Es soll das Ziel verfolgt werden, aus den Interviews Schlüsse zu bestimmten Aspekten zu ziehen. (Mayring, 2015)

Mayring (2015) beschreibt, dass folgende Grundsätze für die Entwicklung einer qualitativen Inhaltsanalyse beachtet werden müssen:

- Die Vorzüge der quantitativen Techniken dürfen bei einer qualitativen Inhaltsanalyse nicht aufgegeben werden. Das ganze Vorgehen muss systematisch abgehandelt werden.
- Das gewonnene Material aus einer qualitativen Inhaltsanalyse darf nicht isoliert betrachtet werden, denn es ist ein Glied der Kommunikationskette und muss in ein Kommunikationsmodell eingeordnet werden.
- Gewisse Grundbegriffe der quantitativen Inhaltsanalyse werden auch in der qualitativen Inhaltsanalyse beibehalten. Ein Beispiel hierfür ist die Anwendung eines Kategoriensystems, womit einzelne Erkenntnisse generiert werden können.

Die Forscherin oder der Forscher beschäftigt sich in der Inhaltsanalyse mit fertigem sprachlichem Material. Somit handelt es sich um eine Ausgangsmethode. Eine genaue Analyse des Ausgangsmaterials macht es möglich, dieses zu interpretieren. (Mayring, 2015)

Folgende Tabelle zeigt die Bestimmung des Ausgangsmaterials der vorliegenden Arbeit.

Festlegung des Materials	Die durchgeführten Experteninterviews werden aufgenommen und im Anschluss transkribiert. Ein Interview basierte auf schriftlichen Fragen und Antworten.
Analyse der Entstehungssituation	Aufgrund der momentanen SARS-CoV-2-Pandemie war ein persönliches Interview nicht möglich. Aus diesem Grund wurde das Collaboration-Tool Microsoft Teams

	eingesetzt. Die Interviews wurden über eine entsprechende Funktion auch aufgenommen. Details zu den befragten Expertinnen oder Experten sind in Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.** zu finden. Ein Interview wurde schriftlich via E-Mail erledigt.
formale Charakteristika des Materials	Das Programm MAXQDA wurde eingesetzt, um die Tonaufnahmen der Interviews geordnet in einem Projekt abzulegen und zu transkribieren. Im Interview enthaltene Grammatikfehler oder dialektale Ausdrücke wurden beim Transkribieren beibehalten, während beim Paraphrasieren die dialektalen Ausdrücke ins Standarddeutsche übertragen wurden.

Tabelle 1: Bestimmung des Ausgangsmaterials (in Anlehnung an Mayring, 2015)

Im nächsten Schritt folgt die Interpretation, wofür eine spezifische Fragestellung notwendig ist. Des Weiteren muss auch die Richtung der Analyse bestimmt werden, denn ein Text kann nicht ohne definierte Zielsetzung interpretiert werden.

Die Fragestellung lässt sich in zwei Schritten bestimmen (Mayring, 2015):

- Im Rahmen dieser Masterarbeit gilt es, folgende Forschungsfrage zu beantworten: *„Welche Initiativen müssen gesetzt werden, um die Informationssicherheit von Unternehmen kritischer Infrastruktur im Kontext Social Engineering zu gewährleisten, ohne einen beträchtlichen Mehraufwand für Mitarbeiterinnen und Mitarbeiter zu verursachen?“* Um diese Frage zu beantworten, werden sowohl quantitative Methoden als auch qualitative Methoden eingesetzt. Im Rahmen der qualitativen Inhaltsanalyse werden anhand von Experteninterviews die folgenden Hypothesen geprüft, um im Anschluss die Forschungsfrage zu beantworten:
    - **Hypothese 1:** Jährliche Schulungen für Mitarbeiterinnen und Mitarbeiter im Kontext des Social Engineerings haben einen positiven Einfluss auf die Informationssicherheit von kritischen Infrastrukturen.
    - **Hypothese 2:** Jährliche Schulungen für Mitarbeiterinnen und Mitarbeiter können als Investition für die Informationssicherheit kritischer Infrastruktur gesehen werden und sparen im Allgemeinen Kosten, wenn die Ausgaben für die Schulung mit jenen infolge eines Vorfalles verglichen werden.

Im nächsten Schritt werden die Analysetechniken festgelegt. Das wird auch als die Stärke der qualitativen Inhaltsanalyse bezeichnet. Durch die Zerlegung in einzelne Interpretationsschritte wird das Vorgehen für andere nachvollziehbar und intersubjektiv überprüfbar. In der vorliegenden Arbeit werden die Analyseschritte gemäß dem Ablaufmodell mittels Kategoriensystem angewendet. Dabei wird auf den Ansatz der deduktiven Kategorienbildung zurückgegriffen, da sich die verwendeten Kategorien auf die einzelnen Fragen des Interviews beziehen.

4.2.2 Leitfaden

Entweder basiert ein Leitfaden auf dem ‚Erzählaufforderung-Erzählung-Schema', das den Befragten mit mehreren Erzählaufforderungen konfrontiert, oder auf offenen Fragen, was als ‚Frage-Antwort-Schema' bezeichnet wird. Bei dieser Form werden die Fragen, die in Listenform angeordnet sind, in fester Reihenfolge gestellt. Eine Kombination dieser beiden Schemata ist ebenso möglich. Die im Leitfaden ausformulierten Fragen können im Interview flexibler gestaltet werden, was auch bedeutet, dass die Formulierungen nicht wörtlich zu übernehmen sind. Ein Leitfaden ist lediglich eine Erinnerungsstütze für das Interview. (Helfferich, 2019)

Der Leitfaden untergliedert sich in die folgenden vier Bereiche:

Allgemeines
Zu Beginn des Leitfadens wird die Forschungsfrage selbst dargestellt, damit die Expertinnen und Experten wissen, auf welcher Basis die Antworten beruhen sollen. Des Weiteren werden in diesem Bereich Informationen an die Expertinnen und Experten weitergegeben. Dazu gehören knappe Angaben zum Thema und der Zielsetzung dieser Arbeit sowie zum Ablauf und der Dauer des Gesprächs. Zum Schluss wird die Datenschutzvereinbarung noch einmal besprochen, damit keine Missverständnisse entstehen können.

Einleitung
In der Einleitung wird großer Wert darauf gelegt, nähere Informationen über die Expertinnen und Experten zu gewinnen. Mit diesen Einstiegsfragen wird ermittelt, welche Erfahrungen die einzelnen Befragten im Bereich der Informationssicherheit aufweisen und wie sie zu ihrer Expertise gekommen sind. Des Weiteren geben die Expertinnen und Experten eine Einschätzung, welche Personengruppe am anfälligsten für Social-Engineering-Angriffe ist.

Hypothese 1

In diesem Bereich des Leitfadens werden die Fragen an die Expertinnen und Experten so gestellt, dass die folgende Hypothese überprüft werden kann: *„Jährliche Schulungen für Mitarbeiterinnen und Mitarbeiter im Kontext des Social Engineerings haben einen positiven Einfluss auf die Informationssicherheit von kritischen Infrastrukturen."*

Die befragten Personen geben hier Auskunft darüber, ob und warum solche Schulungen eingesetzt werden und ob diese einen messbaren Erfolg zeigen. Weiters wird hier abgefragt, ob die Security-Abteilung des Unternehmens die Mitarbeiterinnen und Mitarbeiter selbstständig mit Social-Engineering-Angriffen testet und wie erfolgreich diese sind. Ebenfalls wird von den Expertinnen und Experten die Frage beantwortet, wie der Aufbau einer solchen Security-Awareness-Schulung aussieht und ob es auch andere technische Maßnahmen gibt, die einen Social-Engineering-Angriff erschweren und wie sinnvoll diese sind. Zum Abschluss sollen die Expertinnen und Experten Auskunft darüber geben, ob sich einzelne Arbeitnehmerinnen und Arbeitnehmer über die Security-Awareness-Schulungen beschweren mit der Begründung, dass sich das Durchführen dieser Schulungen negativ auf die Effizienz des Arbeitsflusses auswirkt. Letztlich ist auch von Interesse, ob es einen Unterschied zwischen Unternehmen kritischer Infrastruktur und anderen Unternehmen gibt.

Hypothese 2

Dieser Bereich des Leitfadens dient dazu, folgende Hypothese zu überprüfen: *„Jährliche Schulungen für Mitarbeiterinnen und Mitarbeiter können als Investition für die Informationssicherheit kritischer Infrastruktur gesehen werden und sparen im Allgemeinen Kosten, wenn die Ausgaben für die Schulung mit jenen infolge eines Vorfalles verglichen werden."*

Diese Vermutung wird mit Fragen zu den jährlichen Kosten für die Durchführung von Security-Awareness-Schulungen überprüft. Des Weiteren wird hier die Frage beantwortet, ob das Unternehmen bereits von einem Social-Engineering-Angriff betroffen war und ob dieser erfolgreich war oder nicht. Weiters wird auch danach gefragt, ob es neben Security-Awareness-Schulungen auch andere technische Maßnahmen gibt, die einen Social-Engineering-Angriff erschweren und welche Kosten diese verursachen. Die Expertinnen und Experten geben hier ebenfalls Auskunft darüber, wie häufig Social-Engineering-Angriffe versucht werden und ob sich Security-Awareness-Schulungen rentieren.

Abschluss

Zum Abschluss wird noch eine kurze Zusammenfassung wiedergegeben, damit es zu keinen Missverständnissen kommt. Die Expertinnen und Experten werden darüber informiert, wie die Interviews ausgewertet werden und dass die fertige Auswertung auch weitergegeben werden kann.

Folgende Kategorien wurden aus dem Leitfaden abgeleitet:

- **Erfahrung:** Bei dieser Kategorie geht es um die Erfahrungen der interviewten Personen im Bereich der Informationssicherheit.
- **Entwicklung:** Diese Kategorie beschreibt, wie sich die Informationssicherheit im Kontext von Social Engineering im Laufe der Jahre verändert hat.
- **gefährdete Personengruppe:** Bei dieser Kategorie liegt der Fokus darauf, welche Personengruppe am anfälligsten für Social-Engineering-Angriffe ist.
- **Sinnhaftigkeit von Security-Awareness-Schulungen:** Dies Kategorie beschreibt, inwieweit Security-Awareness-Schulungen sinnvoll sind.
- **Aufbau von Security-Awareness-Schulungen:** Bei dieser Kategorie geht es darum, wie eine Security-Awareness-Schulung aufgebaut werden sollte.
- **technische Maßnahmen gegen Social-Engineering-Angriffe:** Bei dieser Kategorie wird abgefragt, ob es andere technische Maßnahmen gibt, die einen Social-Engineering-Angriff erschweren.
- **Messung:** Mit dieser Kategorie wird erhoben, inwieweit sich die Gefahr von Social-Engineering-Angriffen durch Security-Awareness-Schulungen oder andere Maßnahmen verändert hat.
- **Unterschied zwischen Unternehmen kritischer Infrastruktur und Unternehmen keiner kritischen Infrastruktur:** Bei dieser Kategorie geht es darum, ob es bei den eingesetzten Maßnahmen bzgl. der Sinnhaftigkeit einen Unterschied zwischen Unternehmen kritischer Infrastruktur und Unternehmen keiner kritischen Infrastruktur gibt.
- **Beschwerden:** Diese Kategorie beschreibt, ob sich einzelne Mitarbeiterinnen oder Mitarbeiter bereits über eingesetzte Maßnahmen, die die Informationssicherheit im Kontext von Social Engineering gewährleisten sollen, beschwert haben.
- **Kosten eines Social-Engineering-Angriffs:** Mit dieser Kategorie wird erhoben, welche Kosten durch einen Social-Engineering-Angriff entstehen können.
- **Wahrscheinlichkeit, Opfer eines Social-Engineering-Angriffs zu werden:** Diese Kategorie beschreibt, wie hoch die Wahrscheinlichkeit für ein Unternehmen ist, Opfer eines Social-Engineering-Angriffs zu werden.
- **Varianten von Security-Awareness-Schulungen:** Bei dieser Kategorie geht es darum, ob es verschiedene Varianten von Schulungen gibt, worin sich diese unterscheiden und welche Kosten die verschiedenen Systeme verursachen.
- **Kosten der technischen Maßnahmen gegen Social Engineering:** Diese Kategorie beschreibt, wie hoch die jährlichen Kosten für technische Maßnahmen sind, die einen Social-Engineering-Angriff erschweren sollen.

4.2.3 Expertinnen und Experten

Damit die Hypothesen im Rahmen dieser Arbeit überprüft werden können, muss in diesem Bereich auch eine qualitative Inhaltsanalyse erfolgen. Dies geschieht in Form von Experteninterviews. Es ist essentiell, hier Personen zu befragen, die ein umfassendes Knowhow auf diesem Gebiet haben.

> *„Der Experte definiert sich immer über das spezifische Forschungsinteresse und die soziale Repräsentativität des Experten gleichzeitig – der Experte ist ein Konstrukt des Forschers und der Gesellschaft“.* (Bogner et al., 2014)

Alle interviewten Personen sind Expertinnen und Experten im Bereich der Informationssicherheit. In ihrem beruflichen Umfeld haben sie mit Informationssicherheit und damit einhergehend auch mit Social Engineering zu tun. Die interviewten Personen haben mindestens sechs Jahre Berufserfahrung auf diesem Gebiet.

Diese Personen sind Expertinnen und Experten, da sie spezifische Kenntnisse im Bereich der Informationssicherheit haben und diese auch in ihrem beruflichen Feld einsetzen müssen. Ihre Tätigkeit erfordert es, dass sie immer über aktuelle Bedrohungen Bescheid wissen und gegebenenfalls schnell mit den richtigen Maßnahmen reagieren können.

Im Folgenden werden die Expertinnen und Experten kurz beschrieben. Alle von ihnen verlangten eine Anonymisierung, weswegen sie als Expert*in 1 usw. dargestellt werden.

Expert*in 1
Diese Person ist in einem großen Elektrizitätsversorgungsunternehmen als Chief Information Security Officer tätig. Diese Expertin oder dieser Experte ist für die komplette Informationssicherheit im Unternehmen verantwortlich. In diesen Zuständigkeitsbereich fallen Security-Schulungen, Datenklassifizierungen, Sicherheitsüberprüfungen etc.

Experte*in 2
Diese Person ist im Managed-Service-Provider-Bereich tätig. Sie oder Er ist auch Expertin oder Experte im Bereich der Informationssicherheit, weil bei einer kompletten Planung eines Konzeptes der Sicherheitsaspekt nicht außer Acht gelassen werden darf. Es müssen hier Maßnahmen entwickelt werden, die einerseits die technische Security erhöhen und anderseits Social-Engineering-Angriffe erschweren. Dieses Tätigkeitsfeld umfasst alle sieben Layer des ISO-OSI-Schichtenmodells.

Experte*in 3
Diese Person übt den Beruf einer Penetrationstesterin oder eines Penetrationstesters aus. Diese Tätigkeit erfordert eine Expertise in der Informationssicherheit, weil die Fachkraft versucht, in einzelne Systeme einzudringen.

Experte*in 4

Diese Person ist in einem großen Elektrizitätsversorgungsunternehmen als Operational-Technology-Security-Engineer tätig. Zu den Aufgaben gehört die Absicherung bedeutsamer Daten, die für die Stromerzeugung notwendig sind. Des Weiteren muss auch sichergestellt werden, dass kein unbefugter Zugriff auf diese Komponenten erfolgt, weswegen auch ein Zusammenhang mit Social Engineering besteht.

Expert*in 5

Diese Person ist in einem großen Unternehmen für die Informationssicherheit zuständig. Sie oder er evaluiert Sicherheitsmaßnahmen, die dem Unternehmen einen Mehrwert bringen sollen. Zudem entscheidet sie, welche Rechte die Userinnen und User bekommen sollen, zum Beispiel ob eine gewisse Gruppe Programme selbstständig installieren darf.

5 ERGEBNISSE

In diesem Kapitel werden die Ergebnisse der quantitativen und der qualitativen Methodik beschrieben. Im ersten Schritt wird die Umfrage ausgewertet, um die Hypothesen 3 und 4 zu überprüfen.

Im zweiten Teil dieses Kapitels werden die Daten aus den Experteninterviews analysiert. Im Anschluss werden die Ergebnisse genutzt, um die Hypothesen 1 und 2 dieser Arbeit zu bestätigen oder zu verwerfen.

5.1 Auswertung des Fragebogens

Es nahmen 198 Personen mit verschiedenen Merkmalen an der Umfrage teil. Das bedeutet, dass die Ergebnisse dieser Umfrage nicht nur auf eine gewisse Personengruppe zutreffen, sondern allgemein auf berufstätige Personen, die in ihrem Tätigkeitsbereich mit kritischen Informationen zu tun haben.

Von den 198 Fragebögen waren lediglich 153 vollständig ausgefüllt. Von den Teilnehmenden waren 146 aktuell berufstätig. Somit besteht die Stichprobe, die für diese Arbeit herangezogen wird, aus 146 Personen. Anderenfalls könnte die Auswertung verfälscht werden. Das Ganze kann mit einem Filter und einer Kreuzauswertung im Tool umfrageonline (https://www.umfrageonline.com/) gesetzt werden, infolgedessen eine manuelle Anpassung der Daten nicht mehr von Nöten ist.

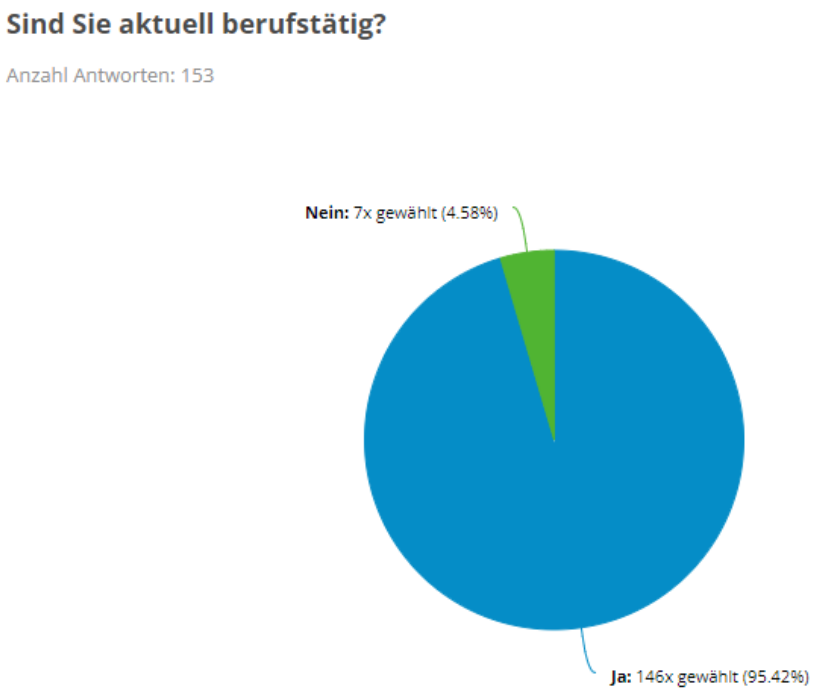

Abbildung 13: Auswertung der Berufstätigkeit

5.1.1 Einleitung

Der Bereich ‚Einleitung' zielt darauf ab, allgemeine Informationen über die Personen zu erheben, um diese in verschiedene Gruppen zu unterteilen. Damit soll herausgefunden werden, ob verschiedene Personengruppen ein unterschiedliches Empfinden der Informationssicherheit haben.

Die Untersuchung hat mit der Frage nach dem Alter begonnen. Hier ist ersichtlich, dass mehr als 50 % der teilnehmenden Personen zwischen 18 und 30 Jahre alt waren. Des Weiteren war das Alter von rund einem Drittel der Befragten zwischen 31 und 50 Jahren. Mit ca. 10 % ist der Anteil der Personen, die zwischen 51 und 65 Jahre alt waren, am geringsten. Diese Aufteilung ist dadurch entstanden, dass die Umfrage hauptsächlich via Social Media verteilt wurde und der Anteil an jüngeren Personen hier höher ist. (Turulski, 2021)

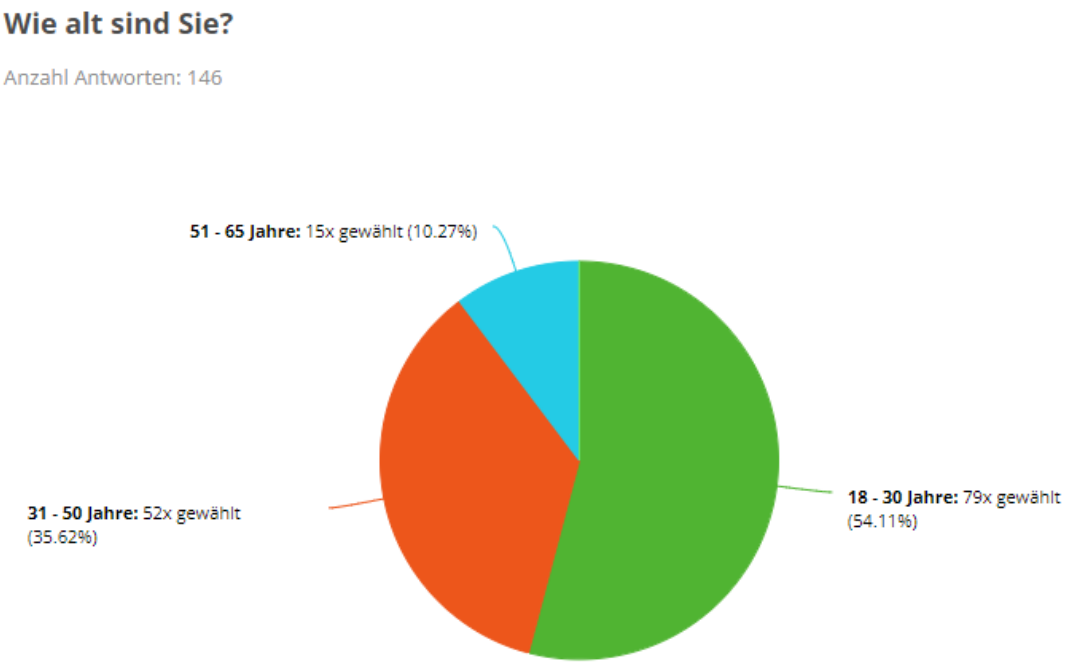

Abbildung 14: Alter der befragten Personen

Bei der Frage zur Unternehmensgröße ist ersichtlich, dass rund die Hälfte der Personen in einem großen Unternehmen mit über 1000 Angestellten beschäftigt war. Circa 15 % der Befragten waren in einem Unternehmen mit einer Größe von 11 bis 50, 51 bis 250 oder 250 bis 1000 Mitarbeiterinnen und Mitarbeitern angestellt. Lediglich elf Personen arbeiteten in einem kleinen Unternehmen mit maximal zehn Personen. Rund 1 % der Befragten war zum Zeitpunkt der Befragung aufgrund von Karenz, Papamonat etc. in keinem aktiven Verhältnis mit einem Unternehmen. Da eine anschließende Rückkehr geplant ist, sind diese Personen auch in der Stichprobe enthalten.

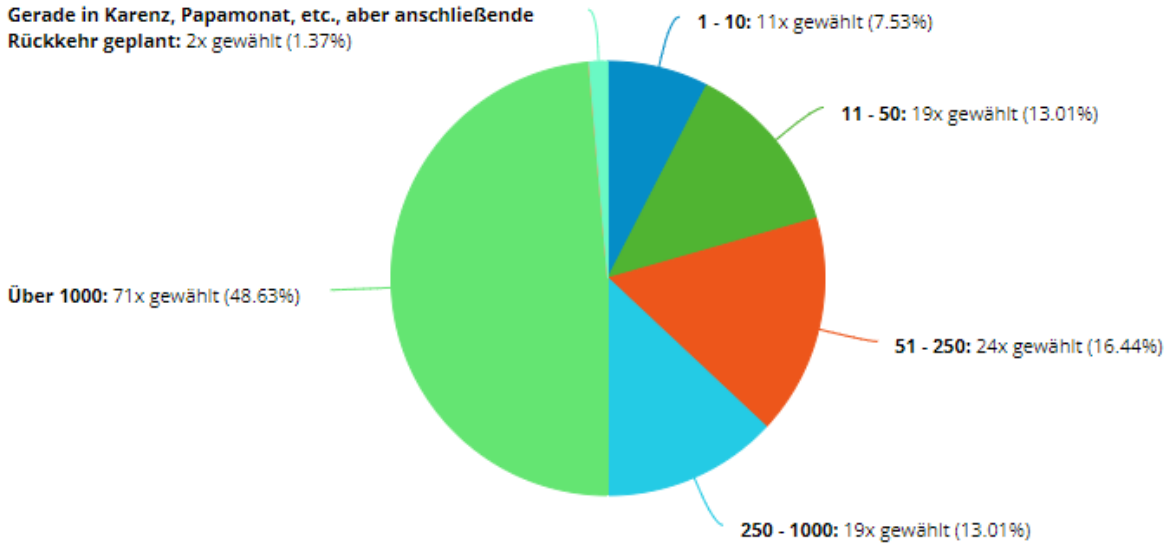

Abbildung 15: Aufteilung nach Unternehmensgröße

Die Frage, ob das Unternehmen als kritische Infrastruktur gekennzeichnet ist, bejahte rund die Hälfte der teilnehmenden Personen.

Antwort	Gewählt	Prozentsatz
ja	71	48,63 %
nein	75	51,37 %

Tabelle 2: Kritische Infrastruktur

Von den befragten Personen haben ca. 40 % eine Verantwortung für andere Personen bzw. sind eine Führungskraft. Mit dieser Frage sollte herausgefunden werden, ob eine höhere Verantwortung ein stärkeres Sicherheitsgefühl hervorruft.

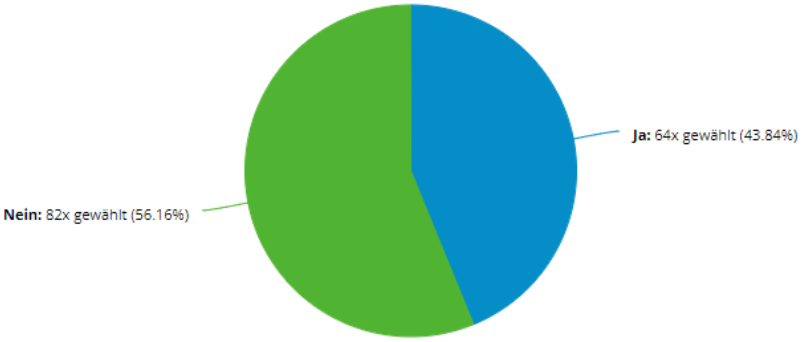

Abbildung 16: Verantwortung für andere Personen

In der nächsten Abbildung ist ersichtlich, dass rund 85 % der befragten Personen angaben, Zugriff auf sicherheitsrelevante Informationen zu haben. Mit dieser Frage sollte ermittelt werden, ob Personen, die in ihrem Berufsalltag mit sicherheitskritischen Daten konfrontiert sind, ein anderes Empfinden für Informationssicherheit haben.

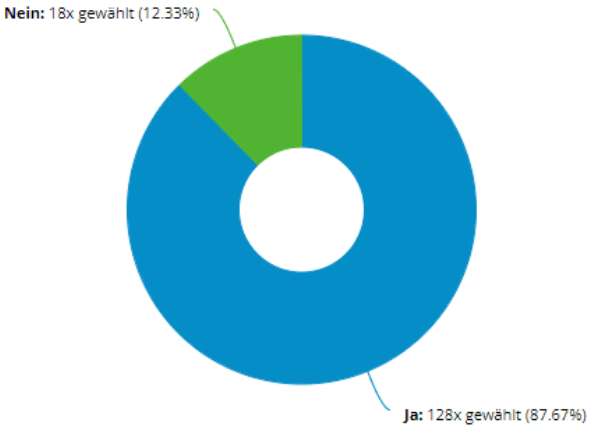

Abbildung 17: Sicherheitsrelevante Informationen

Anhand dieser Einstiegsfragen wurden verschiedene Personengruppen gebildet. In den nächsten Kapiteln soll überprüft werden, ob es zwischen diesen Personengruppen einen Unterschied bzgl. des Sicherheitsempfindens gibt. Im Folgenden wird die Aufteilung in diese Gruppen beschrieben.

- **Alter**
  Hier werden die Personen nach ihrem Alter kategorisiert, um zu sehen, ob sich das Sicherheitsempfinden mit zunehmendem Alter verändert. Dabei wurden folgende Gruppen festgelegt: 18–30-Jährige, 31–50-Jährige und 51–65-Jährige.
- **Größe des Unternehmens**
  Hier wird überprüft, ob sich das Sicherheitsempfinden der einzelnen Mitarbeiterinnen und Mitarbeiter je nach Größe des Unternehmens, in dem sie beschäftigt sind, unterscheidet. Dabei wurden folgende Unternehmensgrößen definiert: 1–10 Personen, 11–50 Personen, 51–250 Personen, 250–1000 Personen und über 1000 Personen.
- **Kritische Infrastruktur**
  Bei diesem Punkt wird danach unterteilt, ob Personen in einem Unternehmen kritischer Infrastruktur angestellt sind oder nicht. Aufgrund dieser Unterscheidung wird das Sicherheitsempfinden gemessen.
- **Verantwortung**
  Hier wird danach unterschieden, ob die Befragten Verantwortung für andere Personen haben oder nicht.
- **Sicherheitsrelevante Informationen**
  Bei diesem Punkt wird danach differenziert, ob die Befragten mit sicherheitsrelevanten Informationen arbeiten oder nicht.

5.1.2 Hypothese 3

In diesem Unterkapitel wird die folgende Hypothese überprüft: *„Mitarbeiterinnen und Mitarbeiter, die keine hohe IT-Affinität haben, kennen die Auswirkungen eines Social-Engineering-Angriffs und der daraus entstehenden Nebenwirkungen nicht.*

Mit der entsprechenden Frage sollen die Teilnehmenden in IT-Begeisterte und Nicht-IT-Begeisterte aufgeteilt werden. Dabei ist ersichtlich, dass sich rund 75 % als IT-begeistert einstufen. Diese Frage wurde jedoch mit der Selbsteinschätzung des IT-Knowhows verbunden, wodurch ersichtlich ist, dass nur rund 30 % eine hohe IT-Affinität aufweisen. Ca. 40 % schätzten ihre Kenntnisse als mittelmäßig ein und ca. 25 % gaben an, keine IT-Affinität zu haben. Dabei gilt es zu beachten, dass es sich um eine Selbsteinschätzung der jeweiligen Person handelt und nicht geprüft wurde, ob die angegebenen Kenntnisse in der Realität vorhanden sind.

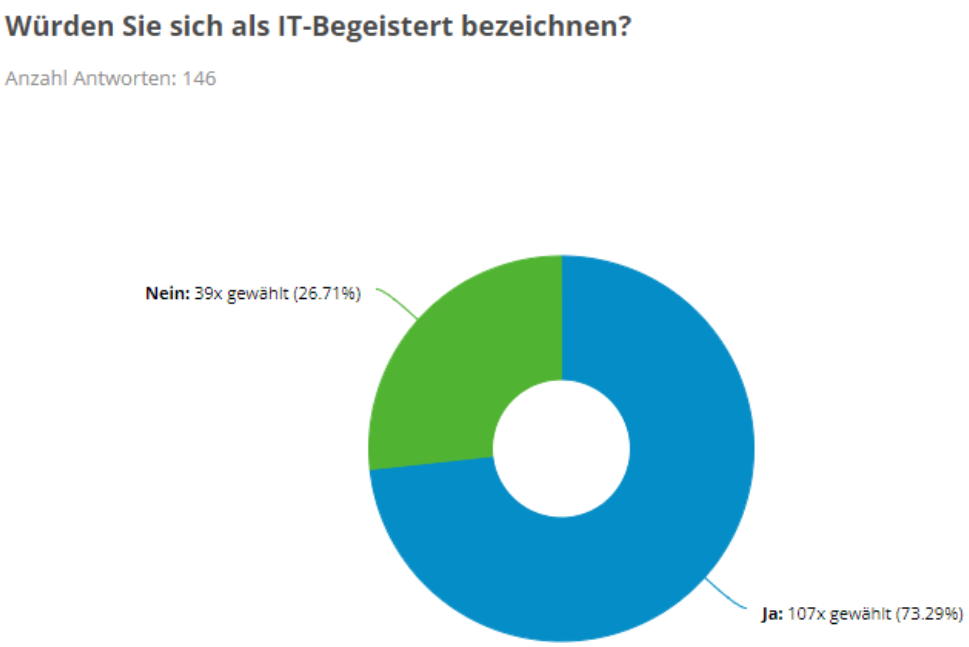

Abbildung 18: Selbsteinschätzung der IT-Begeisterung

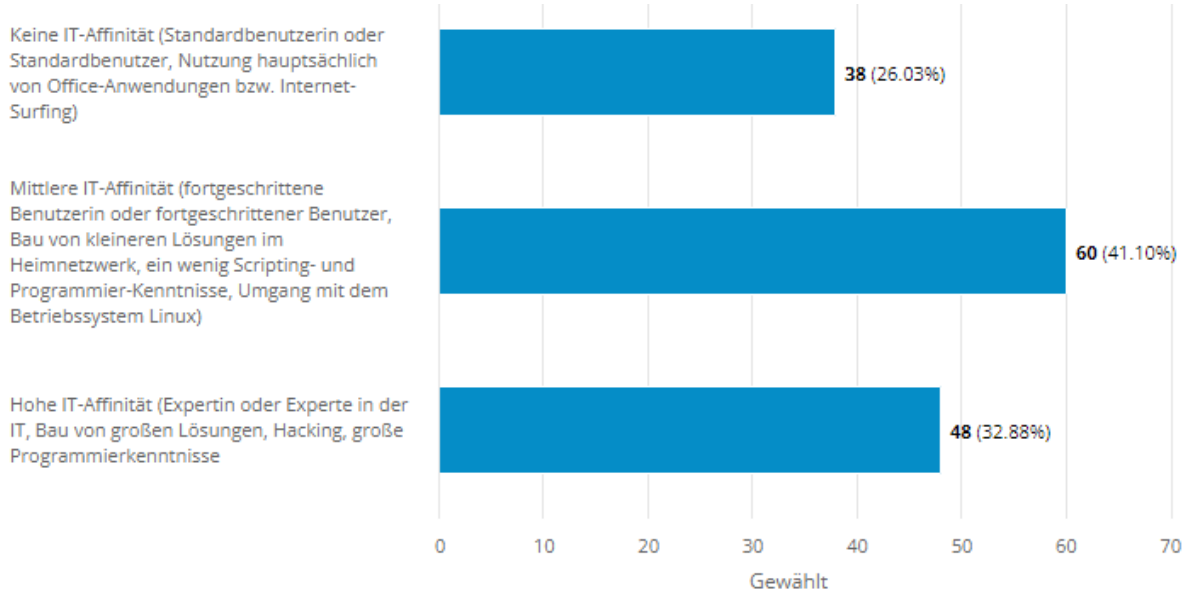

Abbildung 19: IT-Kenntnisse

Die folgende Abbildung gibt einen Überblick darüber, wie die einzelnen Personen ihre IT-Kenntnisse erlernten. Bei den meisten erfolgte dies durch ein Selbststudium aus eigenem Interesse. Dahinter folgt das Erlernen im Rahmen der Ausbildung und Schulungen. Hier ist ersichtlich, dass beide Formen oft miteinander einhergehen. Wenn sich eine Person für IT interessiert, dann wählt sie meistens auch eine Ausbildung in diesem Bereich. Hier gilt es wieder zu erwähnen, dass es sich um eine reine Selbsteinschätzung handelt und nicht überprüft wurde, welche Ausbildung absolviert wurde oder welche Schulungen besucht wurden. Die Antworten geben aber einen guten Überblick darüber, dass viele Personen glauben, IT-Kenntnisse zu haben.

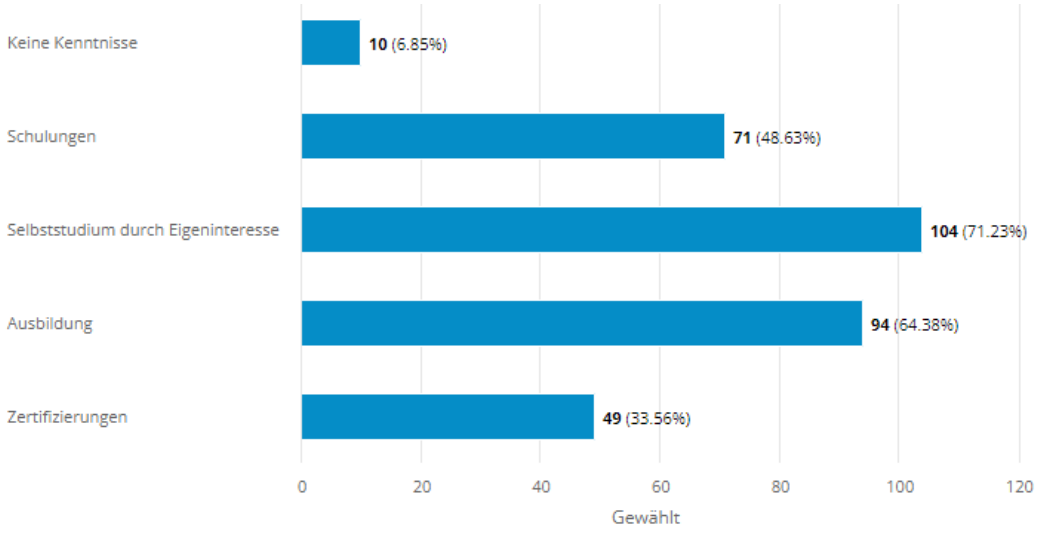

Abbildung 20: Erlernen der IT-Kenntnisse

Zur Überprüfung der Hypothese wurde anhand der vorher genannten Fragen noch zusätzlich die Personengruppe der IT-Expertinnen und IT-Experten erstellt.

- **IT-Expertinnen und IT-Experten**

  Es wurde gefragt, wie die Personen ihre IT-Affinität einschätzen würden. Für die weitere Analyse werden die Personen ohne IT-Affinität und die Personen mit einer mittleren IT-Affinität zu den Nicht-IT-Expertinnen bzw. Nicht-IT-Experten gezählt, während die Personen mit einer hoher IT-Affinität als IT-Expertinnen und IT-Experten gelten.

Bei der folgenden Frage geht es um das Abwägen zwischen Sicherheit und Effizienz. Es ist zu sehen, dass es keinen großen Unterschied zwischen den einzelnen Personengruppen, die aus dem ersten Bereich der Umfrage generiert wurden, gibt. Die Ergebnisse können in den folgenden Abbildungen gesehen werden. Die Verteilung ist ähnlich und es gibt keinen signifikanten Unterschied.

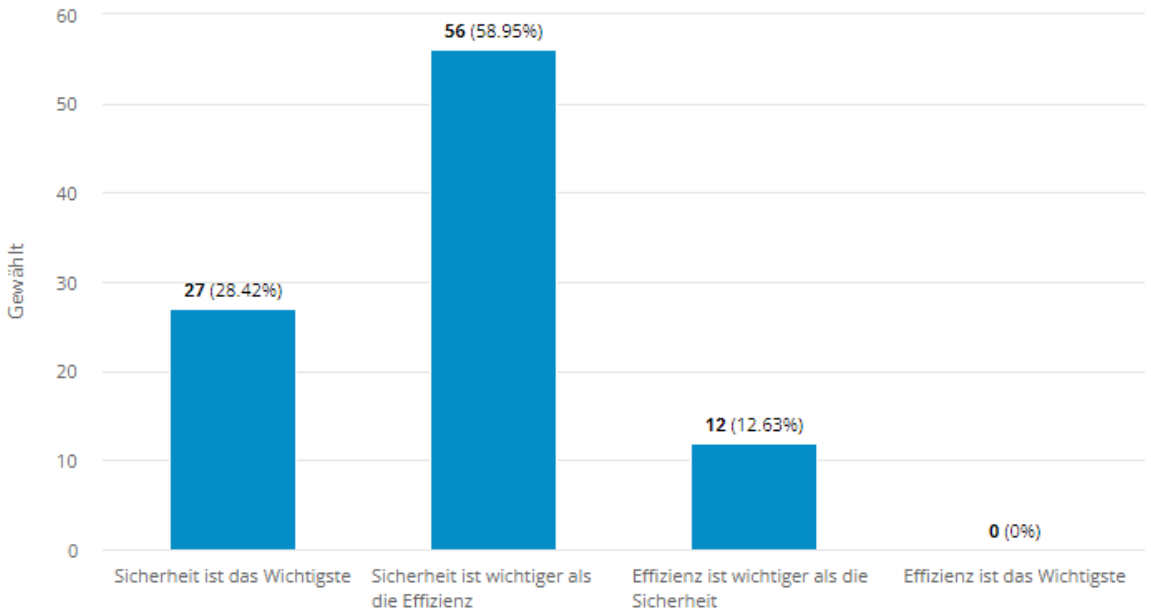

Abbildung 21: Bezug zwischen Sicherheit und Effizienz bei den 18- bis 30-Jährigen

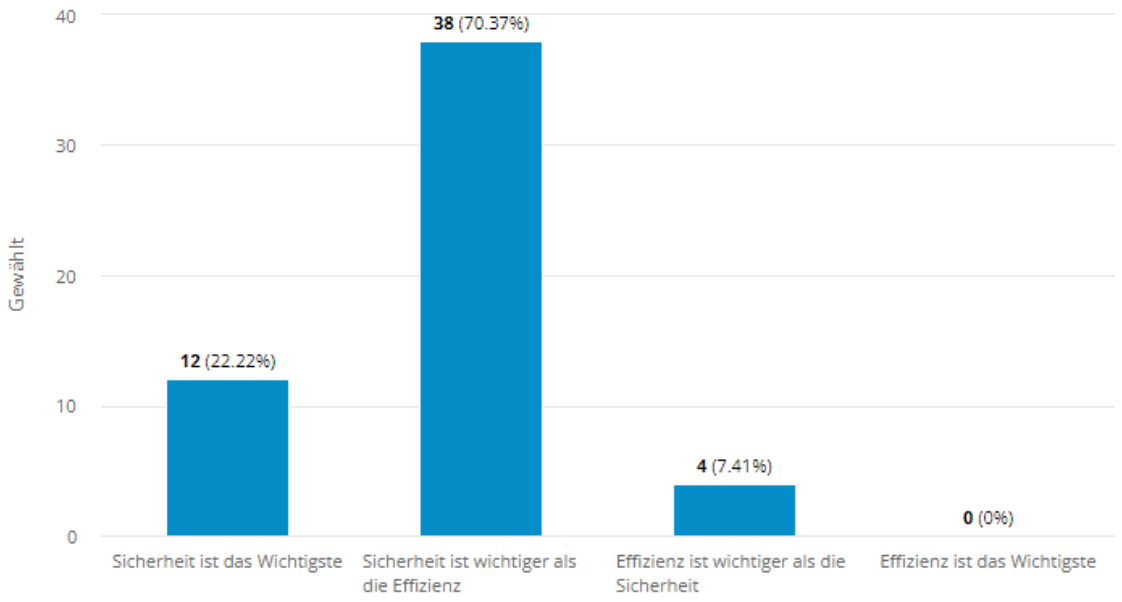

Abbildung 22: Bezug zwischen Sicherheit und Effizienz bei den 31- bis 50-Jährigen

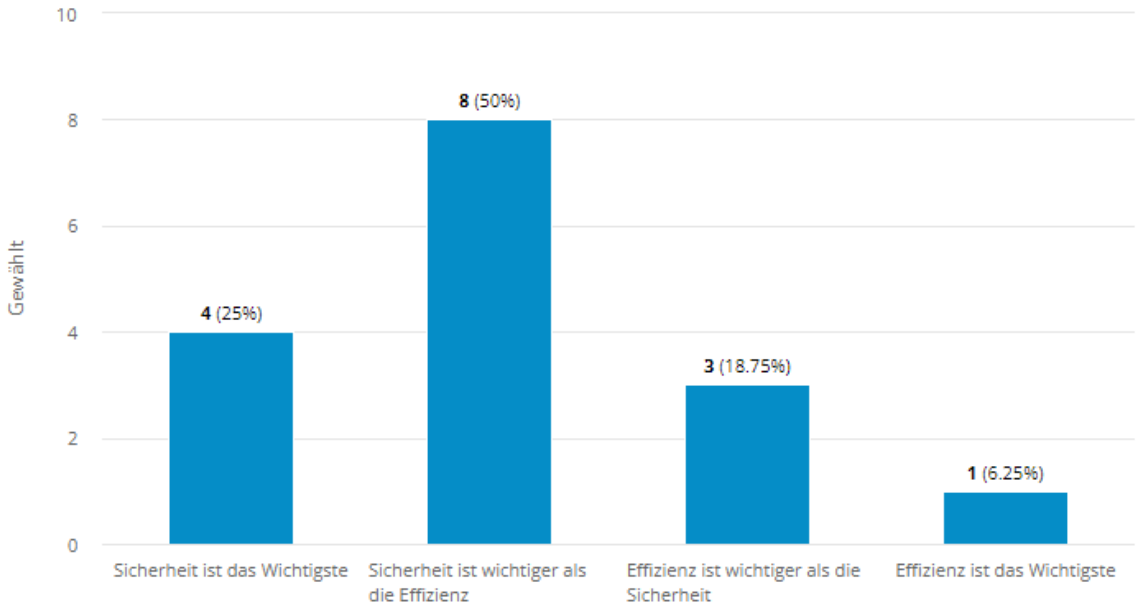

Abbildung 23: Bezug zwischen Sicherheit und Effizienz bei den 51- bis 65-Jährigen

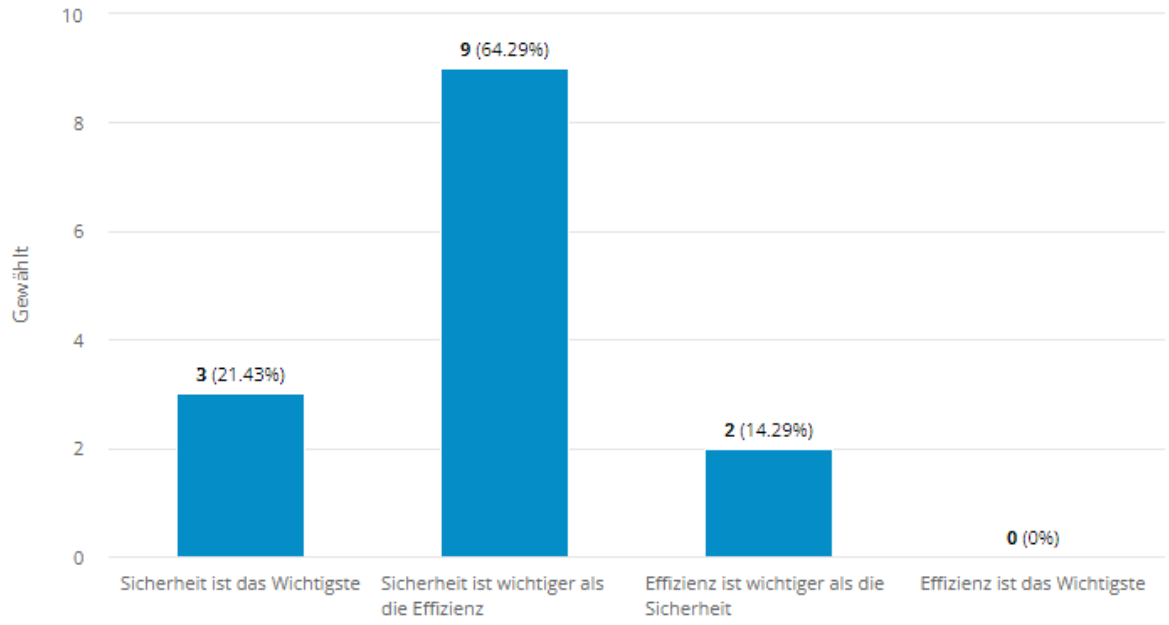

Abbildung 24: Bezug zwischen Sicherheit und Effizienz von 1 - 10 Personen Unternehmen

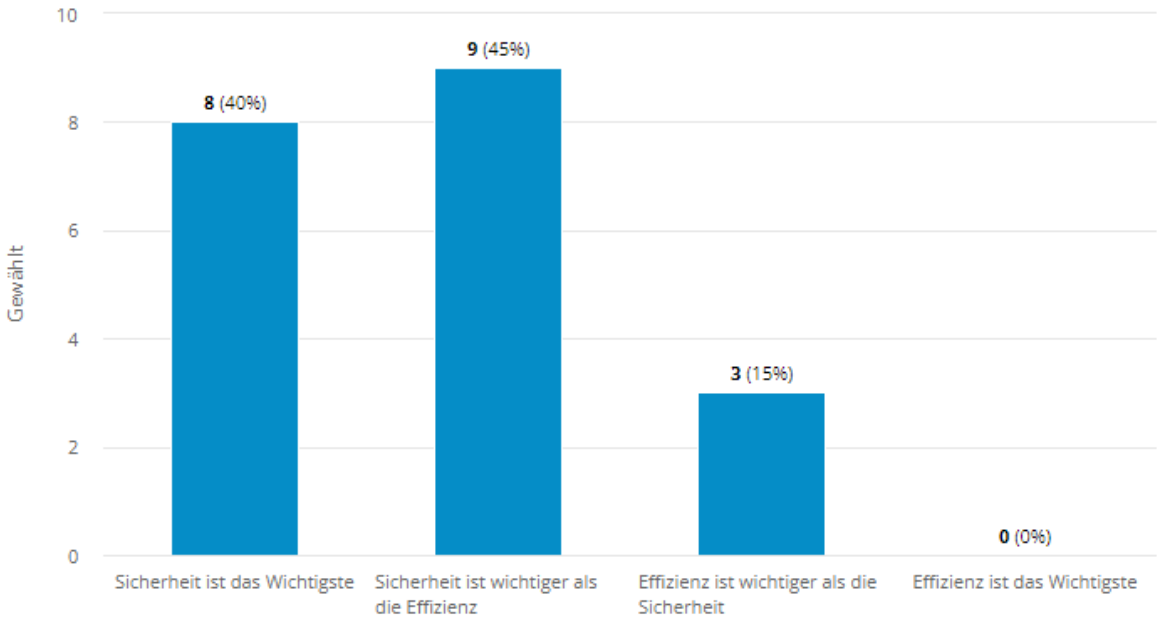

Abbildung 25: Bezug zwischen Sicherheit und Effizienz von 11 - 50 Personen Unternehmen

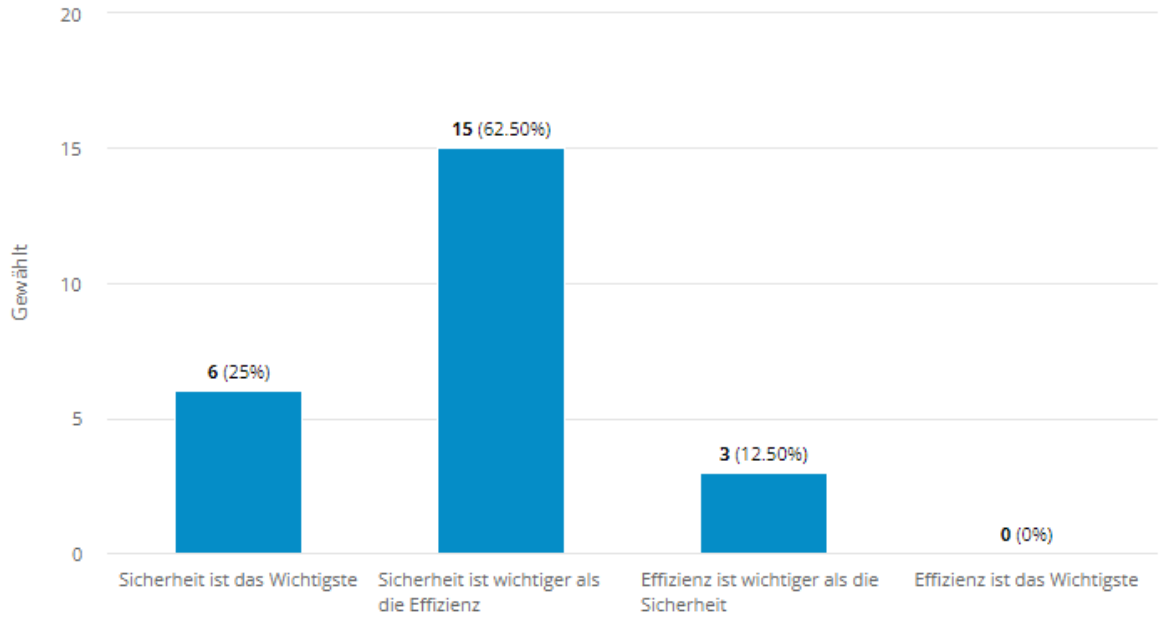

Abbildung 26: Bezug zwischen Sicherheit und Effizienz von 51 - 250-Personen Unternehmen

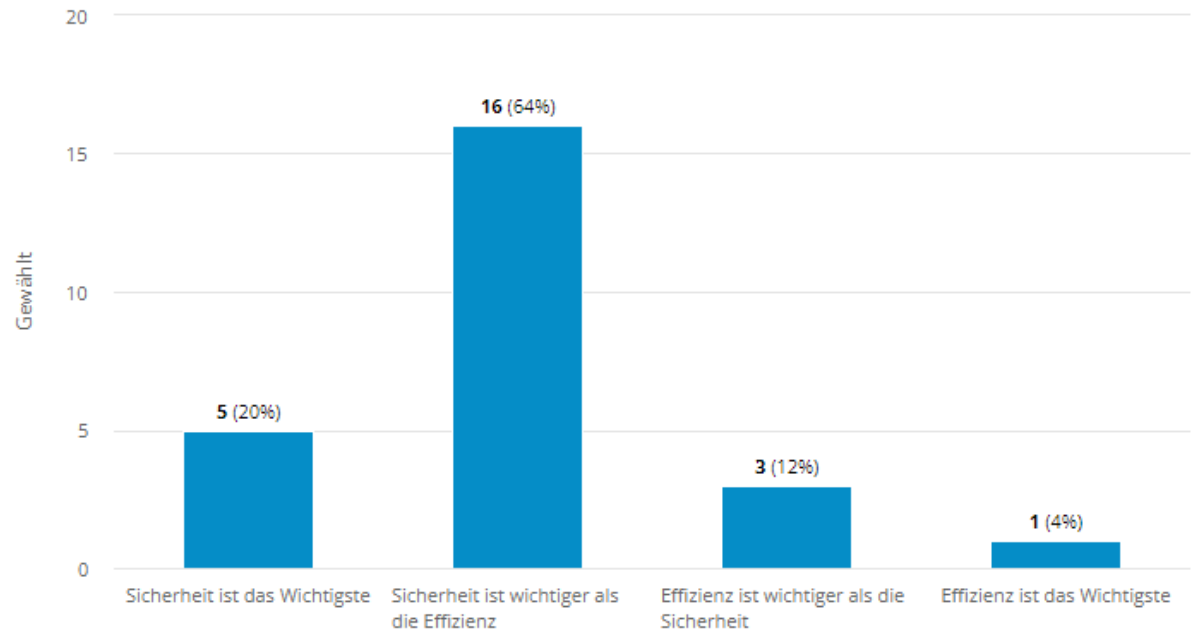

Abbildung 27: Bezug zwischen Sicherheit und Effizienz von 251 - 1000-Personen Unternehmen

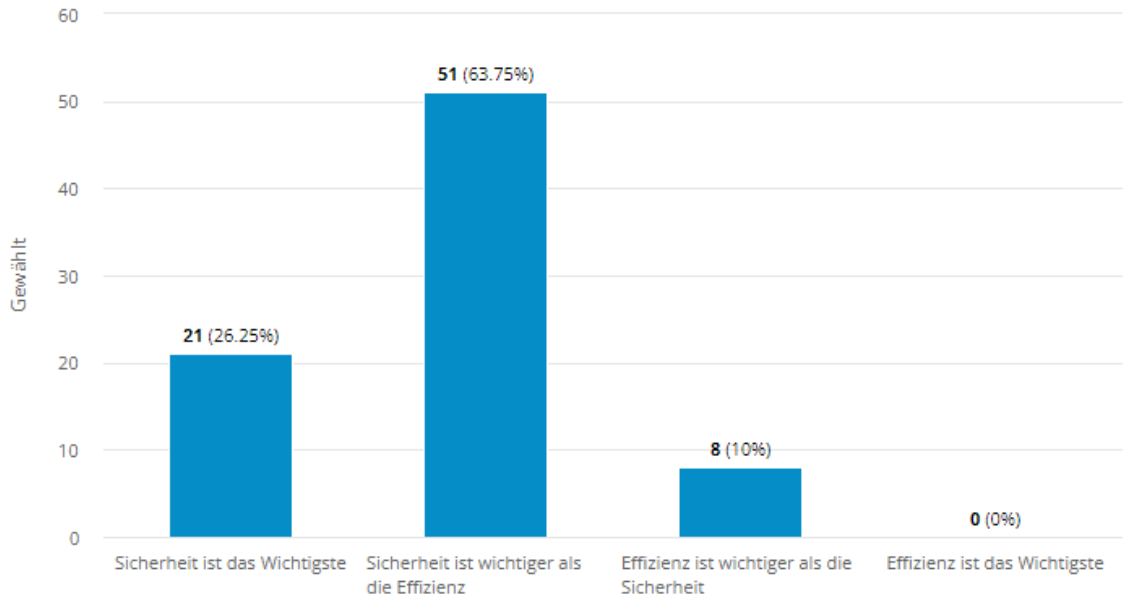

Abbildung 28: Bezug zwischen Sicherheit und Effizienz von über 1000-Personen Unternehmen

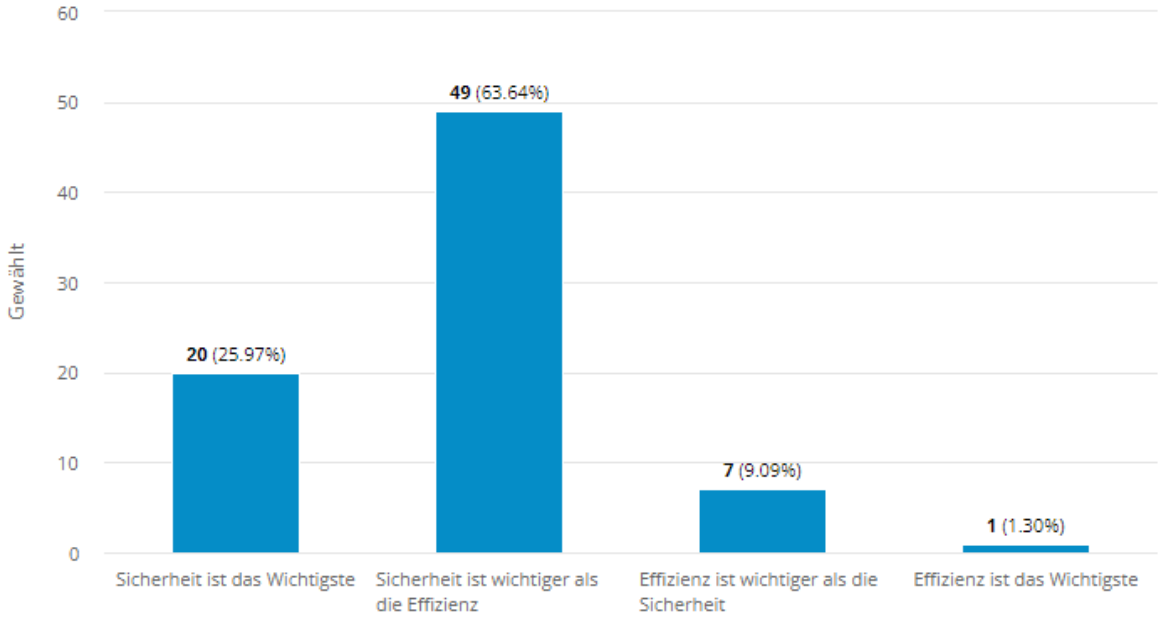

Abbildung 29: Bezug zwischen Sicherheit und Effizienz bei Angestellten eines Unternehmens kritischer Infrastruktur

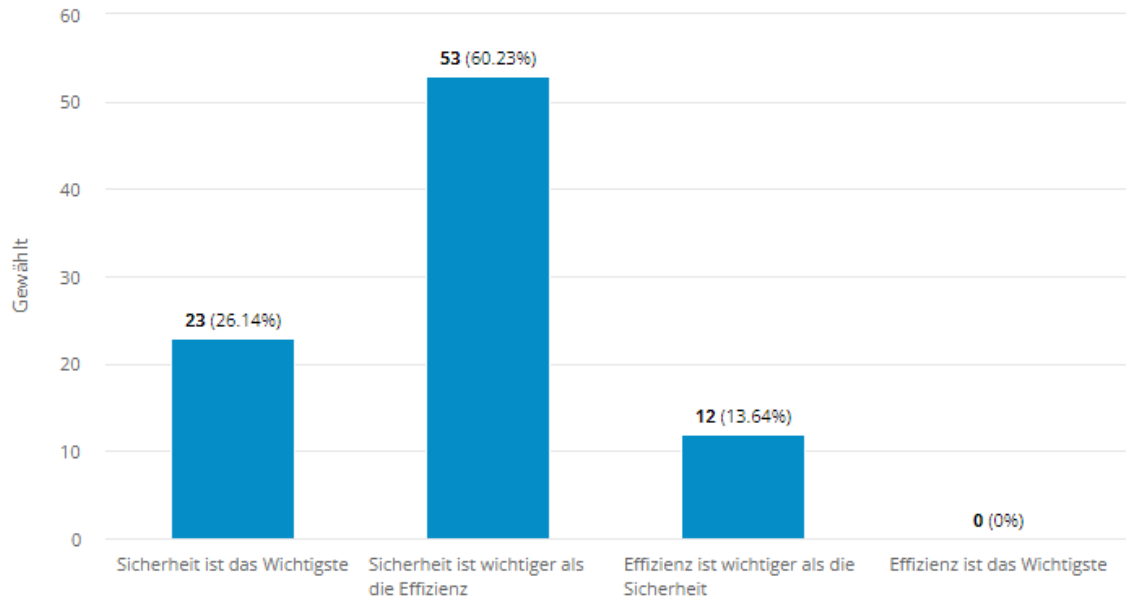

Abbildung 30: Bezug zwischen Sicherheit und Effizienz bei Angestellten eines Unternehmens nicht kritischer Infrastruktur

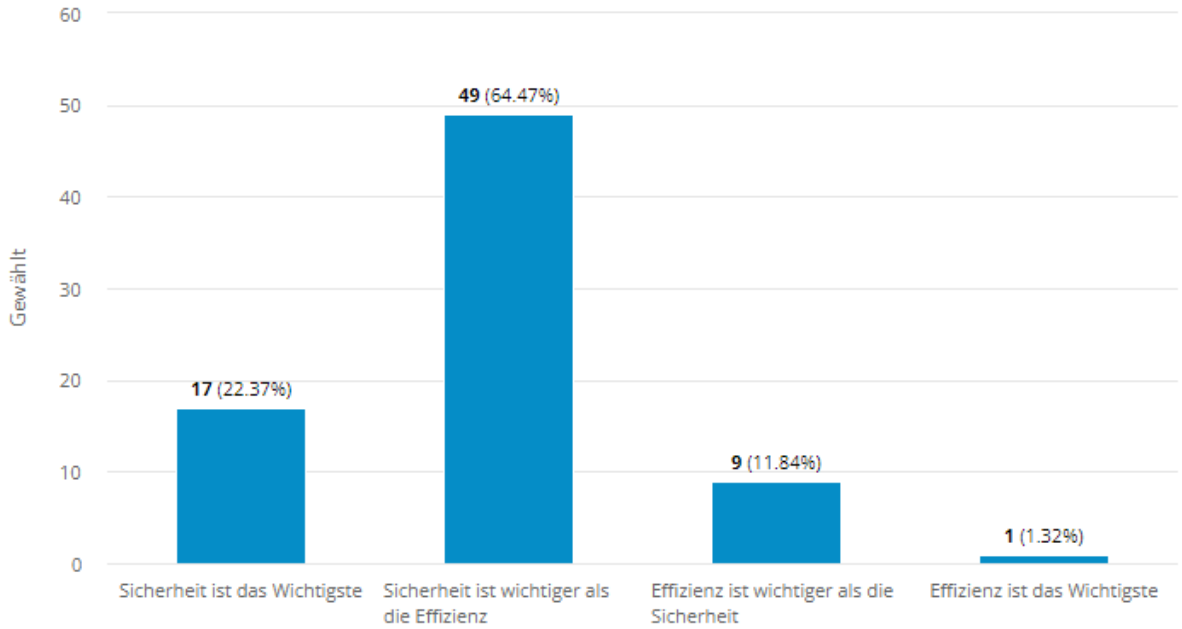

Abbildung 31: Bezug zwischen Sicherheit und Effizienz bei Führungskräften

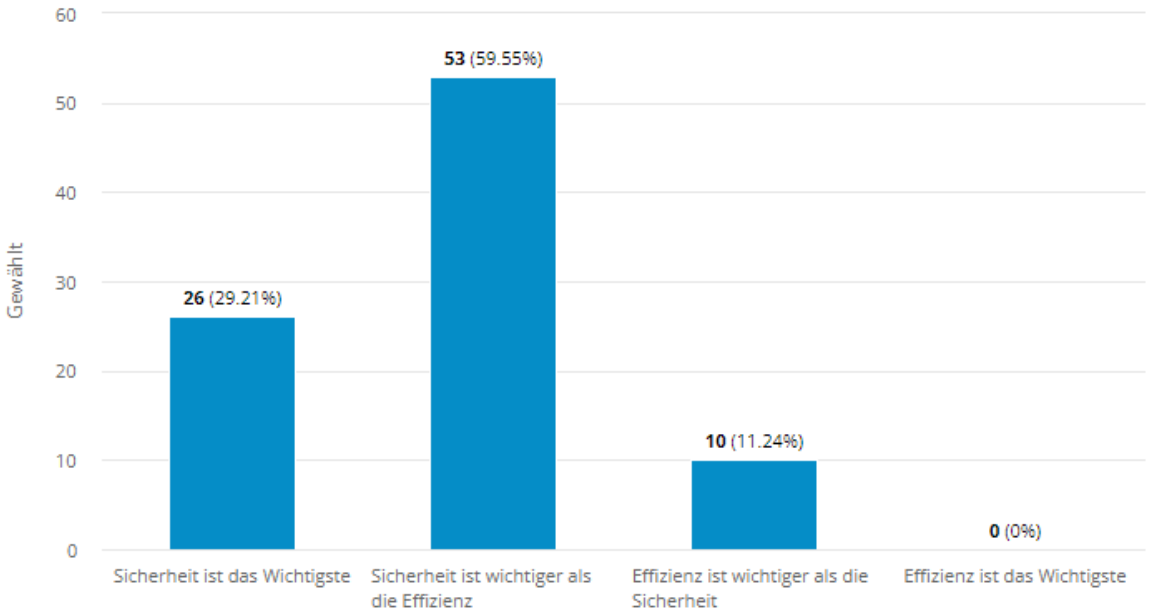

Abbildung 32: Bezug zwischen Sicherheit und Effizienz bei Nichtführungskräften

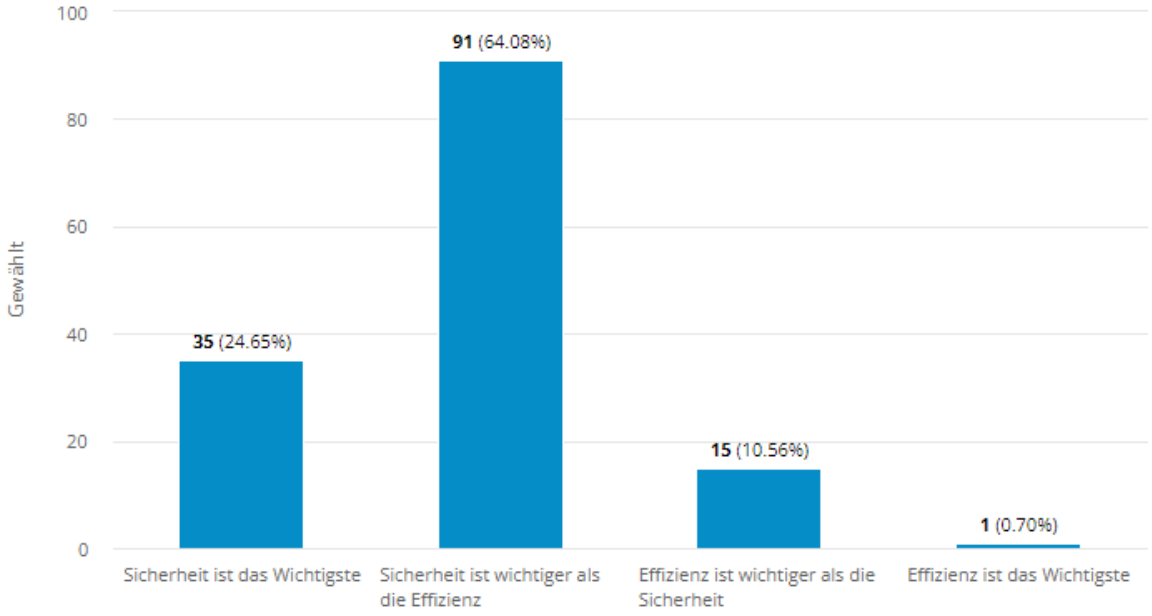

Abbildung 33: Bezug zwischen Sicherheit und Effizienz bei Personen mit Kontakt mit sicherheitskritischen Informationen

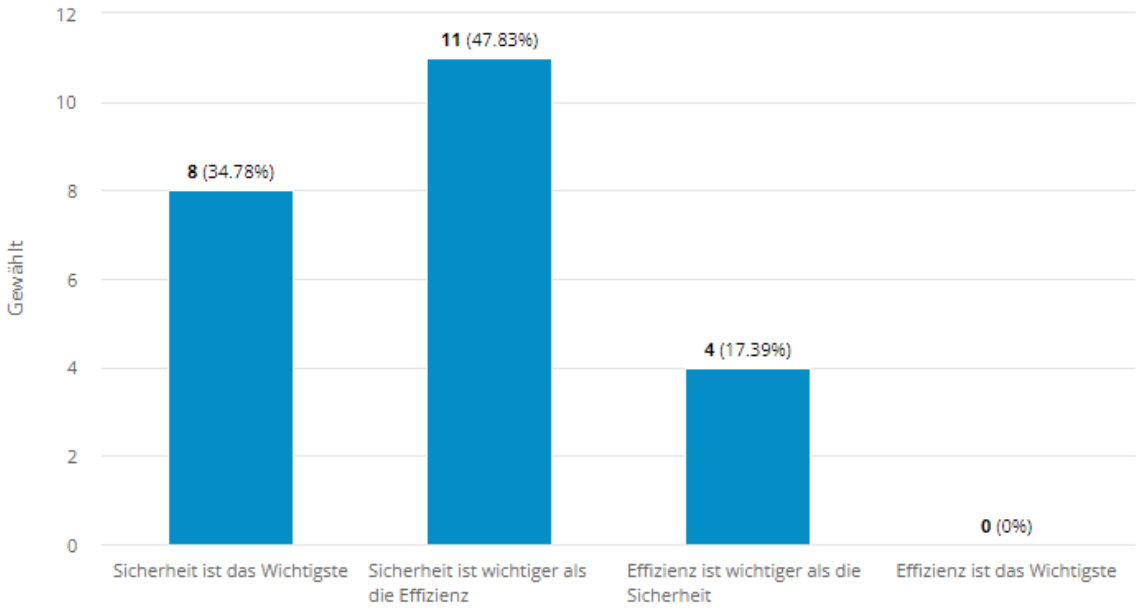

Abbildung 34: Bezug zwischen Sicherheit und Effizienz bei Personen ohne Kontakt mit sicherheitskritischen Informationen

Werden die Gruppen der vorher definierten IT-Experten und der Nicht-IT-Experten betrachtet, ist auch kein signifikanter Unterschied zu erkennen. Die Ergebnisse sind in den folgenden Abbildungen ersichtlich.

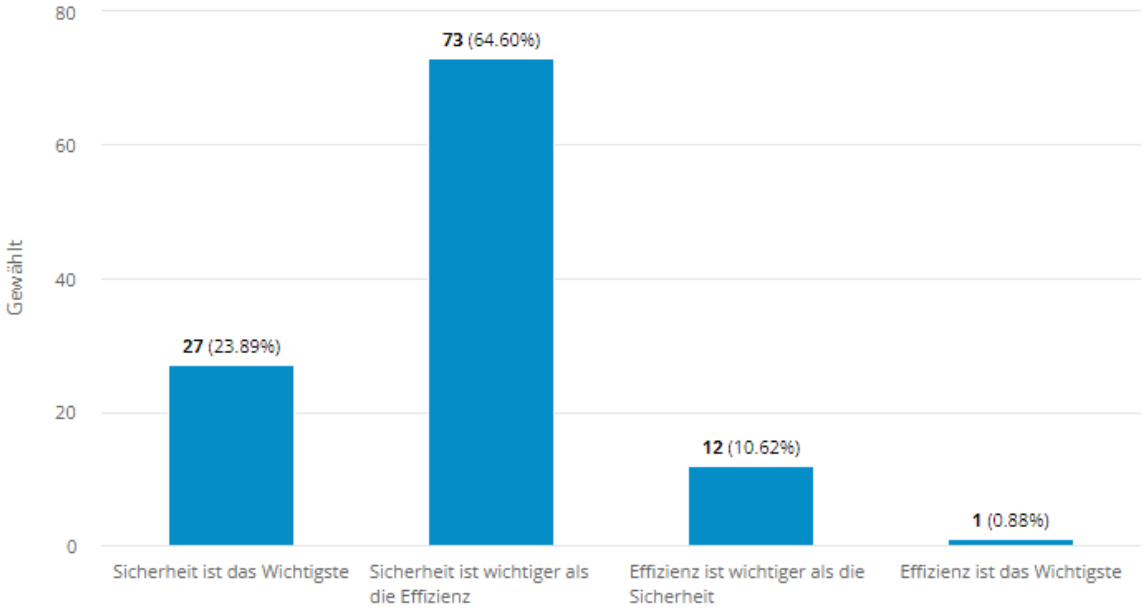

Abbildung 35: Bezug zwischen Sicherheit und Effizienz bei Nicht-IT-Experten

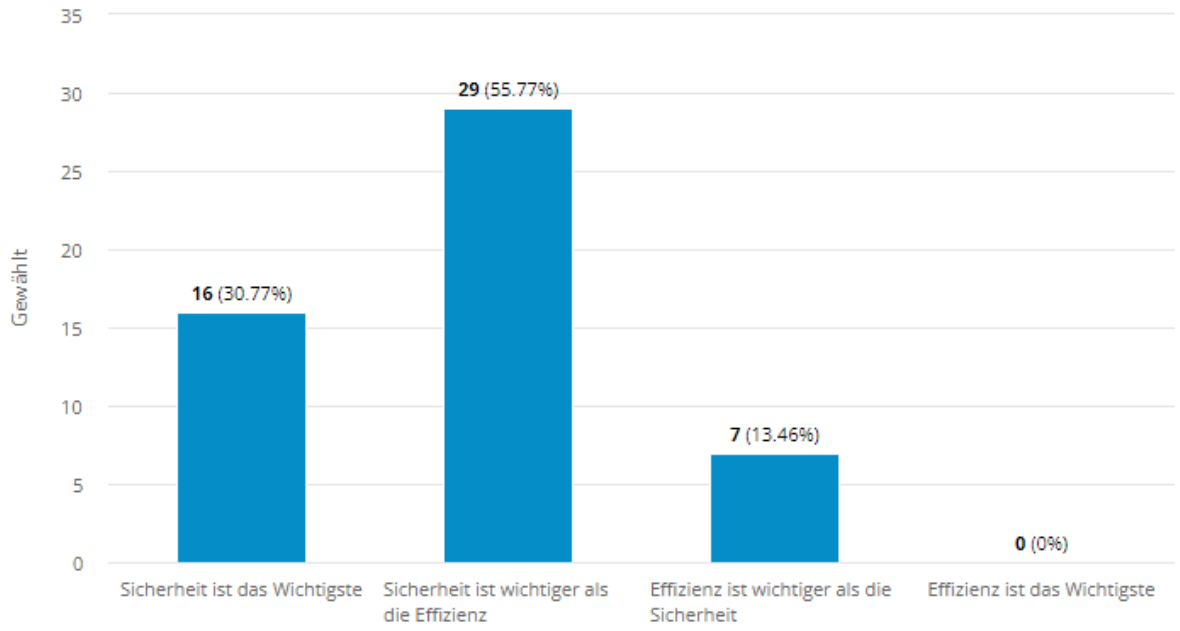

Abbildung 36: Bezug zwischen Sicherheit und Effizienz bei IT-Experten

Zusammengefasst kann gesagt werden, dass der Großteil – unabhängig von der Personengruppe – findet, dass der Sicherheit gegenüber der Effizienz der Vorzug gegeben werden muss. Es gibt keinen Unterschied zwischen den einzelnen Personengruppen. Zwischen 25 und 35 % und somit der zweitgrößte Teil der befragten Personen gaben – ebenfalls unabhängig von der Personengruppe – an, dass die Sicherheit das Wichtigste sei. Es kann hier festgestellt werden, dass die meisten Personen, die in ihrer beruflichen Tätigkeit mit einem Computer oder einem Informationssystem zu tun haben, unabhängig vom IT-Knowhow ein Empfinden für IT-Security haben.

Für die weitere Überprüfung der Hypothese 3 wurde in der Umfrage erhoben, ob die befragten Personen Kenntnisse haben, welche Nebenwirkungen ein Social-Engineering-Angriff hervorrufen kann. In den folgenden Abbildungen ist zu sehen, inwieweit den verschiedenen Altersgruppen die Auswirkungen von Social-Engineering-Angriffen bekannt sind.

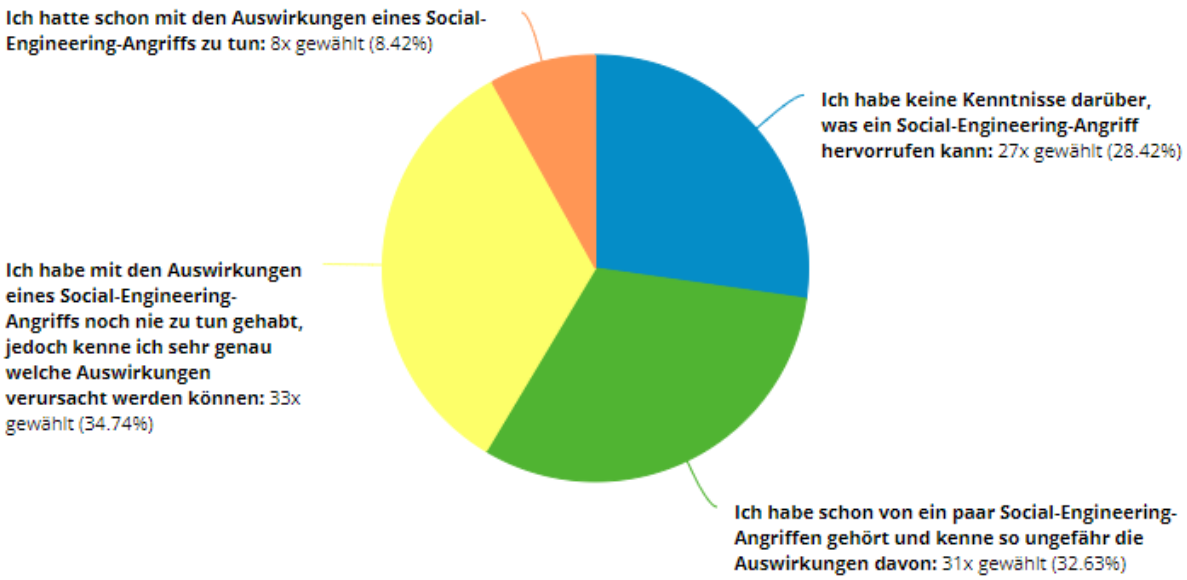

Abbildung 37: Auswirkungen von Social-Engineering-Angriffen (18- bis 30-Jährige)

Abbildung 38: Auswirkungen von Social-Engineering-Angriffen (31- bis 50-Jährige)

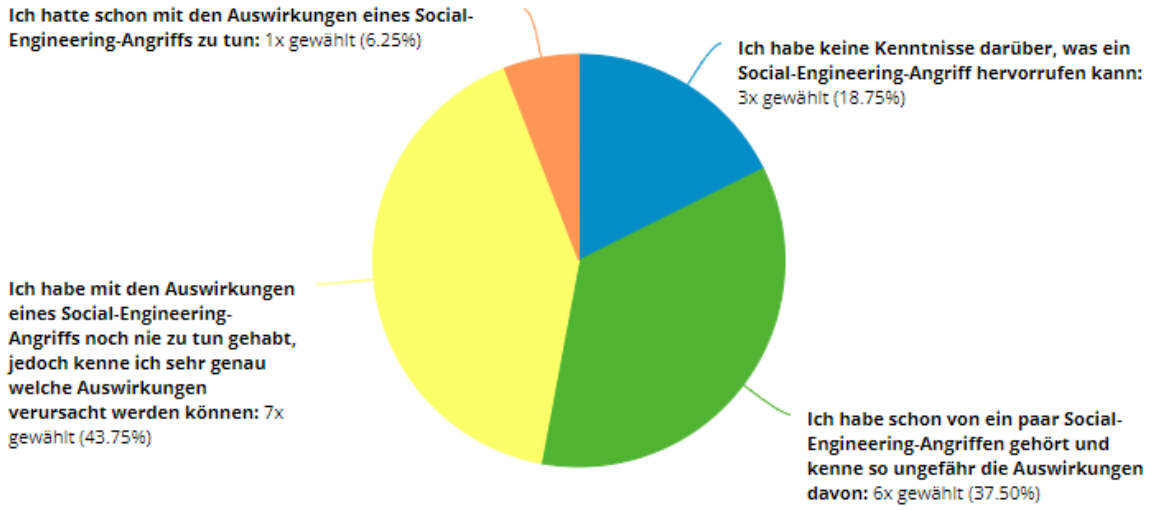

Abbildung 39: Auswirkungen von Social-Engineering-Angriffen (51- bis 65-Jährige)

Werden die verschiedenen Altersgruppen betrachtet, ist ersichtlich, dass es die 31- bis 50-jährigen Personen am häufigsten mit einem Social-Engineering-Angriff zu tun hatten. Ca. 20 % der Befragten in dieser Alterskategorie hatten bereits mit den Auswirkungen eines solchen Vorfalls zu tun. Die Stichprobe dieser Alterskategorie umfasst 52 Antworten, infolgedessen gesagt werden kann, dass das Ergebnis hier nicht durch eine geringe Anzahl verfälscht worden ist. Im Vergleich dazu gab es von den 18- bis 30-Jährigen 79 Antworten.

Bei den verschiedenen Unternehmensgrößen ist ersichtlich, dass die Mitarbeiterinnen und Mitarbeiter umso weniger mit den Nebenwirkungen eines Social-Engineering-Angriffs zu tun haben, je größer das Unternehmen ist.

Sie wissen laut eigener Angabe aber genau Bescheid, welchen Schaden ein solcher Angriff verursachen kann. Zwischen 20 und 35 % der befragten Personen, unabhängig von der Unternehmensgröße, haben keine Kenntnisse darüber, welche Auswirkungen ein Social-Engineering-Angriff hervorrufen kann. Bei den Personen, die in einem Unternehmen mit 51–250 Beschäftigten arbeiten, liegt dieser Wert bei 8 %. Das kann aber auch darin begründet sein, dass lediglich 24 Personen angegeben haben, in einem Unternehmen dieser Größe zu arbeiten. Zusammengefasst kann gesagt werden, dass rund zwei Drittel zumindest eine Vorstellung haben, welche Auswirkungen ein Angriff hervorrufen kann und diese zwei Drittel ändern sich im Verhältnis zwischen einer ungefähren Vorstellung eines Angriffs und einer genauen Expertise was ein durchgeführter Angriff hervorrufen kann, je nach Größe des Unternehmens. Je größer das Unternehmen ist, desto mehr Personen wissen genau Bescheid.

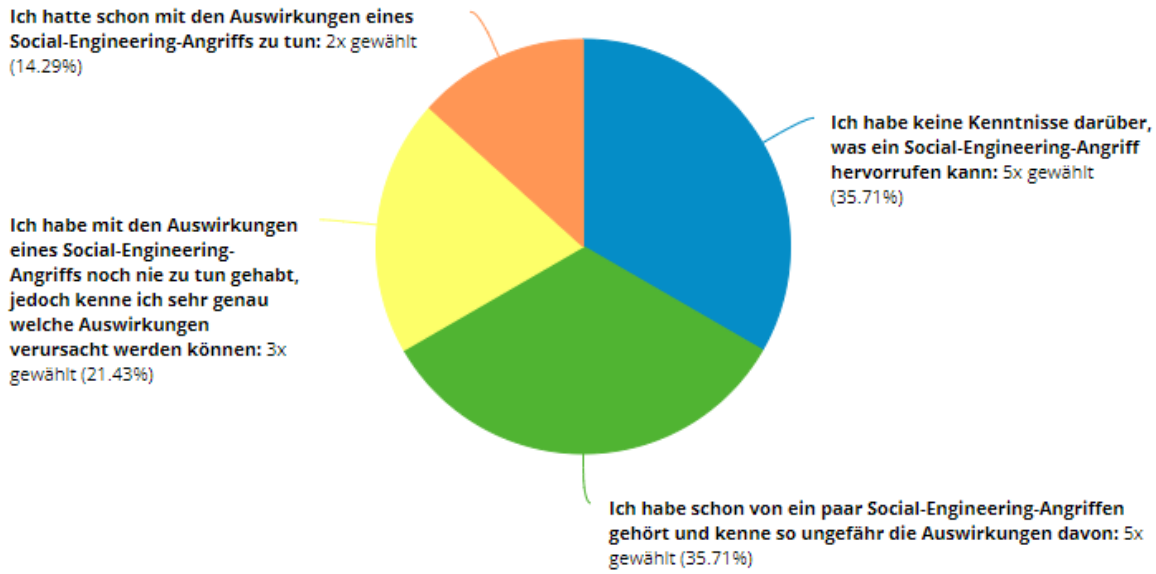

Abbildung 40: Auswirkungen von Social-Engineering-Angriffen von Personen die in einem 1 - 10-Personen Unternehmen angestellt sind

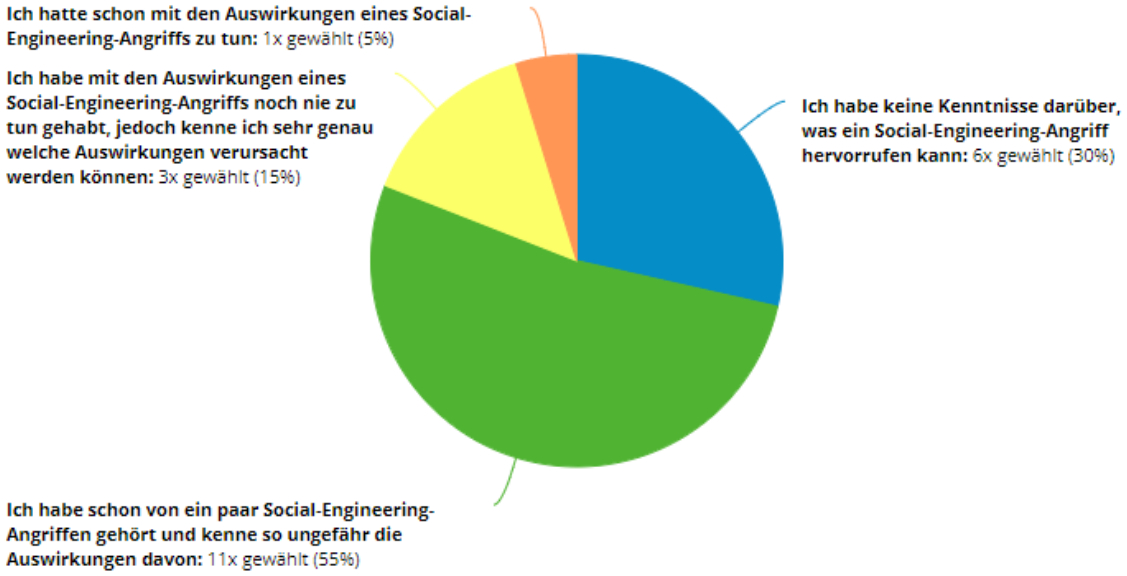

Abbildung 41: Auswirkungen von Social-Engineering- Angriffen von Personen die in einem 11 – 50-Personen Unternehmen angestellt sind

Abbildung 42: Auswirkungen von Social-Engineering-Angriffen von Personen die in einem 51 - 250-Personen Unternehmen angestellt sind

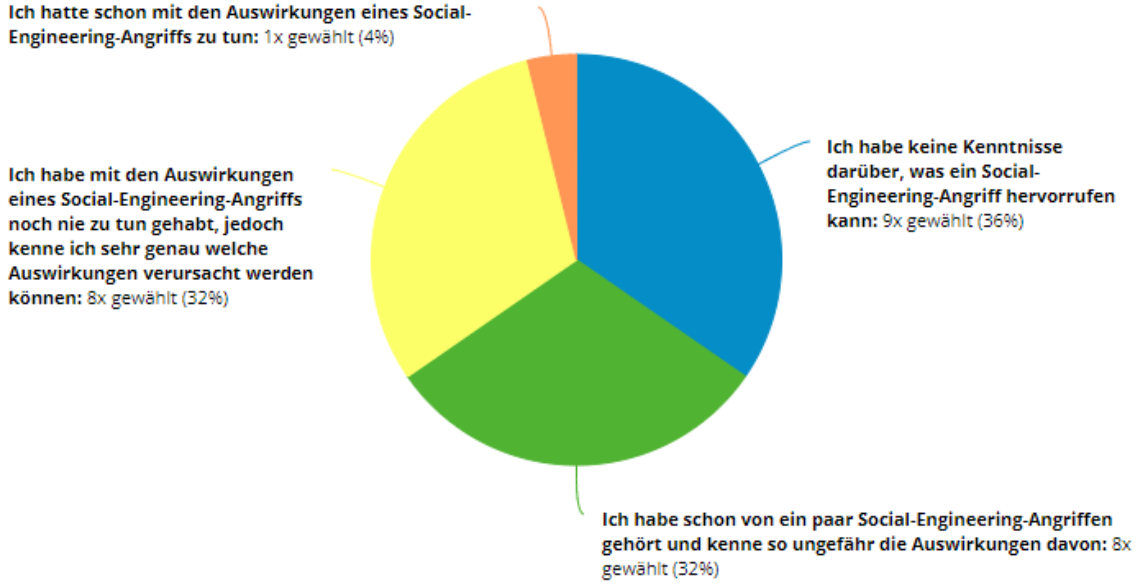

Abbildung 43: Auswirkungen von Social-Engineering-Angriffen von Personen die in einem 251 - 1000-Personen Unternehmen angestellt sind

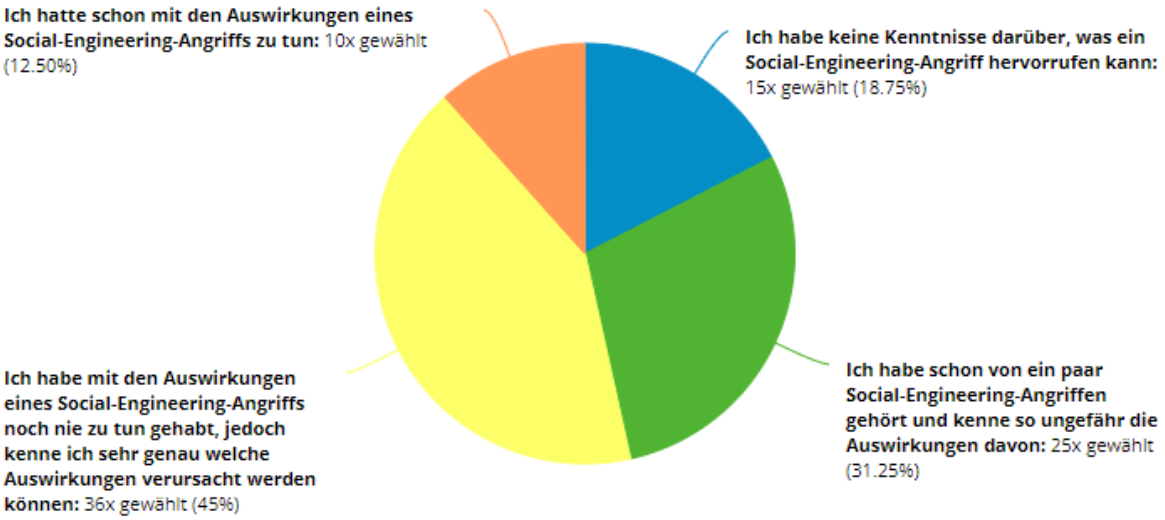

Abbildung 44: Auswirkungen von Social-Engineering-Angriffen von Personen die in einem über 1000-Personen Unternehmen angestellt sind

Ob die Personen in einem Unternehmen kritischer Infrastruktur angestellt sind oder nicht, spielt für die Kenntnisse im Bereich des Social Engineerings keine Rolle. Die Verteilung der einzelnen Stufen, welche Kenntnisse die Person im Bereich des Social Engineerings hat bzw. ob sie schon einmal mit den Auswirkungen konfrontiert war, unterscheidet sich nicht signifikant. Es kann gesagt werden, dass es irrelevant ist, in welcher Art von Unternehmen jemand angestellt ist. Die Resultate können den folgenden Abbildungen entnommen werden.

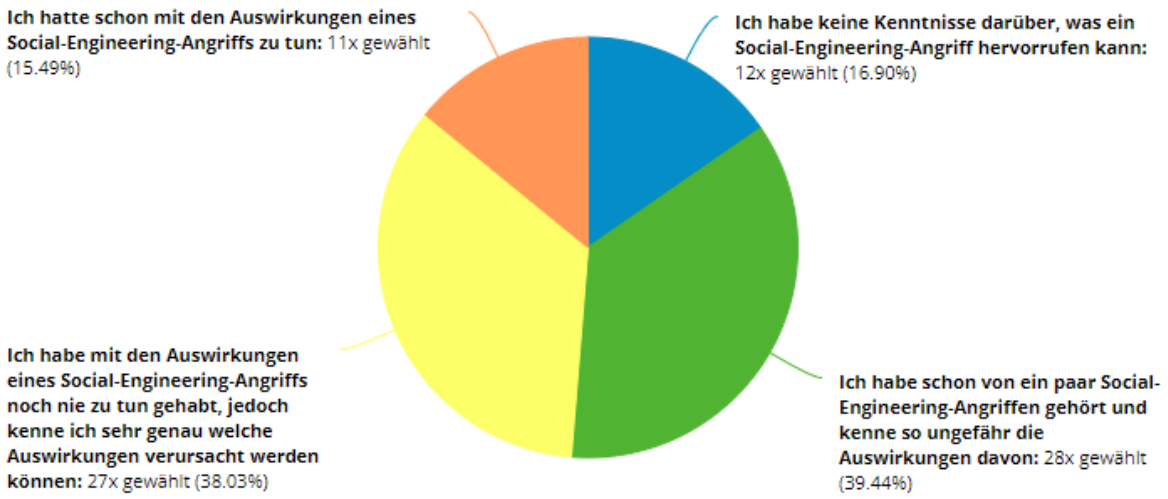

Abbildung 45: Auswirkungen von Social-Engineering-Angriffen bei Angestellten eines Unternehmens kritischer Infrastruktur

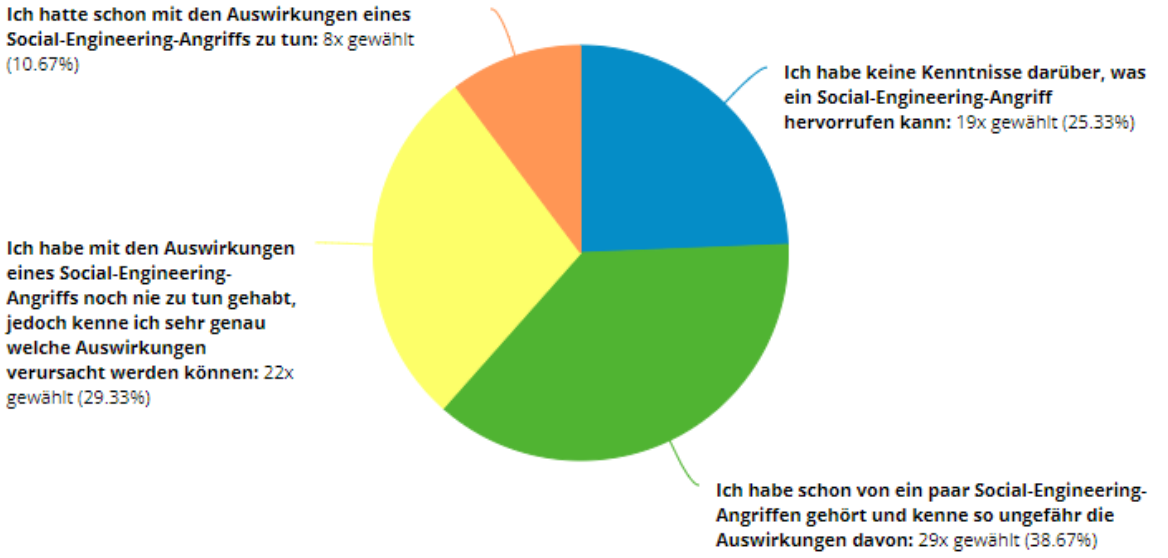

Abbildung 46: Auswirkungen von Social-Engineering-Angriffen bei Angestellten eines Unternehmens nicht kritischer Infrastruktur

In den folgenden Abbildungen ist ersichtlich, dass es keinen Unterschied der Kenntnisse im Bereich des Social Engineerings bzw. der Zuständigkeit mit den Maßnahmen, die eingeleitet werden müssen, wenn es einen Social-Engineering-Angriff gegeben hat, gibt.

Abbildung 47: Auswirkungen von Social-Engineering-Angriffen bei Führungskräften

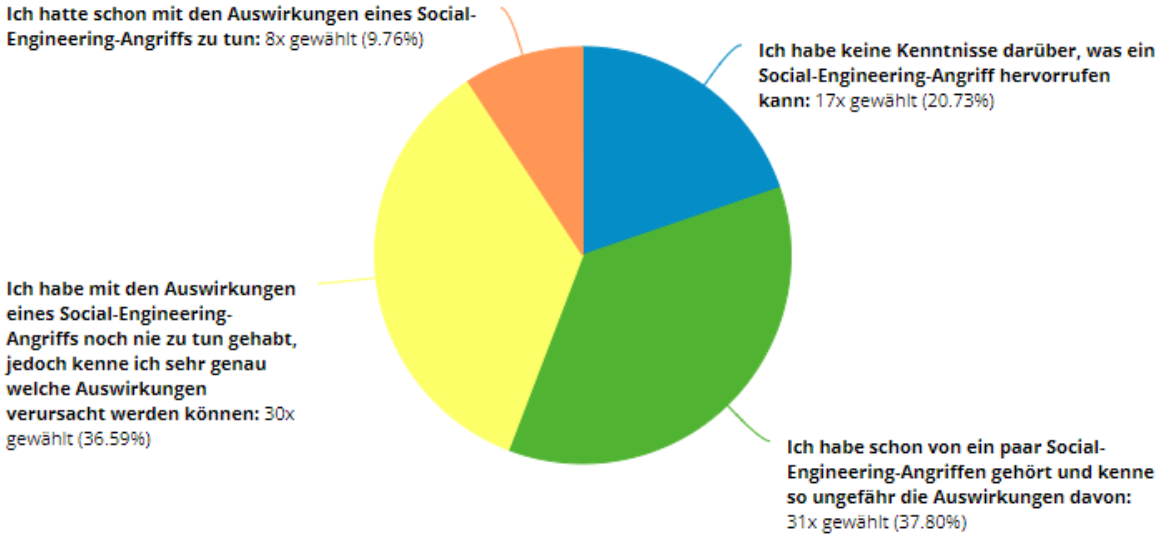

Abbildung 48: Auswirkungen von Social-Engineering-Angriffen bei Nichtführungskräften

Es ist nur ein geringer Unterschied zwischen den Personen, die mit sicherheitsrelevanten Informationen zu tun haben, und den Personen ohne solchen Kontakt sichtbar. Es ist jedoch zu erwähnen, dass nur 18 Personen angegeben haben, nicht mit sicherheitsrelevanten Informationen zu tun zu haben. Das könnte das Ergebnis eventuell verfälscht haben.

Abbildung 49: Auswirkungen von Social-Engineering-Angriffen bei Personen mit Kontakt mit sicherheitsrelevanten Informationen

Abbildung 50: Auswirkungen von Social-Engineering-Angriffen bei Personen ohne Kontakt mit sicherheitskritischen Informationen

Werden die IT-Experten mit den Nicht-IT-Experten in Bezug auf die Kenntnisse im Bereich des Social Engineerings verglichen, so ist ersichtlich, dass zum einen die Anzahl der Personen, die keine Kenntnisse darüber haben, was einen Social-Engineering-Angriff hervorrufen kann, um 10 % zurückgegangen ist und dass der Bereich, wo Personen entweder mit den Auswirkungen eines Social-Engineering-Angriffs zu tun hatten oder genau über diese Bescheid wissen auf rund zwei Drittel gestiegen ist. Damit kann gesagt werden, dass Personen mit einer hohen IT-Affinität eine bessere Expertise im Bereich des Social Engineerings aufweisen. Die genaue Aufteilung ist in den folgenden Abbildungen ersichtlich.

Abbildung 51: Auswirkungen von Social-Engineering-Angriffen bei Nicht-IT-Experten

Abbildung 52: Auswirkungen von Social-Engineering-Angriffen bei IT-Experten

Anhand der erhobenen Daten kann gesagt werden, dass die Hypothese 3 zu verwerfen ist und somit die Gegenhypothese belegt ist. Es konnte nicht nachgewiesen werden, dass Personen ohne IT-Affinität keine Kenntnisse im Bereich des Social Engineerings besitzen. In der Regel ist das Gegenteil der Fall. Es kann jedoch gesagt werden, dass IT-affine Personen meistens besser über die Auswirkungen Bescheid wissen. Bei den anderen Personengruppen gibt es keinen signifikanten Unterschied.

5.1.3 Hypothese 4

In diesem Kapitel soll folgende Hypothese anhand der quantitativen Daten der Umfrage überprüft werden: *„Mitarbeiterinnen und Mitarbeiter halten Einführungen von Regeln, die Social-Engineering-Angriffe verhindern sollen (zum Beispiel, dass ein Telefongespräch nicht weitergeleitet werden darf oder das Ändern des Passwortes in zyklischen Abständen) für einen Mehraufwand und unpraktisch.“*

Die erste Frage bezieht sich auf Security-Awareness-Schulungen. In diesem Zusammenhang wurden die Teilnehmenden gefragt, ob bzw. in welchem Ausmaß solche Security-Awareness-Schulungen im Unternehmen eingesetzt werden.

In den folgenden Abbildungen ist ersichtlich, dass Security-Awareness-Schulungen umso genauer und öfter durchgeführt werden, je größer das Unternehmen ist.

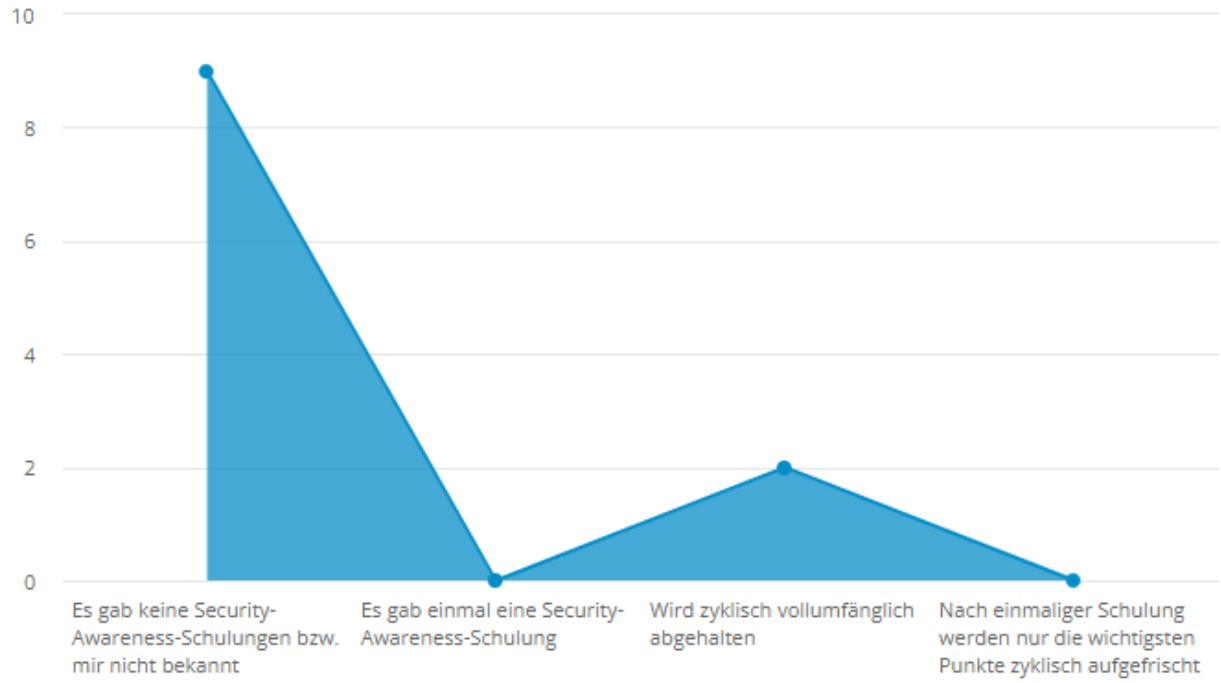

Abbildung 53: Häufigkeit von Security-Awareness-Schulungen In Unternehmen mit 1–10 Angestellten

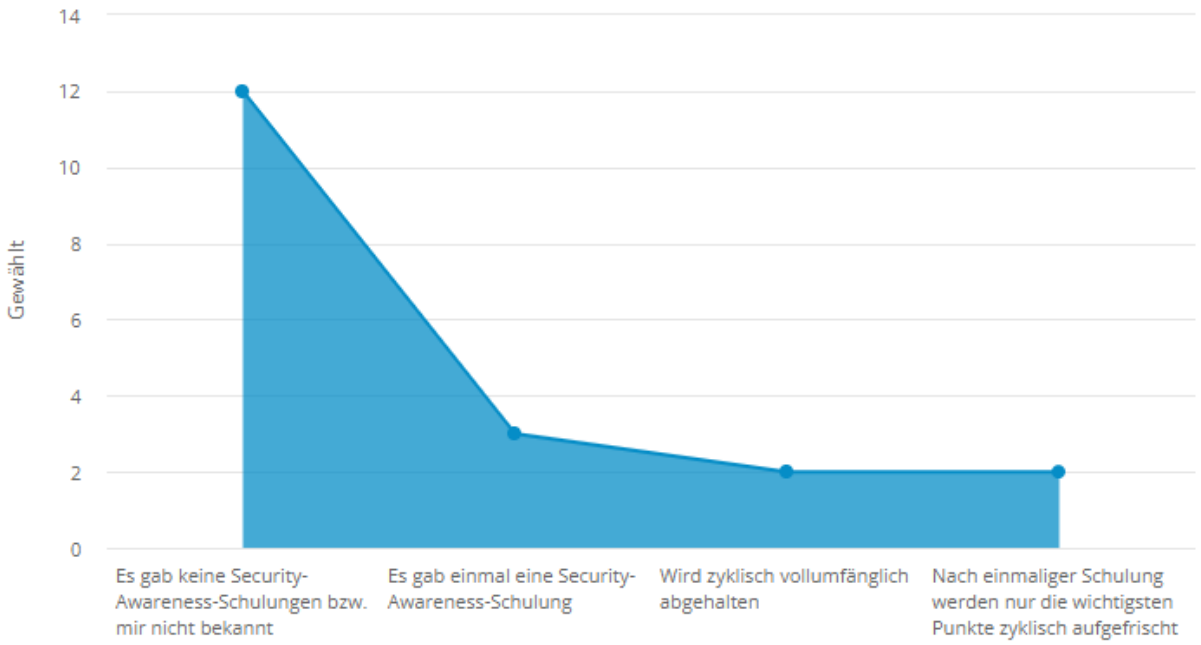

Abbildung 54: Häufigkeit von Security-Awareness-Schulungen in Unternehmen mit 11–50-Personen Angestellten

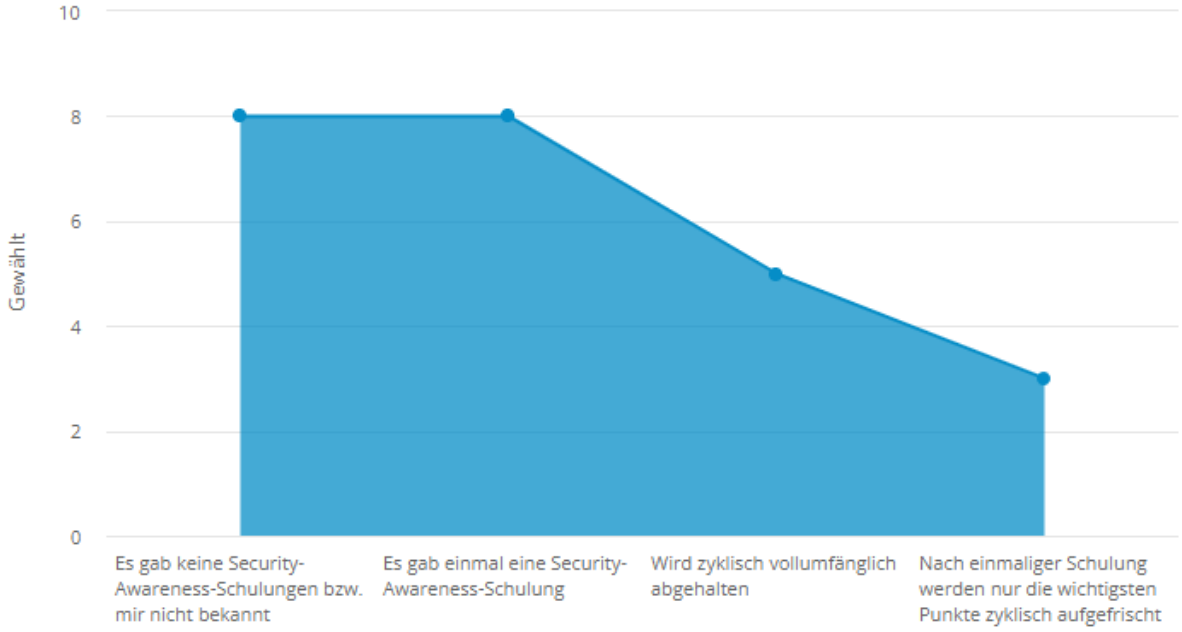

Abbildung 55: Häufigkeit von Security-Awareness -Schulungen in Unternehmen mit 51–250 Angestellten

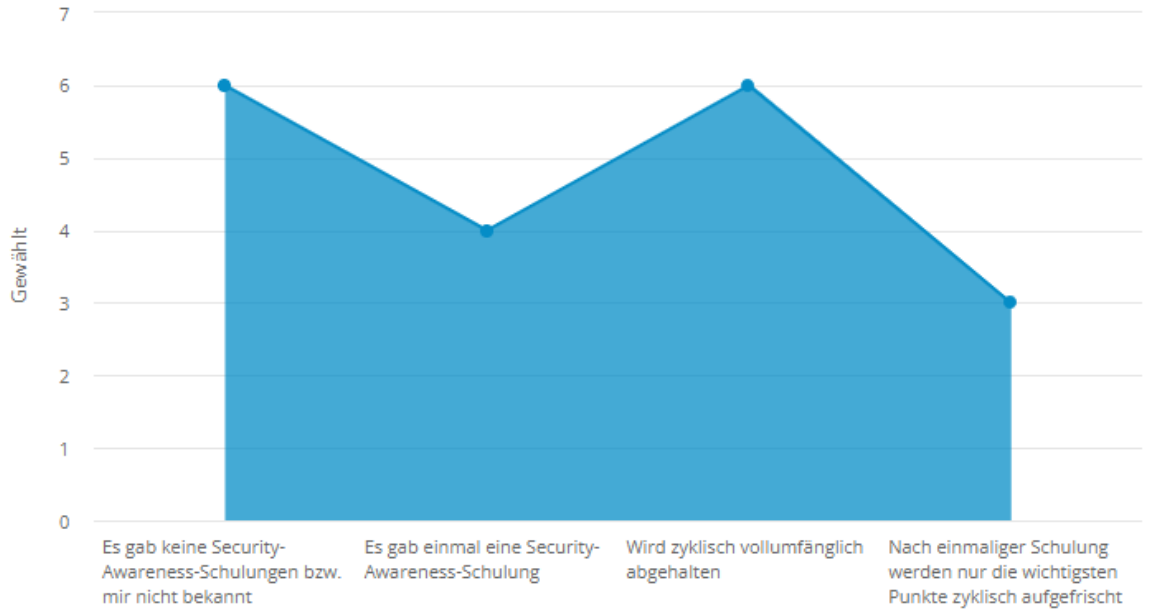

Abbildung 56: Häufigkeit von Security-Awareness -Schulungen in Unternehmen mit 251–1000 Angestellten

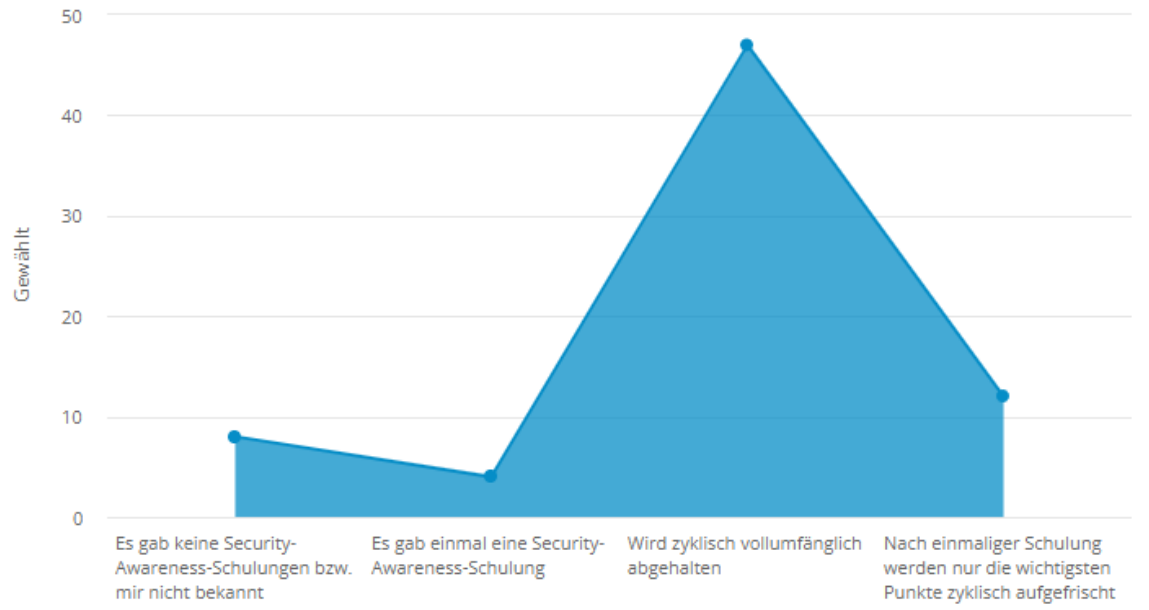

Abbildung 57: Häufigkeit von Security-Awareness-Schulungen in Unternehmen mit mehr als 1000 Angestellten

Die nächste Frage bezieht sich auf andere Maßnahmen, die eingesetzt werden können, um einen Social-Engineering-Angriff zu erschweren. Bei den Antworten wird erneut nach Unternehmensgröße gegliedert.

Laut den Ergebnissen setzen Unternehmen, unabhängig von der Größe, auf beschränkte Zugriffs- und/oder Zutrittsrechte zu bedeutenden Räumen oder Programmen. Im Vergleich gibt es bei dieser Frage keinen Unterschied zwischen Unternehmen unterschiedlicher Größen.

Ebenso zeigt sich bei Unternehmen aller Größen die gleiche Tendenz, Multi-Faktor-Authentifizierungen zu verwenden.

Erst bei Unternehmen ab einer Größe von mehr als zehn Personen kommen Maßnahmen, wie die Überwachung privilegierter Aktivitäten oder duale Kontrollsysteme, zum Einsatz. Es ist ersichtlich, dass diese beiden Maßnahmen nur bei einem geringen Teil der Unternehmen ergriffen werden, wobei deren Größe keinen Einfluss hat.

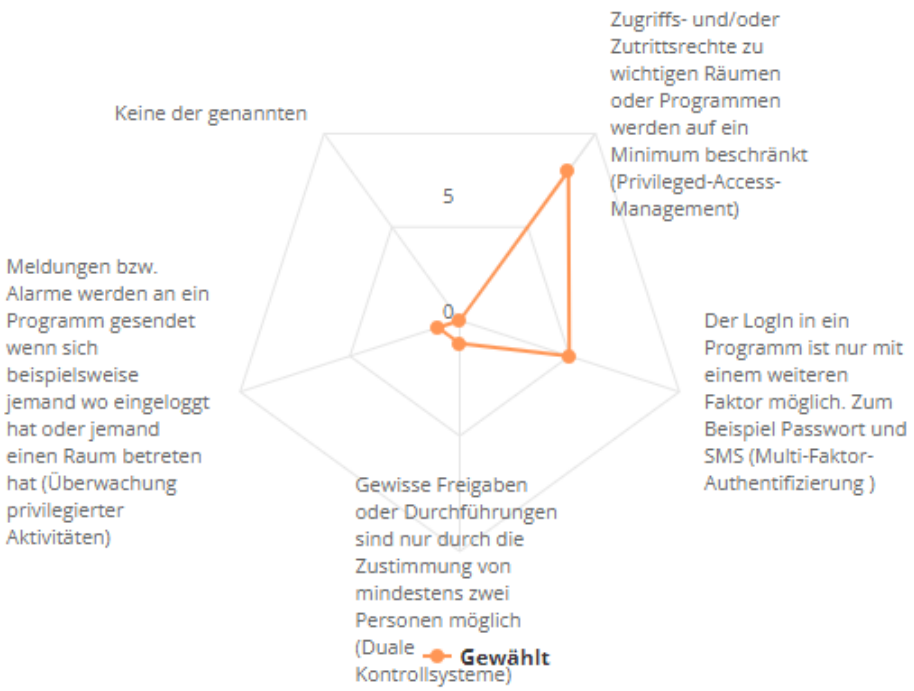

Abbildung 58: Eingesetzte technische oder physische Maßnahmen in Unternehmen mit 1–10-Personen

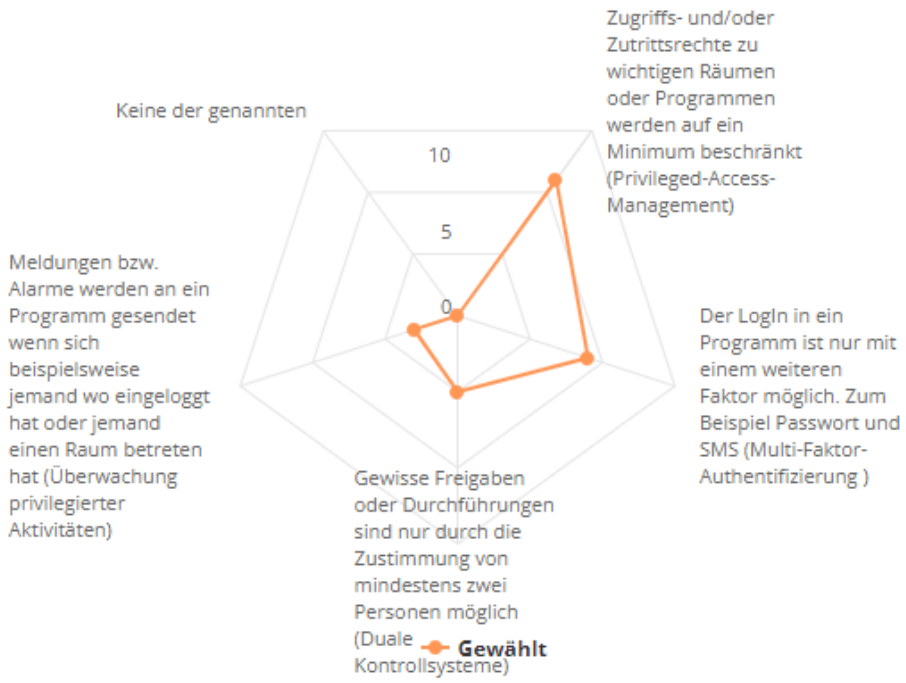

Abbildung 59: Eingesetzte technische oder physische Maßnahmen in Unternehmen mit 11–50Personen

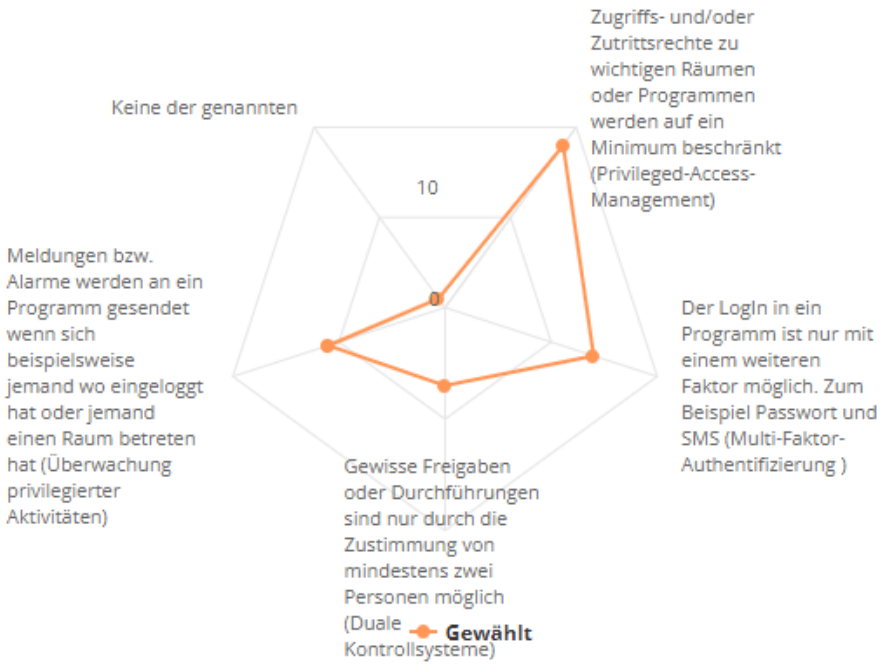

Abbildung 60: Eingesetzte technische oder physische Maßnahmen in Unternehmen mit 51–250-Personen

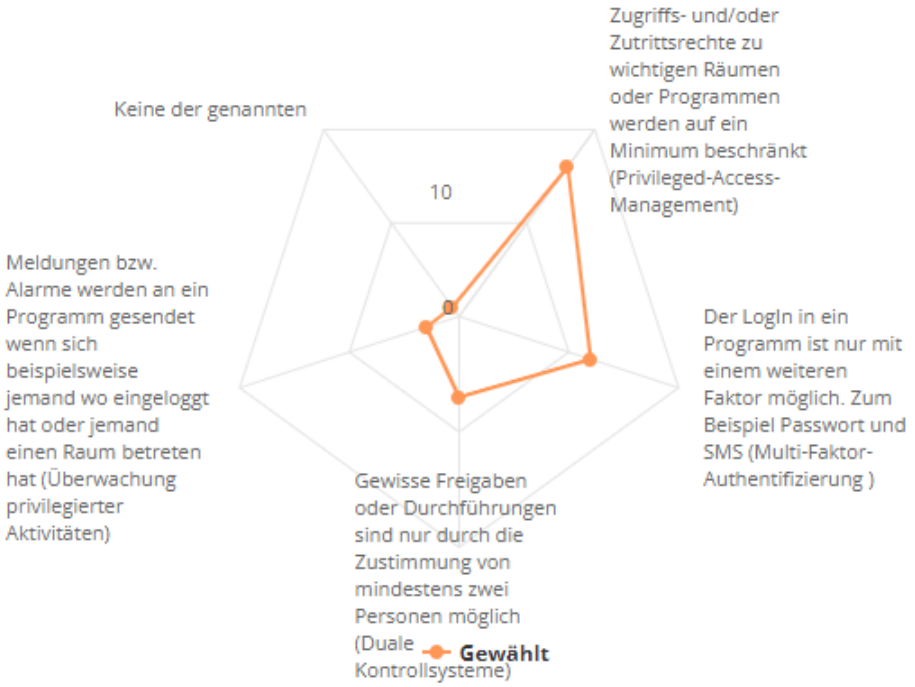

Abbildung 61: Eingesetzte technische oder physische Maßnahmen in Unternehmen mit 251–1000-Personen

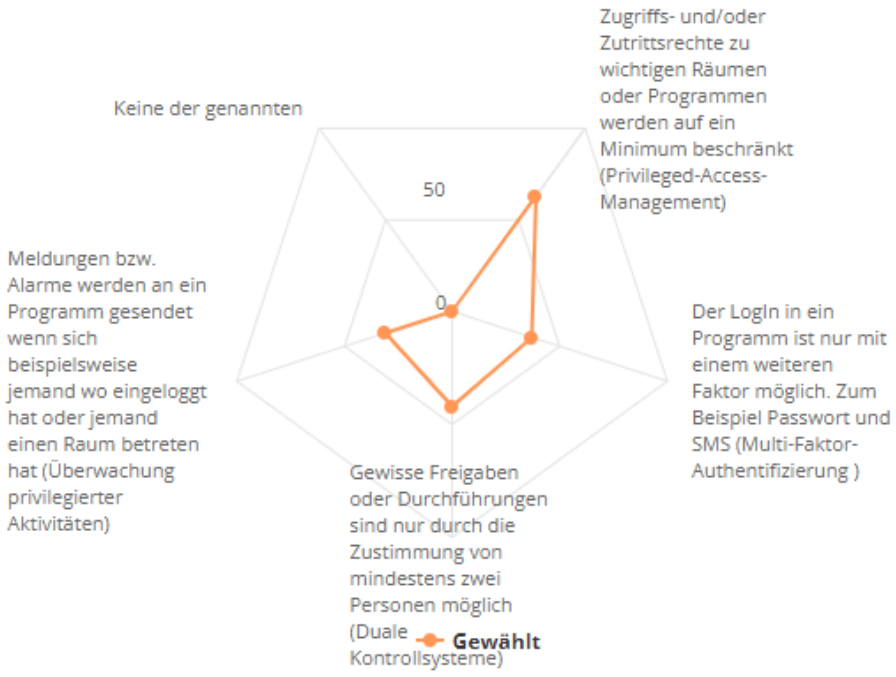

Abbildung 62: Eingesetzte technische oder physische Maßnahmen in Unternehmen mit über 1000-Personen

Die nächste Frage bezieht sich darauf, inwieweit gewisse Maßnahmen die Effizienz der Arbeitstätigkeit negativ beeinflussen. In den folgenden Abbildungen ist die durchschnittliche Antwortverteilung inklusive Standardabweichung nach den verschiedenen Personengruppen ersichtlich. Da es bei diesem Aspekt um die Person selbst geht, wird die Größe der Unternehmen vernachlässigt. Des Weiteren bleiben auch IT-affine Personen unberücksichtigt, da diese nicht die ‚normalen' Userinnen und User repräsentieren.

Die folgenden Abbildungen zeigen, dass das Alter der Personen keinen Einfluss auf die Einstellung gegenüber solchen Maßnahmen hat. Es ist ersichtlich, dass die Durchschnittsantwort alle Maßnahmen mit Ausnahme der dualen Kontrollsysteme immer unter der „wenig beeinflusst" Linie ist.

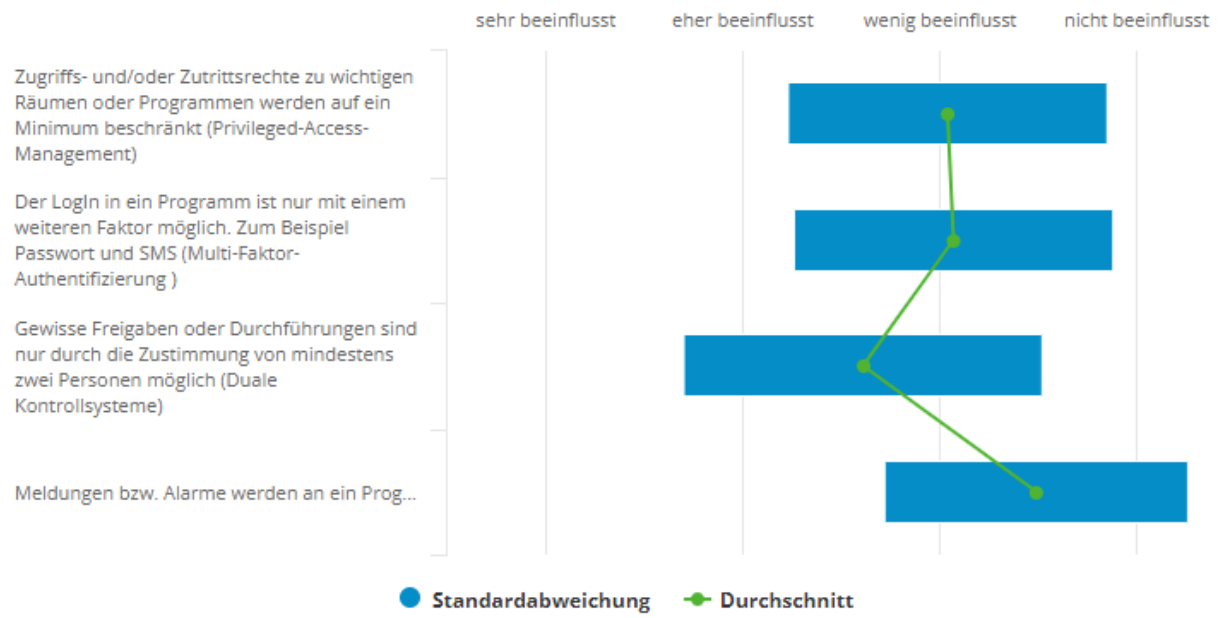

Abbildung 63: Auswirkung auf den Arbeitsfluss (18- bis 30-Jährige)

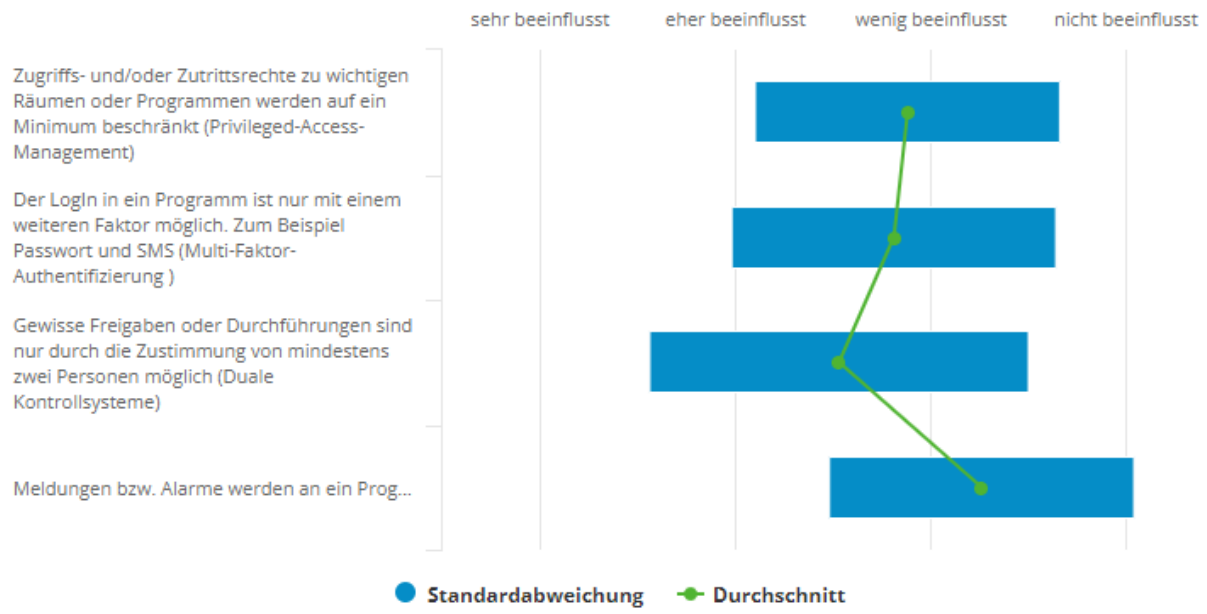

Abbildung 64: Auswirkung auf den Arbeitsfluss (31- bis 50-Jährige)

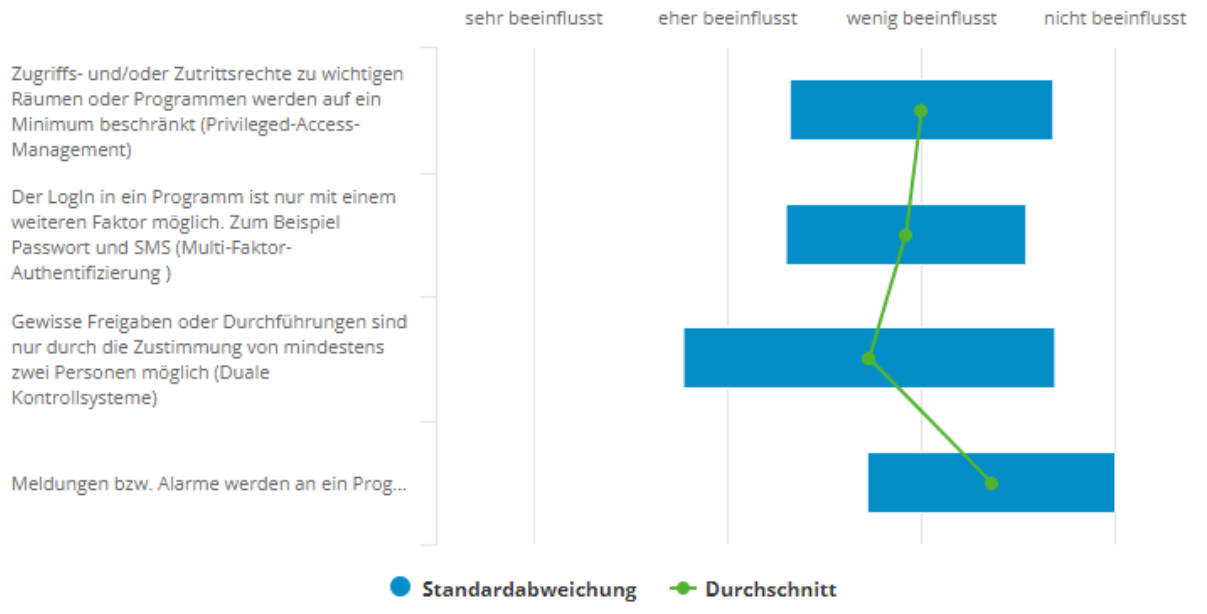

Abbildung 65: Auswirkung auf den Arbeitsfluss (51- bis 65-Jährige)

Den folgenden Abbildungen kann entnommen werden, dass die Art des Unternehmens keinen Einfluss darauf hat, ob sich gewisse Maßnahmen erheblich auf den Arbeitsfluss auswirken. Die Standardabweichung trifft immer die Linie „wenig beeinflusst“.

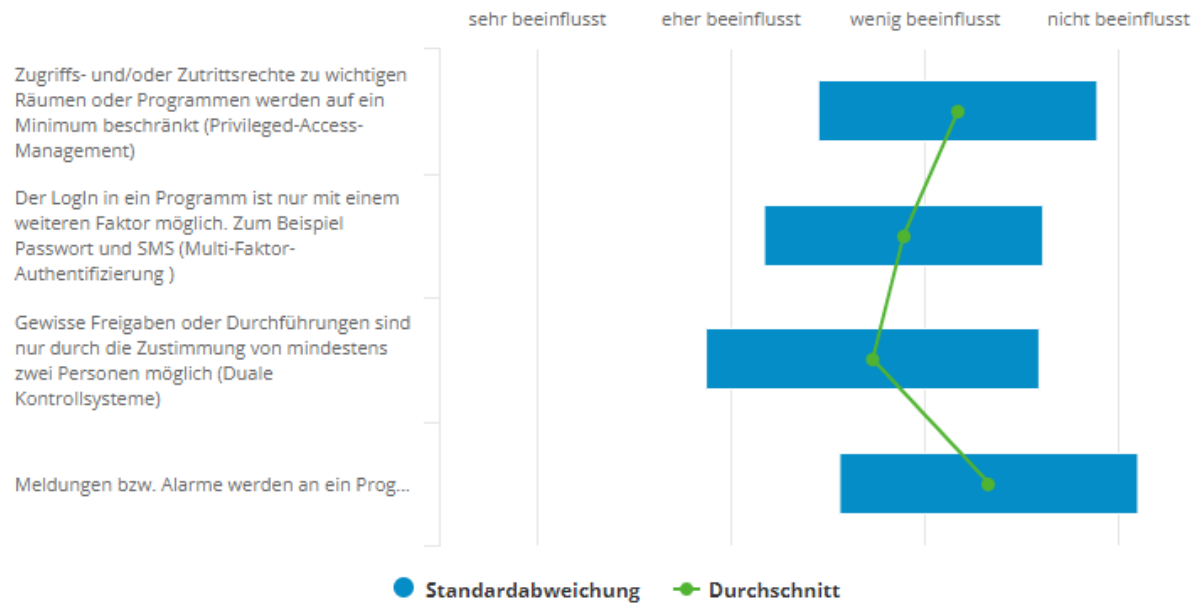

Abbildung 66: Auswirkung auf den Arbeitsfluss von Angestellten eines Unternehmens kritischer Infrastruktur

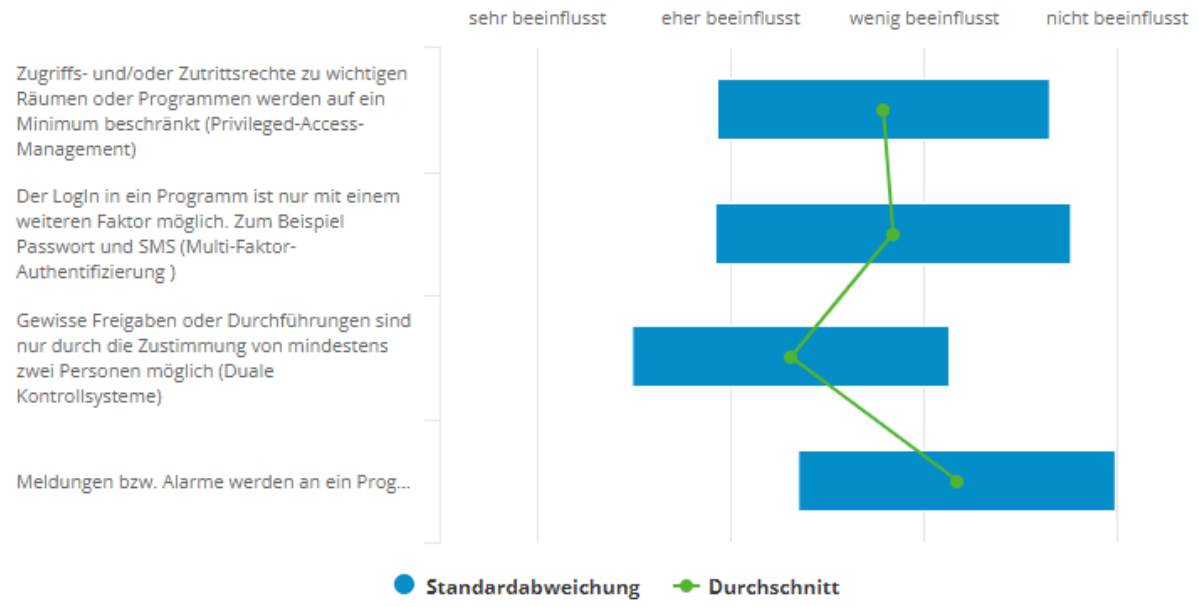

Abbildung 67: Auswirkung auf den Arbeitsfluss von Angestellten eines Unternehmens nicht kritischer Infrastruktur

Es ist ersichtlich, dass sich lediglich bei den dualen Kontrollsystemen eine Tendenz in Richtung „eher beeinflusst“ zeigt. Auch bei dieser Frage gibt es keinen signifikanten Unterschied zwischen Personen mit und Personen ohne Führungsverantwortung.

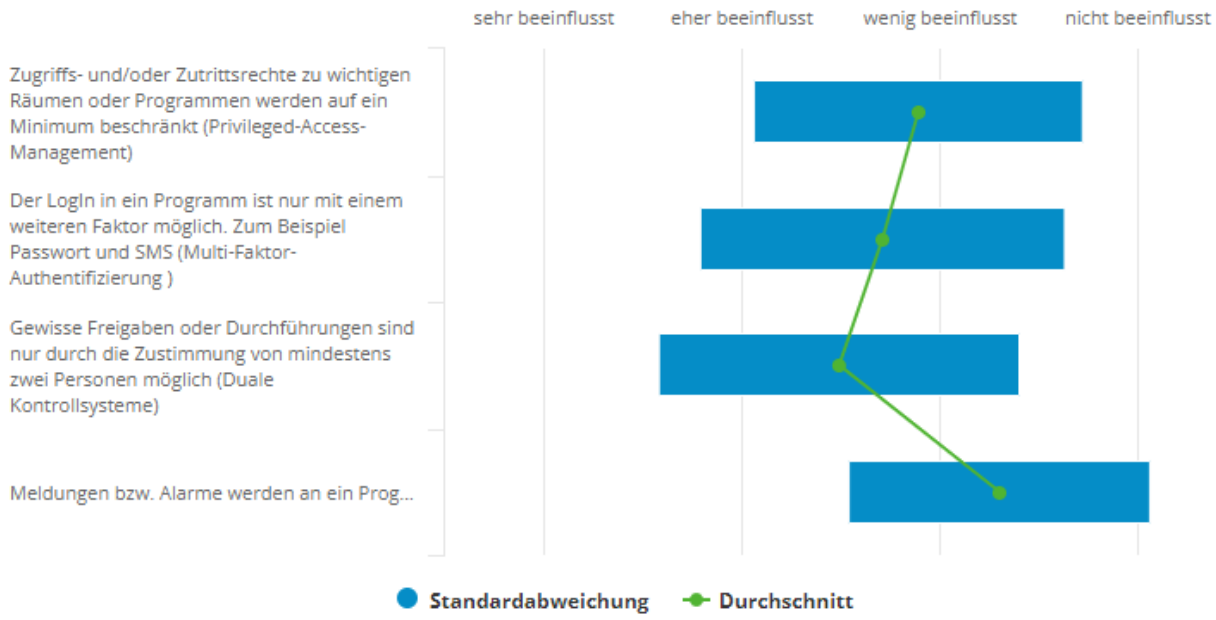

Abbildung 68: Auswirkung auf den Arbeitsfluss von Personen mit Führungsverantwortung

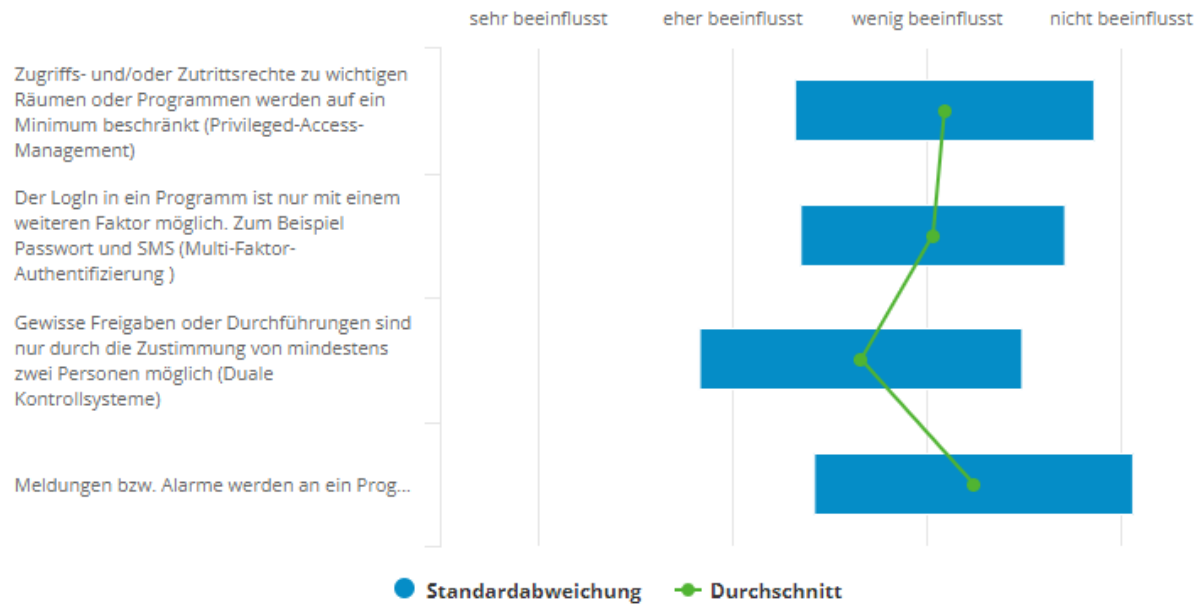

Abbildung 69: Auswirkung auf den Arbeitsfluss von Personen ohne Führungsverantwortung

Es macht keinen Unterschied, ob Personen mit sicherheitskritischen Informationen zu tun haben oder nicht. Dieser Parameter hat keinen Einfluss darauf, ob sich die eingesetzten Maßnahmen negativ auf den Arbeitsfluss auswirken. Die ganzen Maßnahmen haben eine Standardabweichung, die immer die Linie „wenig beeinflusst“ kreuzt.

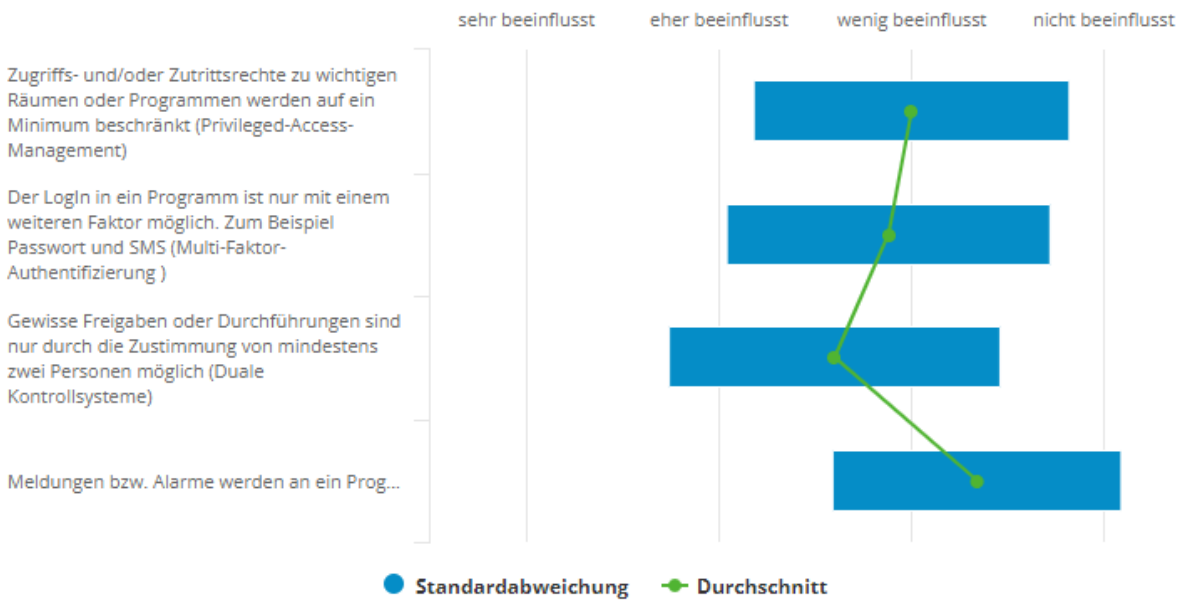

Abbildung 70: Auswirkung auf den Arbeitsfluss von Personen mit Kontakt mit sicherheitskritischen Informationen

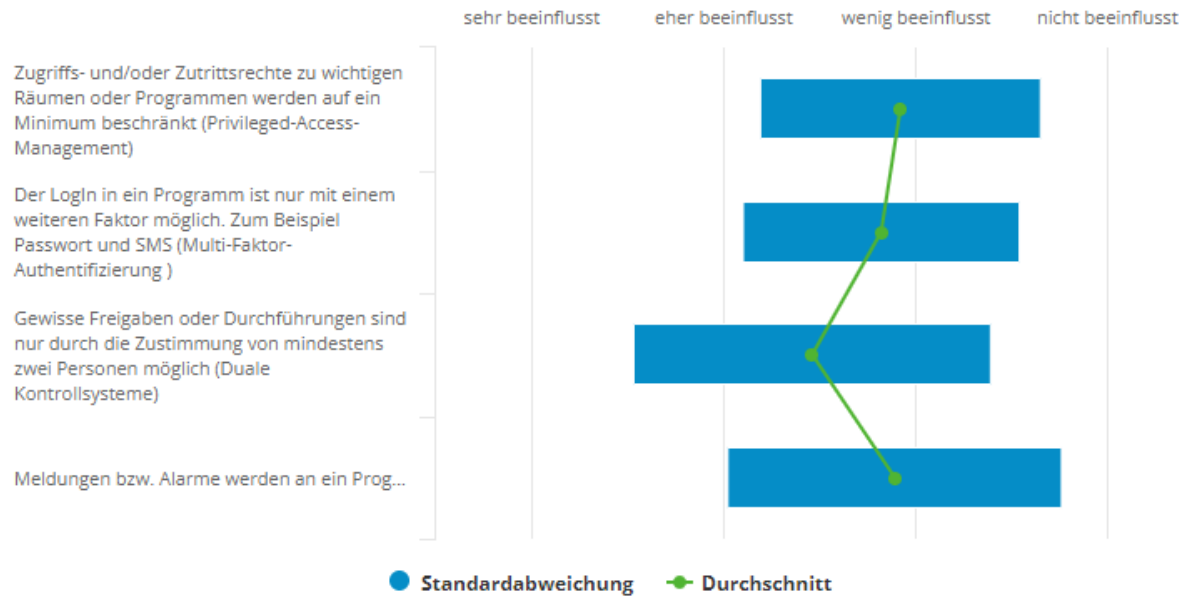

Abbildung 71: Einfluss auf den Arbeitsfluss von Personen ohne Kontakt mit sicherheitskritischen Informationen

Zusammengefasst kann zu dieser Frage gesagt werden, dass es keinen Unterschied zwischen den einzelnen Personengruppen gibt. Für alle Personengruppen wurden ähnliche Ergebnisse ermittelt. Im Allgemeinen kann die Aussage getroffen werden, dass es irrelevant ist, wie alt die Person ist, ob sie Verantwortung für andere Personen hat oder ob sie mit sicherheitskritischen Informationen zu tun hat. Laut dieser Erhebung scheinen alle genannten Faktoren keine erhebliche Auswirkung auf die Frage zu haben, ob die Sicherheitsmaßnahmen als störend für den Arbeitsfluss empfunden werden.

Mit der nächsten Frage soll herausgefunden werden, für wie bedeutsam die befragten Personen die eingesetzten Maßnahmen halten. Die folgende Abbildung zeigt im Allgemeinen, dass die befragten Personen die eingesetzten Maßnahmen als essentiell empfinden.

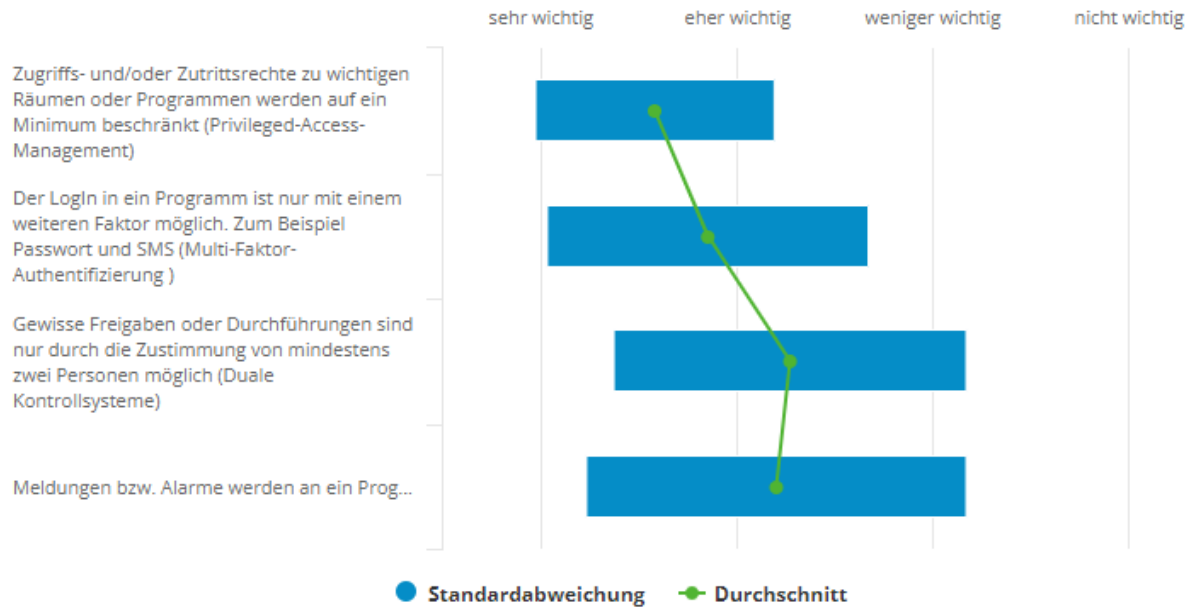

Abbildung 72: Empfundene Bedeutung der eingesetzten Maßnahmen

Die folgenden Abbildungen sollen zeigen, ob es zwischen den einzelnen Personengruppen einen signifikanten Unterschied in Bezug auf die empfundene Bedeutung der einzelnen Maßnahmen gibt.

Es kann gesehen werden, dass bei diesem Aspekt zwischen den einzelnen Personengruppen kein signifikanter Unterschied festzustellen ist.

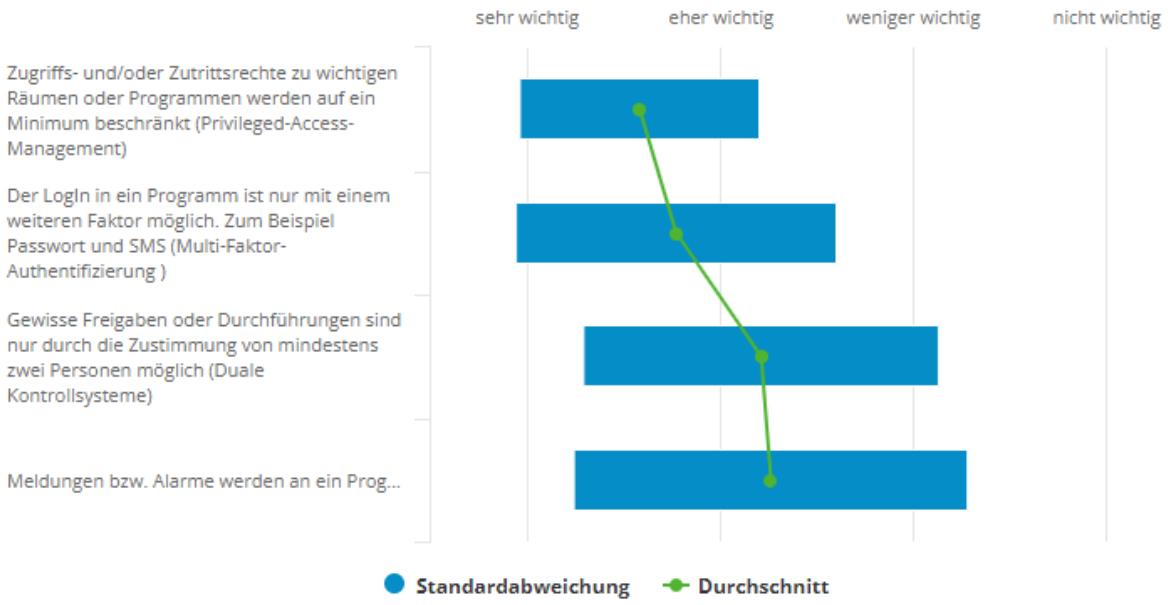

Abbildung 73: Empfundene Bedeutung der eingesetzten Maßnahmen (18- bis 30-Jährige)

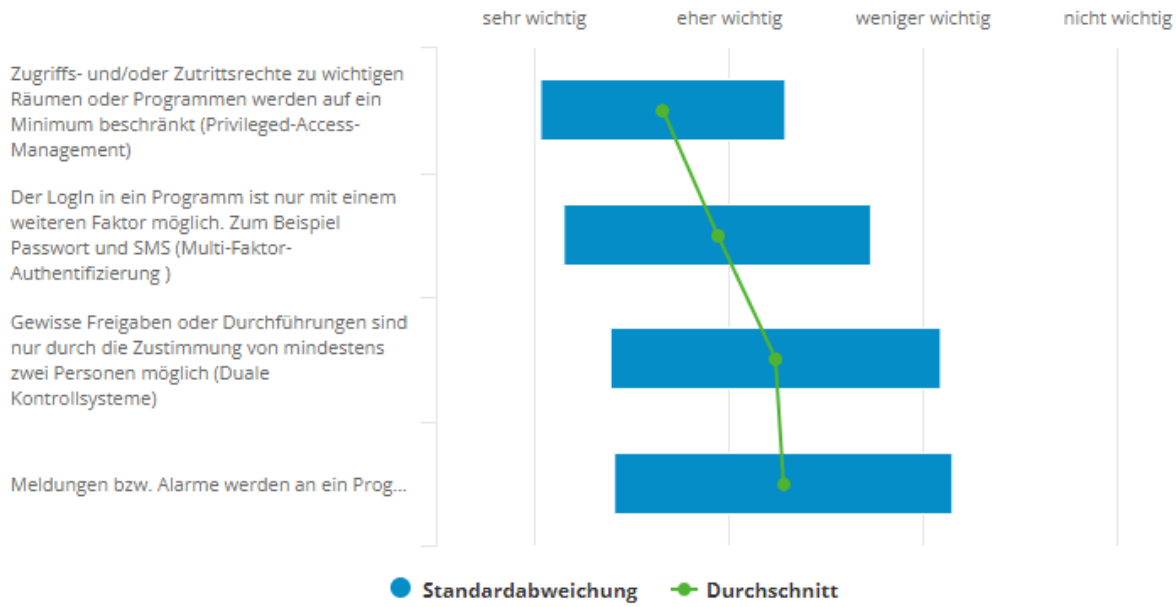

Abbildung 74: Empfundene Bedeutung der eingesetzten Maßnahmen (31- bis 50-Jährige)

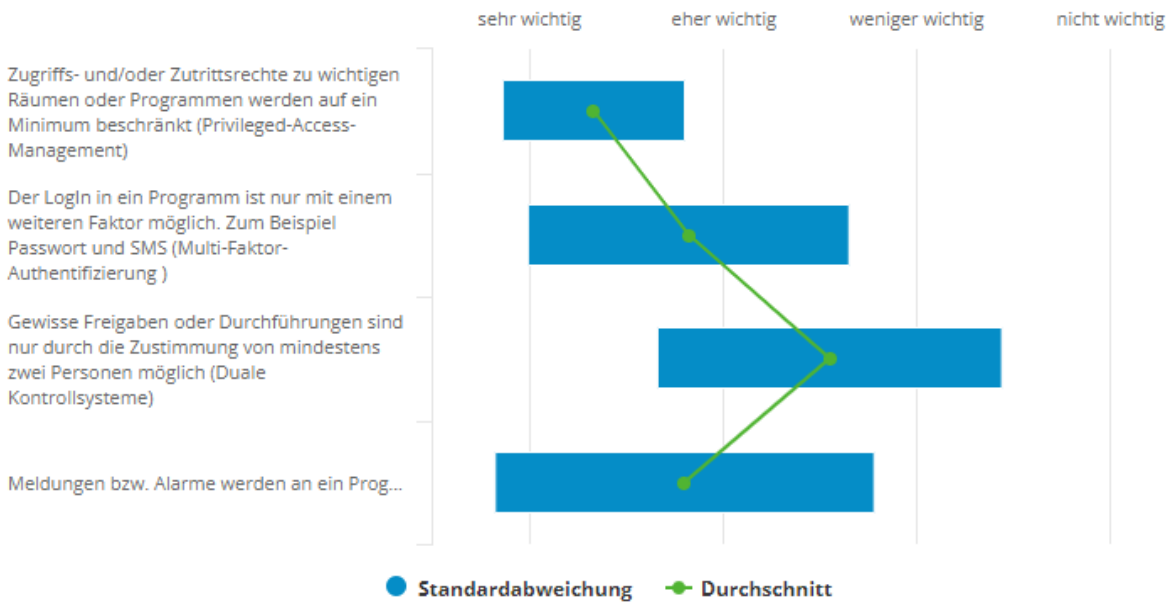

Abbildung 75: Empfundene Bedeutung der eingesetzten Maßnahmen (50- bis 65-Jährige)

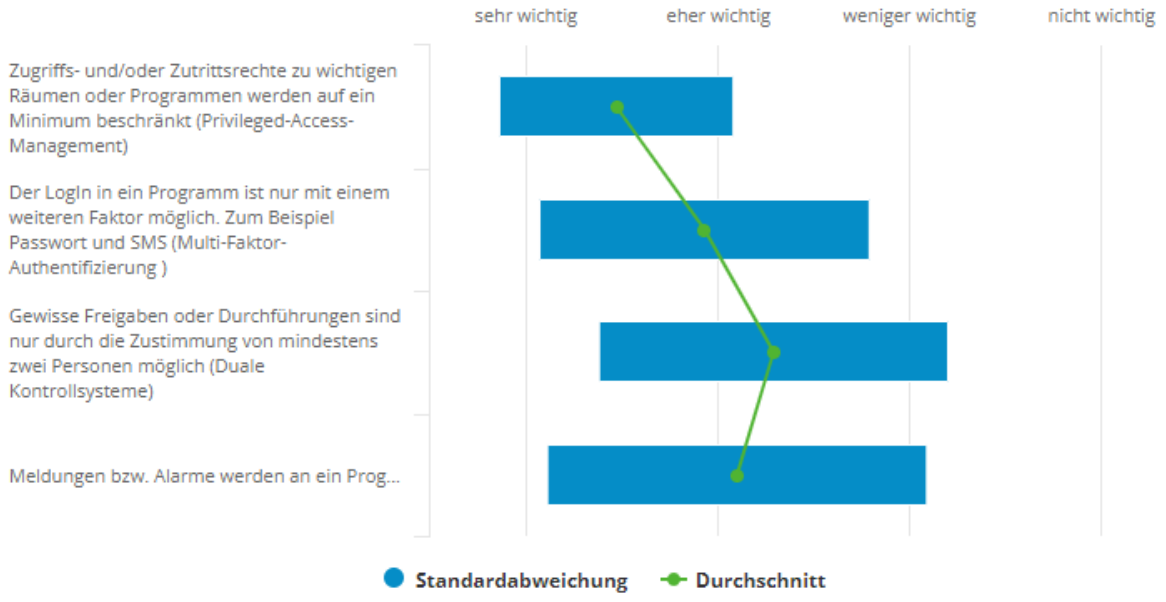

Abbildung 76: Empfundene Bedeutung der eingesetzten Maßnahmen bei Angestellten eines Unternehmens kritischer Infrastruktur

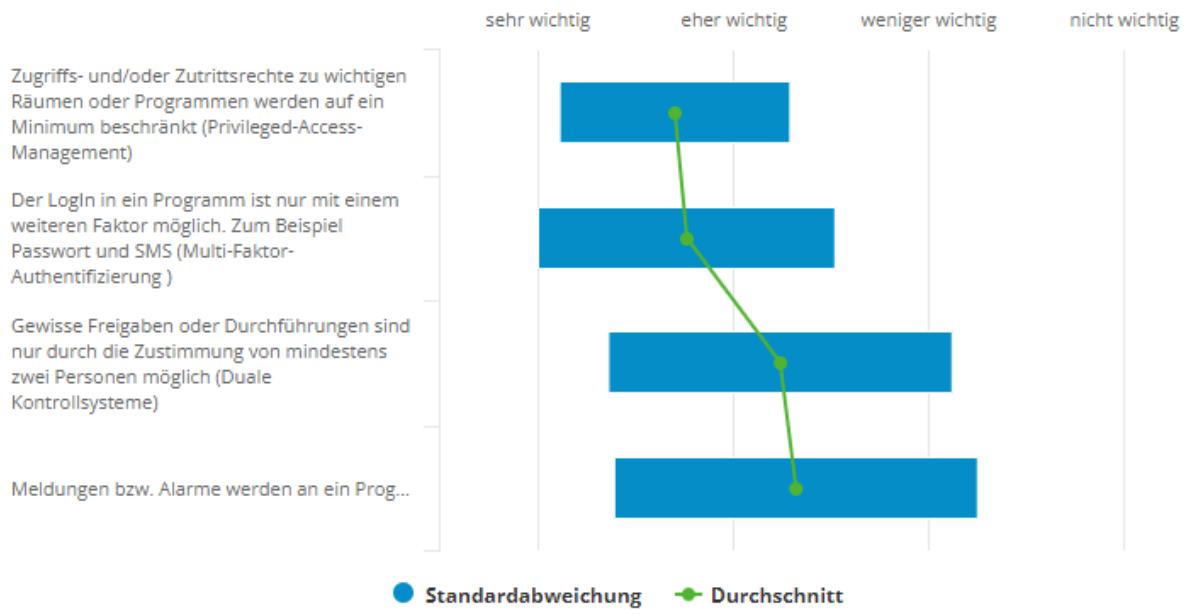

Abbildung 77: Empfundene Bedeutung der eingesetzten Maßnahmen bei Angestellten eines Unternehmens nicht kritischer Infrastruktur

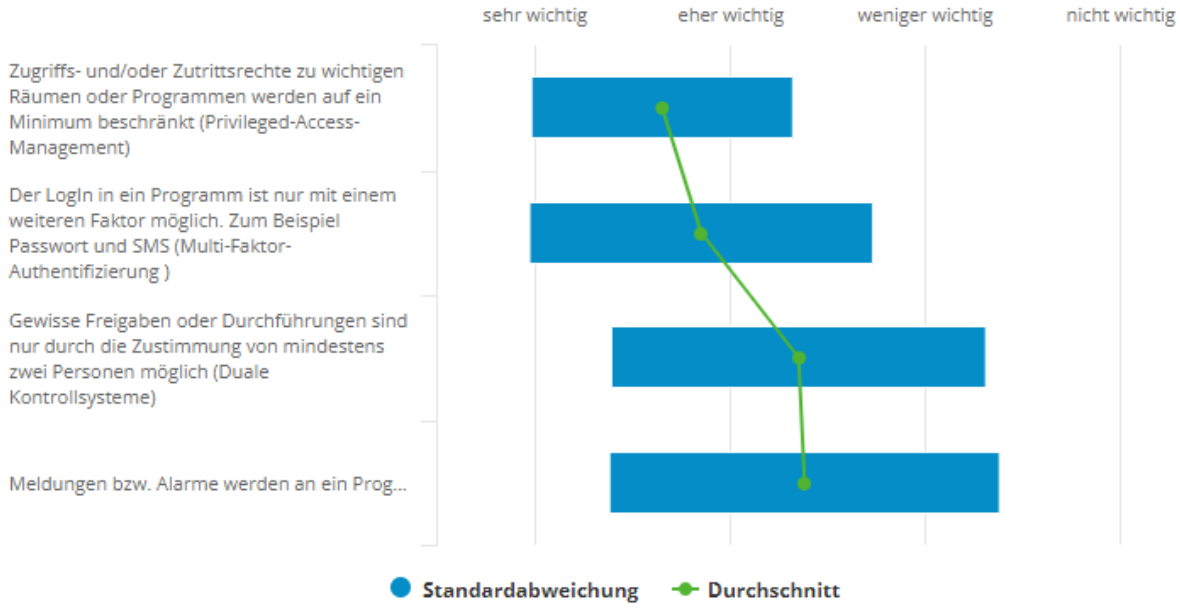

Abbildung 78: Empfundene Bedeutung der eingesetzten Maßnahmen bei Personen mit Führungsverantwortung

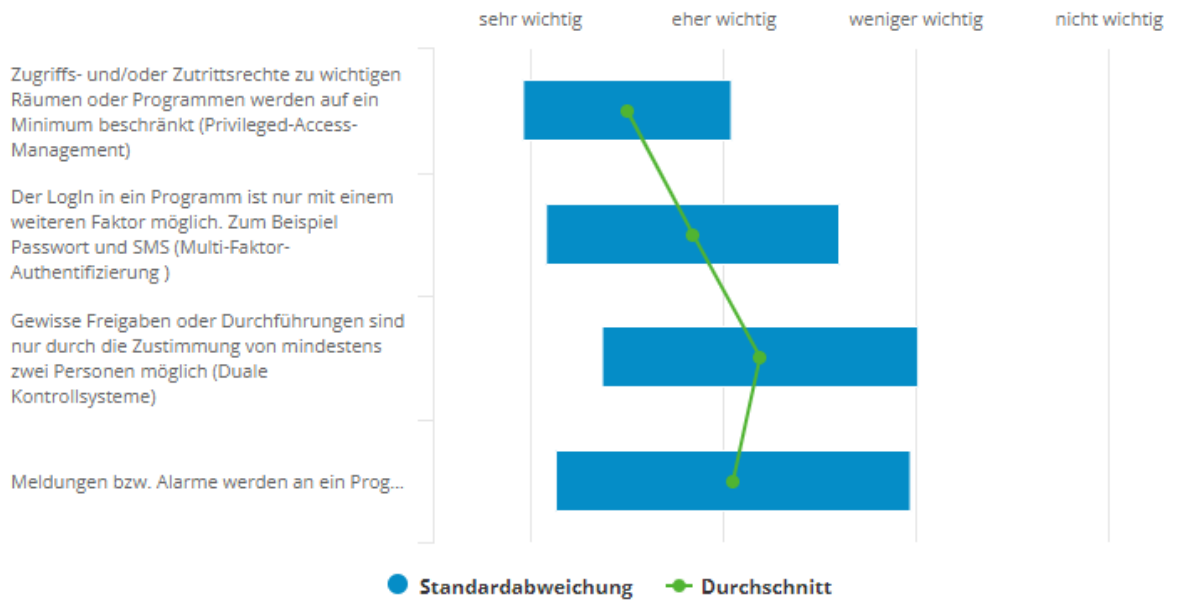

Abbildung 79: Empfundene Bedeutung der eingesetzten Maßnahmen bei Personen ohne Führungsverantwortung

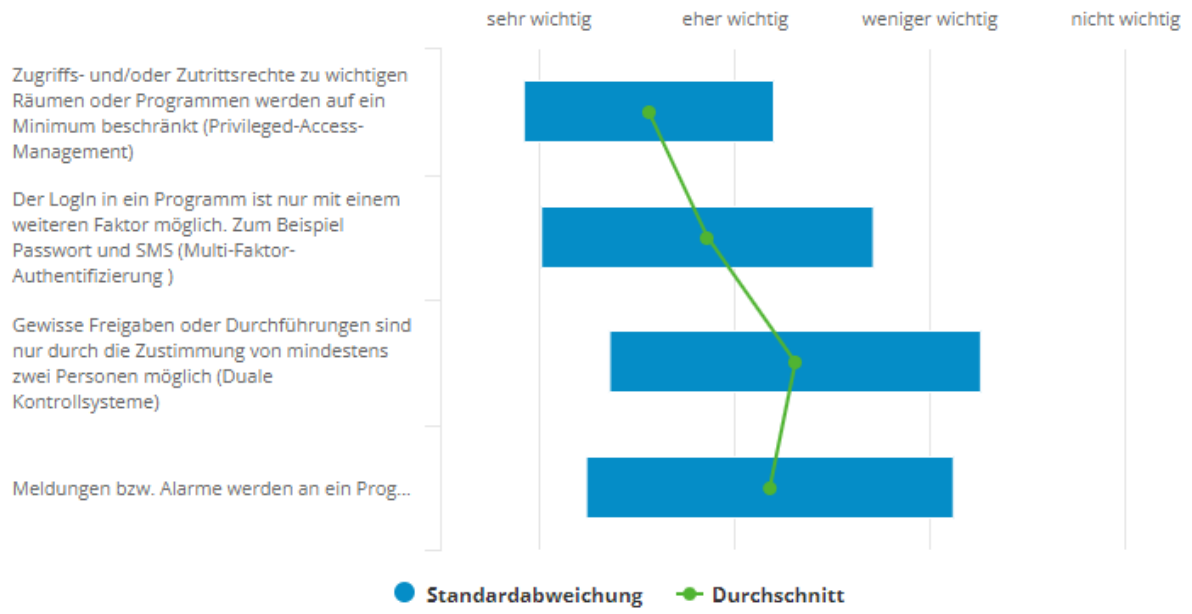

Abbildung 80: Empfundene Bedeutung der eingesetzten Maßnahmen bei Personen, die mit sicherheitskritischen Informationen zu tun haben

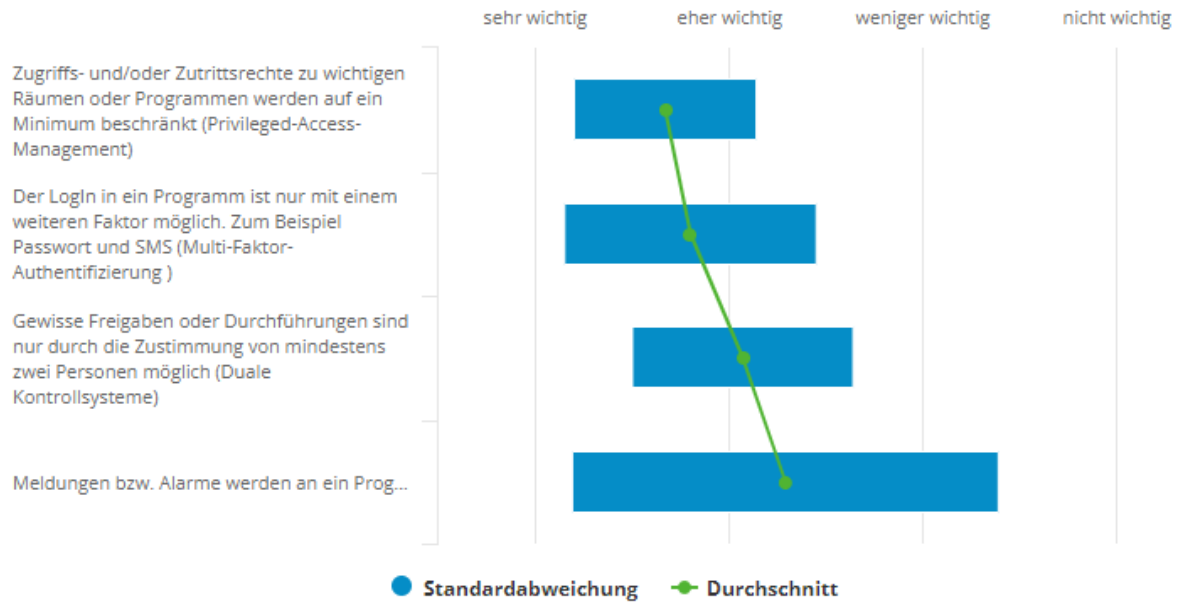

Abbildung 81: Empfundene Bedeutung der eingesetzten Maßnahmen bei Personen ohne Kontakt mit sicherheitskritischen Informationen

Aufgrund der Daten aus der Umfrage muss die Hypothese 4 verworfen werden. Es zeigte sich, dass Mitarbeiterinnen und Mitarbeiter in der heutigen Zeit Verständnis für die eingesetzten Maßnahmen haben. Auch die eingeleiteten Maßnahmen, die einen Social-Engineering-Angriff erschweren sollen, haben keine erheblich negative Auswirkung auf den Arbeitsfluss. Damit ist die Gegenhypothese belegt.

5.2 Auswertung der Experteninterviews

Es wurden Expertinnen und Experten aus verschiedenen Unternehmen unterschiedlicher Größe zum Thema Social Engineering befragt, um qualitativ hochwertige Informationen zu gewinnen.

In diesem Kapitel findet die qualitative Analyse der Interviews statt.

5.2.1 Einleitung

Die folgende Tabelle zeigt einen Ausschnitt der Paraphrasen der Einleitungsfragen. Die komplette Tabelle ist in ANHANG H -ersichtlich. In der Einleitung wird analysiert, welche Erfahrung die einzelnen Expertinnen oder Experten haben, wie sich das Thema Informationssicherheit in den letzten Jahren verändert hat und welche Personengruppe für Social-Engineering-Angriffe besonders anfällig ist.

ca. zehn Jahre	Erfahrung
Überprüfung von Software und Produkten auf deren IT-Sicherheit und Reporting von Schwachstellen	Erfahrung
Ich beschäftige mich auch mit Security-Awareness-Schulungen und der anschließenden Überprüfung	Erfahrung
Vieles ist komplizierter geworden, was es erleichtert und erschwert zugleich, Lücken in Systemen zu finden	Entwicklung
Ein gewisses Bewusstsein für Social Engineering wurde geschaffen	Entwicklung
Mehr als 95 % aller Angriffe sind auf Social Engineering zurückzuführen	Entwicklung
Social Engineering hat einen großen Einfluss auf die Informationssicherheit	Entwicklung
Social Engineering ist ein Einfallsvektor, wie beispielsweise in ein Unternehmen eingetreten werden kann	Entwicklung
Social Engineering wird für Kriminelle immer interessanter	Entwicklung
Normale User, weil ein gewisses Bewusstsein fehlt	gefährdete Personengruppe
Eine gewisse Naivität der normalen User verursacht falsches Vertrauen	gefährdete Personengruppe
Personen, die viel Kontakt nach außen haben	gefährdete Personengruppe
Jede Person ist anfällig für einen Social-Engineering-Angriff	gefährdete Personengruppe
Administratoren mit weitreichenden Berechtigungen können im Falle eines erfolgreichen Social-Engineering-Angriffs die ganze Infrastruktur in Gefahr bringen	gefährdete Personengruppe
Ein Angriff ist meist nicht nur auf eine Zielperson ausgerichtet, sondern arbeitet sich in einem System von einer Person zur nächsten weiter. Das nennt man ‚Lateral Movement'	gefährdete Personengruppe
Es gibt keine spezielle Personengruppe, die besonders anfällig ist. Es ist abhängig, wie gut Personen in diesem Bereich geschult sind	gefährdete Personengruppe
Stress macht eine Person besonders anfällig für einen Social-Engineering-Angriff	gefährdete Personengruppe

Tabelle 3: Ausschnitt der Paraphrasen der Einleitung

Erfahrung

Aussagen, die mit ‚Erfahrung' kodiert wurden, zeigen, dass die Befragten im Bereich der Informationssicherheit zwischen sechs und zehn Jahren Erfahrung haben. Des Weiteren waren alle Expertinnen oder Experten zum Zeitpunkt des Interviews in einem aktiven Angestelltenverhältnis mit einem Unternehmen und haben in ihrer täglichen Tätigkeit mit dem Thema Informationssicherheit zu tun. Damit waren sie in der Lage, qualitativ hochwertige Informationen wiederzugeben. Eine Expertin oder ein Experte beschäftigt sich auch mit Security-Awareness-Schulungen und der anschließenden Überprüfung.

Entwicklung

In den Gesprächen wurde immer wieder erwähnt, dass das Thema der Informationssicherheit mittlerweile ins Bewusstsein der Menschen gelangt ist und deswegen das Topmanagement auch mehr Budget für sicherheitsrelevante Themen zur Verfügung stellt. Es wurde aber von einer befragten Person angeführt, dass es immer zuerst zu einem Vorfall kommen muss, bevor Budget freigegeben wird. Die anderen Expertinnen und Experten erwähnten dies jedoch nicht. Es kann gesagt werden, dass die Informationssicherheit einen höheren Stellenwert bekommen hat, als es noch vor einigen Jahren der Fall war, und dass es einen höheren Geldfluss gibt.

Softwares und Programme werden immer sicherer, weswegen es zunehmend schwieriger wird, Lücken zu finden. Aus diesem Grund wird oftmals auf Social-Engineering-Angriffe gesetzt. Mehr als 95 % aller Angriffe haben ihren Ursprung im Social-Engineering-Bereich, infolgedessen dies auch der stärkste Initialvektor ist. Das bestätigt auch Galov (2021). Social-Engineering-Angriffe sind deswegen auch oft verantwortlich für Datenlecks. Es gilt zu erwähnen, dass es für ein Unternehmen wertvoll ist, wenn das Personal jeglichen Verdacht für einen Social-Engineering-Angriff der Security-Abteilung meldet.

Beachtenswert ist jedoch, dass vor allem kleine Unternehmen sich für zu unwichtig und zu klein halten, um Opfer eines Social-Engineering-Angriffs zu werden. Deswegen ergreifen sie zu wenig Maßnahmen, um die Informationssicherheit zu erhöhen. Ein weiterer Trend besteht darin, dass heutzutage viele Unternehmen auf Managed-Security-Service-Provider setzen.

Gefährdete Personengruppe

Grundsätzlich gibt es keine Personengruppe, die besonders anfällig für Social-Engineering-Angriffe ist. Jeder Mensch kann Ziel eines Angriffs werden, unabhängig vom Knowhow im Bereich der Informationssicherheit. Der Faktor Stress spielt eine große Rolle. Bei geschultem Personal bzw. bei Personen mit einem gewissen Knowhow ist es schwieriger, einen Social-Engineering-Angriff erfolgreich durchzuführen. Am einfachsten funktioniert es bei Personen, die viel Kontakt nach außen haben, wie bei einer hilfsbereiten Mitarbeiterin oder einem hilfsbereiten Mitarbeiter im Vertrieb. Mit der richtigen Technik kann aber jede Person erfolgreich angegriffen werden.

5.3 Auswertung der Hypothese 1

In diesem Unterkapitel wird folgende Hypothese überprüft: „*Jährliche Schulungen für Mitarbeiterinnen und Mitarbeiter im Kontext des Social Engineerings haben einen positiven Einfluss auf die Informationssicherheit von kritischen Infrastrukturen.“*

Dazu werden die Aussagen, die wie folgt kodiert worden sind, genauer betrachtet:

- Sinnhaftigkeit von Security-Awareness-Schulungen
- Aufbau von Security-Awareness-Schulungen
- Technische Maßnahmen gegen Social-Engineering-Angriffe
- Messung
- Unterschied zwischen Unternehmen kritischer Infrastruktur und Unternehmen keiner kritischen Infrastruktur
- Beschwerden

In folgender Tabelle ist ein Ausschnitt der einzelnen Paraphrasen dieser Kodierungen ersichtlich. Die komplette Tabelle befindet sich in ANHANG I -:

Ja, Security-Awareness-Schulungen sind sinnvoll	Sinnhaftigkeit von Security-Awareness-Schulungen
Kontinuierliche Schulungen einmal im Jahr sind sinnvoll	Aufbau von Security-Awareness-Schulungen
Praktische Beispiele, damit sich die Mitarbeiterinnen und Mitarbeiter hineinversetzen können	Aufbau von Security-Awareness-Schulungen
Sinnvoll sind Security-Maßnahmen immer	technische Maßnahmen gegen Social-Engineering-Angriffe
Mir sind keine technischen Maßnahmen bekannt, die ausschließlich darauf ausgelegt sind, Social-Engineering-Angriffe zu erschweren	technische Maßnahmen gegen Social-Engineering-Angriffe
E-Mail-Filter, Blockieren von zwielichtigen URLs	technische Maßnahmen gegen Social-Engineering-Angriffe
Relation von Security und Usability muss beachtet werden	technische Maßnahmen gegen Social-Engineering-Angriffe
keine Beschwerden von Mitarbeiterinnen und Mitarbeitern über eingesetzte Maßnahmen	Beschwerden
Betriebsrat macht Probleme, weil er sich dafür einsetzt, dass Mitarbeiterinnen und Mitarbeiter nicht ohne Wissen überprüft werden dürfen	Messung
Eine Spear-Phishing-Simulation ohne eine Security-Awareness-Schulung hat eine Fehlerquote zwischen 30 % und 60 % und eine Spear-Phishing-Simulation mit einer Security-Awareness-Schulung hat eine Fehlerquote zwischen 5 % und 10 %	Messung
Sinnvoll sind die Maßnahmen in jedem Unternehmen, aber es müssen natürlich die Ressourcen betrachtet werden	Unterschied zwischen Unternehmen kritischer Infrastruktur und Unternehmen keiner kritischen Infrastruktur

Tabelle 4: Ausschnitt der Paraphrasen für die Auswertung der Hypothese 1

Sinnhaftigkeit von Security-Awareness-Schulungen

Security-Awareness-Schulungen sind sinnvoll, was auch von allen Expertinnen und Experten bestätigt wurde. Sie sind das effektivste Mittel, um einen Social-Engineering-Angriff zu erschweren, da das Bewusstsein für Informationssicherheit von geschultem Personal höher ist als bei ungeschultem Personal. Entsprechende Schulungen können einen Angriff zwar nie zu 100 % verhindern, aber die Wahrscheinlichkeit eines erfolgreichen Angriffs ist deutlich geringer.

Es gibt einzelne Szenarien, in denen sich Security-Awareness-Schulungen nicht auszahlen. Dies ist der Fall, wenn das Unternehmen kein lukratives Angriffsziel darstellt. In solchen Unternehmen haben die Schulungen eine niedrigere Priorität, da die Wahrscheinlichkeit, Opfer eines Angriffs zu werden, geringer ist.

Des Weiteren gilt es zu erwähnen, dass Security-Awareness-Schulungen für IT-affine Personen weniger sinnvoll sind als für Personen ohne IT-Affinität. IT-affine Personen haben in ihrer täglichen Tätigkeit meistens mit Informationssicherheit zu tun und wissen deswegen über das Thema Social Engineering besser Bescheid. Es wurde aber auch erwähnt, dass es kein Fehler ist, auch IT-affine Personen zu schulen.

Aufbau von Security-Awareness-Schulungen

Security-Awareness-Schulungen sollten kontinuierlich abgehalten werden, da sich die Informationssicherheit immer ändert. Dadurch wird zudem verhindert, dass Informationen im Laufe der Jahre in Vergessenheit geraten. Gleichzeitig sollten sie aber auch nicht zu oft durchgeführt werden, da sie eine erhebliche negative Auswirkung auf den Arbeitsfluss der einzelnen Mitarbeiterinnen und Mitarbeiter haben. Die Expertinnen und Experten gaben an, dass eine zyklische Durchführung einmal jährlich sinnvoll ist.

Der Aufbau einer Security-Awareness-Schulung sollte nicht kompliziert und langwierig sein. Die Kurse sollten kurz und effektiv sein sowie mit praktischen Beispielen, am besten mit solchen, die auf Abteilungsebene angepasst werden, ergänzt werden. Es ist entscheidend, dass sich das Personal die wesentlichen Informationen einer Schulung merkt, um das Wissen im Falle eines Angriffes anwenden zu können. Es muss erreicht werden, dass die einzelnen Mitarbeiterinnen und Mitarbeiter selbstständig vorsichtiger und aufmerksamer sind.

Es gibt auch Möglichkeiten, das erlangte Wissen aus einer Security-Awareness-Schulung zu überprüfen. Hier wurden folgende Optionen genannt:

- Eine Security-Awareness-Schulung muss bestanden werden.
- Überprüfung der Informationen mit einem Quiz
- Phishing-Simulation

Es gibt verschiedene Varianten, wie Security-Awareness-Schulungen abgehalten werden können. Auf diese Gestaltungsmöglichkeiten wird später eingegangen.

Technische Maßnahmen gegen Social-Engineering-Angriffe

Es gibt technische und physische Maßnahmen, die einen Social-Engineering-Angriff erschweren, jedoch können sie keine Attacke komplett verhindern. Diese Maßnahmen bewahren die Masse besser vor jeweiligen Angriffen, jedoch bieten sie keinen Schutz für eine einzelne Person selbst. Es gibt keine technischen Maßnahmen, die ausschließlich für den Schutz vor Social Engineering ausgelegt sind. Jedoch ist es immer sinnvoll, Security-Tools einzusetzen. Das Unternehmen muss jeweils die Kosten und den Nutzen gegeneinander abwägen.

Die folgende Auflistung enthält verschiedene technische und physische Maßnahmen, die einen Social-Engineering-Angriff erschweren sollen:

- Mail-Security-Appliances
- Einführung eines Patch- und Vulnerability-Managements
- Blockieren von zwielichtigen URLs
- Blockieren von zwielichtigen Telefonnummern
- Multi-Faktor-Authentication
- Zutrittsregelungen
- Verschlüsselung
- Interne Proxys
- Geo-basierte Zugangskontrollen

Eine zyklische Passwortänderung bietet in Bezug auf den Schutz vor Social-Engineering-Angriffen keinen Mehrwert, denn sollte von der Angreiferin oder dem Angreifer das Passwort herausgefunden werden, wartet sie oder er in den meisten Fällen nicht bis zur nächsten Änderung des Passwortes, bevor der Angriff fortgesetzt wird.

Messung

Es kann gesagt werden, dass Personen ohne Security-Awareness-Schulung deutlich anfälliger sind, Opfer eines Social-Engineering-Angriffs zu werden. Eine Expertin oder ein Experte sagte aus, dass ungeschultes Personal bei einer Spear-Phishing-Simulation eine Fehlerquote zwischen 30 und 60 % hat. Geschultes Personal hat hingegen eine Fehlerquote zwischen 5 und 10 %.

Eine aussagekräftige Messung ist nicht immer möglich, da sich der Betriebsrat oftmals gegen eine unwissentliche Massenüberprüfung ausspricht. Bekommt das Personal jedoch im Vorhinein die Information, dass es überprüft wird, könnte dies das Ergebnis verfälschen. Des Weiteren müssten sich die Mitarbeiterinnen und Mitarbeiter selbstständig melden, wenn sie denken, Opfer eines Angriffs geworden zu sein und es sich nicht um eine Überprüfung durch das Unternehmen handelt, um etwas messbares zu haben.

Eine Messung ist aber grundsätzlich möglich, wenn die Erlaubnis des Betriebsrates eingeholt wird. Eine befragte Person meinte, dass in ihrem Unternehmen selbstständig Phishing-

Simulationen durchgeführt werden. Aufbauend darauf können Key-Perfomance-Indicators (KPIs) definiert werden und damit wäre es messbar, wie erfolgreich eine Security-Awareness-Schulung ist.

Beschwerden

In der Regel beschweren sich die Mitarbeiterinnen und Mitarbeiter nicht über eingesetzte Maßnahmen, denn ein großer Teil hat mittlerweile die Bedeutung der Informationssicherheit erkannt. Es ist aber zu erwähnen, dass beispielsweise Security-Awareness-Schulungen nicht zu oft durchgeführt werden dürfen, denn das würde dem Personal wertvolle Arbeitszeit kosten und hätte im Allgemeinen betrachtet keinen großen Mehrwert. Viele Mitarbeiterinnen und Mitarbeiter beschweren sich zwar nicht über eingesetzte Maßnahmen, aber belächeln sie, weil sie das Thema der Informationssicherheit zwar als bedeutend empfinden, jedoch keinen Bezug zu ihrer Tätigkeit sehen. Deswegen ist es essentiell, dass den Mitarbeiterinnen und Mitarbeitern in einer Security-Awareness-Schulung der Bezug zu ihrer Tätigkeit verdeutlicht wird. Sicherheit ist nicht bequem, aber in der Regel hat das Personal eines Unternehmens im Hinterkopf, dass diese wesentlich ist.

Unterschied zwischen Unternehmen kritischer Infrastruktur und Unternehmen keiner kritischen Infrastruktur

Ein Angriff bzw. eine unautorisierte Informationsweitergabe bei Unternehmen kritischer Infrastruktur kann größere Schäden verursachen als bei Unternehmen keiner kritischen Infrastruktur, weswegen die erste Gruppe einen höheren Schutzbedarf hat. Sinnvoll sind Security-Maßnahmen immer, jedoch ist die Frage zu stellen, ob bei Unternehmen keiner kritischen Infrastruktur dieselben Maßnahmen notwendig sind. Jedes Unternehmen muss sich über die Risiken und die potentiellen Auswirkungen eines Angriffs im Klaren zu sein, wobei bei Unternehmen kritischer Infrastruktur die Risiken höher sind.

Es muss erreicht werden, dass die Mitarbeiterinnen und Mitarbeiter von Unternehmen kritischer Infrastruktur ein höheres Informationssicherheitsgefühl haben als das Personal von anderen Unternehmen. Dies gelingt mit jährlich wiederkehrenden Security-Awareness-Schulungen.

Hypothese 1

Mit den Informationen dieses Kapitels konnte die Hypothese 1 belegt werden, denn alle befragten Expertinnen und Experten erachten Security-Awareness-Schulungen für sinnvoll und für das effektivste Mittel gegen Social-Engineering-Angriffe. Auch wird durch Security-Awareness-Schulungen beim Personal ein höheres Gefühl für die Informationssicherheit erreicht, das bei Unternehmen kritischer Infrastruktur notwendig ist.

5.4 Auswertung der Hypothese 2

In diesem Unterkapitel wird folgende Hypothese überprüft: *„Jährliche Schulungen für Mitarbeiterinnen und Mitarbeiter können als Investition für die Informationssicherheit kritischer Infrastruktur gesehen werden und sparen im Allgemeinen Kosten, wenn die Ausgaben für die Schulung mit jenen infolge eines Vorfalles verglichen werden.“*

Um diese Hypothese testen zu können, werden die Aussagen, die wie folgt kodiert worden sind, genauer betrachtet:

- Kosten eines Social-Engineering-Angriffs
- Wahrscheinlichkeit, Opfer eines Social-Engineering-Angriffs zu werden
- Varianten von Security-Awareness-Schulungen
- Kosten der technischen Maßnahmen gegen Social Engineering

Die folgende Tabelle zeigt einen Ausschnitt der Aussagen für die Prüfung der Hypothese 2. Die komplette Tabelle ist im ANHANG J - ersichtlich.

Ein Angriff kostet der Angreiferin oder dem Angreifer auch Geld, weswegen sich ein Angriff auszahlen soll, entweder monetär oder durch Schädigung	Kosten eines Social-Engineering-Angriffs
Konkrete Zahlen kann man nicht nennen	Kosten eines Social-Engineering-Angriffs
Social-Engineering-Angriffe könnten sogar Menschenleben kosten (Atomkraftwerk, Schwerindustrie, Autonomes Fahren usw.)	Kosten eines Social-Engineering-Angriffs
Viele Angreiferinnen oder Angreifer verlangen 2–5 % des Jahresumsatzes	Kosten eines Social-Engineering-Angriffs
Eine Schulung zahlt sich in Relation zu einem Angriff eigentlich immer aus	Kosten eines Social-Engineering-Angriffs
Die Chance, Opfer eines Social-Engineering-Angriffs zu werden, unterscheidet sich nach Größe und Branche	Wahrscheinlichkeit, Opfer eines Social-Engineering-Angriffs zu werden
Je mehr Intellectual Property ein Unternehmen besitzt, desto höher ist die Chance, Opfer eines Social-Engineering-Angriffs zu werden	Wahrscheinlichkeit, Opfer eines Social-Engineering-Angriffs zu werden
Vor-Ort-Schulungen bleiben dem Personal besser in Erinnerung und sind meistens auch teurer als die anderen	Varianten von Security-Awareness-Schulungen
Es kommt darauf an, welches Sicherheitsniveau ich erreichen will	Varianten von Security-Awareness-Schulungen
Es gibt Online-Kurse oder Klassenraumschulungen	Varianten von Security-Awareness-Schulungen
Es gibt Ad-hoc-Meldungen an den Konzern, falls irgendein Social-Engineering-Ereignis eintritt, damit das Personal gewarnt ist	Varianten von Security-Awareness-Schulungen
Es gibt Klassenraumschulungen, interne und externe Schulungen, E-Learning-Programme und es gibt Live-Schulungen, wo wirklich Angriffe simuliert werden	Varianten von Security-Awareness-Schulungen
Ein Personentag bei einer Klassenraumschulung kostet zwischen 1000 € und 1500 €	Varianten von Security-Awareness-Schulungen
Die Relation ist hier wichtig zu betrachten, denn die Kosten von einem Vorfall sind meistens höher als die Kosten, sich dagegen zu schützen	Varianten von Security-Awareness-Schulungen
Sinnvoll sind Security-Awareness-Schulungen immer, aber notwendig sind sie bei kleinen Unternehmen, mit wenig Bezug zur IT und wenig Budget nicht	Varianten von Security-Awareness-Schulungen

Die Erstellung einer E-Learning-Schulung kostet ca. 10000 € bis 15000 € und dann gehört noch abgeschätzt, wie groß das Unternehmen ist und ob sich dann die Erstellung einer E-Learning-Schulung rentiert	Varianten von Security-Awareness-Schulungen
Diese Kosten sind sehr individuell	Kosten der technischen Maßnahmen gegen Social Engineering
Es gehört beantwortet, welche technischen Maßnahmen in welchem Ausmaß für mein Unternehmen notwendig sind.	Kosten der technischen Maßnahmen gegen Social Engineering
Es gehört eine Risikoabschätzung gemacht, was ein Produkt kostet und wie viel mich in Relation ein Angriff kosten könnte und ob sich dann genau diese technische Maßnahme auszahlen würde	Kosten der technischen Maßnahmen gegen Social Engineering

Tabelle 5: Ausschnitt der Paraphrasen für die Auswertung der Hypothese 2

Kosten eines Social-Engineering-Angriffs

Es kann keine genaue Zahl genannt werden, wie hoch die Kosten eines Social-Engineering-Angriffs sein können. Hier spielen viele Faktoren eine Rolle. Da die Angreiferin oder der Angreifer in den meisten Fällen auch Geld verdienen will, sollte sich ein Angriff immer auszahlen. Deswegen hat es sich etabliert, zwischen 3 und 5 % des Jahresumsatzes eines Unternehmens zu verlangen.

Es sollte bedacht werden, dass ein erfolgreicher Social-Engineering-Angriff existenzbedrohend für ein Unternehmen sein kann und in den schlimmsten Fällen sogar das Leben von Menschen gefährdet, wenn beispielsweise die Wasserversorgung betroffen ist.

Wahrscheinlichkeit, Opfer eines Social-Engineering-Angriffs zu werden

Die Wahrscheinlichkeit, Opfer eines Social-Engineering-Angriffs zu werden, unterscheidet sich stark nach Branche und Größe. Im Vergleich zu kleineren Unternehmen sind größere Unternehmen und Unternehmen kritischer Infrastruktur ein beliebteres Ziel eines Angriffs. Bei diesen ist ein Informationsverlust kritischer und diese Unternehmen sind auch bereit, mehr Geld für die Schadensbegrenzung zu investieren. Ein weiterer wesentlicher Punkt ist die Intellectual Property eines Unternehmens. Je höher diese ist, desto höher ist die Wahrscheinlichkeit, Opfer eines Angriffs zu werden.

Varianten von Security-Awareness-Schulungen

Die folgende Grafik zeigt die verschiedenen Varianten von Security-Awareness-Schulungen mit ihren Vor- und Nachteilen:

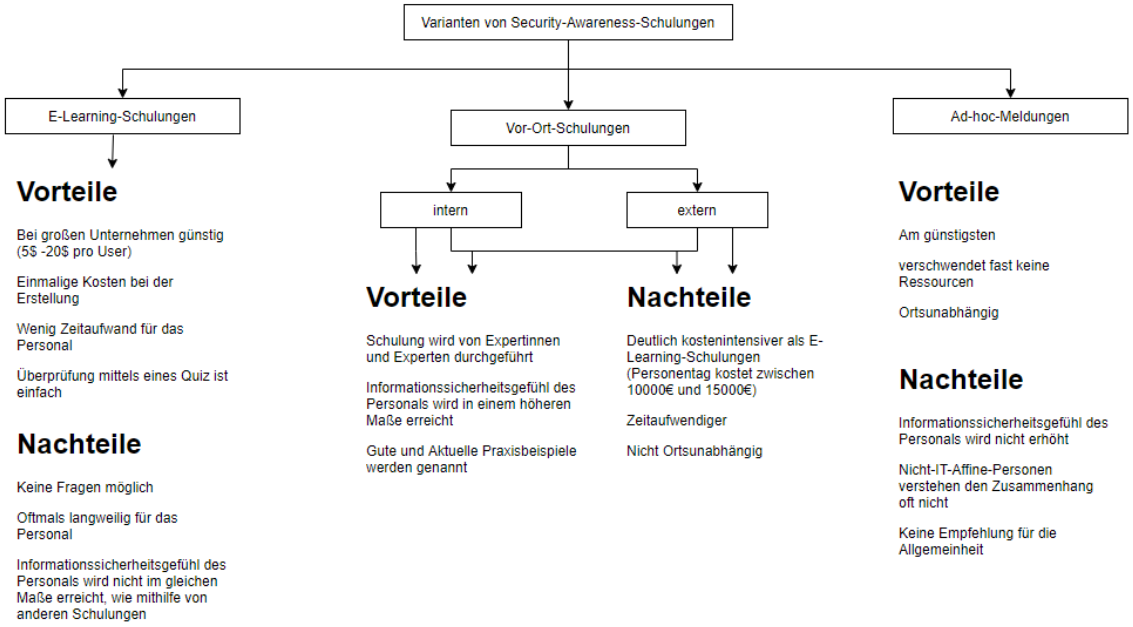

Abbildung 82: Varianten von Security-Awareness-Schulungen

In diesem Zusammenhang ist zu erwähnen, dass immer der mögliche finanzielle Schaden, der durch einen Social-Engineering-Angriff entsteht, und die Kosten einer Security-Awareness-Schulung gegeneinander abgewogen werden müssen. Hier spielen viele Faktoren, wie die Größe des Unternehmens oder die Branche, eine bedeutende Rolle. Im Grunde zahlt sich eine Security-Awareness-Schulung in den meisten Fällen aus. Es gilt zu überprüfen, welche Variante die beste Wahl für ein Unternehmen ist. Ausnahmen, in denen sich eine Security-Awareness-Schulung nicht auszahlt, sind kleine Unternehmen mit wenig Budget und mit wenig Bezug zur IT oder mit ausschließlich IT-affinen Personen in der Belegschaft.

Da Unternehmen kritischer Infrastruktur einen höheren Schutzbedarf benötigen, wird hier eine Vor-Ort-Schulung mit praxisnahen Beispielen empfohlen.

Kosten der technischen Maßnahmen gegen Social Engineering

Es ist schwierig, zu präzisieren, welche Kosten bei den technischen Maßnahmen anfallen. Einerseits gibt es keine technischen Maßnahmen, die ausschließlich darauf ausgelegt sind, Social-Engineering-Angriffe zu verhindern. Andererseits kommt es darauf an, welchen Schutzbedarf ein Unternehmen aufweist. Im Grunde ist es möglich, ausschließlich kostenlose Security-Tools einzusetzen, was aber für Unternehmen kritischer Infrastruktur nicht empfohlen wird. Die Kosten sind hier individuell. Ein Unternehmen muss die Frage beantworten, welche technischen Maßnahmen in welchem Ausmaß notwendig sind.

Hypothese 2

Mit den Informationen dieses Kapitels kann die Hypothese 2 als bewiesen erklärt werden. Alle befragten Expertinnen und Experten erwähnten, dass sich Security-Awareness-Schulungen in der Regel immer auszahlen. Dies gilt vor allem für Unternehmen mit einem erhöhten Schutzbedarf, weil bei diesen die Kosten eines Social-Engineering-Angriffs größere Dimensionen annehmen können.

6 CONCLUSIO UND AUSBLICK

Die relevante Definition von Social Engineering dieser Arbeit lautet: *„Social-Engineering ist die Manipulation von Menschen, damit diese mit freiwillig gegebenen Informationen oder durch von ihnen durchgeführte Aktionen einen Mehrwert für die Interessen der Angreiferin oder des Angreifers liefern.“ (Eigendefinition zusammengefasst aus (Hoss, 2015; Mann, 2008; Mitnick & Simon, 2003)*

In dieser Arbeit hat sich herausgestellt, dass heutzutage die meisten Cyber-Angriffe mit Social Engineering durchgeführt werden. Das passiert vor allem, weil bei einem Angriff auf die psychologische Seite eines Menschen gesetzt wird.

Unten werden Methoden von Social Engineering aufgelistet.

- Pretexting
- Reverse-Social-Engineering
- Tailgaiting
- Phishing
- SMSishing
- Cross-Site-Request-Forgery
- Malware
- Vishing

Es gibt eine Vielzahl an Personen, die Social Engineering durchführen. Es ist nicht immer eine illegale Aktivität. Zum Beispiel setzen Verkäuferinnen oder Verkäufer psychologische Tricks ein, um jemanden vom Kauf eines Produktes zu überzeugen, was einen Mehrwert für die Verkäuferin oder den Verkäufer bringt, aber nicht illegal ist.

Eine Umfrage hat ergeben, dass die eingesetzten Maßnahmen, wie Security-Awareness-Schulungen oder die Multi-Faktor-Authentication, in der Regel keinen erheblichen negativen Einfluss auf die Arbeitstätigkeit haben. Des Weiteren ging aus der Umfrage hervor, dass es in Bezug auf das Verständnis der eingesetzten Maßnahmen keinen signifikanten Unterschied zwischen IT-affinen Personen und Personen ohne IT-Affinität gibt. IT-affine Personen wissen lediglich besser über das Thema der Informationssicherheit Bescheid.

Die qualitative Analyse hat ergeben, dass sich das Thema der Informationssicherheit in letzter Zeit dahingehend verändert hat, dass mittlerweile der Großteil der Personen über das Thema Bescheid weiß und auch die Auswirkungen eines Angriffs kennt. Deswegen wird in der Regel auch mehr Budget für Security eingeplant. Security-Awareness-Schulungen werden in den meisten Fällen empfohlen, da diese im Vergleich mit den möglichen Kosten eines Social-Engineering-Angriffs günstiger sind. Es gilt abzuwägen, auf welche Variante ein Unternehmen

setzt, wie viel ein Unternehmen für Security-Awareness-Schulungen ausgeben möchte und wie hoch die Wahrscheinlichkeit ist, Opfer eines Social-Engineering-Angriffs zu werden. Es gibt zusätzlich noch technische und physische Maßnahmen, die einen Social-Engineering-Angriff erschweren können. Dies bezieht sich jedoch nur auf die Masse und nicht auf die einzelne Userin oder den einzelnen User. Solche Maßnahmen sind aber dennoch sinnvoll.

Die unten aufgelisteten Maßnahmen müssen ergriffen werden, um die Informationssicherheit von Unternehmen kritischer Infrastruktur im Kontext von Social Engineering zu gewährleisten. Diese Maßnahmen haben im Allgemeinen keinen beträchtlichen Mehraufwand für die Mitarbeiterinnen und Mitarbeiter zur Folge.

- Einführung von Vor-Ort-Security-Awareness-Schulungen
- Auffrischung von Security-Awareness-Schulungen einmal jährlich
- Überprüfung des Wissens nach einer Security-Awareness-Schulung
- Der Aufbau einer Security-Awareness-Schulung muss unkompliziert und verständlich für alle sein.
- Eine Security-Awareness-Schulung muss verständliche Praxisbeispiele beinhalten. Am besten sind solche Beispiele, die jede Mitarbeiterin oder jeder Mitarbeiter aus dem jeweiligen Tätigkeitsbereich kennt.
- Physische Maßnahmen, wie Zutrittsregelungen, müssen eingesetzt werden und die Autorisierung einzelner Mitarbeiterinnen und Mitarbeiter muss auf ein Minimum beschränkt werden.
- Technische Maßnahmen, wie Mail-Filter, Multi-Faktor-Authentication, Zugriffsregelungen auf ein Minimum setzen sowie das Blockieren von zwielichtigen URLs und zwielichtigen Telefonnummern
- Einführung eines Patch- und Vulnerability-Managements

Damit ist die folgende Forschungsfrage beantwortet: *„Welche Initiativen müssen gesetzt werden, um die Informationssicherheit von Unternehmen kritischer Infrastruktur im Kontext Social Engineering zu gewährleisten, ohne einen beträchtlichen Mehraufwand für Mitarbeiterinnen und Mitarbeiter zu verursachen?“*

Offen bleibt das Überprüfen dieser Initiativen, ob diese tatsächlich bei einem Unternehmen kritischer Infrastruktur einen Erfolg bei der Informationssicherheit im Kontext von Social Engineering bringen. Dies könnte getestet werden, indem zwei ähnliche Unternehmen kritischer Infrastruktur – eines mit geschultem Personal und eingesetzten technischen Maßnahmen und eines ohne die oben genannten Initiativen – selbstständig ihre Mitarbeiterinnen und Mitarbeiter mit Social Engineering attackieren und die Ergebnisse im Anschluss verglichen werden.

ANHANG A - Umfrage

Fragen, die von den teilnehmenden Personen ausgefüllt werden müssen, werden mit einem * dargestellt.

Einleitung

Vielen Dank, dass Sie die Zeit finden an dieser Umfrage teilzunehmen. Der Sinn dieser Umfrage besteht darin herauszufinden, wie Mitarbeiterinnen und Mitarbeiter eingesetzte Maßnahmen zur Gewährleistung der Informationssicherheit finden und ob diese die Effizienz des Arbeitsflusses erheblich beeinflussen. Es soll ebenso das Sicherheitsempfinden der einzelnen Mitarbeiterinnen und Mitarbeiter gemessen werden.

Mit den Ergebnissen dieser Umfrage werden Interviews mit Expertinnen und Experten durchgeführt. Im Anschluss wird mit den transkribierten Interviews eine qualitative Inhaltsanalyse durchgeführt, um einen Leitfaden für die Gewährleistung der Informationssicherheit von Unternehmen kritischer Infrastruktur zu erstellen. Die Effizienz des Arbeitsflusses der einzelnen Mitarbeiterinnen und Mitarbeiter soll durch die empfohlenen Maßnahmen des Leitfadens jedoch nicht, wenn nicht unbedingt nötig, zu stark negativ beeinflusst werden.

Diese Umfrage ist anonym und es werden keine Rückschlüsse auf einzelne Personen/Unternehmen gezogen.

Frage 1

Wie alt sind Sie? *

- Eigenschaften: Einzelnennung
- Antwortmöglichkeiten:
    - Unter 18 Jahre
    - 18 - 30 Jahre
    - 31 – 50 Jahre
    - 51 – 65 Jahre
    - Über 65 Jahre

Frage 2

Sind Sie aktuell berufstätig? *

- Eigenschaften: Einzelnennung
- Antwortmöglichkeiten:
    - Ja
    - Nein

Frage 3

Wie viele Angestellte weist das Unternehmen, in dem Sie angestellt sind, auf? *

- Eigenschaften: Einzelnennung
- Antwortmöglichkeiten:
    - 0 - 10
    - 11 - 50
    - 51 - 250
    - 250 – 1000
    - Über 1000
    - Nicht berufstätig
    - Gerade in Karenz oder Papamonat, aber anschließende Rückkehr geplant

Frage 4

Ist das Unternehmen, in dem sie angestellt sind, als kritische Infrastruktur gekennzeichnet? *
Kritische Infrastruktur bedeutet, dass das Unternehmen essentiell für den Systemerhalt ist. Beispiele hier sind Elektrizitätsversorgungsunternehmen, Wasserversorgung, etc.)

- Eigenschaften: Einzelnennung
- Antwortmöglichkeiten:
    - Ja
    - Nein

Frage 5

Würden Sie sich als IT-Begeistert bezeichnen? *

- Eigenschaften: Einzelnennung
- Antwortmöglichkeiten:
    - Ja
    - Nein

Frage 6

Haben Sie Verantwortung gegenüber anderen Personen oder sind Sie als Führungskraft tätig? *

- Eigenschaften: Einzelnennung
- Antwortmöglichkeiten:
    - Ja
    - Nein

Frage 7

Haben Sie Zugriff zu sicherheitsrelevanten Informationen, wie personenbezogene Daten, sensiblen Informationssystemen oder andere? *

Sicherheitsrelevante Informationen sind beispielsweise personenbezogene Daten, wie Arbeitszeiten, Gehalt, Adressen von Personen, etc. oder der Zugriff auf Informationssystemen/Programme welche essentiellen Daten des Unternehmens preisgeben. Ebenso sind Passwörter, Arbeitspläne, Pläne von Räumen oder IP-Adressen und vieles mehr sicherheitsrelevante Informationen.

- Eigenschaften: Einzelnennung
- Antwortmöglichkeiten:
    - Ja
    - Nein

Hypothese 3

In diesem Bereich soll folgende Hypothese überprüft werden:

„Mitarbeiterinnen und Mitarbeiter, die keine hohe IT-Affinität haben, kennen die Auswirkungen eines Social-Engineering-Angriffs und der daraus entstehenden Nebenwirkungen nicht.“

Frage 8

Wie würden sie Ihre Kenntnisse in der IT einschätzen? *

- Eigenschaften: Einzelnennung
- Antwortmöglichkeiten:
    - Keine IT-Affinität (Standardbenutzerin oder Standardbenutzer, Nutzung hauptsächlich von Office-Anwendungen bzw. Internet-Surfing)
    - Mittlere IT-Affinität (fortgeschrittene Benutzerin oder fortgeschrittener Benutzer, Bau von kleineren Lösungen im Heimnetzwerk, geringe Scripting- und Programmier-Kenntnisse, Umgang mit dem Betriebssystem Linux)
    - Hohe IT-Affinität (Expertin oder Experte in der IT, Bau von großen Lösungen, Hacking, große Programmierkenntnisse

Frage 9

Wie erlernten sie Ihre Kenntnisse der IT? *

- Eigenschaften: Mehrfachnennung
- Antwortmöglichkeiten:
    - Keine Kenntnisse
    - Schulungen
    - Selbststudium durch Eigeninteresse
    - Ausbildung
    - Zertifizierungen

Frage 10

Wie würden Sie persönlich die Wichtigkeit von Sicherheit und Effizienz in Bezug zueinander einstufen? *

- Eigenschaften: Einzelnennung
- Antwortmöglichkeiten:
    - Sicherheit ist sehr relevant und das wichtigste
    - Sicherheit ist eher wichtiger als die Effizienz
    - Effizienz ist eher wichtiger als die Sicherheit
    - Effizienz ist sehr relevant und das wichtigste

Frage 11

Hatten Sie schon einmal mit Nebenwirkungen eines erfolgreich durchgeführten Social-Engineering-Angriff zu tun und, oder wissen Bescheid welchen Schaden ein solcher Angriff hervorrufen kann? *

Bei Social Engineering handelt es sich um ein Verfahren, um sicherheitstechnisch relevante Daten durch das Ausnutzen menschlichen Verhaltens zu gewinnen. Dabei wählt der Täter den Menschen als vermeintlich schwächtes Glied der Sicherheitskette aus, um seine Absichten in die Tat umzusetzen. (Quelle: Wikipedia)

Ein einfach betrachtetes Beispiel wäre, wenn man nach einer Bestellung einer Fast-Food-Kette zu einer Mitarbeiterin bzw. einem Mitarbeiter geht und sagt, dass bei dieser Bestellung eine Portion Pommes fehlen würde. Bekommt man im Anschluss diese Portion Pommes, dann war der Angriff erfolgreich. Dieses Beispiel dient nur zur Veranschaulichung. Social Engineering Angriffe können viel größer gestrickt sein und auch viel mehr Schaden verursachen.

- Eigenschaften: Einzelnennung
- Antwortmöglichkeiten:
    - Ich habe keine Kenntnisse darüber, was ein Social-Engineering-Angriff hervorrufen kann
    - Ich habe schon von ein paar Social-Engineering-Angriffen gehört und kenne so ungefähr die Auswirkungen davon
    - Ich habe mit den Nebenwirkungen eines Social-Engineering-Angriffs noch nie zu tun gehabt, jedoch kenne ich sehr genau, welche Auswirkungen verursacht werden können
    - Ich hatte schon mit den Auswirkungen eines Social-Engineering-Angriffs zu tun

Hypothese 4

In diesem Bereich soll folgende Hypothese überprüft werden:

„Mitarbeiterinnen und Mitarbeiter halten Einführungen von Regeln, die Social-Engineering-Angriffe verhindern sollen (zum Beispiel, dass ein Telefongespräch nicht weitergeleitet werden darf oder das Ändern des Passwortes in zyklischen Abständen) für einen Mehraufwand und unpraktisch.“

Frage 12

Gab es im Unternehmen, in dem Ihr beschäftigt seit Security-Awareness-Schulungen (Schulungen, die auf die Gefahren von einem Informationsverslust hindeuten und wie dieser verhindert werden kann) und wenn ja, werden diese zyklisch abgehalten? *

Security-Awareness-Schulungen sind Schulungen, die Personen aufklären, wie Angriffe durchgeführt werden können bzw. wie diese verhindert werden können.

Ein Beispiel wäre hier, dass die Mitarbeiterinnen und Mitarbeiter einer Fast-Food-Kette in einer Schulung aufgefordert werden, im Falle einer Beschwerde, dass bei der Bestellung ein Produkt fehlen würde, immer die Rechnung zu verlangen

- Eigenschaften: Einzelnennung
- Antwortmöglichkeiten:
    - Es gab keine Security-Awareness-Schulungen bzw. mir nicht bekannt
    - Es gab einmal eine Security-Awareness-Schulung
    - Wird zyklisch vollumfänglich abgehalten
    - Nach einmaliger Schulung werden nur die wichtigsten Punkte zyklisch aufgefrischt

Frage 13

Welche anderen Maßnahmen zur Gewährleistung der Informationssicherheit werden von Ihrem Unternehmen eingesetzt? *

- Eigenschaften: Mehrfachnennung
- Antwortmöglichkeiten:
    - Zugriffs- und/oder Zutrittsrechte zu wichtigen Räumen oder Programmen werden auf ein Minimum beschränkt (Privileged-Access-Management)
    - Der Login in ein Programm ist nur mit einem weiteren Faktor möglich. Zum Beispiel Passwort und SMS (Multi-Faktor-Authentifizierung)
    - Gewisse Freigaben oder Durchführungen sind nur durch die Zustimmung von mindestens zwei Personen möglich (Duale Kontrollsysteme)
    - Meldungen bzw. Alarme werden an ein Programm gesendet, wenn sich beispielsweise jemand wo eingeloggt hat oder jemand einen Raum betreten hat (Überwachung privilegierter Aktivitäten)
    - Keine der genannten

Frage 14

Wie stark wird die Effizienz ihrer Arbeitstätigkeit durch eingesetzte Maßnahmen negativ beeinflusst? *

- Eigenschaften: Bewertungsmatrix zur Einschätzung der Beeinflussung der Effizienz in Bezug zur Informationssicherheit
- Skalenniveau:
    - Sehr beeinflusst
    - Eher beeinflusst
    - Wenig beeinflusst
    - Nicht beeinflusst
    - Nicht beurteilbar/nicht passend
- Antwortmöglichkeiten
    - Zugriffs- und/oder Zutrittsrechte zu wichtigen Räumen oder Programmen werden auf ein Minimum beschränkt (Privileged-Access-Management)
    - Der LogIn in ein Programm ist nur mit einem weiteren Faktor möglich. Zum Beispiel Passwort und SMS (Multi-Faktor-Authentifizierung)
    - Gewisse Freigaben oder Durchführungen sind nur durch die Zustimmung von mindestens zwei Personen möglich (Duale Kontrollsysteme)
    -

Frage 15

Geben Sie an, wie wichtig sie die eingesetzten Maßnahmen finden? *

- Eigenschaften: Bewertungsmatrix zur Einschätzung der Wichtigkeit über Sicherheitsmaßnahmen
- Skalenniveau:
    - Sehr wichtig
    - Eher wichtig
    - Weniger wichtig
    - Nicht wichtig
    - Nicht beurteilbar/nicht passend
- Antwortmöglichkeiten
    - Zugriffs- und/oder Zutrittsrechte zu wichtigen Räumen oder Programmen werden auf ein Minimum beschränkt (Privileged-Access-Management)
    - Der LogIn in ein Programm ist nur mit einem weiteren Faktor möglich. Zum Beispiel Passwort und SMS (Multi-Faktor-Authentifizierung)
    - Gewisse Freigaben oder Durchführungen sind nur durch die Zustimmung von mindestens zwei Personen möglich (Duale Kontrollsysteme)
    - Meldungen bzw. Alarme werden an ein Programm gesendet, wenn sich beispielsweise jemand wo eingeloggt hat oder jemand einen Raum betreten hat (Überwachung privilegierter Aktivitäten)

Abschluss

Dieser Bereich des Fragebogens soll klären, ob die teilnehmenden Personen diesen auch verstanden haben und auch richtig auf ihre Person selbst ausgefüllt haben. Wird der Fragebogen von einzelnen Teilnehmerinnen und Teilnehmer nicht verstanden oder wurde die Auswahl der Fragen von gewissen Personen zufällig ausgefüllt, so müssen diese für die weitere Analyse entfernt werden, damit keine Verfälschung stattfindet.

Frage 16

Hatten Sie Probleme bzw. waren Sie unsicher bei der Beantwortung einiger Fragen (wenn ja, bitte im Textfeld das unverständliche Eintragen)? *

- Eigenschaften: Einzelnennung
- Antwortmöglichkeiten:
    - Ja
    - Nein

Frage 17

Haben sie den Fragebogen nach bestem Wissen und Gewissen, richtig auf ihre Person bezogen, ausgefüllt? *

- Eigenschaften: Einzelnennung
- Antwortmöglichkeiten:
    - Ja
    - Nein

Frage 18

Wurden Sie beim Ausfüllen des Fragebogens von Dritten beeinflusst? *

- Eigenschaften: Einzelnennung
- Antwortmöglichkeiten:
    - Ja
    - Nein

ANHANG B - Leitfaden

Einleitung

- **Forschungsfrage**
  - Welche Initiativen müssen gesetzt werden, um die Informationssicherheit von Unternehmen kritischer Infrastruktur im Kontext Social Engineering zu gewährleisten, ohne einen beträchtlichen Mehraufwand für Mitarbeiterinnen und Mitarbeiter zu verursachen?
- **Einstieg**
  - Begrüßung und Dank für die Zeit
  - Kurzer Umriss des Themas
  - Kurze Beschreibung des Interviewablaufs und der ungefähren Dauer
  - Datenschutzvereinbarung
- **Einstiegsfragen**
  - Wie lange haben Sie schon mit Informationssicherheit zu tun?
    Rückfragen:
    - Wie hat es sich seitdem verändert?
    - Welchen Einfluss hat Social-Engineering hierbei?
  - Was gehört zu Ihren täglichen Aufgaben und besteht hier auch eine Verbindung zu Social-Engineering?
    Rückfragen:
    - Beschreiben Sie bitte diese Verbindung zu Social-Engineering genauer
  - Welche Personengruppe ist am meisten für Social-Engineering-Angriffe gefährdet?
    Rückfragen:
    - Warum genau diese Personengruppe?

Schlüsselfragen

- **Hypothese 1: „Jährliche Schulungen für Mitarbeiterinnen und Mitarbeiter im Kontext des Social Engineerings haben einen positiven Einfluss auf die Informationssicherheit von kritischen Infrastrukturen.“**
  - Erachten Sie solche Schulungen für sinnvoll?
    Rückfragen:
    - Wenn ja, warum?
    - Wenn nein, warum?
  - Werden aktuell solche Security-Awareness-Schulungen bei Ihnen im derzeitigen Unternehmen eingesetzt oder wurden solche Schulungen in Ihren vergangenen Unternehmen eingesetzt?
  - Kann gemessen werden, ob solche Schulungen erfolgreich sind?
  - Testet die Security-Abteilung-selbstständig die Mitarbeiterinnen und Mitarbeiter mit Social-Engineering-Angriffe?

Rückfragen:

- Wie erfolgreich wären solche Tests ohne eine Security-Awareness-Schulung im Gegensatz zu solchen mit Security-Awareness-Schulungen?

- Wie sieht der Aufbau einer Security-Awareness-Schulung aus?
- Gibt es noch andere, technische Maßnahmen, um einen Social-Engineering-Angriff zu erschweren?

Rückfragen:

- Erläutern Sie bitte die anderen Maßnahmen genauer
- Wie sinnvoll empfinden Sie diese Maßnahmen?
- Kann es in einzelnen Szenarien, wie in einem Unternehmen kritischer Infrastruktur, sinnvoll sein, Maßnahmen einzusetzen, die in anderen, nicht kritischen Infrastrukturen, nicht notwendig wären?

- Beschweren sich bereits Mitarbeiterinnen und Mitarbeiter, dass solche Schulungen einen erheblichen negativen Einfluss auf den Arbeitsfluss haben?

- **Hypothese 2: „Jährliche Schulungen für Mitarbeiterinnen und Mitarbeiter können als Investition für die Informationssicherheit kritischer Infrastruktur gesehen werden und sparen im Allgemeinen Kosten, wenn die Ausgaben für die Schulung mit jenen infolge eines Vorfalles verglichen werden.“**
  - Gibt es verschiedene Varianten von Security-Awareness-Schulungen?

    Rückfragen:

    - Wie unterscheiden sich diese in den jährlich anfallenden Kosten?
    - Kann folgendes pauschal gesagt werden?“Jje teurer eine Security-Awareness-Schulung, desto besser ist die Informationssicherheit eines Unternehmens geschützt.“
  - Wie hoch können die Kosten eines Social-Engineering-Angriff werden?

    Rückfragen:

    - Wie hoch ist die Chance, Opfer eines Social-Engineering-Angriffs zu werden und unterscheidet sich diese auch je nach Sparte und Größe des Unternehmens?
  - Wie hoch können die jährlichen Kosten einer Security-Awareness-Schulung werden?

    Rückfragen:

    - Gibt es Fälle, in dem sich Security-Awareness-Schulungen nicht auszahlen? Wenn ja, was wären diese?
  - Wie hoch sind die jährlichen Kosten für technische Maßnahmen, die einen Social-Engineering-Angriff ebenfalls erschweren soll?

    Rückfragen:

    - Gibt es technische Maßnahmen, die nur darauf ausgelegt sind, Social-Engineering-Angriffe zu erschweren und wenn ja, welche sind diese?

Abschluss

- Rückblick
  - Kurze Zusammenfassung des Gesagten
  - Erneuter Dank für die Zeit
- Ausblick
  - Information über Auswertung der Ergebnisse
  - Verabschiedung

Dieser Leitfaden dient nur als Hilfestellung. Eine genaue und chronologische Einhaltung des Leitfadens ist nicht notwendig.

ANHANG C - Experteninterview – Experte 1

MG: Vielen Dank einmal, dass Sie sich Zeit für diese Experteninterview nehmen. Im Endeffekt geht es bei diesem Interview darum die Forschungsfrage: "Welche Initiativen müssen gesetzt werden, um die Informationssicherheit von Unternehmen kritischer Infrastrukturen im Kontext Social-Engineering zu gewährleisten, ohne einen beträchtlichen Mehraufwand für Mitarbeiterinnen und Mitarbeiter zu verursachen. Ähh, Ich habe auch bereits begonnen mit der quantitiven bzw. der Umfrage, die ausgesendet wurde, ist auch schon fertig. Hier fehlt lediglich noch die Auswertung der Daten. Hier wurden Unternehmen quer durch die Bank ausgewählt und es wurde eine Anzahl von ca. 200 Beantwortungen erreicht. Damit wollte ich eben herausfinden, welche Maßnahmen die einzelnen Mitarbeiterinnen und Mitarbeiter auf die Nerven geht. Und jetzt will ich halt mit den Experteninterview abklären, ob das irgendwie passend ist und ob gewisse Maßnahmen unbedingt notwendig sind. Das Interview wird so ablaufen und es beginnt mit dem Einstieg, was jetzt gerade durchgeführt wird, nämlich mit den Einstiegsfragen. Im Anschluss kommen die Schlüsselfragen, die die Hypothesen überprüfen sollen und zum Schluss kommt der Abschluss mit einer kurzen Zusammenfassung und einem Ausblick, wie mit den analysierten Daten dann weitergearbeitet wird. Das Interview wird so ca. 30-40 Minuten dauern. Und die Datenschutzvereinbarung wurde bereits durchgegangen, damit eine Aufnahme entstehen darf. Verwendet wird diese Aufnahme ausschließlich für die Arbeit und wie bereits erwähnt, wenn gewünscht wird das Ganze auch anonymisiert. Dann werde ich jetzt mit den Einstiegsfragen beginnen und die erste Frage lautet: "Wie lange haben Sie mit Informationssicherheit schon zu tun?"

E1: Ca. 10 Jahre

MG: Ah, wie sind Sie zu diesem Bereich gekommen?

E1: Immer schon Interesse in diese Richtung gehabt, dann studiert und begonnen Tätigkeiten in diesem Bereich in Unternehmen zu machen und das mache ich jetzt schon länger und deckt auch meine Interessen.

MG: Wie hat sich das in den letzten 10 Jahren verändert? Gibt es noch Faktoren die gleich sind oder ändert sich das immer.

E1: Also, im Großen und Ganzen muss man sagen, dass die Aufmerksamkeit was Cyberrisiko, Informationssicherheit, etc. endlich beim Top-Management angekommen ist. Das hat vor 10 Jahren dort so gut wie niemanden noch interessiert. In letzter Zeit ist auch viel, durch die Digitalisierung, durch Hackerangriffe, etc. passiert und dadurch bekommt das Thema immer einen höheren Stellenwert. Das Ganze geht jetzt auch noch immer weiter, dass eben auch viele Zeitungen darüber berichten und weil diese auch auf diese Schiene aufgesprungen sind, wissen normale Personen und normale Mitarbeiterinnen und Mitarbeiter über dieses Thema besser Bescheid und wissen das es dieses Thema und diese Gefahren gibt.

MG: Ähmm, welchen Einfluss hat Social-Engineering hierbei?

E1: Ahh, im Großen und Ganzen einen sehr, sehr großen. Zum einen haben wir mit Social-Engineering einen Einfallsvektor, wie man in ein Unternehmen reinkommen könnte, wie man gewisse Sachen einfach nachfragt und Mitarbeiterinnen und Mitarbeiter dann einfach weiterhelfen, vermeintlich weiterhelfen. Ähm und man kennt es ja aus der Vergangenheit, die Geschichte mit Social-Engineering, der klassische Enkeltrick. Hier bringt man vermeintlich alte Menschen um ihr Erspartes bringt, weil man irgendeine Geschichte vorlügt. Das Ganze ist halt mit der digitalen Welt weitergegangen, dass man mit Social-Engineering eben versucht Passwörter abzufragen oder in Kombination mit Phishing-Mail zuerst das Phishing-Mail aussendet, dann den entsprechenden Mitarbeiter dem dieses Mail geschickt wurde, gleich anruft und den dann durch irgendeine Social-Engineering-Kampagne die man sich überlegt hat, den Mitarbeiter dazu bringt irgendwas in dem Mail anzuklicken bzw. aufgrund des Sachverhaltes der gesendet wurde, einfach Fragen zu stellen und der Mitarbeiter plaudert dann Geschäftsgeheimnisse aus oder macht irgendwas, was der Angreifer haben möchte. Ja, Social-Engineering wird auch immer interessanter für Kriminelle und deswegen steigt hier auch das Interesse stark mit.

MG: Okay, dann hast du die nächste Frage teilweise schon ein bisschen beantwortet. Was gehört zu deinen täglichen Aufgaben und wie arg ist die Verbindung zu Social-Engineering?

E1: Ah, Es gibt klassische Lehrbuchmethoden, wie man Social-Engineering entgegenwirkt, das fängt an mit Kursen, Online-Kursen, Klassenraumschulungen. Das geht weiter bis hin zu durchgeführte Social-Engineering-Angriffe vom Security-Team eines Konzerns auf die Mitarbeiter oder von externem Beauftragen. Was wir im Unternehmen machen, sind eher die Arten, die die Mitarbeiter nicht permanent mit Schulungen, etc. Belästigen. Das heißt Mitarbeiter werden einfach regelmäßig in Hinsicht Informationssicherheit allgemein geschult und ein Teil davon ist auch Social-Engineering und Phishing. Ähm, was wollte ich jetzt sagen. Und es gibt jetzt noch Ad-hoc Meldungen, falls irgendwann etwas auftritt, dass die Mitarbeiterinnen und Mitarbeiter einfach gewarnt sind. Aber man will das Ganze auf einem gesunden Mittelweg machen und die Mitarbeiter nicht überfrachten mit Trainings, etc. Das muss halbwegs dezent ablaufen, damit sie auch Zeit haben zu arbeiten und nicht nur Informationssicherheitsschulungen durchführen müssen. Es gibt neben Informationssicherheit auch noch eine Vielzahl weiterer Dinge auf, die die Mitarbeiterinnen und Mitarbeiter geschult werden müssen.

MG: Okay danke, wir kommen eh später noch genauer auf diese Thematik zu. Gibt es eine spezielle Personengruppe, die besonders anfällig sind für Social-Engineering-Angriffe?

E1: Ich würde hier sagen, dass grundsätzlich jede Personengruppe anfällig ist auf Social-Engineering. Man muss nur wissen, wie man mit der jeweiligen Personengruppe interagiert, damit diese irgendwelche Informationen weitergeben. Und natürlich ein Mitarbeiter, der sehr hilfsbereit ist, wird man am einfachsten ausnutzen können, dass er was preisgibt, ohne dass man sich jetzt tiefer mit Psychologie beschäftigen muss. Mit der richtigen Technik bekommt man von jeder Personengruppe die Informationen, die man will.

MG: Okay danke, dann kommen wir nun zu den Schlüsselfragen. Beginnen wir mal mit der ersten Hypothese: "Jährliche Schulungen für Mitarbeiterinnen und Mitarbeiter im Kontext Social-Engineering haben einen positiven Einfluss auf die Informationssicherheit von kritischen

Infrastrukturen." Die erste Frage lautet hier: „Erachten Sie Security-Awareness-Schulungen für sinnvoll und wenn ja, warum?"

E1: Ja, die erachte ich als sehr sinnvoll, da hier das Thema an Mitarbeiterinnen und Mitarbeiter einfach kontinuierlich ins Bewusstsein gerufen wird und somit die Mitarbeiter im Falle eines Angriffs im Hinterkopf haben, okay ja, da war etwas, das haben wir in der Schulung bereits gehört. Diese Person verhält sich jetzt so ähnlich und das könnte kritisch sein. Ich gebe die Information über den Anruf besser an unsere Security-Abteilung weiter.

MG: Also solche Security-Awareness-Schulungen werden auch aktuell auch in Ihrem Unternehmen eingesetzt.

E1: Ja

MG: Kann gemessen werden, ob solche Schulungen erfolgreich sind?

E1: Ja kann gemessen werden. Man kann es so messen, dass man die Mitarbeiterinnen und Mitarbeiter im Nachgang einer solchen Schulung einen Social-Engineering-Angriff aussetzt, die halt vom Unternehmen selbst gesteuert werden und hier kann man eben KPIs definieren, wie viele Mitarbeiter sind reingefallen, wie viele haben sofort das Gespräch beendet, etc.

MG: Wie werden solche Security-Awareness Schulungen durchgeführt? Werden sie zyklisch durchgeführt, einmalig oder muss es jede Mitarbeiterin und jeder Mitarbeiter nur einmal beim Eintritt ins Unternehmen machen?

E1: So von einmaligen Schulungen halte ich grundsätzlich nichts, da diese in der Regel immer in Vergessenheit geraten, vor allem wenn Personen länger als 10 Jahren in einem Unternehmen angestellt sind. Wie bereits erwähnt, ändert sich die Informationssicherheit immer und nach einer Zeit vergisst man einfach das meiste wieder und es gehört aufgefrischt. Jährliche Schulungen sind einfach besser, um das wesentliche wieder kurz ins Gedächtnis rufen zu können.

MG: Die nächste Frage, die kommt, haben Sie bereits kurz einmal angeschnitten. Die Security-Abteilung von gewissen Unternehmen führt selbstständig solche Social-Engineering-Angriffe durch. Macht das ihr Unternehmen auch oder werde Dritte beauftragt?

E1: Wir machen das im Unternehmen nicht. Meine Antwort auf die vorherige Frage sagte lediglich aus, wie so etwas gemessen werden kann. Wir führen keine Massentests durch, weil das eben auch die Mitarbeiter zu sehr belasten würde, wenn jeder Schulungsinhalt auf eine Art und Weiße geprüft wird. Bei uns werden lediglich Dritte beauftragt, um einzelne Szenarien zu testen, aber eben keine Massentests.

MG: Wie erfolgreich wäre so ein Angriff bei Personen ohne einer Security-Awareness-Schulung im Gegensatz zu Personen mit einer Security-Awareness-Schulung?

E1: Das ist schwierig pauschal zu sagen, aber ich würde sagen, dass die Erfolgsquote von ungeschultem Personal sehr hoch ist. Man findet diesbezüglich einige Beispiele in Fachliteraturen, dass es eine signifikante Tendenz der Erfolgsquote nach unten gibt, wenn die Mitarbeiterinnen und Mitarbeiter regelmäßig geschult werden.

MG: Gibt es noch andere, eventuell technische Maßnahmen, um einen Social-Engineering-Angriff zu erschweren?

E1: Ja, gibt es. Man fängt an, indem man vernünftige Mail-Security-Appliances installiert, wo von Haus aus sämtlicher Spam, sämtliche suspicious Absender einfach rausgefiltert werden. Man kann ähnliches auch im Bereich der Mobiltelefonie machen, dass einfach Telefonnummern mit einer schlechten Reputation automatisch einfach geblockt werden. Was man zu den ganzen technischen Geschichten sagen muss, ist dass diese nur gewisse Massensachen abwehren, also gezielte Angriffe wird man mit solchen Lösungen nie sofort erschlagen.

MG: Gibt es technische Maßnahmen, die nicht so sinnvoll wären, denn die Passwortänderung zum Beispiel fällt oftmals in die Kritik, dass das so oft geschehen muss?

E1: Hinsichtlich Social-Engineerings muss ich sagen bringt ein Passwort-Reset nicht sonderlich viel, weil wenn man sich ansieht, wie Social-Engineering funktioniert wird das klar. Man versucht mittels eines Gesprächs oder mittels Phishing-Mails, etc. an Informationen, wie jetzt das Passwort zu kommen, dann wird das ja unmittelbar nach Erlangen der Informationen benutzt und nur in den seltensten Fällen wird ein Monat gewartet, um weiter zu agieren. Abgezielt auf rein Social-Engineering bringt es nicht sonderlich viel. Abgezielt darauf, dass jetzt zum Beispiel ein Mitarbeiter ein Passwort auf anderen Seiten verwendet, um sich zu registrieren und dieser Service wird zum Beispiel gehackt, dann bringt die zyklische Änderung schon was, denn dann ist die Wahrscheinlichkeit einfach höher, dass das Passwort bereits geändert ist.

MG: Also sind Sie der Meinung, dass eine monatliche Änderung nicht sinnvoll ist, dass der Abstand auch zu gering ist?

E1: Ja es stimmt, dass eine monatliche Änderung nicht mehr empfohlen wird, aber es gibt einen Haken. Das funktioniert nur dann, wenn man sich sicher sein kann, dass die einzelnen Mitarbeiterinnen und Mitarbeiter ihr Firmenpasswort privat nirgends verwenden. Wenn man das Ausschließen kann bzw. die vernünftigen Services, wie zum Beispiel von Microsoft nutzt, die überprüfen, ob der Passwort-Hash des Unternehmenspasswort auf irgendeiner geleakten Website mit Passwörtern auch vorgekommen ist und sperren dann den User, dann ist diese empfohlene Änderung nach 6 Monaten korrekt, ansonsten nicht. Ein anderes Szenario wo eine seltenere Änderung auch sinnvoller wäre, ist es, wenn es bereits eine flächendeckende 2-Faktor-Authentifizierung im Unternehmen gibt. Das Thema ist einfach, dass es nur schwer sichergestellt werden kann, dass Mitarbeiterinnen und Mitarbeiter dasselbe Passwort auf Online-Seiten auch benutzen, obwohl es verboten ist. Wie gesagt, hier ist ein öfterer Wechsel sinnvoll. Es sind auch schon sehr oft Data-Bridges aufgetaucht, wo große, seriöse Firmen gehackt worden sind und die Passwortlisten in Umlauf gekommen sind. Dadurch kann man auch, wenn sich irgendwo der Mitarbeiter mit der Firmenmail und Firmenpasswort registriert, sich mit deren Identität einloggen und gegebenfalls nach Firmeninformationen suchen. Das Ganze steht auch im BSI Leitfaden, wenn man sich den im Detail durchliest. Auf Social-Engineering aufgedruckt, ist es mehr oder weniger egal, auf Informationssicherheit allgemein nicht.

MG: Gibt es einzelne Szenarien die sinnvoll sind einzusetzen in einem Unternehmen kritischer Infrastruktur, aber nicht sinnvoll in einem Unternehmen Nicht-kritischer Infrastruktur in Bezug auf Social-Engineering?

E1: Ähmm.., was Social-Engineering angeht, würde ich es unterschreiben, dass die Maßnahmen ähnlich sind, dass es keinen Unterschied zwischen kritischer Infrastruktur und Nicht-kritischer Infrastruktur gibt. Der einzige Unterschied ist, dass es Mitarbeiterinnen und Mitarbeiter kritischer Infrastruktur wirklich bewusst gemacht werden muss, dass es bei einer nicht autorisierten Informationsweitergabe für die Gesamtheit kritischer ist, als bei Nicht-kritischen Infrastrukturen, wie zum Beispiel einer Hausverwaltung oder eines Buchladens. Das Risiko hinter einem erfolgreichen Social-Engineering-Angriff ist einfach größer. Deswegen soll es einen höheren Stellenwert haben, aber die Maßnahme an sich, wie man die Mitarbeiterinnen und Mitarbeiter schult, wird ziemlich ähnlich bis gleich sein, weil es ja auch dasselbe Angriffsziel ist.

MG: Beschwerden sich bereits Mitarbeiterinnen und Mitarbeiter über solche Schulungen, dass diese einen erheblich negativen Einfluss auf die Arbeit haben?

E1: Nein, bei uns nicht, da die Schulungen kurz abgehalten werden und jetzt nicht die Mitarbeiter übermäßig Schulungen absolvieren müssen. Ähh, von anderen Unternehmen habe ich das aber schon sehr wohl gehört, aber hier gibt es auch das fünf bis Zehnfache an Schulungen, die absolviert werden müssen.

MG: Gut, das war es bereits mit Hypothese 1. Kommen wir nun zu Hypothese 2: "Jährliche Schulungen für Mitarbeiterinnen und Mitarbeiter können als Investition für die Informationssicherheit kritischer Infrastruktur gesehen werden und sparen im Allgemeinen Kosten, wenn die Kosten für die Schulung in Relation mit den Kosten eines Vorfalles verglichen werden.“ Und die erste Frage hier lautet:" Gibt es verschiedenen Varianten von Security-Awareness-Schulungen?"

E1: Ja klar, habe ich eh schon am Anfang erwähnt. Es gibt klassische Klassenraumschulungen, es gibt Schulungen wo externe vorbeikommen und irgendwas erzählen, es gibt E-Learning-Programme, es gibt Live-Schulungen, wo wirklich Angriffe simuliert werden. Die Bandbreite ist groß. Es gibt auch zahlreiche Firmen am Markt, die die unterschiedlichsten Methodiken anbieten.

MG: Das heißt, hier gibt es auch einen Unterschied über die jährlich anfallenden Kosten, wenn man die einzelnen Varianten vergleicht? Denn es ist sicher teurer, wenn eine externe Firma vorbeikommt und einen Vortrag hält, im Gegensatz zu einem E-Learning-Kurs.

E1: Genau, es hängt immer mit dem dazugehörigen Aufwand zusammen. Eine vor Ort Schulung hat einen höheren Aufwand als eine E-Learning-Schulung. E-Learning ist eine der günstigsten Arten, so eine Schulung sinnvoll zu gestalten. Denn es gibt auch Möglichkeiten, es noch günstiger zu machen, wie zum Beispiel es wird ein Poster irgendwo aufgehängt oder ein Artikel ausgesendet mit den wichtigsten Informationen, aber ob das dann wirklich einen Impact auf das Sicherheitsempfinden der einzelnen Mitarbeiterinnen oder Mitarbeiter hat, ist fraglich.

MG: Dann kommen wir zur nächsten Frage. Kann pauschal gesagt werden, je teurer eine Security-Awareness-Schulung ist, desto höher ist die Informationssicherheit eines Unternehmens?

E1: Pauschal kann das nicht gesagt werden. Sagen wir mal so. Die Frage gehört anders gestellt. Je teurer eine Schulung, desto besser wird die Awareness der einzelnen Mitarbeiterinnen und Mitarbeiter sein, sofern die Kosten vernünftig in die Schulung gesteckt werden. Eine

Klassenraumschulung ist halt teurer, aber die Awareness bei den einzelnen Personen wird hier höher sein, als nach einer E-Learning-Schulung. Da aber in der Frage steht, ob die Informationssicherheit besser geschützt ist, nur durch Security-Awareness -Schulungen ist schwer zu beantworten. Es fallen einfach noch mehr Aspekte bzgl. der Informationssicherheit an.

MG: Dann ändern wir die Frage, ob teure Schulungen die Awareness von Personen besser positive beeinflusst als günstigere.

E1: Ja, dann ist es so. Je intensiver, desto besser. Und in der Regel ist etwas Teureres auch intensiver.

MG: Okay, können Sie einen Vergleich über die Kosten einer Klassenraumschulung und einer E-Learning-Schulung geben?

E1: Das ist schwierig, da es immer darauf ankommt, wie viele Lizenzen bei E-Learning benötigt werden. Es kann grob gesagt werden, dass ein Personentag bei einer Klassenraumschulung ca. 1000€ - 1500€ kostet. Beim Erstellen einer E-Learning-Schulung können mit Kosten von ca. 10000-15000€ gerechnet werden. Zehn Tage wird daran gearbeitet und dann hat man einen Kurs und dieser muss dann in ein bestehendes E-Learning-Modul implementiert werden. Es kommt darauf an, bei einem kleinen Unternehmen wird eine Klassenraumschulung billiger sein, aber das gehört auch durchgerechnet, denn die Mitarbeiterinnen kosten ja auch in dieser Zeit, wo sie die Schulung besuchen, als bei einem größeren Unternehmen.

MG: Okay danke, dann kommen wir zur nächsten Frage. Kann gesagt werden, wie hoch die Kosten eines Social-Engineering-Angriffs sein können?

E1: Leider kann man das pauschal nicht beantworten. Es reicht von 100€ bis hin zur Existenz eines Unternehmens. Es kann bis in hohe Millionenbeträge gehen. Man stelle sich einen Mitarbeiter vor, der Jahrzehnte lang an einer geheimen Formel geforscht hat. Bringt man diesen nun dazu, diese Formel zu verraten, kann das Unternehmen in den Ruin gebracht werden. Pauschal kann nichts gesagt werden. Die Bandbreite geht von nichts, bis hin zur Existenzbedrohung eines Unternehmens.

MG: Dann lautet die nächste Frage:" Wie groß ist die Chance Opfer eines Social-Engineering-Angriffs zu werden und unterscheidet sich diese je nach Sparte und Größe eines Unternehmens?"

E1: Ja, unterscheidet sich definitiv nach Sparte. Je mehr Mitbewerber man hat und vor allem wenn man in Bereichen tätig ist, die sehr viel Intellectual-Proberty besitzen, hier werden häufiger Social-Engineering-Angriffe durchgeführt. Das sind einfach lohnendere Ziele als Unternehmen die eher weniger Intellectual-Proberty, wie zum Beispiel eine Hausverwaltung, aufweisen. Hier wird man mit den Daten weniger anfangen können.

MG: Gibt es eigentlich Fälle, in dem sich Security-Awareness-Schulungen im Vergleich zu einem Angriff nicht auszahlen?

E1: In einem Blumengeschäft wird eine Schulung wahrscheinlich teurer sein als ein Angriff. In einem großen Konzern sieht das aber wieder anders aus. Es hängt stark mit der Größe des

Unternehmens zusammen und mit dem Zweck, den sie ausüben. Aber für einen normal großen KMU bis hin zu großen Unternehmen wird sich eine Schulung immer auszahlen.

MG: Okay, Sie haben vorher auch erwähnt, dass es technische Maßnahmen gibt, die einen Angriff erschweren. Wie hoch sind die Kosten dafür?

E1: Das braucht man sowieso. Ein vernünftiges Unternehmen benötigt diese Tools sowieso. Man würde es auch aus anderen Gründen und nicht nur im Kontext Social-Engineering einsetzen. Damit soll eben die grundlegende Security gewährleistet werden. Hier reichen die Kosten von klein bis groß. Je nach Anforderung und welches Produkt es ist. Es beginnt aber schon bei 10000€ und bis nach oben hin gibt es keine Grenzen.

MG: Gut, dann kommen wir zur letzten Frage. Gibt es eigentlich technische Maßnahmen, die nur darauf ausgelegt sind, Social-Engineering-Angriffe zu erschweren?

E1: Mir wäre nichts bekannt.

MG: Gut, das war es dann mit dem Interview. Ich bedanke mich für die Zeit. Ich werde das Interview dann mit dem Programm MAXQDA transkribieren und werde dieses Tool auch zur Analyse benutzen. Die Aufnahme wird wie bereits gesagt, ausschließlich für die Masterarbeit verwendet. Falls Interesse besteht, kann ich das Ergebnis dann gerne teilen.

E1: Okay, passt, dann wünsch ich noch gutes Gelingen und auf Wiederhören.

MG: Auf Wiederhören.

ANHANG D - Experteninterview – Experte 2

MG: Also danke für die Zeit und, dass du so nett bist und mir hilfst mir bei der Beantwortung der Forschungsfrage: "Welche Initiativen müssen gesetzt werden, um die Informationssicherheit von Unternehmen kritischer Infrastruktur im Kontext zwischen Engineering zu gewährleisten, ohne einen beträchtlichen Aufwand für Mitarbeiterinnen Mitarbeiter zu verursachen?" Ein kurzer Umriss über das Thema ist, dass es mittlerweile sehr viele Maßnahmen in der Informationssicherheit gibt und auf die Social-Engineering Angriffe steigen dadurch. Muss man halt schauen, dass man etwas, das man den ganzen entgegenwirkt und sich fragen, welche Maßnahmen quasi überflüssig sind, welche unbedingt notwendig sind dem Kontext Social-Engineering. Das Interview wird ca. 30 bis 40 Minuten dauern und die Datenschutz Vereinbarung haben sie eh schon unterschrieben, dass wir das ganze aufnehmen dürfen. Und dann werde ich beginnen mit den Fragen mit den Einstiegsfragen. Wie lange haben Sie schon mit Informationssicherheit zu tun?

E2: Also prinzipiell beschäftige ich mich mit dem Thema Security schon, kann man sagen eher intensiver, seit Beginn meiner IT-Zeiten noch intensiver, seit sieben Jahren und seit fünf, sechs Jahren wirklich dann auch vermehrt und wirklich im Bereich Informationssicherheit. Also nicht nur die Security allgemein. Baut man heute ein System auf, dann kümmert man sich auch darum, dass dessen sicher ist, man kümmert sich um die Zugänge, um die Informationssicherheit. Mittlerweile ändert sich das Ganze schon. Die ganze Sicherheitsthemen werden mittlerweile als erstes betrachtet, wirklich Security-First. Der Trend geht dahin, dass mittlerweile Multi-Faktor oder Ähnliches eingesetzt werden. Und das ist das, was ich in den letzten Jahren schon sehr stark von dem geändert hatte, was ursprünglich auch immer mit Security in Verbindung gebracht worden ist.

MG: Welchen Einfluss hat Social Engineering hierbei?

E2: Nun wie gesagt, das Verschieben der Sicherheit in den Vordergrund. Mittlerweile ist der User die Nummer 1 Schwachstelle. Der hat noch Zugriff auf System und so kann man auch Zugriff bekommen, auf ein System, das keine Schwachstellen hat. Man muss die User benutzen und dadurch rückt auch Social-Engineering in den Vordergrund und macht den User natürlich angreifbar und auch als primäres Ziel für etwaige Angriffe. Egal in was für einer Art und Weise.

MG: Was gehört zu Ihren täglichen Aufgaben und besteht hier auch eine Verbindung zu Social Engineering?

E2: Ich bin im Managed-Service-Provider-Bereich tätig und hier hat man auch sehr viel mit Security zu tun. Im Allgemeinen kann gesagt werden, dass meine Tätigkeit durch alle 7 Layer geht, auch oftmals Layer 8, den User selbst. Unternehmen kommen zu uns wollen ein Konzept im Datacenter Bereich, den Domänen Bereich. Aber auch andere Firmen wenden sich an uns und sagen Okay, wir brauchen bitte Konzepte für die User Absicherung aus dem Bereich Social-Engineering. Welche Abwehrmaßnahme gibt es dagegen, etc. Es ist teilweise auch Beratertätigkeit und eben auch weitere Schritte, die Umsetzung von verschiedensten Tools geht immer so mit dabei. Also ist es wirklich sehr starke Bindung, die man dazwischen aufbaut. Und

wie gesagt, deswegen meine Hauptaufgaben sind die Umsetzung von Konzepten, um auch unter anderem Social Engineering zu verhindern.

MG: Okay, und was ist deiner Meinung nach eine Personengruppe, die am meisten gefährdet ist für Social Engineering Angriffe?

E2: Is a bisserl schwer zu sagen, aber eigentlich ist es jeder. Das kommt darauf an, unabhängig von Schulungen, unabhängig wie gut jemand ist oder ob man Profi ist. Es gibt immer Arten, wie man jemanden manipuliert. Und meistens passiert es dann, wenn er einen unachtsamen Moment hat, wenn jemand mit Stress oder andere Gedanken zu tun hat. Dann kann auch der beste Sicherheitsexperte Opfer werden. Aber Hauptziel, sind die Personen, die wahllos auf alles draufklicken, die wahllos Fragen beantworten. Das sind Leute, die nicht achtsam sind und natürlich helfen natürlich nur Schulungen, aber prinzipiell es ist jeder. Angreifbar ist jeder, man muss indem Sinne nur der richtige Moment warten.

MG: Dann denke mal, das war's mit der Einleitung und nun kommen wir zu den Schlüsselfragen und als erstes gehen wir auf folgende Hypothese ein. Jährliche Schulungen für Mitarbeiterinnen und Mitarbeiter im Kontext Social-Engineering haben einen positiven Einfluss auf die Informationssicherheit und kritischen Infrastrukturen. Und die erste Frage hier lautet: "Erachten Sie solche Schulungen für sinnvoll und wenn ja, warum? Und wenn nein, warum?"

E2: Schulungen sind absolut sinnvoll. Ja, eigentlich für jeden auch wieder. Man muss aber sagen, dass die Schulungen kurz, knackig und effektiv sein. Es hat keinen Sinn auf langwierigen Schulungen zu setzen, die keinen interessieren. Man muss wirklich kurz auf den Punkt kommen. Warum ist Informationssicherheit und Social-Engineering für dich wichtig in deinem Bereich mit dem, was du tust? All das ist das Wichtige bei einer Schulung. Die müssen kurz sein. Man muss sich das merken können, was gesagt wird, man muss es auch anwenden können. Und ganz klar, man muss es dann auch überprüfen. Ich bin Befürworter von einem kurzen Quiz, um den Wissensstand abzufragen und die Schulungen dann einfach immer wieder zu wiederholen. Nicht zu häufig, aber natürlich regelmäßig, damit man sich was merkt, wiederholen kann und auch anwenden kann. Und Schulungen sollten auf den Tätigkeitsbereich der einzelnen Personen abgestimmt werden.

MG: Du hast gesagt, dass die Schulungen auf die Person selbst oder bzw. den Tätigkeitsbereich von der Person selbst abgestimmt werden soll? Sollte es eine allgemeine Schulung für alle geben?

E2: Es kommt ganz aufs Unternehmen an. Meistens ist es so, dass mit einer gelungenen Schulung man nichts anfangen kann. Manche kriegen vielleicht gar keine E-Mails. Um das wirklich effizient zu machen, sage ich Abteilungsspezifische Schulungen. Allgemeine Schulung für das Ganze Unternehmen kann man machen, aber es kommt die Unternehmensstruktur an. Wo muss ich ansetzen? Grundlagenschulung? Ja können wir darüber reden? Für alle Phishing Schulung? Okay. Auf was muss ich schauen? Ich bin jetzt zum Beispiel im Versand tätig. Hier gehören die Fragen beantwortet, Wo kann ich genauer hinschauen? Der andere sitzt im Verkauf. Hier gehören andere Fragen beantwortet, denn dieser Person interessieren Sachen nicht, die im Versand passieren könnten. Gleiche Schulung für alle, ja, aber es kommt auf das Unternehmen darauf an!

MG: Okay, danke und werden solche Schulungen in Ihrem derzeitigen Unternehmen bzw. bei Kunden von Ihrem Unternehmen eingesetzt.

E2: Bei uns selbst ist das Thema IT-Security quasi omnipräsent. Damit haben wir keine Schulungen, weil wir die Theorie quasi kennen und wir auch indirekt Unternehmen schulen. Wir müssen schauen, wie man das auf Vordermann bringt, wie unser Konzept dann funktioniert und auch sicher ist. Also ja, wir sind selbst dauernd damit beschäftigt, dass wir uns jetzt in dem Sinne nicht selbst schulen aber indirekt unsere Kunden.

MG: Okay, kann eigentlich gemessen werden, aber solche Schulungen erfolgreich sind

E2: Ja, ganz klar. Zum einen Wissenstests, um das Verständnis abzufragen, dann gibt es natürlich die Möglichkeit, dass man probiert, selbst dediziert Angriffe durchzuführen. Da muss man vorsichtig sein, denn im Nachhinein zum User laufen und sagen du hast einen Fehler gemacht, ist nicht immer gut. Die nächste Frage ist auch, was der Betriebsrat dazu sagt, denn diese wollen eigentlich so gut wie nie unwissentliche Überprüfungen von Mitarbeitern. Also man muss vorsichtig sein, wie man damit umgeht, ohne dass man seine User zu verärgert und ihm das Gefühl gibt, dass diesem User nicht mehr vertraut wird im Unternehmen. Da ist immer Vorsicht geboten.

MG: Also sagen Sie, dass Personen leichter anfällig für einen Angriff sind, die keine Schulung besucht haben als Personen, die eine Schulung besucht haben.

E2: Es gehört die Frage gestellt, ob ich mich damit beschäftige oder nicht. Wie gesagt, es ist jeder dafür anfällig. Da muss nur im Stress schnell was passieren. Kurze regelmäßige Trainings, um das ganze mal aufzufrischen, ist kein Fehler und man ist dann im Schnitt auch weniger anfälliger.

MG: Wie sollte Ihrer Meinung nach, der Aufbau einer Security-Awareness-Schulung sein? Das haben Sie vorher glaube ich eh schon beantwortet. Auf Abteilungsebene und eventuell einen kurzen Grundkurs für alle, wenn das Unternehmen dafür geschaffen ist?

E2: Meine Ansicht ist kurz und effektiv durch Schlagworte. Keine langwierigen, mit sehr vielen Informationen, die sich kein Mitarbeiter merken kann und will. Deswegen kurz. Aber ich bin der Meinung, dass eine Schulung bestanden werden muss. Auch Abteilungsspezifisch, da verschiedene Abteilungen andere Angriffsvektoren haben, die die andere Abteilung nicht interessiert. Es gehört gesagt, was kann bei euch passieren? Dann wird es auch besser ankommen und besser verstanden. Und dann natürlich in der Schulung die ganz normalen Tipps mitgeben, die aber effektiv sind.

MG: Gibt es eigentlich noch andere technische Maßnahmen, um einen Social Engineering Angriff zu erschweren?

E2: Es gibt technische Maßnahmen, es gibt physikalische Maßnahmen. Es fängt an beim Zutritt von Unternehmen, wie sind diese abgesichert. Da gibt es unzählige Ausführungen. Das erschwert natürlich einen Social-Engineering Angriff. In dem Sinne an technischen Maßnahmen. Natürliche Multi-Faktor, Spamfilter, man filtert hier die Mails vorher durch Richtlinien, Verschlüsselung. Man filtert hier eben zum Beispiel einfach gestrickte Mails raus, aber die perfekt und sehr gut aufgebaut

sind, eben nicht. Und da helfen dann auch nur Schulungen. Dann natürlich weitere technische Maßnahmen wie interne Proxys, Geo-Basierte Zugangskontrollen. Es gibt unzählige Maßnahmen, die man einsetzen kann, um, erstens, das Risiko eines Angriffs zu minimieren und dann natürlich, wenn ein Angriff stattgefunden hat, die Auswirkungen zu minimieren. Das sind zwei wichtige Punkte. In jeder Schicht muss ich Sicherheitsmaßnahmen haben, um mich zu verteidigen. Es hilft nicht nur Schulung zu machen, man muss das gesamte Spektrum abdecken, um sicher zu sein.

MG: Bei der nächsten Frage weiß ich nicht, ob sie die genau beantworten kannst, weil Sie glaube ich nicht keine Kunden kritische Infrastruktur haben, aber versuchen wir trotzdem mal darauf einzugehen. Gibt es eigentlich einzelne Szenarien, wo es sinnvoller ist, Maßnahmen, also Maßnahmen für kritische Infrastruktur, einfach sinnvoll sind, aber diese gleichen Maßnahmen eben für andere Unternehmen nicht kritische Infrastrukturen nicht so sinnvoll wären?

E2: Sinnvoll sind Security-Maßnahmen immer. Ob sie notwendig sind, ist eine andere Frage. Bei kritischer Infrastruktur sind einfach härtere Maßnahmen und ein restriktivere Policy notwendiger als bei anderen Unternehmen. Natürlich ist überall 2-Faktor sinnvoll oder auch Zutrittskontrollen, aber ist es für andere Unternehmen auch leistbar bzw. der Nutzen dadurch um ein Vielfaches höher?

MG: Da du ja auch schon indirekt Personal geschult hast, haben sich hier Kundinnen und Kunden über Maßnahmen beschwert, weil diese eben den Arbeitsplatz negativ beeinflussen.

E2: Da habe ich schon vieles mitgekriegt. Sicherheit macht nichts leichter. Sicherheit ist nicht bequem. Es ist die Bequemlichkeit der einzelnen User. Das ist Bequemlichkeit. Man muss da wirklich bei denen gegenüberstehen, welches Risiko sie haben. Welche Auswirkungen das für das Unternehmen haben kann und wie gefährlich sie sind. Was bei vielen Usern wirklich hilft, ist, dass man sagt, diese Maßnahmen nicht umgesetzt werden sollen, weil es die Versicherung verlangt. Die Versicherung fordert es und damit verstehen die meisten es. Es sollte nicht die IT dahinterstecken, zumindest beim Verteilen der Informationen, ansonsten schon.

MG: Okay, das war es jetzt mit der Hypothese 1 und nun kommen wir zur zweiten, nämlich: "jährliche Schulungen für Mitarbeiterinnen und Mitarbeiter können als Investition für die Informationssicherheit kritische Infrastruktur gesehen werden und sparen im Allgemeinen Kosten, wenn die Kosten für die Schulung in Relation mit den Kosten eines Vorfalles verglichen werden." Die erste Frage hier lautet: "Gibt es eigentlich verschiedene Varianten von Security-Awareness-Schulungen?"

E2: Die Relation ist es, die es ausmacht, weil die Kosten von einem Vorfall sind, meistens immens höher, wie die Kosten, sich dagegen zu schützen. Natürlich gibt es verschiedene Schulungen. Es gibt interne Schulungen, es gibt Schulungen von externen Beratern. Eine andere Variante wäre, man macht die Schulungen online über Plattformen, man erstellt Videos.

MG: Das heißt, die verschiedenen Varianten unterscheiden sich auch in den jährlich anfallenden Kosten?

E2: Wenn jetzt externe Beratung die Schulung durchführen, sind die Kosten höher, wie wenn die interne IT sich um die Schulung kümmert. Bei Online-Kursen kommt es auf die Lizenzen an, wie

viele werden benötigt, wie viele kostet eine. Dann muss man sich durchrechnen, je nach Größe des Unternehmens, welche Variante günstiger ist.

MG: Kann eigentlich pauschal gesagt werden, dass je teurer eine Schulung ist, desto besser ist die Informationssicherheit eines Unternehmens bzw. desto besser ist die Awareness der einzelnen Mitarbeiter, in der Regel?

E2: Prinzipiell ist es so, aber dass teuer nicht immer gleich gut ist, gehört bedacht. Natürlich kommt es auf, die Unternehmensgröße auch auf das Sicherheitsniveau, das es schon gibt, es erreicht werden will an. Aber in der Regel ist es so, dass ein Vorort Termin mit externen Experten, die eine Schulung durchführen, besser in Erinnerung bei den Usern bleibt. Solche Vorort Schulungen sind natürlich auch meistens teurer als zum Beispiel Online-Kurse.

MG: Okay, jetzt kommen wir mal zur anderen Seite und zwar kann man sagen, wie hoch die Kosten eines Social-Engineerings-Angriff werden können bzw. in welchen Bereichen sich das Abspielen könnte?

E2: Ich habe ja schon Beispiele wirklich dazu erlebt. Wir haben hier das ganze Unternehmen wieder auf Vordermann gebracht, nach einem Angriff. Da muss man unterscheiden, was passiert im Angriff? Welche Daten werden abgriffen? Das kann natürlich fürs Unternehmen äußerst schädigend sein. Ich muss erzählen, dass einen Angriff sogar einen Admin passiert ist. Der Angriff auf das Gesamtunternehmen verschlüsselte die ganzen Daten und das Unternehmen mit mehreren hundert Mitarbeiter steht für drei Wochen. Da kann man sich ungefähr vorstellen, dass die Kosten hier nicht ohne sind. Und unabhängig von den Kosten, viele Angreifer verlangen, wenn sie eine Ransomware erfolgreich im Unternehmensnetzwerk verteilen, was hauptsächlich durch Social-Engineering geschieht, im Bereich von zwei bis fünf Prozent des Jahresumsatzes des Unternehmens. Es gibt Unternehmen, die haben zig Millionen Euro Jahresumsatz. Das ist dann eine große Summe. Und es sind auch schon Unternehmen wegen Social-Engineering in den Ruin getrieben worden. Und wenn man die dann diese Kosten gegenüberstellt mit den Kosten, um das zu verhindern, dann sieht man, dass sich solche Schulungen eigentlich immer auszahlen.

MG: Wie hoch ist eigentlich die Chance, Opfer eines Social-Engineering-Angriffs zu werden und unterscheidet sich diese auch je nach Branche und Größe des Unternehmens?

E2: Es kann grundsätzlich jedem passieren. Aber bei großen Unternehmen, die sehr viele Mitarbeiter haben, die vielleicht auch kritische Infrastruktur sind, die irgendwelche Provider sind, Banken und so weiter, bei diesen ist die Chance höher, da diese einfach mehr Gewinne abwerfen, da sie eher bereit sind zum Zahlen oder mehr Schaden verursachen, da es sich hier oft um kritische Informationen handelt und ein Ausfall katastrophal wäre. Aber es kann genauso gut bei Privatpersonen passieren und es kommt immer darauf an, welche Kontakte man hat. Deshalb ist auch oft eine Privatperson die erste Anlaufstelle für Angriffe auf Unternehmen.

MG: Okay, können Sie sagen, wie hoch die jährlichen Kosten einer Security-Awareness - Schulung werden können?

E2: Das steht immer in Relation dazu. Mit der Unternehmensgröße mit dem Niveau welche Sicherheit erreicht werden will. Bei externen Beratern im Haus sind die Kosten um ein Wesentliches höher wie, wenn dasselbe die eigene IT macht. Am. Man kann aber sagen, egal

wie hoch die jährlichen Kosten sind. Aber es ist schwer, zum einen bestimmten Wert zu nennen, was sie wirklich kosten. Es kommt darauf an welche Art von Schulung und wie intensiv ich schulen möchte.

MG: Und dann die nächste Frage lautet: "Gibt es Fälle, in dem sich Schulungen nicht auszahlen? Und wenn ja, was wären diese?"

E2: Also kann sich höchstens für eine bestimmte spezifische Person nicht auszahlen, die eh schon drauf achtet und die ganze Theorie kennt, also zum Beispiel, wenn ich jetzt Berater bin und nur im Bereich Security und nur Schulung selbst betreibe. Ich muss aber auch sagen, auch hier ist es kein Fehler geschult zu werden. Natürlich auf eine andere Art und Weise. Sicherheit ist wirklich die Nummer eins, auf die geschaut werden muss. Und erst in zweiter Linie auf alles andere.

MG: Du hast vorher auch schon gesagt, es gibt eben auch zusätzliche technische und physische Maßnahmen, die einen solchen Angriff ebenfalls erschweren. Und kann man dann sagen, wie hoch hier die jährlichen Kosten dafür sind?

E2: Auch hier, wie gesagt, bestimmte Kosten sind schwer zu sagen. Aber ich kann sagen, man kann sich mit genug Zeit und Ressourcen Tools finden, die nichts kosten und dennoch positiv für die Sicherheit sind. Es gibt auch Tools, die von namhaften Herstellern vertrieben werden und auch besser sind als frei verfügbare Tools. Das sind dann aber wieder mehr Kosten. Es gehört halt auch hier abgeschätzt, wie viel Budget habe ich und wie kann ich das Beste davon herausholen. Die Preise können hier von quasi nichts, wenn man jetzt die Mitarbeiterkosten vernachlässigt, bis hin zu mehrere Millionen Euro gehen. Es gehört einfach abgewogen, was bin ich für ein Unternehmen, bin ich zum Beispiel kritische Infrastruktur, werde ich auf Bessere, teurere Tools zurückgreifen müssen.

MG: Dann kommen wir zur letzten Frage, und zwar gibt es eigentlich technische Maßnahmen, die nur ausschließlich darauf ausgelegt sind, Social-Engineering-Angriffe zu erschweren?

E2: Mir sind hier eigentlich keine bekannt, die spezifisch nur auf das ausgelegt sind. Eventuell das Multi-Faktor als Hauptziel Social-Engineering hat, aber auch hier ist es nicht nur eine Maßnahme gegen Social-Engineering. Also nein, ich weiß von keinen.

MG: Okay, danke, dann war es das mit dem Interview und ich bedanke mich noch einmal für die Zeit. Ich werde das Interview transkribieren und im Anschluss mit der qualitativen Inhaltsanalyse nach Mayring ausarbeiten und wenn keine Fragen mehr offen sind, werde ich die Aufnahme beenden.

E2: Bitte, gern geschehen. Nein, ich habe keine Fragen mehr.

ANHANG E - Experteninterview – Experte 3

MG: Vielen Dank, dass Sie sich Zeit nehmen, mich bei meiner Masterarbeit zu unterstützen. Im Grunde geht es darum, die Forschungsfrage: "Welche Initiativen müssen gesetzt werden, um die Informationssicherheit von Unternehmen kritischer Infrastruktur im Kontext Social-Engineering zu gewährleisten, ohne einen beträchtlichen Mehraufwand für Mitarbeiterinnen und Mitarbeiter zu verursachen? Also, ein kurzer Umriss des Themas wäre eben, wie die Forschungsfrage bereits schon sagt, herausfinden, welche Initiativen gesetzt werden müssen. Ich habe auch schon eine Umfrage an normale Mitarbeiterinnen Mitarbeiter ausgesendet für eine quantitative Analyse. Es betrifft hier eben keine spezielle Personengruppe, sondern einfach normale Mitarbeiterinnen und Mitarbeiter, um herauszufinden, ob gewisse Maßnahmen, diesen Personen auf die Nerven gehen oder ob alle wissen, ob das für sie die Maßnahmen als sinnvoll erahnen. Und jetzt will ich das Ganze mit Experteninterviews prüfen bzw. Experteninterviews durchführen, um zu wissen, ob gewisse Maßnahmen weggelassen werden können oder so. Das Interview wird zwischen 30 und 40 Minuten dauern und die Datenschutz Vereinbarung, die hast du mir eh schon unterzeichnet, dass, dass ich das Ganze aufnehmen darf. Die Aufnahme wird ausschließlich, für die für die Masterarbeit verwendet und dann würde ich mit den Einstiegsfragen, mit der Einleitung gleich beginnen. Und die erste Frage lautet hier: "Wie lange haben Sie schon mit Informationssicherheit zu tun?"

E3: Es müssten jetzt ungefähr zehn Jahre sein.

MG: Wie hat es sich seitdem verändert?

E3: Am. Die Frage an sich ist so dahingehend nicht sehr einfach zu beantworten, da sich ja vieles verändert hat von den Methoden bis hin zu ganz banalen Themen wie Benennungen von verschiedenen Lücken oder so. Also es hat sich im Grunde sehr viel getan und da jetzt wirklich festzumachen, inwiefern sie sich verändert hat, ist sehr schwierig. Aber ich glaube, im Großen und Ganzen könnte man sagen, es ist alles noch viel komplizierter und viel erwachsener geworden, als es ohnehin schon war. Und die IT-Systeme haben an Komplexität zugelegt, was es zum einen in die andere Richtung erschwert und zum anderen natürlich um einiges einfacher macht, weil in komplexen Systemen Lücken zu finden, ist natürlich wesentlich wahrscheinlicher als in einfachen.

MG: Ist mittlerweile auch beim Top-Management angekommen, dass ein Budget für Informationssicherheit. Gegeben werden muss?

E3: Dadurch, dass ich halt durch meinen Beruf auch sehr tiefen Einblick in die Sicherheitspolitik anderer Unternehmen habe, merkt man, dass es auch in der heutigen Zeit noch immer so ist, dass bevor es ein Budget in diese Richtung gibt, doch erst was passieren muss.

MG: Okay, das heißt, das hat sich nicht verändert in den letzten Jahren

E3: Mehr oder weniger. Man merkt schon, dass ein gewisses Bewusstsein geschaffen wurde. Also zumindest Social-Engineering ist mittlerweile fast jedem ein Begriff. Dennoch fehlt die

Relation zur Wirkung, zur Wirklichkeit. Wie schnell soll so ein Social-Engineering Angriff doch durchgeführt werden kann.

MG: Okay, und die nächste Frage bezieht sich jetzt eh schon auf Social-Engineering. Und zwar Welchen Einfluss hat Social-Engineering zur gesamten Informationssicherheit.

E3: Dadurch, dass noch immer über 25 Prozent aller Angriffe auf Social-Engineering und Phishing zurückzuführen sind, die Quelle hierfür kann ich dir gerne zur Verfügung stellen, sehe ich Social-Engineering als großen Einfluss. Nach wie vor oder gerade jetzt als einer der größten Einflüsse auf Data-Leaks überhaupt, weil, es gibt auch immer mehr Forschung hier. In Richtung Produktsicherheit, Software, Produktsicherheit, das heißt, zwei Lücken in Softwareprodukten werden natürlich immer weniger bzw. kontinuierlich aufgedeckt und ausgebessert. Dementsprechend muss man sich auf eine humanitäre und soziale Komponente verlassen, um einen erfolgreichen Angriff durchzuführen.

MG: Was gehört zu Ihren täglichen Aufgaben und besteht hier auch eine Verbindung zu Social Engineering?

E3: Zu meinen täglichen Aufgaben gehören die Überprüfung von Software, Produkten auf deren IT-Sicherheit und Aufdecken von Schwachstellen sowie das Reporting eben jener Schwachstellen. Und Social-Engineering wird hier nur am Rande gestreift, aber gehört trotzdem nicht vernachlässigt.

MG: Dann kommen wir zur nächsten Frage Welche Personengruppe ist am meisten für Social Engineering Angriffe gefährdet?

E3: Ich würde sagen, der Otto Normal Mitarbeiter fällt in diese Personengruppe, die für solche Angriffe am gefährdetsten ist, weil, das Bewusstsein für solche Angriffe einfach fehlt. Entweder weil man nicht so häufig mit diesem Thema in Kontakt kommt oder weil eine gewisse Naivität gegenüber fremden Menschen herrscht und einfach das vorgestellte Vertrauen des Menschen ist durchaus eine Komponente, die zum Erfolg unserer Ansichten beiträgt.

MG: Danke, das war es mit den Einstiegsfragen und nun kommen wir zu den Schlüsselfragen. Und hier kommen wir zu den Fragen, die sich auf folgende Hypothese beziehen, die lautet: „Jährliche Schulungen für Mitarbeiterinnen und Mitarbeiter im Kontext zur Nehring haben einen positiven Einfluss auf die Informationssicherheit von kritischen Infrastrukturen." Erachten Sie solche Schulungen für sinnvoll?

E3: Ja, durchaus. Man muss aber auch dazu sagen, dass man die Mitarbeiter nicht mit solchen Dingen überfordern sollte. Ich würde vorgeschlagen einmal jährlich sollte ausreichen, um die Ebene für dieses Thema aufgefrischt zu halten bzw. auch neue Mitarbeiter in diese Richtung zu schulen.

MG: Werden aktuell solche Schulungen bei Ihnen im derzeitigen Unternehmen eingesetzt oder wurden solche Schulungen in Ihren vergangenen Unternehmen eingesetzt bzw. kennen Sie Unternehmen, wo solche Schulungen eingesetzt werden?

E3: In meinem derzeitigen Unternehmen wüsste ich nicht, dass es solche Schulungen tatsächlich gibt. Die Awareness wird dahingehend in anderer Form verbreitet. Hier wird ein Firmenweites

Mail ausgesendet, wenn ein Angriff geschehen ist bzw. es wichtige Informationen gibt zu verbreiten In einem Unternehmen bzw. einer Abteilung, wo Personen arbeiten, die sowieso Ahnung davon haben, ist eine Schulung in einem großen Ausmaß nicht unbedingt notwendig, aber dennoch sinnvoll.

MG: Das bezieht sich jetzt aber nur auf Ihr und Ihr derzeitiges Unternehmen, oder?

E3: Exakt, exakt.

MG: Aber Sie kennen auch Unternehmen, wo Schulungen eingesetzt werden, also nicht typische IT-Unternehmen, sondern andere Unternehmen, wie zum Beispiel kritische Infrastrukturen.

E3: Bei meinem früheren Unternehmen im Gesundheitssektor wurde ein eine ähnliche Vorgehensweise wie in meinem aktuellen Unternehmen gewählt, hier wurde sich hier auf das Einsetzen von ausgeklügelten Spam Filtern und sehr restriktiven Regeln verlassen. Das hat durchaus funktioniert, aber aktive Schulungen in diese Richtung gab es nicht. Dennoch sind mir einige Unternehmen bekannt, die auch auf Schulungen setzen bzw. auch Workshops von externen Dienstleistern in Anspruch nehmen, die in diese Richtung gehen.

MG: Sind Sie der Meinung, dass? Das jetzt quasi, wenn ein Vorfall passiert und eine Mail ausgeschickt wird, dass das reicht oder benötigte es für den Otto Normal Mitarbeiter eine Schulung, um das erwähnte Sicherheitsgefühl zu steigern.

E3: Hierbei kommt es denke sehr stark auf die Branche an. In der IT-Branche reicht es alle Fälle. Diesen Mitarbeitern ist Spam und Phishing ein Begriff. In Unternehmen abseits der IT-Branche werden Schulungen und dediziert in dieser Richtung auf alle Fälle ein, ein besserer Weg.

MG: Kann eigentlich gemessen werden, ob solche als Schulungen erfolgreich sind.

E3: Am. Hierbei muss man sich wieder auf die menschliche Komponente verlassen. Sollte es zu einem Data-Breach kommen, der durch einen Mitarbeiter verursacht wird, dann muss sich dieser auch melden. Ob diese Schulungen erfolgreich sind oder nicht, kann daran gemessen werden, ob es mehr Klicks auf vom Unternehmen produzierte Phishing Mails kommt oder nicht. Anders, bei einem richtigen Angriff kann dies nur insofern gezählt oder gemessen werden, wenn sich der betroffene Mitarbeiter auch von selbst meldet. Außer es gibt eben technische Mechanismen, die solche Versuche intern schon abzufangen und die diesen auch als solchen identifizieren.

MG: Testet die Abteilung eigentlich von deiner Firma selbstständig die Mitarbeiterinnen und Mitarbeiter mit selbst durchgeführten Social-Engineering Angriffe bzw. hast es an Dritte aus,

E3: Wäre mir dahingehend nichts bekannt.

MG: Andere Unternehmen wahrscheinlich schon, oder?

E3: Aus Erfahrung kann ich sagen, dass es hierbei immer große Probleme in Richtung des Betriebsrates gibt. Da dieser sich insofern einsetzt, dass Mitarbeiter nicht ohne Wissen überprüft werden dürfen. Und wenn Mitarbeiter natürlich wissen, dass sie in einem gewissen Zeitraum überprüft werden, sind sie aufmerksamer als sonst und das könnte natürlich die Messwerte verfälschen. Die Thematik ist leider nicht ganz einfach von einem rechtlichen Standpunkt aus, da man seine Mitarbeiter eben nicht ohne Weiteres überprüfen darf.

MG: Aber solche Angriffe wären wahrscheinlich erfolgreicher, wenn das Personal nicht geschult wäre.

E3: Auf alle Fälle.

MG: Wie sieht eigentlich der Aufbau einer Security-Schulung aus? Oder wie würdest du eine Security-Schulung aufbauen?

E3: Am. Also ich glaube, der richtige Zugang zu diesen Themen ist mit praktischen Beispielen, mit Beispielen, indem sich die sich die die Teilnehmer der Schulung hineinversetzen können und wo sie am Ende wirklich das Gefühl haben Ja, Ich hätte dort auch hinaufgeklickt. Es gehört eben der Aha-Moment in den Teilnehmerinnen und Teilnehmern ausgelöst, der sie selbst dazu bewegt, vorsichtiger und aufmerksamer zu sein.

MG: Gibt es eigentlich noch andere technische Maßnahmen, um eine Social Engineering Angriff zu erschweren?

E3: Ja. E-Mail-Filter und Blockieren von Zwielichtigen URLs. Ist seit jeher ein beliebtes, eine beliebte Methodik, um Social Engineering Angriffe zu verhindern bzw. zu erschweren. Inwieweit diese helfen, ist natürlich abhängig von, von dem strikten Grad der Regelungen. Und dort muss immer abgewogen werden zwischen Security und Usability. Dementsprechend fällt. Fällt es mir schwer, einen genauen Wert zu nennen, inwiefern technische Maßnahmen hierbei helfen können. Allerdings sind eben zum Beispiel Spamfilter und so, zum Beispiel zum Einschränken oder Markieren von E-Mails, die von einem externen Absender kommen, ein guter Ansatz, die Mitarbeiter etwas indirekt aufmerksamer zu machen.

MG: Das heißt, Sie empfinden solche technischen Maßnahmen als sinnvoll? Sie erwähnten, dass sie auch vorher im Gesundheitswesen angestellt waren? Ist Ihnen die kritische Infrastruktur ein Begriff? Und hier nun die Frage, kann es in einzelnen Szenarien wie in einem Unternehmen kritischer Infrastruktur sinnvoll sein, Maßnahmen einzusetzen, die in anderen, nicht kritischen Infrastrukturen nicht notwendig wären?

E3: Ja, auf jeden Fall. Also in kritischer Infrastruktur gibt es natürlich immer eine, einen anderen Grund die Infrastruktur vor Ausfall oder Data Breaches zu schützen. Eben, weil es sich hierbei um Infrastruktur handelt, die zu jederzeit verfügbar sein muss oder sollte. Deshalb macht es großen einen großen Unterschied, ob. A das Krankenhaus-Netzwerk für einen Tag nicht erreichbar ist oder zum Beispiel die Webseite der Tischlerei Meyer. Name frei erfunden.

MG: Wie würden solche Maßnahmen kritische Infrastruktur aussehen, die hier sinnvoll wären und in anderen Unternehmen nicht?

E3: Zum Beispiel machte es Sinn, einen Mail Filter in einem kleineren Unternehmen zu installieren, oder so der die die Policy nicht so stark hat, wie ein Filter in Unternehmen kritischer Infrastruktur. Des Weiteren müssen die Mitarbeiter in einem Unternehmen kritische Infrastruktur auch dermaßen geschult werden, dass das Awareness Gefühl einfach höher ist, denn ein Ausfall hier ist um einiges schlimmer als in einem anderen Unternehmen. Also andere, restriktivere Maßnahmen müssen nicht, allerdings für sinnvoll, für sinnvoll halte ich es trotzdem. Dennoch, gilt zu sagen, dass solche Maßnahmen immer sinnvoll sind, aber in einem kleinen Unternehmen die

Ressourcen natürlich ganz anders vorhanden sind. Deshalb können solche Maßnahmen in kleinere Unternehmen durchaus nach hinten gereiht werden. Und in kritischer Infrastruktur sollte das natürlich als Priorität behandelt werden, um ein Risiko von einem solchen Angriff zu minimieren.

MG: Das heißt, wenn ich das kurz zusammenfassen darf. Sinnvoll ist es für jedes Unternehmen, egal ob kritische Infrastruktur oder nicht. Aber es gehört eben mit den Kosten abgewogen, ob es sich auszahlt.

E3: Genau.

MG: Beschwerten sich bereits einige Mitarbeiterinnen Mitarbeiter, dass solche Schulungen einen erheblichen negativen Einfluss auf den Arbeitsplatz haben bzw. sind ihnen solche Personen bekannt, die sich beschwerten?

E3: Ist mir nichts in diese Richtung bekannt. Weder in meinem jetzigen Unternehmen noch in vorhergehenden noch in Unternehmen, wo ich mit Sicherheit sagen kann, dass es solche Schulungen gibt.

MG: Also glaubst du schon, dass Mitarbeiterinnen und Mitarbeiter mittlerweile verstehen, dass Informationssicherheit wichtig ist und diese Maßnahmen durchgeführt werden müssen?

E3: Ja, exakt.

MG: Gut, dann war es das mit der ersten Hypothese und nun kommen wir zu zweiten, nämlich: „Jährliche Schulungen für Mitarbeiterinnen und Mitarbeiter können als Investition für den Informationssicherheit kritische Infrastruktur gesehen werden und sparen im Allgemeinen Kosten, wenn die Kosten für die Schulung in Relation mit den Kosten eines Vorfalles verglichen werden." Die erste Frage hierzu: "Gibt es verschiedene Varianten von Security-Awareness-Schulungen und wie unterscheiden sich diese in den jährlich anfallenden Kosten?"

E3: Also ich würde die größte Differenzierung dort machen, wer diese Schulungen durchführt. Ob das eine interne IT macht oder ob das ein Dienstleister macht. Eine, von einer dritten Firma durchgeführte Schulung hat höhere Kosten. Wenn eine interne Schulung stattfindet, sind die Kosten natürlich viel kalkulierbarer und geringer, als wenn eine Firma beauftragt werden muss.

MG: Wenn man jetzt quasi Kosten mit Qualität vergleicht, kann dann gesagt werden, dass in der Regel je teurer eine Security-Awareness-Schulung ist, desto besser ist Informationssicherheit eines Unternehmens geschützt bzw. desto besser ist die Awareness der einzelnen Mitarbeiter.

E3: Kann man wohl leider nicht sagen, denn der Preis von solchen Schulungen ist nicht immer abhängig von der Qualität. Ich würde grundsätzlich sagen, dass es sich lohnt, verschiedenste Angebote einzuholen, sofern es sich um Fremdfirmen handelt und wenn es sich um die interne IT handelt, dann sollte man versuchen nach bestem Wissen und Gewissen die Schulungen so aufzubereiten, dass es nirgends große Lücken gibt.

MG: Nun kommen wir zur nächsten Frage Wie hoch können die Kosten eines Social-Engineering Angriffs werden? Gibt es hier konkrete Zahlen, die man nennen kann? Von bis?

E3: Hier konkrete Zahlen zu nennen ist wer. Die Faktoren hierfür sind zum einen, dass es sicherlich eine große Dunkelziffer gibt an Angriffen, die gar nie publik gemacht werden. Und zum anderen ist die die, die Spanne von den Kosten immens groß. Da es einen großen Unterschied macht, ob eine Privatperson auf auf so einen solchen Angriff reinfällt oder ein. Unternehmen mit 5000 Mitarbeitern oder mehr. Es ist hier wirklich schwer zu sagen. Hier kann es losgehen von 100 Euro bis mehrere Millionen Euro schaden, je nachdem, wer das Opfer ist.

MG: Okay, dann äh, wie hoch ist die Chance, Opfer eines Angriffs zu werden und unterscheidet sich diese auch je nach Sparte und Größe des Unternehmens?

E3: Ohne einen konkreten Prozentwert an Wahrscheinlichkeit zu nennen. Es ist auch hierbei schwierig was zu sagen. Aber was man sicher sagen kann, dass die Größe des Unternehmens eine wichtige Rolle spielt. Denn generell das Ziel eines Angriffs wird man meistens nur dann erreichen, wenn sich auch das Ziel als lukrativ behaupten kann. Das heißt, zum einen kostet ein Angriff dem Angreifer natürlich auch immer eine gewisse Menge an Geld. Deshalb sollte am Ende natürlich auch zu mindestens das gleiche wieder herausspringen, aber, man kann sich natürlich vorstellen, dass ein Angriff natürlich gewinnorientiert ausgeführt werden wird oder in dem Grund das Unternehmen oder das Opfer nachhaltig zu schädigen zu wollen.

MG: Kann eigentlich gesagt werden, wie hoch die jährlichen Kosten einer Security-Awareness-Schulung werden können?

E3: Wie bereits erwähnt kommt es sehr stark darauf an, ob die Schulung durch die interne IT durchgeführt wird oder durch eine fremde Firma. Die jährlichen. Die jährlichen Kosten sind hierbei nicht zu kalkulieren, da es natürlich stark darauf ankommt, wie weit man in Schulden gehen möchte und welchen Umfang diese haben. Ich würde sagen, hierbei handelt es sich um einen stark individualisiertes Bildungspaket und die Kosten hier allgemein festzulegen ist nahezu unmöglich.

MG: Gibt es eigentlich Fälle, in dem sich Security-Schulungen nicht auszahlen und wenn ja, was wären diese? Jetzt mal die Tischlerei Meier außen vorgelassen. Hier wird es sich wahrscheinlich nicht so auszahlen.

E3: Ich denke, wenn man von sich selbst und als Unternehmen sagen kann, dass man kein lukratives Angriffsziel darstellt, wenn man weder die Größe noch das richtige Fachgebiet im Unternehmen hat, sind solche Schulungen in der Priorität natürlich hinten anzustellen, bzw. wenn man als Unternehmen gar keinen, keine Anbindung in Richtung Technik und Computersysteme hat, fällt die Schulung völlig außen vor. Grundsätzlich kann man aber sagen, dass es nie eine schlechte Idee ist, aber man eben wissen muss, ob mich ein solcher Angriff schädigen kann. Bei einem kleinen Friseur zum Beispiel, werden die Kosten einer Schulung einfach viel zu hoch sein und der Nutzen wird hier auch eher weniger sein. Bei kleinsten Unternehmen kann man auch sagen, es reicht wahrscheinlich einfach einmal eine Rundmail auszusenden, die ein bisschen darauf aufmerksam macht und die Leute bittet, diese zu lesen, denn die interne IT besteht meistens eh nur einer Person und hier fehlt auch einfach die Zeit und wie schon erwähnt, gehört abgewogen, ob das Unternehmen ein lukratives Ziel ist. Am. Ich denke, das ist der beste Weg hier, den hier wird so der Kosten-Nutzen optimal für so Kleinstunternehmen ausgenutzt. Aber es gibt natürlich auch Kleinstunternehmen die lukrativ sind.

MG: Und kommen wir nun zu den letzten beiden Fragen, und zwar die erste lautet: "Wie hoch sind die jährlichen Kosten für die technischen Maßnahmen oder physischen Maßnahmen, die einen Social-Engineering Angriff ebenfalls erschweren sollten? Kann man hier eine Zahl nennen?"

E3: Oh, also ähm, wie schon bei den Schulungen auch, sind diese auch oft sehr individuell. Bei individuellen Lösungen ist es dementsprechend auch schwer, sehr konkrete Zahlen zu nennen. Dort muss man natürlich auch verschiedenste Anbieter für solche technischen Maßnahmen vergleichen. Dort sind die Preise auch wirklich von vorn bis hinten angesiedelt. Also. Auch hier kann man kaum einen konkreten, getragenen.

MG: Nun zur letzten Frage: „Gibt es eigentlich technische Maßnahmen, die ausschließlich nur darauf ausgelegt sind, Social-Engineering Angriffe zu erschweren und wenn ja, welche sind diese?"

E3: Also wer mir dahingehend nichts bekannt.

MG: Okay. Das war es dann mit dem Interview und ich bedanke mich noch einmal für deine Zeit. Kurze Information. Ich werde das Interview jetzt transkribieren und die Ergebnisse werde ich mittels der qualitativen Inhaltsanalyse nach Mayring ausarbeiten und. Ja, diese Auswertung wird ausschließlich für die Master verwendet. Jetzt möchte ich mich noch einmal bedanken und werde die Aufnahmen jetzt beenden. Vielen Dank!

E3: Sehr gerne.

ANHANG F - Experteninterview – Experte 4

MG: Vielen Dank für Ihre Zeit, dass Sie mir helfen, bei der Beantwortung meiner Forschungsfrage, die lautet: "Welche Initiativen müssen gesetzt werden? Die Informationssicherheit von Unternehmen, kritische Infrastruktur im Kontext Social-Engineering zu gewährleisten, ohne einen beträchtlichen Mehraufwand für Mitarbeiterinnen und Mitarbeiter zu verursachen?" Kurzer Umriss des Themas über meine Arbeit ist, dass in der heutigen Zeit viele Angriffe auf Social-Engineering Basis passieren. Und es werden dort auch Maßnahmen gesetzt mit Schulungen oder Maßnahmen, die den Angriff auch erschweren sollen. Um herausfinden, ob das einerseits Mitarbeiterinnen und Mitarbeiter auf die Nerven geht und ob der Arbeitsfluss deswegen hier erheblich negativ beeinflusst wird, habe ich eine quantitative Analyse gemacht und mache jetzt eben Experteninterviews. Das Interview wird circa 30 bis 40 Minuten dauern und die Datenschutz Vereinbarung für die Aufnahme haben Sie bereits unterzeichnet und mir weitergeleitet. Dann würde ich sagen Beginnen wir mal mit den Einstiegsfragen und die erste Frage lautet: "Wie lange haben Sie schon mit Informationssicherheit zu tun?"

E4: Informationssicherheit habe ich ja beruflich seit ca. 6 Jahren zu tun.

MG: Wie hat sich seitdem verändert?

E4: Allgemein kommt das Thema mehr in den Fokus. Mittlerweile fließt auch viel Geld in das Thema, und zwar auch auf beiden Seiten. Einerseits auf der Angreifer, der Hacker Seite und auch auf der Verteidiger Seite, was eben Unternehmen und auch Privatpersonen darstellt.

MG: Das heißt, du bist der Meinung, dass mittlerweile auch das Management Ahnung davon hat, was ein Social-Engineering-Angriff oder welche Kosten ein Angriff verursachen kann.

E4: Mittlerweile sollte das jedes Management haben. Das war am Anfang sicher noch nicht so.

MG: Welchen Einfluss hat Social-Engineering hierbei?

E4: Social-Engineering ist im Wesentlichen der stärkste Vektor. Also Mitarbeiter, die nicht geschult sind, also gar nicht geschult sind, gar keine Ahnung davon haben, sind natürlich ein sehr hohes Sicherheitsrisiko.

MG: Das heißt, man kann mit Social-Engineering auch einen sehr großen Schaden bzw. sehr leicht an Informationen kommen.

E4: Natürlich, mit Social-Engineering kann man im Wesentlichen Fuß im Unternehmen fassen. Also auf jeden Fall.

MG: Was gehört zu Ihren täglichen Aufgaben und besteht hier eine Verbindung zu Social-Engineering?

E4: Bei meinen täglichen Aufgaben würde ich sagen, nicht direkt, nein, aber indirekt. Indirekt bei jedem Mitarbeiter. Jeder Mitarbeiter ist dann eine potentielle Schwachstelle. Ich bin für OT-Security zuständig und natürlich gehören die einzelnen Komponenten auch abgesichert, damit eben auch Social-Engineering erschwert wird und natürlich darf ich auch keine Informationen weitergeben, haha.

MG: Was ist deiner Meinung nach eine Personengruppe, die am meisten anfällig für Social-Engineering?

E4: Es sind solche Personen, die viel Kontakt nach außen haben und auch immer mit neuen Personen Kontakte knüpfen, wie zum Beispiel eine Personalabteilung oder der Vertrieb, das werden klassische Personengruppen sein. Diese werden am öftersten von unbekannten Personen angeschrieben, angerufen.

MG: Okay, dann war's das mit der Einleitung kommen wir nun zu den Schlüsselfragen und hier versuchen wir oder versuche ich die Hypothesen zu überprüfen? Und die erste Hypothese lautet: "Jährliche Schulungen für Mitarbeiterinnen und Mitarbeiter im Kontext Social-Engineering haben einen positiven Einfluss auf die Informationssicherheit von kritischen Infrastrukturen." Und meine erste Frage hier: "Erachten Sie solche Schulungen für sinnvoll? Und wenn ja, warum? Wenn nein, auch warum?"

E4: Natürlich sind diese sinnvoll und ja, das ist das einfachste und sicher auch das effektivste Mittel, um Social-Engineering entgegenzutreten. Im Endeffekt muss es der Mitarbeiter wissen, dass er das ausgenutzt werden kann. Und dafür braucht man Schulungen. Welche Form die Schulungen haben, ist wieder eine andere Frage.

MG: Und werden solche Schulungen bei Ihnen im derzeitigen Unternehmen eingesetzt oder wurden solche Schulungen in Ihren vergangenen Unternehmen eingesetzt?

E4: Ja, ich hoffe, es wird in jedem Unternehmen eingesetzt.

MG: Okay, kann eigentlich gemessen werden, ob solche Schulungen erfolgreich sind?

E4: Man kann natürlich keine hartnäckigen Prüfungen machen, aber es sollte eher spielerisch überprüft werden. Das geht natürlich.

MG: Sind Sie der Meinung, dass man, dass man das nicht wirklich messen kann, ob seine Schulungen erfolgreich sind?

E4: Wirklich aussagekräftig nicht. Natürlich kann es durch einen Angriff oder so überprüft werden, aber dieser müsste irgendwann stattfinden, wo keiner daran denkt und auch mit einem speziellen Ziel. Leider ist das nicht immer möglich, weil sich hier der Betriebsrat und so aufregen würde bzw. weiß ich gar nicht ob das Ganze überhaupt legal ist, unwissentlich Mitarbeiter zu überprüfen und dann eben an den Pranger stellen, wenn sie den Test nicht bestehen.

MG: Testet die Security-Abteilung Ihres derzeitigen Unternehmens oder Ihrer vergangenen Unternehmen selbstständig die Mitarbeiterinnen und Mitarbeiter mit Social-Engineering-Angriffe oder geben Sie den Auftrag an eine Dritte Firma?

E4: Nein, wenn dann nur teilweise an eine bestimmte Gruppe, wer auf wessen Link klickt. Aber direkt oder einen Massentest nicht. Wie gesagt, das würde auch Probleme mit dem Betriebsrat geben. Ich bin sowieso der Meinung, dass eine Überprüfung immer auf einen einzelnen oder einer einzelnen Gruppe sinnvoll ist, weil bei Massentest kommen dann auch wieder Gespräche in der Kaffeeküche auf.

MG: Und glaubst du, dass so ein Angriff viel erfolgreich wäre, wenn die Mitarbeiterinnen und Mitarbeiter keine Schulung besucht hätten?

E4: Die werden auf jeden Fall erfolgreicher. Man kann zwar schwer messen, wie erfolgreich eine Schulung genau bei jedem ist, aber im Allgemeinen helfen sie sehr gut.

MG: Wie sieht deiner Meinung nach der Aufbau einer solcher Security-Awareness-Schulung aus?

E4: Ja, das kann in verschiedensten Formen sein, natürlich. Bei unserem Unternehmen zum Beispiel wird jeder erstmalig bei den Welcome Days persönlich mit den Basics geschult. Das ist eine Form in den meisten Unternehmen, würde ich behaupten. Es gibt dann auch noch Online-Kurse, die einmal jährlich oder so durchgeführt werden. Hier ist der Vorteil, dass die Mitarbeiter diese durchführen können, wann sie wollen. Diese Schulung ist dann natürlich auch günstigere. Es gibt dann noch Vor-Ort-Schulungen, wo entweder die interne IT eine Schulung gestaltet oder das Ganze an ein anderes Unternehmen ausgelagert wird. Von der Effizienz sind diese wahrscheinlich die mit dem besten Erfolg. Ja, ich glaube, das waren die Varianten.

MG: Erachtest du sogenannte Online-Schulungen auch für sinnvoll?

E4: Sicher nicht bei jedem, weil für viele ist es eigentlich lästig. Aber ja, wenn die Schulungen wirklich wiederkehrend sind und zum Beispiel einmal im Jahr, dann ist das sicher eine gute und günstige Maßnahme.

MG: Okay, dann zu einer anderen Frage. Gibt es eigentlich noch andere technische Maßnahmen oder physische Maßnahmen, um einen Social-Engineering Angriff zu erschweren?

E4: Technische Maßnahmen. Schwierig, wahrscheinlich nicht, dass alle Social-Engineering Angriffe blockiert werden. Natürlich kann man immer technisch eingreifen, aber nicht in vollem Umfang. Eine einzelne Person wird deswegen nicht angegriffen. Sie helfen sicher für die Masse ein bisschen, aber für die einzelne Person nicht, nein.

MG: Das heißt, du bist der Meinung, mit technischen Maßnahmen wie zum Beispiel einen Spamfilter oder eine Indikation kann man nur im Allgemeinen in Masse schützen, aber nicht die einzelne Person.

MG: Okay, und welche Maßnahmen wären das zum Beispiel?

E4: Im wesentlichen Mail Filter, beschränkte Zugriffsberechtigungen. Also wenn zum Beispiel die Personalabteilung auf alle Dateien im Unternehmen zugreifen kann ist das natürlich viel gefährlicher, als wenn sie nur begrenzten Zugriff hat. Im Endeffekt sind fast alle diese Mechanismen, die es gibt, also Zugangsbeschränkungen, Security Tools wie Spamfilter, Firewall, Segmentierung auch ein Schutz gegen Social-Engineering für die Masse, aber eben nicht für den einzelnen.

MG: Okay, äh, wie sinnvoll empfindest du diese Maßnahmen?

E4: Sie sind sehr sinnvoll und müssen auf jeden Fall getätigt werden. Ja sicher, aber nicht nur wegen Social-Engineering. Aber ja, Social-Engineering ist natürlich ein Teil, warum sie implementiert werden.

MG: Kann es in einzelnen Szenarien wie in einem Unternehmen kritische Infrastruktur sinnvoll sein, Maßnahmen einzusetzen, die in anderen, nicht kritischen Infrastrukturen nicht notwendig wären?

E4: Kritische Infrastrukturen haben per Definition einen erhöhten Schutzbedarf. Aber natürlich ist es auch sinnvoll bei den Nicht-kritischen Infrastrukturen Maßnahmen einzusetzen. Es gehört unterschieden zwischen sinnvoll und notwendig. Sinnvoll ist es immer, notwendig, da gehört schon abgewogen. Da ein Angriff auf kritische Infrastruktur viel gefährlicher sein kann, muss hier die Notwendigkeit der Maßnahmen eben rauf geschraubt werden. Die Mitarbeiter selber müssen eben auch wissen, dass falls Informationen nach außen geraten, in einer kritischen Infrastruktur schlimmer sein kann als in anderen Unternehmen.

MG: Das heißt wahrscheinlich einfach das Sicherheitsempfinden der Mitarbeiterinnen Mitarbeiter soll bei kritischer-Infrastruktur einfach höher sein als bei anderen?

E4: Genau, genau, es ist notwendig das Sicherheitsgefühl der einzelnen Mitarbeiter zu erhöhen.

MG: Kennst du eigentlich einige Mitarbeiterinnen und Mitarbeiter, die sie über sich über solche Schulungen oder solche technischen Maßnahmen beschwerten, weil sie einen erheblich negativen Einfluss auf den Arbeitsfluss haben?

E4: In der Regel nicht beschweren. Nein, eher belächeln. Aber, es wird wahrscheinlich jeder sagen, dass die Sinn machen. Ja, also jeder kennt mittlerweile sicher Vorfälle, auch im privaten Umkreis und auch Vorfälle, die negativ ausgegangen sind. Also ich glaube Beschwerden würde sich keiner.

MG: Belächeln, weil sie das Ganze nicht so verstehen?

E4: Ja, viele verstehen es nicht ganz. Sie wissen, dass ein Angriff schlimm sein kann, aber sie verstehen nicht ganz, dass schon Kleinigkeiten, wie das Aufheben eines USB-Sticks auf der Straße, der erste Schritt eines großen Angriffs sein kann. Deswegen ist es auch wichtig, immer wiederkehrend zu schulen, damit auch Kleinigkeiten immer in Erinnerung gerufen wird. Auch wenn es belächelt wird, die Mitarbeiter merken es sich.

MG: Das war es mit der Hypothese eins und kommen wir nun zur nächsten Hypothese, nämlich: "Jährliche Schulungen für Mitarbeiterinnen und Mitarbeiter können als Investition für die Informationssicherheit kritische Infrastruktur gesehen werden und sparen im Allgemeinen Kosten, wenn die Kosten für die Schulung in Relation mit den Kosten eines Vorfalles verglichen werden." Du hast es vorher schon angeschnitten, aber ich will jetzt noch mal genauer darauf eingehen. Du meintest, es gibt verschiedene Varianten von Schulungen. Wie unterscheiden sich diese und unterscheiden sich diese auch mit den Kosten?

E4: Ja, Kosten kann ich natürlich nicht genau beantworten, aber natürlich gibt es Unterschiede. Die unterschiedlichen Varianten kann man natürlich auch in unterschiedlichen Preisklassen ansiedeln. Aber natürlich, wenn es nicht die Standard-Schulung ist, die die auf YouTube vielleicht schon ist, kostet es natürlich Geld. Aber je kreativer man in der Regel ist, desto effektiver sind diese und natürlich auch teurer. Wie oben bereits gesagt, Vor-Ort-Schulungen sind teurer, aber eben wahrscheinlich auch besser für die Sicherheit.

MG: Okay, das heißt, dann hast du die nächste Frage ebenso ein wenig beantwortet. Also es kann gesagt werden, dass in der Regel, je teurer eine Security-Awareness -Schulung ist, desto besser. Es gehört eben auch die Qualität der einzelnen Angebote verglichen, aber ich bin der Meinung, dass im Vergleich eine Online-Schulung nicht das gleiche Resultat erzielt, wie eine Vor-Ort und die Online sind meistens immer günstiger.

MG: Nun kommen wir zu einer anderen Frage, nämlich auf der anderen Seite. Wie hoch können die Kosten eines Angriffs werden? Kann man da etwas sagen?

E4: Die Kosten, die können ja unendlich groß werden. Am. Sie können Unternehmen in den Konkurs bringen. Aber natürlich können solche Angriffe auch nicht der Rede wert sein.

MG: Und wie hoch ist die Chance, Opfer eines solchen Angriffs zu werden und unterscheidet sich diese auch je nach Sparte und Größe des Unternehmens?

E4: Die unterscheidet sich natürlich, aber selbst Privatpersonen werden Opfer von solchen Angriffen. Also jedes Unternehmen ist damit konfrontiert und die Chance unterscheidet sich nämlich. Aber man muss immer aufpassen, vor allem bei Unternehmen kritischer Infrastruktur. Je größer zum Beispiel ein Unternehmen ist, desto mehr kann aus einem Angriff rausgeholt werden, jetzt aus Angreifer-Sicht.

MG: Okay, und die nächste Frage: "Da du nicht direkt im operativen Teil in der Informationssicherheit tätig bist, wirst du mir hier wahrscheinlich keine konkreten Zahlen nennen können. Aber wie hoch können die jährlichen Kosten einer Security Schulung werden?"

E4: Ja genau. Kann ich nicht ganz genau sagen. Man muss halt wissen, auf welche Schulung setze ich. Wie gesagt, je mehr Zeit eine Schulung in Anspruch nimmt, wenn zum Beispiel einzelne Szenarien Live dargestellt werden, am, desto besser und desto teurer ist die Schulung in der Regel. Es kommt halt auf die Variante an.

MG: Gibt es eigentlich Fälle, in denen sich Security-Awareness-Schulungen nicht auszahlen? Wenn ja, was wären diese?

E4: Ja, natürlich. Die Schulungen müssen natürlich für die Zielgruppe passen, darf nicht zu oft sein, darf nicht zu lang sein. Man braucht auf jeden Fall die Aufmerksamkeit vom Publikum. Natürlich gibt es diese Fälle, in denen es sich nicht auszahlt. Mir fällt jetzt zum Beispiel sehr kleine Unternehmen ein, die eigentlich wenig Bezug zur IT haben. Was weiß ich, eine Dönerbude zum Beispiel, haha.

MG: Okay, aber im Allgemeinen bei großen Unternehmen, bei KMUs, vor allem Unternehmen, die viel mit IT zu tun haben oder viel mit Informationen zu tun haben, die für den Erfolg des Unternehmens zu haben, zahlen sich solche Schulungen immer aus?

E4: Ja, immer. Wie oben schon gesagt, sinnvoll sind sie dennoch immer, aber die Notwendigkeit ist halt bei einigen kleinen Unternehmen, einzelnen Personengruppen geringer. Ja.

MG: Okay, die nächste Frage lautet: "Kannst du mir eventuell hier eine Zahl nennen, wie hoch die jährlichen Kosten für technische Maßnahmen sind, die einen Angriff erschweren sollen, sein können.

E4: Es gibt hier keine konkrete Zahl. Je nachdem was man haben will und was man braucht. Setze ich auf gratis Produkte oder leiste ich mir teure, aber sehr gute Produkte. Dann muss man auch die Kosten der Mitarbeiter berücksichtigen, die das Ganze warten oder implementieren. Es kann auch hier immense Kosten verursachen. Was ist halt wieder notwendig für mein Unternehmen gehört abgeschätzt. Am. Es gehört eine Risikoabschätzung gemacht, was mich ein Angriff kosten kann und ob sich genau diese technischen Maßnahmen dann hier auszahlen.

MG: Gibt es eigentlich technische Maßnahmen, die nur darauf ausgelegt sind, Angriffe zu erschweren und wenn ja, welche sind diese?

E4: Nur darauf ausgelegt sind. Mhmm. Die gibt es nur für Social-Engineering wahrscheinlich nicht. Mir ist halt nichts bekannt. Eben Spamfilter, 2-Faktor-Authentication helfen natürlich, aber sind nicht nur auf Social-Engineering ausgelegt.

MG: Gut, dann wars das mit dem Interview. Dann würde ich mich noch einmal bedanken für die Zeit und das Interview werde ich jetzt transkribieren und dann im Anschluss mit der qualitativen Inhaltsanalyse nach Mayring mit dem Programm MAXQDA durchführen. Die Aufnahme wird ausschließlich für die Masterarbeit verwendet. Und dann, wenn keine Fragen mehr sind, werde ich die Aufnahme jetzt beenden.

E4: Keine Fragen mehr und gern geschehen.

ANHANG G - Experteninterview – Experte 5

MG: Wie lange haben Sie schon mit Informationssicherheit zu tun und wie hat es sich seitdem verändert?

E5: ca. 7 Jahre

Meiner Meinung nach hat sich das Bewusstsein hier zumindest bei mittleren und großen Unternehmen schon deutlich verbessert. Kleine Unternehmen ignorieren das Thema leider noch immer oft. Gründe dafür können vielfältig sein, z.B. dass der potentielle Schaden zu gering ist oder unterschätzt wird, manche Firmen machen auch den Fehler, dass sie sich zu klein bzw. unwichtig halten, um Ziel eines Cyber-Angriffs zu werden.

Ein weiterer Trend, der zumindest im Konzernumfeld zunimmt ist, ist zu Zusammenarbeit mit einem Managed Security Service Provider (MSSP). Je nach Ausprägung übernimmt hier ein spezialisierter Dienstleister Teile der Aufgaben, die im Unternehmen selbst nicht adäquat erledigt werden können. (z.B. 24/7 Eventmonitoring oder Incident-Response)

MG: Welchen Einfluss hat Social-Engineering in Bezug auf Informationssicherheit?

E5: Social Engineering wird bei einem Großteil der nicht automatisierten Cyber-Angriffen als initialer Angriffsvektor verwendet. Das liegt sicherlich daran, dass es für einen Angreifer in der Regel viel einfacher ist mit SE Techniken einmal einen Fuß im Netzwerk zu haben als z.B. eine Zero Day Lücke in einem Produkt zu finden und erfolgreich auszunutzen.

Speziell in größeren Firmen sorgt ein funktionierendes Patch- und Vulnerability-Management dafür, dass ein Angreifer nicht auf bekannte Lücken zurückgreifen kann.

MG: Was gehört zu Ihren täglichen Aufgaben und besteht hier auch eine Verbindung zu Social-Engineering?

E5: Zu meinen täglichen Aufgaben gehört unter anderem die Einschätzung und Validierung von Security relevanten Events, die in den verschiedensten Tools generiert und zuvor von einem MSSP klassifiziert und bei Bedarf an mich weitergeleitet werden. Dabei geht es zu Beginn oft darum abzuklären ob der User selbst eine Aktion z.B. Download, Login,… ausgeführt hat oder nicht.

Social Engineering spielt hier eine große Rolle, viele Tickets werden auch von aufmerksamen Usern generiert, die z.B. auf einen Link in einem potentiellen Phishing-Mail geklickt haben und das abgeklärt haben möchten. Im besten Fall geben wir nach unserer Analyse Entwarnung, manchmal ist das aber auch der Startschuss für gezielte Gegenmaßnahmen oder weiter Nachforschungen. Mitarbeiter, die solche Vorfälle melden sind extrem wertvoll für ein Unternehmen und können dazu beitragen die Awareness generell zu schärfen und eine Fehlerkultur zu etablieren die es Angreifern noch einmal schwerer macht.

Ein weiteres Thema, mit dem ich mich beschäftige, sind Security Awareness Schulungen und Überprüfungen. Hier geht es darum globale, aber auch lokale Trainings Kampagnen zu erstellen und durchzuführen.

MG: Welche Personengruppe ist am meisten für Social-Engineering-Angriffe gefährdet und warum genau diese?

E5: Grundsätzlich ist jeder Mitarbeiter ein potentielles Ziel, selbst wenn dieser nicht einmal über einen Computer verfügt. Viele Social Engineering Techniken funktionieren so gut, weil wir seit unserer Geburt darauf trainiert und dazu erzogen werden höflich und zuvorkommend zu sein. Tailgating ist hier eine sehr simple Technik, die auch heute noch bei viel zu vielen Unternehmen problemlos funktioniert. Dabei versucht der Angreifer unbefugt auf das Firmengelände zu kommen indem er/sie versucht einfach nach einem Mitarbeiter, der die Tür entriegelt hat einzutreten.

Das ist auch der Grund, warum es in hoch sensiblen Bereichen nicht ausreicht, nur Personen die täglich mit einem PC arbeiten zu schulen.

Aus der Perspektive des Angreifers gibt es natürlich Unterschiede bei den Zielpersonen. Ein klassischer „blue-collar“ Mitarbeiter z.B. in der Produktion könnte dazu missbraucht werden, um physischen Zugang zu erhalten, typische Büroangestellte, die über Rechte im IT-System verfügen sind dann schon interessanter, um limitierten Zugang zu erhalten. Besonders gefährdet sind alle Mitarbeiter, die für kritische Unternehmensprozesse zuständig sind und z.B. Zahlungen freigeben können, aber natürlich auch Administratoren, die über sehr weitreichende Berechtigungen verfügen und bei einer Kompromittierung schnell die ganze Infrastruktur in Gefahr bringen können.

Wie auch bei technischen Angriffen ist der initial verwendete Angriffsvektor meist nicht auf die eigentliche Zielperson ausgerichtet, sondern arbeitet sich der Angreifer von einem System bzw. Mitarbeiter zum nächsten. Man spricht dann von Lateral Movement.

MG: Erachten Sie Security-Awareness-Schulungen für sinnvoll und wenn ja, warum und wenn nein, warum nicht?

E5: Ja. SE Schulungen können zwar Angriffe niemals zu 100% verhindern, machen es für einem Angreifer aber schwieriger. Außerdem kann ein geschärftes Bewusstsein auch dabei helfen Angriffe frühzeitig zu erkennen und größeren Schaden noch abzuwenden.

MG: Werden aktuell solche Security-Awareness-Schulungen bei Ihnen im derzeitigen Unternehmen eingesetzt oder wurden solche Schulungen in Ihren vergangenen Unternehmen eingesetzt?

E5: Ja.

MG: Kann gemessen werden, ob solche Schulungen erfolgreich sind?

E5: Ja. Dazu gibt es verschiedene Möglichkeiten wie z.B. Phishing Simulationen, Kontrollfragen nach einer Schulung, Gewinnspiele, usw…

MG: Testet die Security-Abteilung-selbstständig die Mitarbeiterinnen und Mitarbeiter mit Social-Engineering-Angriffe?

E5: Ja.

MG: Wie erfolgreich wären solche Tests, bei Personen ohne Besuch einer Security-Awareness-Schulung im Gegensatz zu Personen mit dem Besuch einer Security-Awareness-Schulungen?

E5: Aus meiner Erfahrung kann ich sagen, dass die Fehlerquote bei einer Phishing Simulation ohne vorheriges Training zwischen 30 und 60 % liegt. Dabei zu beachten ist, dass diese hohen Werte aber nur mit Spear Phishing möglich sin, also extrem auf die Zielperson oder Gruppe zugeschnittene Angriffe.

Nach Absolvierung mehrerer Trainings kann dieser Wert ca. auf 5 – 10% reduziert werden, die Wirkung lässt aber schnell nach, daher sollten Schulungen regelmäßig durchgeführt werden.

MG: Wie sieht der Aufbau einer Security-Awareness-Schulung aus?

E5: Da gibt es verschiedene Ansätze, reine online Kurse und Module, persönlich oder auch Mischungen aus beidem. Üblicherweise misst man vor der allerersten Schulung einmal die Fehlerquote, um eine Baseline zu erhalten, z.B. mit einer Phishing Simulation. Anschließend werden die Mitarbeiter geschult und nach einer angemessenen Frist eine erneute Überprüfung durchgeführt und das Ergebnis bewertet.

MG: Gibt es noch andere, technische Maßnahmen, um einen Social-Engineering-Angriff zu erschweren?

E5: Ja natürlich, die Gegenmaßnahmen können vielfältig sein.

MG: Erläutern Sie bitte die anderen Maßnahmen genauer?

E5: Eine sehr einfache, aber effektive Maßnahme ist das Einführen eines E-Mail-Headers. Dabei werden alle Emails, die von extern empfangen werden mit einem farblich hervorgehobenen Header versehen, der die Mitarbeiter darauf hinweist, dass es sich um ein externes Mail handelt und besondere Vorsicht geboten ist. Beim Thema E-Mail bieten sich noch weitere Möglichkeiten je nach Unternehmen an, wie z.B. das Blockieren von verdächtigen Attachments, oder generell die Nutzung von Signaturen und Verschlüsselung.

Technisch ist 2FA ein großer Schritt in die richtige Richtung.

MG: Wie sinnvoll empfinden Sie diese Maßnahmen?

E5: Das hängt immer vom Fall ab, z.B. ist 2FA bei IT lastigen Unternehmen oft schon in Verwendung, wäre aber für die meisten Arbeiter in einem Produktionsbetrieb wahrscheinlich nicht sinnvoll umsetzbar.

Grundsätzlich muss hier eine Abwägung von Machbarkeit und Sicherheit getroffen werden. Man kennt die berühmten Bilder von Passwörtern, die unter die Tastatur oder sogar neben den Monitor geklebt werden. Das ist oft das Resultat, wenn die Passwortrichtlinien zur Belastung für die Mitarbeiter werden oder Accounts von mehreren Personen verwendet werden.

MG: Kann es in einzelnen Szenarien, wie in einem Unternehmen kritischer Infrastruktur, sinnvoll sein, Maßnahmen einzusetzen, die in anderen, nicht kritischen Infrastrukturen, nicht notwendig wären?

E5: Natürlich, der Atomkraftwerksbetreiber muss ganz andere Sicherheit gewährleisten als der Betreiber eines Online-Portals. Im Grunde geht es immer darum den potentiellen Schaden dem Aufwand entgegenzustellen.

Nicht alle Risiken und Gefahren können sinnvoll verhindert werden, es ist für ein Unternehmen aber essentiell sich über diese Risiken und deren potentielle Auswirkungen im Klaren zu sein.

MG: Beschwerden sich bereits Mitarbeiterinnen und Mitarbeiter, dass solche Schulungen einen erheblichen negativen Einfluss auf den Arbeitsfluss haben?

E5: Manchmal passiert das, dem kann man mit verpflichtenden Schulungen und spannendem und abwechslungsreichen Schulungsmaterial aber sehr gut begegnen.

MG: Gibt es verschiedene Varianten von Security-Awareness-Schulungen?

E5: Es gibt verschiedenste Varianten und Anbieter auf dem Gebiet, mache bieten diese Schulungen als Nebenprodukt zu einer Lizenz einer anderen Software an, andere Firmen vertreiben Security Schulungen auch als Hauptprodukt.

MG: Wie unterscheiden sich diese in den jährlich anfallenden Kosten?

E5: Bei kombinierten Angeboten, ist das nicht so einfach zu sagen, fällt aber bei den eigentlichen Lizenzkosten soweit ich weiß, nicht wirklich ins Gewicht.

Bei Anbietern, die sich auf das Thema spezialisiert haben, sind die Kosten stark von der Anzahl der User ab. Man kann mit ca. 5 – 20$ pro User pro Jahr rechnen, große Konzerne mit mehreren Tausend Mitarbeitern kommen hier natürlich noch deutlich günstiger davon.

MG: Kann pauschal gesagt werden, je teurer eine Security-Awareness-Schulung, desto besser ist die Informationssicherheit eines Unternehmens geschützt

E5: Nein, die Schulungen sind nur ein Puzzlestein, um die Informationssicherheit eines Unternehmens zu erhöhen, können aber auch völlig ins Leere gehen, wenn es zu einer Alibi Aktion wird.

MG: Wie hoch können die Kosten eines Social-Engineering-Angriff werden?

E5: Im Schlimmsten Fall kann ein SE Angriff ein Unternehmen die Existenz kosten. Der schlimmste überhaupt denkbare Ausgang wäre, wenn zusätzlich noch Menschen sterben (Atomkraftwerk, Schwerindustrie, Autonomes Fahren,….), oder sogar Kriege ausgelöst werden.

MG: Wie hoch ist die Chance, Opfer eines Social-Engineering-Angriffs zu werden und unterscheidet sich diese auch je nach Sparte und Größe des Unternehmens?

E5: Das ist schwer zu sagen, generell sind größere Konzerne meist anonymer als kleine familiäre Unternehmen. Dadurch ist es leichter für einen Angreifer z.B. per Pretexting und CEO-Fraud Druck auf einzelne Mitarbeiter auszuüben und z.B. Accounts zu übernehmen. Auf der anderen Seite sind sich große Unternehmen meist der Gefahr bewusst und ergreifen davor schon Maßnahmen, um Angriffe zu erschweren und zu vereiteln.

Ich denke, dass jeder schon einmal Opfer eines SE Angriffs war, wenn auch meistens nur mit minimalem Schaden. Viele Verkäufer beispielsweise nutzten sehr ähnliche Techniken, um ihre

„Opfer“ zum Kauf zu bewegen. Ähnliche Techniken werden auch in Politik und in der Kommunikation untereinander oft unbewusst eingesetzt. Ich würde sogar noch einen Schritt weiter gehen und sagen die meisten Menschen nutzten gewisse SE-Techniken, um Andere im täglichen Leben zu beeinflussen oder zu manipulieren.

MG: Wie hoch können die jährlichen Kosten einer Security-Awareness-Schulung werden?

E5: Ich denke in hochsensiblen Bereichen kann der Umfang des Trainings und die Kosten sicher noch deutlich höher sein, ich kann aber hier keine genaue Zahl nennen.

MG: Gibt es Fälle, in dem sich Security-Awareness-Schulungen nicht auszahlen, wenn ja, was wären diese?

E5: Immer dann, wenn der zu erwartende Schaden in keinem sinnvollen Verhältnis zum Aufwand der Schulung steht.

MG: Wie hoch sind die jährlichen Kosten für technische Maßnahmen, die einen Social-Engineering-Angriff ebenfalls erschweren soll?

E5: Das kann man allgemein nicht sagen, hier spielen so viele Dinge hinein, das reicht von der physischen Sicherheit, über Support bis hin zu 2FA und der etablierten Firmenkultur.

MG: Gibt es technische Maßnahmen, die nur darauf ausgelegt sind, Social-Engineering-Angriffe zu erschweren und wenn ja, welche sind diese?

E5: Generell geht es im IT-Umfeld ums Ausnutzen von erlerntem Menschlichen Verhalten, um technische Sicherheitsmaßnahmen zu umgehen. Mir fällt keine technische Maßnahme ein die ausschließlich zur Abwehr von SE Angriffen dient. Es können gewisse Mechanismen in Prozessen integriert werden, die darauf abzielen, diese bieten aber auch wieder Schnittstellen und Möglichkeiten angegriffen zu werden.

Ein bekanntes Beispiel aus einem Buch, das ich dir sehr empfehlen kann, wurde in den 80ern bei Banken eingesetzt. („The Art of Deception“, Kevin Mitnick) Hier wurde eine zusätzliche Hürde für Zahlungen eingeführt, ein Zahlencode der täglich geändert wurde und bei jeder Überweisung die intern per Telefon angestoßen wurde auch von Anrufer genannt werden musste. Kevin Mitnick war zu dieser Zeit als externer Techniker vor Ort und musste nicht lange suchen, bis er den benötigten Code irgendwo auf einem Post-it fand. Im nächsten Schritt hat er von einem internen Telefon aus Zahlungen in Millionenhöhe veranlasst die auch anstandslos durchgeführt wurden, nachdem er den aktuellen Code nannte.

ANHANG H - Paraphrasen der Einleitung

ca. zehn Jahre	Erfahrung
Überprüfung von Software und Produkten auf deren IT-Sicherheit und Reporting von Schwachstellen	Erfahrung
ca. sechs Jahre	Erfahrung
Ich bin im Bereich der OT-Security tätig und sichere hier einzelne Komponenten ab, damit unter anderem auch Social-Engineering erschwert wird	Erfahrung
ca. sieben Jahre	Erfahrung
Die Einschätzung und Validierung von Security relevanten Events	Erfahrung
Die Abklärung ob zum Beispiel ein User eine Aktion (Download, Login) ausgeführt hat oder nicht	Erfahrung
Ich beschäftige mich auch mit Security-Awareness-Schulungen und der anschließenden Überprüfung	Erfahrung
ca. sechs Jahre	Erfahrung
Ich bin im Managed-Service-Provider tätig und hier habe ich auch sehr viel mit Informationssicherheit zu tun	Erfahrung
Meine Hauptaufgaben sind die Umsetzung von Konzepten, die unter anderem auch Social-Engineering verhindern sollen	Erfahrung
Ca. zehn Jahre	Erfahrung
Vieles ist komplizierter geworden, was es erleichtert und erschwert zugleich, Lücken in Systemen zu finden	Entwicklung
Budget wird meistens erst nach einem Vorfall genehmigt	Entwicklung
Ein gewisses Bewusstsein für Social-Engineering wurde geschaffen	Entwicklung
Mehr als 95% aller Angriffe sind auf Social-Engineering zurückzuführen	Entwicklung
Großer Einfluss auf Data-Leaks	Entwicklung
Software und Programme werden immer sicherer und Lücken sind immer schwieriger zu finden, deswegen wird oft auf die humanitäre Ebene gesetzt	Entwicklung
Informationssicherheit wird allgemein bekannter	Entwicklung
Großer Geldfluss sowohl auf der Angreifer:in Seite, als auch auf der Verteidiger:in Seite	Entwicklung
Management weiß mittlerweile, dass die Informationssicherheit ein wichtiger Bereich ist	Entwicklung
Social-Engineering ist im Wesentlichen der stärkste Vektor	Entwicklung
Mit Social-Engineering kann man im wesentlichen Fuß im Unternehmen fassen	Entwicklung
Das Bewusstsein für Informationssicherheit von mittelgroßen und großen Unternehmen hat sich deutlich verbessert	Entwicklung
Kleine Firmen ignorieren das Thema Informationssicherheit noch oft	Entwicklung
Manche Unternehmen halten sich für zu klein oder unwichtig, um Opfer eines Cyber-Angriffs zu werden	Entwicklung
Ein Trend ist, dass mittlerweile viele Unternehmen mit Managed-Security-Service-Provider zusammenarbeiten	Entwicklung
Social-Engineering wird oft als initialer Angriffsvektor verwendet	Entwicklung
Social-Engineering hat eine große Rolle, auch für aufmerksame User	Entwicklung
Oft wird nach einem vermeintlichen Vorfall Entwarnung gegeben, aber manchmal ist hier auch der Startschuss für einen Social-Engineering-Angriff	Entwicklung
Mitarbeiterinnen und Mitarbeiter die Vorfälle melden sind wertvoll für ein Unternehmen	Entwicklung
Viele Social-Engineering-Techniken funktionieren, weil wir erzogen worden sind, höflich und zuvorkommend zu sein	Entwicklung
Security Themen werden mittlerweile als erstes betrachtet	Entwicklung
Der User ist die Nummer 1 Schwachstelle	Entwicklung
Top-Management schenkt der Informationssicherheit mehr Beachtung	Entwicklung

Durch Digitalisierung, Hackerangriffe, etc. bekommt das Thema Informationssicherheit einen immer höher werdenden Stellenwert	Entwicklung
Viele Medien sind auch auf das Thema aufgesprungen und deswegen wissen auch nicht-IT-Affine Personen über das Thema Informationssicherheit bescheid	Entwicklung
Social-Engineering hat einen großen Einfluss auf die Informationssicherheit	Entwicklung
Social-Engineering ist ein Einfallsvektor, wie beispielsweise in ein Unternehmen eingetreten werden kann	Entwicklung
Social-Engineering wird für Kriminelle immer interessanter	Entwicklung
Normale User, weil ein gewisses Bewusstsein fehlt	gefährdete Personengruppe
Eine gewisse Naivität der normalen User verursacht falsches Vertrauen	gefährdete Personengruppe
Personen, die viel Kontakt nach Außen haben	gefährdete Personengruppe
Jede Person ist anfällig für einen Social-Engineering-Angriff	gefährdete Personengruppe
Blue-Collar Mitarbeiterinnen und Mitarbeiter werden dazu missbraucht physischen Zugang zu erhalten	gefährdete Personengruppe
Typische Büroangestellte werden missbraucht, um Zugang zu IT-Systemen zu bekommen	gefährdete Personengruppe
Eine besonders kritische Personengruppe sind Personen, die für kritische Unternehmensprozesse zuständig sind, z.B. Zahlungen freigeben	gefährdete Personengruppe
Administratoren mit weitreichenden Berechtigungen können im Falle eines erfolgreichen Social-Engineering-Angriffs die ganze Infrastruktur in Gefahr bringen	gefährdete Personengruppe
Ein Angriff ist meist nicht nur auf eine Zielperson ausgerichtet, sondern arbeitet sich in einem System von einer Person zur nächsten weiter. Das nennt man Lateral-Movement	gefährdete Personengruppe
Es gibt keine spezielle Personengruppe die besonders anfällig sind, es ist abhängig wie gut Personen in diesem Bereich geschult sind	gefährdete Personengruppe
Stress macht eine Person besonders anfällig für einen Social-Engineering-Angriff	gefährdete Personengruppe
Auch die besten Sicherheitsexpertinnen und Sicherheitsexperten könnten Opfer eines Angriffs werden	gefährdete Personengruppe
Jede Personengruppe ist anfällig für Social-Engineering	gefährdete Personengruppe
Es muss mit der jeweiligen Personengruppe einfach agiert werden, um an Informationen zu kommen	gefährdete Personengruppe
Am einfachsten ist ein Social-Engineering-Angriff bei einer Person, die sehr hilfsbereit ist	gefährdete Personengruppe
Mit der richtigen Technik bekommt man von jeder Person die Informationen, die benötigt werden	gefährdete Personengruppe

Tabelle 6: Paraphrasen der Einleitung

ANHANG I - Paraphrasen für die Prüfung von Hypothese 1

Ja, Security-Awareness-Schulungen sind sinnvoll	Sinnhaftigkeit von Security-Awareness-Schulungen
Zu viele Security-Awareness-Schulungen sind weniger sinnvoll	Sinnhaftigkeit von Security-Awareness-Schulungen
Personen mit IT-Knowhow benötigen keine Security-Awareness-Schulungen im großen Ausmaß	Sinnhaftigkeit von Security-Awareness-Schulungen
Wenn Unternehmen kein lukratives Angriffsziel darstellt, nicht die Größe oder das richtige Fachgebiet hat oder keine Anbindung in Richtung Technik und Computersysteme, haben Security-Awareness-Schulungen eine niedrigere Priorität	Sinnhaftigkeit von Security-Awareness-Schulungen
Ungeschultes Personal sind ein sehr hohes Sicherheitsrisiko	Sinnhaftigkeit von Security-Awareness-Schulungen
Security-Awareness-Schulungen sind sinnvoll und auch das effektivste Mittel, um Social-Engineering entgegenzutreten	Sinnhaftigkeit von Security-Awareness-Schulungen
Die Mitarbeiterin oder der Mitarbeiter muss wissen, dass er oder sie ausgenutzt werden kann, und das wird mit Schulungen erreicht	Sinnhaftigkeit von Security-Awareness-Schulungen
Ja, Security-Awareness-Schulungen werden bei uns im Unternehmen eingesetzt	Sinnhaftigkeit von Security-Awareness-Schulungen
Bei kleinen Unternehmen, die wenig Bezug zur IT haben, zahlt sich eine Schulung nicht aus	Sinnhaftigkeit von Security-Awareness-Schulungen
Bei großen Unternehmen zahlt sich eine Security-Awareness-Schulung immer aus	Sinnhaftigkeit von Security-Awareness-Schulungen
Security-Awareness-Schulungen können einen Angriff nicht zu 100% verhindern, aber sie machen es für eine Angreiferin oder einen Angreifer schwieriger	Sinnhaftigkeit von Security-Awareness-Schulungen
Ein geschärftes Bewusstsein hilft auch Angriffe frühzeitig zu erkennen	Sinnhaftigkeit von Security-Awareness-Schulungen
Ja, Security-Awareness-Schulungen werden bei uns im Unternehmen durchgeführt	Sinnhaftigkeit von Security-Awareness-Schulungen
Security-Awareness-Schulungen sind nur ein Puzzlestein, um die Informationssicherheit eines Unternehmens zu erhöhen	Sinnhaftigkeit von Security-Awareness-Schulungen
Eine Security-Awareness-Schulung zahlt sich nicht aus, wenn der zu erwartende Schaden in keinem sinnvollen Verhältnis zum Aufwand steht	Sinnhaftigkeit von Security-Awareness-Schulungen
Ja, Schulungen sind sehr sinnvoll	Sinnhaftigkeit von Security-Awareness-Schulungen
Abteilungsspezifische Schulungen sind sinnvoll und empfehle ich und allgemeine Schulungen machen auch Sinn, wenn es mit der Unternehmensstruktur zusammenpasst	Sinnhaftigkeit von Security-Awareness-Schulungen
Da das Thema IT-Security omnipräsent in unserem Unternehmen ist und wir andere Unternehmen schulen, schult unser Unternehmen nicht aktiv	Sinnhaftigkeit von Security-Awareness-Schulungen
Ungeschultes Personal ist anfälliger für Angriffe	Sinnhaftigkeit von Security-Awareness-Schulungen
Eventuell für spezifische Personengruppen, die mit dem Thema sehr viel zu tun haben, aber auch hier ist es kein Fehler zu schulen	Sinnhaftigkeit von Security-Awareness-Schulungen
Neben Informationssicherheit gibt es noch eine Vielzahl weitere Dinge, die geschult werden müssen	Sinnhaftigkeit von Security-Awareness-Schulungen
Ja, Security-Awareness-Schulungen sind sehr sinnvoll	Sinnhaftigkeit von Security-Awareness-Schulungen

Schulungen werden Mitarbeiterinnen und Mitarbeitern kontinuierlich ins Bewusstsein gerufen	Sinnhaftigkeit von Security-Awareness-Schulungen
Ja, Security-Awareness-Schulungen werden bei uns im Unternehmen eingesetzt	Sinnhaftigkeit von Security-Awareness-Schulungen
Einmalige Schulungen sind weniger sinnvoll, dass diese mit dem Lauf der Jahre in Vergessenheit geraten	Sinnhaftigkeit von Security-Awareness-Schulungen
Die Erfolgsquote bei ungeschultem Personal ist sehr hoch	Sinnhaftigkeit von Security-Awareness-Schulungen
In der Fachliteratur ist ersichtlich, dass es eine signifikante Tendenz der Erfolgsquote nach unten gibt, wenn das Personal nicht regelmäßig geschult wird	Sinnhaftigkeit von Security-Awareness-Schulungen
IT-Branche benötigt nicht unbedingt notwendigerweise vollumfängliche Schulungen	Sinnhaftigkeit von Security-Awareness-Schulungen
Abseits der IT-Branche ist es sehr sinnvoll Personen entsprechend zu schulen	Sinnhaftigkeit von Security-Awareness-Schulungen
Schulungen zahlen sich in der Regel immer aus, außer es handelt sich um ein sehr kleines Unternehmen, wie beispielsweise ein Blumengeschäft	Sinnhaftigkeit von Security-Awareness-Schulungen
Kontinuierliche Online-Schulungen, zum Beispiel einmal jährlich	Aufbau von Security-Awareness-Schulungen
Kontinuierliche Schulungen einmal im Jahr sind sinnvoll	Aufbau von Security-Awareness-Schulungen
Firmenweite Aussenden von Mails mit Informationen zu einem Social-Engineering-Angriffs	Aufbau von Security-Awareness-Schulungen
Branche gibt an, wie Security-Awareness-Schulungen aussehen sollten	Aufbau von Security-Awareness-Schulungen
Praktische Beispiele, damit sich die Mitarbeiterinnen und Mitarbeiter hineinversetzen können	Aufbau von Security-Awareness-Schulungen
Es muss ausgelöst werden, dass Personen selbständig, vorsichtiger und aufmerksamer sind	Aufbau von Security-Awareness-Schulungen
Es gibt die verschiedensten Formen von Security-Awareness-Schulungen	Aufbau von Security-Awareness-Schulungen
Wiederkehrend zu schulen ist sinnvoll, denn so merken sich die einzelnen Mitarbeiterinnen und Mitarbeiter die ganzen Kleinigkeiten	Aufbau von Security-Awareness-Schulungen
Tailgating ist sehr beliebt und auch eine Technik, die heute noch sehr gut funktioniert, deswegen ist es auch notwendig Personen in hoch sensiblen Bereichen zu schulen, auch wenn sie nicht täglich am PC arbeiten	Aufbau von Security-Awareness-Schulungen
Es gibt verschiedene Ansätze von Security-Awareness-Schulungen	Aufbau von Security-Awareness-Schulungen
Eine Phishing-Simulation vor der ersten Schulung, danach die Schulung und zum Schluss eine erneute Phishing-Simulation	Aufbau von Security-Awareness-Schulungen
Schulungen müssen kurz, knackig und effektiv sein	Aufbau von Security-Awareness-Schulungen
Personen müssen sich das wichtigste nach einer Schulung merken und anwenden können	Aufbau von Security-Awareness-Schulungen
Schulungen müssen beispielsweise mit einem Quiz überprüft werden	Aufbau von Security-Awareness-Schulungen
Schulungen gehörten regelmäßig, aber nicht zu oft, wiederholt	Aufbau von Security-Awareness-Schulungen
Schulungen müssen bestanden werden	Aufbau von Security-Awareness-Schulungen
Die Informationssicherheit ändert sich ständig und deswegen gehört das Ganze auch immer wieder aufgefrischt	Aufbau von Security-Awareness-Schulungen
Wir führen selbstständig keine Massentests durch, wir beauftragen lediglich Dritte, um einzelne Szenarien zu testen	Aufbau von Security-Awareness-Schulungen

Wir schulen unser Personal nicht permanent und belästigen sie hiermit, sondern wir schulen einfach regelmäßig in Hinsicht Informationssicherheit allgemein und ein Teil davon ist Social-Engineering	Aufbau von Security-Awareness-Schulungen
Ja, es gibt technische Maßnahmen, die einen Social-Engineering-Angriff erschweren sollen	technische Maßnahmen gegen Social-Engineering-Angriffe
Sinnvoll sind Security-Maßnahmen immer	technische Maßnahmen gegen Social-Engineering-Angriffe
Mir sind keine technischen Maßnahmen bekannt, die ausschließlich darauf ausgelegt sind, Social-Engineering-Angriffe zu erschweren	technische Maßnahmen gegen Social-Engineering-Angriffe
E-Mail-Filter, Blockieren von zwielichtigen URLs	technische Maßnahmen gegen Social-Engineering-Angriffe
Abhängig vom Grad der Regelungen	technische Maßnahmen gegen Social-Engineering-Angriffe
Relation von Security und Usability muss beachtet werden	technische Maßnahmen gegen Social-Engineering-Angriffe
Es gibt keine technischen Maßnahmen, die ausschließlich als Aufgabe haben, Social-Engineering-Angriffe zu erschweren	technische Maßnahmen gegen Social-Engineering-Angriffe
Keine technischen Maßnahmen, die alle Social-Engineering-Angriffe blockieren	technische Maßnahmen gegen Social-Engineering-Angriffe
Technische Maßnahmen können gegen Social-Engineering helfen, aber nicht in vollem Umfang	technische Maßnahmen gegen Social-Engineering-Angriffe
Durch technische Maßnahmen wird die Masse besser geschützt, aber für eine einzelne Person helfen diese nicht so viel	technische Maßnahmen gegen Social-Engineering-Angriffe
Technische Maßnahmen, die einen Social-Engineering-Angriff erschweren sollen sind Mail-Filter und beschränkte Zugriffsberechtigungen	technische Maßnahmen gegen Social-Engineering-Angriffe
Weitere Maßnahmen die einen Schutz gegen Social-Engineering-Angriffe liefern sind Zugangsbeschränkungen, Security-Tools, wie Spamfilter, Firewall und Segmentierung	technische Maßnahmen gegen Social-Engineering-Angriffe
Technische Maßnahmen sind sehr sinnvoll und gehören implementiert, aber eben nicht nur wegen Social-Engineering	technische Maßnahmen gegen Social-Engineering-Angriffe
Es gibt keine technischen Maßnahmen, die ausschließlich darauf ausgelegt sind, Social-Engineering-Angriffe zu verhindern	technische Maßnahmen gegen Social-Engineering-Angriffe
Ein Patch- und Vulnerability-Management sorgen dafür, dass eine Angreiferin bzw. ein Angreifer nicht auf bekannte Lücken zurückgreifen kann	technische Maßnahmen gegen Social-Engineering-Angriffe
Ja, es gibt andere technische Maßnahmen, die einen Social-Engineering-Angriff erschweren sollen	technische Maßnahmen gegen Social-Engineering-Angriffe
Einführung eines E-Mail-Headers, damit Mails, die von extern kommen, hervorgehoben werden und die Mitarbeiter darauf hinweist und das Vorsicht geboten ist.	technische Maßnahmen gegen Social-Engineering-Angriffe
Blockieren von verdächtigen Attachments und das Nutzen von Signaturen und Verschlüsselung bei Mails	technische Maßnahmen gegen Social-Engineering-Angriffe
2FA-Authentication ist eine weitere Maßnahme	technische Maßnahmen gegen Social-Engineering-Angriffe
Viele Maßnahmen muss man aber abwägen, wo es sinnvoll ist diese einzusetzen. 2-Faktor-Authentication macht bei IT-lastigen Themen Sinn, aber bei einem Produktionsbetrieb eher weniger	technische Maßnahmen gegen Social-Engineering-Angriffe
Es muss eine Abwägung von Machbarkeit und Sicherheit getroffen werden, denn zum Beispiel eine zu belastende Passwortrichtlinie führt oft dazu, dass Personen Bilder von ihrem Passwort unter die Tastatur legen	technische Maßnahmen gegen Social-Engineering-Angriffe

Mir fällt keine technische Maßnahme ein, die ausschließlich dafür gedacht sind, Social-Engineering-Angriffe zu erschweren	technische Maßnahmen gegen Social-Engineering-Angriffe
Es gibt technische und physikalische Maßnahmen, die einen Social-Engineering-Angriff erschweren	technische Maßnahmen gegen Social-Engineering-Angriffe
Zutrittsregelungen sind Maßnahmen, die einen Social-Engineering-Angriff erschweren sollen	technische Maßnahmen gegen Social-Engineering-Angriffe
technische Maßnahmen sind Multi-Faktor-Authentifizierung, Spamfilter, Verschlüsselung, interne Proxys, Geo-Basierte-Zugangskontrollen, etc.	technische Maßnahmen gegen Social-Engineering-Angriffe
Es gibt unzählige Maßnahmen, die das Risiko eines Angriffs minimieren und auch die Auswirkungen nach einem Angriff zu minimieren	technische Maßnahmen gegen Social-Engineering-Angriffe
Es muss das gesamte Spektrum abgedeckt werden, weswegen neben Schulungen auch technische Maßnahmen eingesetzt werden sollten	technische Maßnahmen gegen Social-Engineering-Angriffe
Zum Beispiel Mail-Security-Appliances oder Ähnliches in der Mobiltelefonie	technische Maßnahmen gegen Social-Engineering-Angriffe
Technische Lösungen wehren nur Massensachen ab	technische Maßnahmen gegen Social-Engineering-Angriffe
Abgezielt auf rein Social-Engineering bringt sich ein zyklisches Ändern des Passwortes nicht sonderlich viel, denn es wird in den allermeisten Fällen nicht bis zum nächsten Zyklus gewartet, um den Angriff fortzusetzen	technische Maßnahmen gegen Social-Engineering-Angriffe
Eine zyklische Änderung hat Sinn, dass die Mitarbeiterin oder der Mitarbeiter in der Regel nicht dasselbe Passwort in der Firma und auf Online-Seiten haben	technische Maßnahmen gegen Social-Engineering-Angriffe
Rein auf Social-Engineering-Ebene hat der zyklische Passwortwechsel keinen Einfluss, auf Informationssicherheit allgemein jedoch schon	technische Maßnahmen gegen Social-Engineering-Angriffe
Mir sind keine technischen Maßnahmen bekannt, die ausschließlich auf Social-Engineering ausgelegt sind	technische Maßnahmen gegen Social-Engineering-Angriffe
Keine Beschwerden von Mitarbeiterinnen und Mitarbeiter über eingesetzte Maßnahmen	Beschwerden
Personen müssen melden, wenn sie Opfer eines Angriffs waren	Messung
Durch Klicks auf vom Unternehmen produzierte Phishing-Mails	Messung
technische Maßnahmen, die versuchen Phishing-Mails abzufangen	Messung
Mein Unternehmen testet nicht selbstständig die Mitarbeiterinnen und Mitarbeiter durch gewollte Social-Engineering-Angriffe	Messung
Betriebsrat macht Probleme, weil er sich dafür einsetzt, dass Mitarbeiterinnen und Mitarbeiter nicht ohne Wissen überprüft werden dürfen	Messung
Mitarbeiterinnen und Mitarbeiter sind aufmerksamer, wenn sie wissen, dass sie überprüft, werden	Messung
Ja, es kann durch spielerische Überprüfungen gemessen werden	Messung
Aussagekräftige Messungen sind nicht möglich	Messung
Es gehört mit dem Betriebsrat geklärt, ob Personal unwissentlich überprüft werden darf	Messung
Es werden keine Massentests durchgeführt, sondern es werden nur bestimmte Gruppen getestet	Messung
Angriffe wären viel erfolgreicher, wenn Personal nicht geschult wird	Messung
Genaue Messung, wie erfolgreich eine Schulung ist, ist nicht möglich, aber im Allgemeinen helfen sie sehr gut	Messung

Ja, es kann gemessen werden, ob Security-Awareness-Schulungen helfen, nämlich mit Phishing-Simulationen, Kontrollfragen nach einer Schulung, Gewinnspiele, etc.	Messung
Ja, unser Unternehmen testet selbstständig die Mitarbeiterinnen und Mitarbeiter	Messung
Eine Spear-Phishing-Simulation ohne eine Security-Awareness-Schulung hat eine Fehlerquote zwischen 30% und 60% und eine Spear-Phishing-Simulation mit einer Security-Awareness-Schulung hat eine Fehlerquote zwischen 5% und 10%	Messung
Ja, es kann mit Wissenstest oder mit dedizierten Angriffen gemessen werden	Messung
Bei selbst dedizierten Angriffen ist Vorsicht geboten, denn der Betriebsrat ist meistens gegen unwissentliche Überprüfungen an Mitarbeiterinnen und Mitarbeiter	Messung
Es gibt auch von Unternehmen selbst durchgeführt oder selbst beauftrage Social-Engineering-Angriffe auf die Mitarbeiterinnen und Mitarbeiter	Messung
Das Unternehmen führt selbst oder beauftragt jemanden einen Social-Engineering-Angriff durchzuführen und hierbei können KPIs definiert werden, ob jemand zum Beispiel ein Gespräch sofort beendet hat oder nicht	Messung
Man kann messen, ob Security-Awareness-Schulungen einen Einfluss gegenüber Social-Engineering-Angriffe haben	Messung
Personal versteht mittlerweile, dass Informationssicherheit wichtig ist	Beschwerden
Beschwerden nicht, eher belächeln	Beschwerden
Mittlerweile sollte jeder, Vorfälle, auch im privaten Umkreis, kennen, die negativ ausgegangen sind	Beschwerden
Eher belächeln, weil das Personal zwar weiß, dass ein Angriff schlimm sein kann, aber eben nicht versteht, dass bereits Kleinigkeiten der erste Schritt eines Social-Engineering-Angriffs sein kann	Beschwerden
Manchmal beschwerten sich bereits Personen, aber dem kann man mit spannendem und abwechslungsreichen Schulungsmaterial sehr gut entgegentreten	Beschwerden
Sicherheit ist nicht bequem	Beschwerden
Was Usern hilft die ganze Thematik besser zu verstehen, ist dass die Maßnahmen eingesetzt werden müssen, weil es eine Versicherung verlangt	Beschwerden
In unserem Unternehmen beschwerte sich das Personal nicht, da unsere Schulungen kurz und nicht im übermäßigen Konsum abgehalten werden	Beschwerden
Bei Unternehmen mit einer Vielzahl von Schulungen kommt es vor, dass sich einzelne Mitarbeiterinnen und Mitarbeiter beschweren	Beschwerden
Sinnvoll sind die Maßnahmen in jedem Unternehmen, aber es müssen natürlich die Ressourcen betrachtet werden	Unterschied Unternehmen kritischer Infrastruktur im Gegensatz zu Unternehmen keiner kritischen Infrastruktur
Kritische Infrastruktur muss besser geschützt werden, da ein Ausfall oder Data-Breaches schwerwiegendere Folgen haben als bei anderen Unternehmen	Unterschied Unternehmen kritischer Infrastruktur im Gegensatz zu Unternehmen keiner kritischen Infrastruktur
striktere Policy in kritischen Infrastrukturen	Unterschied Unternehmen kritischer Infrastruktur im Gegensatz zu Unternehmen keiner kritischen Infrastruktur

Personal muss geschult werden, dass im Schnitt das Awareness-Gefühl höher ist	Unterschied Unternehmen kritischer Infrastruktur im Gegensatz zu Unternehmen keiner kritischen Infrastruktur
Kleinere, nicht-kritische Infrastrukturen, haben in der Regel weniger Ressourcen und die Priorität ist weiter hinten als bei kritischen Infrastrukturen	Unterschied Unternehmen kritischer Infrastruktur im Gegensatz zu Unternehmen keiner kritischen Infrastruktur
Kritische Infrastruktur hat einen erhöhten Schutzbedarf	Unterschied Unternehmen kritischer Infrastruktur im Gegensatz zu Unternehmen keiner kritischen Infrastruktur
Sinnvoll sind Maßnahmen für die Informationssicherheit in jedem Unternehmen	Unterschied Unternehmen kritischer Infrastruktur im Gegensatz zu Unternehmen keiner kritischen Infrastruktur
Man muss unterscheiden zwischen sinnvoll und notwendig	Unterschied Unternehmen kritischer Infrastruktur im Gegensatz zu Unternehmen keiner kritischen Infrastruktur
Personal muss über die Auswirkungen Bescheid wissen, wenn Informationen von Unternehmen kritischer Infrastruktur, nach außen gelangen	Unterschied Unternehmen kritischer Infrastruktur im Gegensatz zu Unternehmen keiner kritischen Infrastruktur
Bei kritischer Infrastruktur ist es notwendig, dass Sicherheitsgefühl der einzelnen Mitarbeiterinnen und Mitarbeiter zu erhöhen	Unterschied Unternehmen kritischer Infrastruktur im Gegensatz zu Unternehmen keiner kritischen Infrastruktur
Der potentielle Schaden muss dem Aufwand entgegengestellt werden, denn ein zum Beispiel ein Atomkraftwerksbetreiber muss mehr Sicherheit gewährleisten können als ein Betreiber eines Online-Portals	Unterschied Unternehmen kritischer Infrastruktur im Gegensatz zu Unternehmen keiner kritischen Infrastruktur
Für ein Unternehmen ist es essentiell sich über die Risiken und deren potentiellen Auswirkungen im Klaren zu sein	Unterschied Unternehmen kritischer Infrastruktur im Gegensatz zu Unternehmen keiner kritischen Infrastruktur
Ob alle Maßnahmen notwendig sind, ist eine andere Frage	Unterschied Unternehmen kritischer Infrastruktur im Gegensatz zu Unternehmen keiner kritischen Infrastruktur
Bei kritischen Infrastrukturen ist eine restriktivere Policy notwendiger als bei anderen Unternehmen	Unterschied Unternehmen kritischer Infrastruktur im Gegensatz zu Unternehmen keiner kritischen Infrastruktur
Auf Social-Engineering-Ebene sind die Maßnahmen von kritischer Infrastruktur und Nicht-kritischer Infrastruktur ähnlich	Unterschied Unternehmen kritischer Infrastruktur im Gegensatz zu Unternehmen keiner kritischen Infrastruktur
Dem Personal von kritischer Infrastruktur muss bewusst gemacht werden, dass eine nicht autorisierte Informationsweitergabe für die Gesamtheit kritischer ist als bei anderen Unternehmen	Unterschied Unternehmen kritischer Infrastruktur im Gegensatz zu Unternehmen keiner kritischen Infrastruktur
Das Risiko eines erfolgreichen Social-Engineering-Angriffs ist höher und deswegen sollte das Thema in kritischer Infrastruktur einen höheren Stellenwert bekommen	Unterschied Unternehmen kritischer Infrastruktur im Gegensatz zu Unternehmen keiner kritischen Infrastruktur

Tabelle 7: Paraphrasen für die Auswertung der Hypothese 1

ANHANG J - Paraphrasen für die Prüfung von Hypothese 2

Ein Angriff kostet der Angreiferin oder dem Angreifer auch Geld, weswegen sich ein Angriff auszahlen soll, entweder monetär oder durch Schädigung	Kosten eines Social-Engineering-Angriffs
Konkrete Zahlen kann man nicht nennen	Kosten eines Social-Engineering-Angriffs
Große Dunkelziffer an Angriffen, die nie publik gemacht worden sind	Kosten eines Social-Engineering-Angriffs
Spanne ist immens groß	Kosten eines Social-Engineering-Angriffs
Von 100 Euro bis mehrere Millionen Euro	Kosten eines Social-Engineering-Angriffs
Opfer spielt eine große Rolle	Kosten eines Social-Engineering-Angriffs
Es gibt eine sehr große Preisspanne, nämlich von "Nicht einmal der Rede wert sein" bis hin zum Konkurs eines Unternehmens	Kosten eines Social-Engineering-Angriffs
Social-Engineering-Angriffe können Unternehmen die Existenz kosten	Kosten eines Social-Engineering-Angriffs
Social-Engineering-Angriffe könnten sogar Menschenleben kosten (Atomkraftwerk, Schwerindustrie, Autonomes Fahren, ...)	Kosten eines Social-Engineering-Angriffs
Viele Angreiferinnen oder Angreifer verlangen zwei bis fünf Prozent des Jahresumsatzes	Kosten eines Social-Engineering-Angriffs
Es wurden auch schon Unternehmen in den Ruin getrieben, durch einen Social-Engineering-Angriff	Kosten eines Social-Engineering-Angriffs
Eine Schulung zahlt sich in Relation zu einem Angriff eigentlich immer aus	Kosten eines Social-Engineering-Angriffs
Das kann nicht genau gesagt werden, die Bandbreite reicht von nichts, bis hin zur Existenzbedrohung eines Unternehmens	Kosten eines Social-Engineering-Angriffs
Ein konkreter Wert ist schwer zu nennen	Wahrscheinlichkeit Opfer eines Social-Engineering-Angriffs zu sein
Größe des Unternehmens spielt eine wesentliche Rolle	Wahrscheinlichkeit Opfer eines Social-Engineering-Angriffs zu sein
Es muss ein lukratives Ziel sein	Wahrscheinlichkeit Opfer eines Social-Engineering-Angriffs zu sein
Wahrscheinlichkeit, Opfer eines Social-Engineering-Angriffs zu werden unterscheidet sich nach Größe und Branche	Wahrscheinlichkeit Opfer eines Social-Engineering-Angriffs zu sein
Jedes Unternehmen kann angegriffen werden, nur die Chance unterscheidet sich	Wahrscheinlichkeit Opfer eines Social-Engineering-Angriffs zu sein
Vorsicht ist bei Unternehmen kritischer Infrastruktur geboten oder bei größeren Unternehmen, denn hier kann mehr aus einem Angriff herausgeholt werden	Wahrscheinlichkeit Opfer eines Social-Engineering-Angriffs zu sein
Große Unternehmen sind meist anonymer als kleine familiäre Unternehmen, weswegen eher z.B. per Pretexting und CEO-Fraud Druck auf Personen ausgeübt wird, aber auf der anderen Seite sind diese Unternehmen sich auch der Gefahr bewusst	Wahrscheinlichkeit Opfer eines Social-Engineering-Angriffs zu sein
Jeder war schon einmal Opfer eines Social-Engineering-Angriffs. Die meisten Menschen nutzen gewisse Social-Engineering-Techniken, um Andere im täglichen Leben zu beeinflussen	Wahrscheinlichkeit Opfer eines Social-Engineering-Angriffs zu sein
Unternehmen mit vielen Mitarbeiterinnen und Mitarbeiter und Unternehmen kritischer Infrastruktur haben eine höhere Chance Opfer zu werden, da hier auch der Gewinn höher sein wird	Wahrscheinlichkeit Opfer eines Social-Engineering-Angriffs zu sein

Privatperson ist oftmals die erste Anlaufstelle für Angriffe auf Unternehmen	Wahrscheinlichkeit Opfer eines Social-Engineering-Angriffs zu sein
Die Chance Opfer eines Social-Engineering-Angriffs zu werden unterscheidet sich nach der Sparte und nach der Größe	Wahrscheinlichkeit Opfer eines Social-Engineering-Angriffs zu sein
Je mehr Intellectual Property ein Unternehmen besitzt, desto höher ist die Chance Opfer eines Social-Engineering-Angriffs zu werden	Wahrscheinlichkeit Opfer eines Social-Engineering-Angriffs zu sein
Security-Awareness-Schulungen von externen Dienstleistern in Anspruch nehmen	Varianten von Security-Awareness-Schulungen
Schulungen durch die interne IT	Varianten von Security-Awareness-Schulungen
Schulungen durch externe Dienstleister	Varianten von Security-Awareness-Schulungen
Externer Dienstleister sind in der Regel teurer	Varianten von Security-Awareness-Schulungen
Interne Security-Awareness-Schulungen sind in der Regel günstiger	Varianten von Security-Awareness-Schulungen
Kosten haben keinen Zusammenhang mit Qualität	Varianten von Security-Awareness-Schulungen
Bei Fremdfirmen verschiedenste Angebote einholen	Varianten von Security-Awareness-Schulungen
Interne Schulungen so durchführen, dass es nirgends Lücken gibt	Varianten von Security-Awareness-Schulungen
Jährliche Kosten sind hierbei nicht zu kalkulieren, da man wissen möchte, in welchem Umfang man schulen möchte	Varianten von Security-Awareness-Schulungen
Handelt sich um ein stark individualisiertes Bildungspaket	Varianten von Security-Awareness-Schulungen
Bei Eintritt des Unternehmens eine Basisschulung	Varianten von Security-Awareness-Schulungen
Online-Schulungen sind Zeit und Ortsunabhänging und auch günstiger	Varianten von Security-Awareness-Schulungen
Es gibt Vor-Ort-Schulungen, entweder durch die interne IT oder durch einen externen Dienstleister	Varianten von Security-Awareness-Schulungen
Vor-Ort-Schulungen haben den besten Erfolg	Varianten von Security-Awareness-Schulungen
Online-Schulungen sind nicht für jedermann, weil es für viele ein Mehraufwand ist, aber ein Rythmus von einmal jährlich ist eine gute und günstige Maßnahme	Varianten von Security-Awareness-Schulungen
Unterschiedliche Varianten sind in unterschiedlichen Preisklassen angesiedelt	Varianten von Security-Awareness-Schulungen
Je kreativer eine Schulung abgehalten wird, desto effektiver ist diese und desto teurer ist diese	Varianten von Security-Awareness-Schulungen
Online-Schulungen erzielen nicht das gleiche Resultat, wie Vor-Ort-Schulungen, aber sind in der Regel günstiger	Varianten von Security-Awareness-Schulungen
Es gibt verschiedenste Varianten und Anbieter auf dem Gebiet, manche bieten Schulungen als Nebenprodukt zu einer Lizenz an und andere vertreiben Security-Awareness-Schulungen als Hauptprodukt	Varianten von Security-Awareness-Schulungen
Bei kombinierten Angeboten fallen die Kosten zu den eigentlichen Lizenzkosten nicht wirklich ins Gewicht	Varianten von Security-Awareness-Schulungen
Die Kosten hängen stark mit der Anzahl der User zusammen	Varianten von Security-Awareness-Schulungen
Es kann mit ca. 5-20$ pro User pro Jahr gerechnet werden, große Konzerne mit mehreren Tausen Angestellten kommen hier natürlich noch deutlich günstiger davon	Varianten von Security-Awareness-Schulungen
Es gibt interne, externe und Online-Schulungen	Varianten von Security-Awareness-Schulungen

Externe Schulungen sind teurer als interne Schulungen und bei Online-Kursen spielt die Anzahl der Lizenzen eine große Rolle	Varianten von Security-Awareness-Schulungen
Prinzipiell ist eine teurere Schulung besser für die Informationssicherheit, aber es gehört bedacht, dass teuer nicht immer gut bedeutet	Varianten von Security-Awareness-Schulungen
Grundsätzlich ist schulen immer sinnvoll, man muss die Kosten aber in Relation mit den Auswirkungen eines Angriffs setzen	Varianten von Security-Awareness-Schulungen
Vor-Ort-Schulungen bleiben dem Personal besser in Erinnerung und sind meistens auch teurer, als die anderen	Varianten von Security-Awareness-Schulungen
Es kommt darauf an, welches Sicherheitsniveau ich erreichen will	Varianten von Security-Awareness-Schulungen
Es gibt Online-Kurse, Klassenraumschulungen	Varianten von Security-Awareness-Schulungen
Es gibt Ad-hoc Meldungen an den Konzern, falls irgendein Social-Engineering-Ereignis eintritt, damit das Personal gewarnt ist	Varianten von Security-Awareness-Schulungen
Es gibt Klassenraumschulungen, interne und externe Schulungen, E-Learning-Programme und es gibt Live-Schulungen, wo wirklich Angriffe simuliert werden	Varianten von Security-Awareness-Schulungen
Es herrscht eine große Bandbreite und es gibt zahlreiche Unternehmen, die die unterschiedlichsten Methoden für eine Schulung anbieten	Varianten von Security-Awareness-Schulungen
Die Kosten hängen mit dem Aufwand zusammen. Eine Schulung vor Ort hat einen höheren Aufwand als eine E-Learning-Schulung	Varianten von Security-Awareness-Schulungen
Je teurer eine Schulung, desto besser wird die Awareness der einzelnen Mitarbeiterinnen und Mitarbeiter	Varianten von Security-Awareness-Schulungen
Eine Klassenraumschulung ist teurer als ein E-Learning-Kurs, aber die Awareness bei den einzelnen Personen ist nach einer Klassenraumschulung höher	Varianten von Security-Awareness-Schulungen
Ein Personentag bei einer Klassenraumschulung kostet zwischen 1000€ und 1500€	Varianten von Security-Awareness-Schulungen
Die Relation ist hier wichtig zu betrachten, denn die Kosten von einem Vorfall sind meistens höher, als die Kosten sich dagegen zu schützen	Varianten von Security-Awareness-Schulungen
Sinnvoll sind Security-Awareness -Schulungen immer, aber notwendig sind sie bei kleinen Unternehmen, mit wenig Bezug zur IT und wenig Budget, nicht	Varianten von Security-Awareness-Schulungen
Die Erstellung einer E-Learning-Schulung kostet ca. 10000€ bis 15000€ und dann gehört noch abgeschätzt wie groß das Unternehmen ist und ob sich dann die Erstellung einer E-Learning-Schulung rentiert	Varianten von Security-Awareness-Schulungen
Diese Kosten sind sehr individuell	Kosten der technischen Maßnahmen gegen Social-Engineering
Verschiedene Anbieter gehören verglichen	Kosten der technischen Maßnahmen gegen Social-Engineering
Große Preisspanne	Kosten der technischen Maßnahmen gegen Social-Engineering
Die genauen Kosten können nicht beantwortet werden, es kommt darauf an, was ein Unternehmen benötigt	Kosten der technischen Maßnahmen gegen Social-Engineering
Es gibt auch technische Produkte, wo die Software gratis ist, die implementiert wird, aber man darf hier die eigenen Ressourcen nicht vernachlässigen, die für die Implementierung benötigt werden	Kosten der technischen Maßnahmen gegen Social-Engineering
Es gehört beantwortet, welche technischen Maßnahmen, in welchem Ausmaß für mein Unternehmen notwendig sind	Kosten der technischen Maßnahmen gegen Social-Engineering
Es gehört eine Risikoabschätzung gemacht, was ein Produkt kostet und wie viel mich in Relation ein Angriff kosten könnte	Kosten der technischen Maßnahmen gegen Social-Engineering

und ob sich dann genau diese technische Maßnahme auszahlen würde	
Genaue Kosten können hier nicht genannt werden, das reicht von der physischen Sicherheit bis hin zu Support, 2-Faktor-Authentication und der etablierten Firmenkultur	Kosten der technischen Maßnahmen gegen Social-Engineering
Es gehört abgewogen, wie viel ich in die Informationssicherheit investieren möchte. Hier kann keine Summe genannt werden, da es bis hin zu mehreren Millionen Euro gehen kann	Kosten der technischen Maßnahmen gegen Social-Engineering
Kann nicht pauschalisiert beantwortet werden. Die Kosten reichen von klein bis groß und es ist abhängig um welches Produkt es sich handelt	Kosten der technischen Maßnahmen gegen Social-Engineering

Tabelle 8: Paraphrasen für die Auswertung der Hypothese 2

ABKÜRZUNGSVERZEICHNIS

European Program for Critical Infrasturcture Protection	EPCIP
Informationstechnologie	IT
Cross-Site-Request-Forgery	CSRF
Search-Engine-Poisoning	SEP
Transaction-Authentication-Number	TANs
Personal-Identification-Number	PIN
Key-Perfomance-Indicators	KPIs

ABBILDUNGSVERZEICHNIS

TABELLENVERZEICHNIS

LITERATURVERZEICHNIS

Abraham, S. & Chengalur-Smith, I. (2010). An overview of social engineering malware: Trends, tactics, and implications. *Technology in Society*, *32*(3), 183–196.

Accenture. (2017). *Anteil der befragten Unternehmen weltweit, bei denen folgende Vorfälle oder Typen von Cybercrime stattfanden im Jahr 2017*. https://de.statista.com/statistik/daten/studie/499324/umfrage/vorfaelle-von-cybercrime-in-unternehmen-weltweit/

ATTESLANDER, P. M., Cromm, J. & GRALOW, B. (2003). Begriffe-Variablen-Indikationen. *Methoden der empirischen Sozialforschung*, *10*.

Baer, M. H. (2008). Corporate Policing and Corporate Governance: What Can We Learn from Hewlett-Packard's Pretexting Scandal? In *University of Cincinnati Law Review, Corporate Law Symposium*.

Becker, S. (2015). Wissenstransfer durch Spionage.

Berelson, B. (1952). Content analysis in communication research.

Bhagyavati, B. (2007). Social Engineering. In L. Janczewski & A. Colarik (Hrsg.), *Cyber Warfare and Cyber Terrorism* (S. 182–190). IGI Global. https://doi.org/10.4018/978-1-59140-991-5.ch023

Birkmann, J. (2010). *State of the Art der Forschung zur Verwundbarkeit kritischer Infrastrukturen am Beispiel Strom, Stromausfall*. *Schriftenreihe Sicherheit: Bd. 2*. Forschungsforum Öffentl. Sicherheit.

Bogner, A., Littig, B. & Menz, W. (2014). Wer ist ein Experte? Wissenssoziologische Grundlagen des Expertinneninterviews. In A. Bogner, B. Littig & W. Menz (Hrsg.), *Interviews mit Experten* (S. 9–15). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-531-19416-5_2

BSI. *Aktuelle Beispiele für Phishing-Angriffe*. https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Spam-Phishing-Co/Passwortdiebstahl-durch-Phishing/Aktuelle-Beispiele-fuer-Phishing/aktuelle-beispiele-fuer-phishing.html

Cialdini, R. B. (2013). Die Psychologie des Überzeugens: Wie Sie sich selbst und Ihren Mitmenschen auf die Schliche kommen. *Aufl. Huber, Bern*.

Czerni, W. (2012). Kritische Infrastrukturen. *Strategie und Sicherheit*, *2012*(1), 451–462.

Dimensional Research (2011). The Risk of Social Engineering on Information Security:: A Survery of IT Proffesionals. *Dimensional Research*, *2011*.

EUROPOL (2018). INTERNET ORGANISED CRIME THREAT ASSESSMENT. *IOCTA*.

FBI. (2010). *Protect Your Computer: Don't Be Scared by 'Scareware'*. https://archives.fbi.gov/archives/news/stories/2010/july/scareware/scareware

Fischer, W. (2007). *Www.InfrastrukturInternet-Cyberterror.Netzwerk: Analyse und Simulation strategischer Angriffe auf die kritische Infrastruktur Internet*. *Schriften des Forschungszentrums Jülich. Reihe Informationstechnik: Bd. 14*. Forschungszentrum Jülich, Zentralbibliothek.

Fox, D. (2013). Social engineering. *Datenschutz und Datensicherheit-DuD*, *37*(5), 318.

Friedrichs, J. (1990). *Methoden empirischer sozialforschung*. Springer-Verlag.

Galov, N. (2021). *17+ Sinister Social Engineering Statistics for 2021*. https://hostingtribunal.com/blog/social-engineering-statistics/

Granger, S. (2001). Social engineering fundamentals, part I: hacker tactics. *Security Focus, December*, *18*.

Griffin, S. E. & Rackley, C. C. (2008). Vishing. In *Proceedings of the 5th annual conference on Information security curriculum development*.

Grohmann, W. (2018). *Social Engineering: Was ist Tailgaiting: (Durchslüpfen)*. https://blog.mailfence.com/de/social-engineering-was-ist-tailgating/

Hadnagy, C. (2012). *Die Kunst des Human Hacking: Social Engineering in der Praxis*. *mitp Professional*. mitp/bhv.

Helfferich, C. (2019). Leitfaden- und Experteninterviews. In N. Baur & J. Blasius (Hrsg.), *Handbuch Methoden der empirischen Sozialforschung* (S. 669–686). Springer Fachmedien Wiesbaden.

Holznagel, B. (Hrsg.). (2001). *Arbeitsberichte zum Informations-, Telekommunikations- und Medienrecht: Bd. 7*. *IT-Sicherheit in der Informationsgesellschaft - Schutz kritischer Infrastrukturen*. Lit.

Hoss, D. (2015). Social Engineering — unterschätzte Bedrohung für die Informationssicherheit. *Wirtschaftsinformatik & Management*, *7*(6), 54–61. https://doi.org/10.1007/s35764-015-0596-8

Huber, M., Kowalski, S., Nohlberg, M. & Tjoa, S. (2009). Towards automating social engineering using social networking sites. In *2009 International Conference on Computational Science and Engineering.* Symposium im Rahmen der Tagung von IEEE.

it-daily.net. (2020). *Fünf Maßnahmen zum Schutz vor Social-Engineering-Attacken*. https://www.it-daily.net/it-sicherheit/cloud-security/25236-fuenf-massnahmen-zum-schutz-vor-social-engineering-attacken

Ivaturi, K. & Janczewski, L. (2011). A taxonomy for social engineering attacks. In *International Conference on Information Resources Management.* Symposium im Rahmen der Tagung von Centre for Information Technology, Organizations, and People.

Janczewski, L. & Colarik, A. (Hrsg.). (2007). *Cyber Warfare and Cyber Terrorism*. IGI Global. https://doi.org/10.4018/978-1-59140-991-5

Kamal, M. & Crews, D. (2008). The psychology of IT security in business. *Journal of American Academy of Business*, *13*(1), 145–150.

KirstenS. *Cross Site Request Forgery (CSRF)*. https://owasp.org/www-community/attacks/csrf

Lardschneider, M. (2008). Social Engineering - Eine ungewöhnliche aber höchst effiziente Security Awareness Maßnahme. *Datenschutz und Datensicherheit*, *32*(9), 574–578. https://doi.org/10.1007/s11623-008-0137-1

Lee, D. H., Choi, K. H. & Kim, K. J. (2007). Intelligence Report and the Analysis Against the Phishing Attack Which Uses a Social Engineering Technique. In D. Hutchison, T. Kanade, J. Kittler, J. M. Kleinberg, F. Mattern, J. C. Mitchell, M. Naor, O. Nierstrasz, C. Pandu Rangan, B. Steffen, M. Sudan, D. Terzopoulos, D. Tygar, M. Y. Vardi, G. Weikum, O. Gervasi & M. L. Gavrilova (Hrsg.), *Lecture Notes in Computer Science. Computational Science and Its Applications – ICCSA 2007* (Bd. 4706, S. 185–194). Springer Berlin Heidelberg.

Lehle, B. & Reutter, O. (1997). Viren, Würmer und Trojaner.

Lipski, M. (2009). *Social Engineering: Der Mensch als Sicherheitsrisiko in der IT* (1. Aufl.). Diplom.de.

Long, J. (2011). *No tech hacking: A guide to social engineering, dumpster diving, and shoulder surfing*. Syngress.

Mann, I. (2008). *Hacking the human: Social engineering techniques and security countermeasures*. Ashgate.

Manske, K. (2000). An introduction to social engineering. *Inf. Secur. J. A Glob. Perspect.*, *9*(5), 1–7.

Mayring, P. (2015). *Qualitative Inhaltsanalyse: Grundlagen und Techniken* (12.). Beltz.

Merten, R. (2009). *Darstellung der Bedrohung durch Social Engineering und Analyse der als Gegenmaßnahme vorhandenen IT-Sicherheitsprozesse am Beispiel eines großen Unternehmens*. diplom. de.

Mitnick, K. D. & Simon, W. L. (2003). *The art of deception: Controlling the human element of security*. John Wiley & Sons.

Mouton, F., Malan, M. M., Leenen, L. & Venter, H. S. (2014). Social engineering attack framework. In *2014 Information Security for South Africa* (S. 1–9). IEEE. https://doi.org/10.1109/ISSA.2014.6950510

Naraine, R. (2008). *Twitter being used to distribute malware*. https://www.zdnet.com/article/twitter-being-used-to-distribute-malware/

Rabe, L. (2020). *Prognose zur Anzahl der monatlich aktiven Nutzer von Instagram weltweit für die Jahre 2019 bis 2023: (in Millionen)*.

https://de.statista.com/statistik/daten/studie/795086/umfrage/anzahl-der-nutzer-von-instagram-weltweit/

Raithel, J. (2008). *Quantitative Forschung*. VS Verlag für Sozialwissenschaften, Wiesbaden.

Schalbruch, M. (2009). Elektronische Identitäten im Internet.

Schimmer, K. (2008). Wenn der Hacker zweimal fragt! *Datenschutz und Datensicherheit-DuD*, *32*(9), 569–573.

Schmidt, A., Tschalow, I., Wiedemann, S., Carbon, C.-C., Ortlieb, S. & Raab, M. Je oller, je doller?

Schnell, R., Hill, P. B., Esser, E. & others (1999). Methoden der empirischen Sozialforschung.

Schumacher, S. (2014). Die psychologischen Grundlagen des Social-Engineerings. *Information-Wissenschaft & Praxis*, *65*(4-5), 215–230.

Statista Research Department. (2015). *KRITIS: War ihr Unternehmen innerhalb der letzten zwei Jahre von Datendiebstahl, Wirtschaftsspionage oder Sabotage betroffen?* https://de.statista.com/statistik/daten/studie/437017/umfrage/umfrage-unter-den-betreibern-kritischer-infrastrukturen-zum-thema-risiken/

Statista Research Department. (2022). *Anzahl der monatlich aktiven Facebook Nutzer weltweit vom 1. Quartal 2009 bis zum 2. Quartal 2021: (in Millionen)*. https://de.statista.com/statistik/daten/studie/37545/umfrage/anzahl-der-aktiven-nutzer-von-facebook/

Thompson, S. T. C. (2006). Helping the hacker? Library information, security, and social engineering. *Information Technology and Libraries*, *25*(4), 222–225.

Thornburgh, T. (2004). Social engineering. In M. E. Whitman & A. Woszczynski (Hrsg.), *Proceedings of the 1st annual conference on Information security curriculum development - InfoSecCD '04* (S. 133). ACM Press.

Townsend, L., Floersch, J. & Findling, R. L. (2010). The conceptual adequacy of the drug attitude inventory for measuring youth attitudes toward psychotropic medications: A mixed methods evaluation. *Journal of Mixed Methods Research*, *4*(1), 32–55.

Turulski, A.-S. (2021). *Haben Sie in den letzten drei Monaten soziale Netzwerke genutzt?* https://de.statista.com/statistik/daten/studie/298406/umfrage/nutzung-von-sozialen-netzwerken-in-oesterreich-nach-altersgruppen/

Yeboah-Boateng, E. O. & Amanor, P. M. (2014). Phishing, SMiShing & Vishing: an assessment of threats against mobile devices. *Journal of Emerging Trends in Computing and Information Sciences*, *5*(4), 297–307.