

Bachelorarbeit an der Hochschule Luzern - Informatik

Security Awareness Kampagne

03.01.2023

Student: Andri Widmer

Betreuer: Björn Näf

Experte: Gian-Luca Frei

Auftraggeber: Verein Kooperative Speicherbibliothek Schweiz

Bachelorarbeit an der Hochschule Luzern – Informatik

Titel: Security Awareness Kampagne

Studentin/Student: Andri Widmer

Studiengang: BSc Information & Cyber Security

Abschlussjahr: 2023

Betreuungsperson: Björn Näf

Expertin/Experte: Gian-Luca Frei

Auftraggeberin/Auftraggeber: Verein Kooperative Speicherbibliothek Schweiz

Codierung / Klassifizierung der Arbeit:

Öffentlich (Normalfall)

Vertraulich

Eidesstattliche Erklärung

Ich erkläre hiermit, dass ich die vorliegende Arbeit selbständig und ohne unerlaubte fremde Hilfe angefertigt habe, alle verwendeten Quellen, Literatur und andere Hilfsmittel angegeben habe, wörtlich oder inhaltlich entnommene Stellen als solche kenntlich gemacht habe das Vertraulichkeitsinteresse des Auftraggebers wahren und die Urheberrechtsbestimmungen der Hochschule Luzern respektieren werde.

Ort / Datum, Unterschrift

Abgabe der Arbeit auf der Portfolio Datenbank:

Bestätigungsvisum Studentin/Student

Ich bestätige, dass ich die Bachelorarbeit korrekt gemäss Merkblatt auf der Portfolio Datenbank ablege. Die Verantwortlichkeit sowie die Berechtigungen gebe ich ab, so dass ich keine Änderungen mehr vornehmen oder weitere Dateien hochladen kann.

Ort / Datum, Unterschrift

Verdankung

An dieser Stelle will ich mich bei allen bedanken, die mich während dieser Arbeit unterstützt sowie auch motiviert haben. Mein Dank für die Möglichkeit der Umsetzung dieser Arbeit gebührt dem Verein Kooperative Speicherbibliothek Schweiz. Speziell möchte ich dabei den Herren Mike Märki und Josias Bruderer danken für die Betreuung seitens des Vereins Kooperative Speicherbibliothek Schweiz. Mein Dank gilt ebenfalls Herrn Björn Näf für die Betreuung sowie die Begutachtung dieser Arbeit.

Abstract

Unternehmen werden zunehmend Opfer von Cyberangriffen. Um sich zu schützen, werden die Mitarbeitenden mit Security Awareness Kampagnen geschult. Darum ist es wichtig zu verstehen, wie solche Kampagnen aufgebaut sind und welche Inhalte geschult werden müssen.

Um die Cybersicherheit des Vereins Kooperative Speicherbibliothek Schweiz zu erhöhen, soll eine zielgerichtete Security Awareness Kampagne erstellt und die Mitarbeiter sollen initial geschult werden. Dazu soll nach dem Critical Security Control Nummer 14, «Security Awareness and Skills Training» vorgegangen werden. Das Critical Security Control ist ein Framework mit 18 Controls zur Erhöhung der IT-Sicherheit.

Durch eine Literaturrecherche wurde das Themengebiet «Security Awareness» sowie das Critical Security Control Nummer 14 erfasst. Die Anforderungen an die Security Awareness Kampagne sind durch die Best-Practice-Richtlinien von CIS bereits vordefiniert.

Anhand dieser Anforderungen wurde ein Schulungskonzept erarbeitet, welches die einzelnen Schutzmassnahmen von CIS Control 14 abdeckt und nach Rücksprache mit dem Verein Kooperative Speicherbibliothek Schweiz genehmigt wurde. Anhand des Schulungskonzeptes wurden die Schulungsunterlagen für die Schutzmassnahmen erstellt, sowie eine initiale Schulung eines Themenbereichs vorgenommen.

Inhaltsverzeichnis

Abstract	iv
Inhaltsverzeichnis	v
Abkürzungsverzeichnis	ix
1 Problem, Fragestellung, Vision	1
1.1 Problemstellung.....	1
1.2 Fragestellung	1
1.3 Aufbau der Arbeit.....	1
2 Stand der Technik	3
2.1 Security Awareness	3
2.2 Social-Engineering	3
2.2.1 Klassifizierung	4
2.2.2 Kategorien von Angriffen	5
2.2.2.1 Phishing-Attacken	6
2.2.2.2 Baiting-Angriffe	8
2.2.2.3 Pretexting.....	8
2.2.2.4 Tailgating.....	8
2.2.2.5 Ransomware	8
2.2.2.6 Impersonation on Help Desk	9
2.2.2.7 Diversion Theft.....	9
2.2.2.8 Dumpster Diving	9
2.2.2.9 Shoulder Surfing.....	9
2.2.2.10 Quid pro quo	9
2.2.2.11 Pop-up-Windows	9
2.2.2.12 Robocalls	10
2.2.2.13 Reverse-Social-Engineering	10
2.2.2.14 Online-Social-Engineering	10
2.2.2.15 Telefon- und E-Mail-Angriffe	10
2.2.2.16 Stealing-Important-Documents	11

2.2.2.17	Fake-Software.....	11
2.2.2.18	Pharming.....	11
2.4	Authentifizierung	12
2.4.1	Passwort	12
2.5.1	Multi-Faktor-Authentifizierung	15
2.5.2	Verwaltung der Zugangsdaten	16
2.5.2.1	Single-Sign-on-Technologie.....	16
2.5.2.2	Passwortsynchronisierung	17
2.6.1.1	Lokale Passwortverwaltung.....	18
2.7	Datenverarbeitung	19
2.8	Datenexposition.....	21
2.9	Erkennen und Melden von Sicherheitsvorfällen	22
2.10	Sicherheitsupdates.....	22
2.11	Unsichere Netzwerke	23
2.11.1	Externe versus interne Attacken	24
2.11.2	Passive Attacken	24
2.11.3	Aktive Attacken	24
2.12	Struktur.....	24
2.13	Umsetzung.....	25
3	Methoden.....	26
3.1	Critical Security Controls.....	26
3.1.1	Critical Security Controls 14	26
3.1.1.1	Schutzmassnahme 1	26
3.2.1.1	Schutzmassnahme 2.....	27
3.2.1.2	Schutzmassnahme 3.....	27
3.2.1.3	Schutzmassnahme 4.....	27
3.2.1.4	Schutzmassnahme 5.....	27
3.2.1.5	Schutzmassnahme 6.....	27
3.2.1.6	Schutzmassnahme 7.....	27

3.2.1.7	Schutzmassnahme 8.....	28
3.2.1.8	Schutzmassnahme 9.....	28
4	Ideen und Konzepte.....	29
4.1	Schulungskanäle.....	29
4.1.1	Präsentation.....	29
4.1.2	Video.....	29
4.1.3	Blogpost.....	29
4.1.4	Plakate.....	29
4.1.5	Onlinetest.....	30
4.2	Themen.....	30
4.2.1	Social-Engineering.....	30
4.2.2	Authentifizierung.....	30
4.3.1	Datenverarbeitung.....	31
4.3.2	Datenexposition.....	31
4.3.3	Sicherheitsvorfälle.....	31
4.3.4	Updates.....	31
4.3.5	Unsichere Netzwerke.....	32
4.3.6	Rollenspezifische Skills.....	32
5	Realisierung.....	33
5.1	Schulungskanäle für einzelne Themen.....	33
5.2	Dokumentation der Schulungsunterlagenerstellung.....	34
5.2.1	Social-Engineering.....	34
5.2.1.1	Phishing-Simulation.....	34
5.2.1.2	Schulungspräsentation.....	36
5.3.1.1	Onlinetest.....	37
5.4.1	Authentifizierung.....	38
5.4.1.1	Schulungspräsentation.....	38
5.4.1.2	Onlinetest.....	39
5.4.2	Datenverarbeitung.....	39
5.4.2.1	Blogpost.....	40
5.4.2.2	Onlinetest.....	40

5.4.3	Datenexposition	40
5.5.1.1	Plakate	41
5.5.1.2	Onlinetest.....	44
5.5.2	Sicherheitsvorfälle	44
5.5.2.1	Blogpost.....	44
5.5.2.2	Onlinetest.....	44
5.5.3	Updates	44
5.5.3.1	PowerPoint.....	44
5.5.3.2	Onlinetest.....	46
5.5.4	Unsichere Netzwerke	46
5.5.4.1	Blogpost.....	46
5.5.4.2	Onlinetest.....	46
5.7	Zeitplan.....	47
5.7.1	Social-Engineering:.....	47
5.7.2	Authentifizierung	47
5.7.3	Datenverarbeitung.....	48
5.7.4	Datenexposition	48
5.7.5	Sicherheitsvorfälle	48
5.7.6	Updates	48
5.7.7	Unsichere Netzwerke	49
5.8	Weiterführung der Kampagne.....	49
6	Evaluation und Validation	51
6.1	Erstellung Schulungskonzept.....	51
6.1.1	Critical Security Controls 14	51
6.1.2	Schulungskanäle	51
6.1.3	Zeitplan	51
6.2	Schulungsunterlagen	52
6.3	Onlinetests.....	52
6.4	Initiale Schulung	52
6.4.1	Ergebnisse Onlinetest.....	53

6.4.2	Auswertung Onlinetest Social-Engineering.....	55
7	Ausblick.....	57
7.1	Reflexion der Arbeit.....	57
7.2	Ausblick	58
8	Anhang.....	59
A.	Aufgabenstellung	59
B.	Schulungsunterlagen und Schulungskonzept.....	60
C.	Onlinetests.....	61
D.	Ergebnisse Onlinetest Social-Engineering	68
9	Abbildungs-, Tabellen-, Literaturverzeichnis.....	70
	Abbildungsverzeichnis.....	70
	Tabellenverzeichnis	70
	Literaturverzeichnis	71

Abkürzungsverzeichnis

CIS	<i>Critical Security Controls</i>
DNS.....	<i>Domain Name System</i>
FIPS.....	<i>Federal Information Processing Standard</i>
ICT	<i>Information and Communication Technology</i>
IP	<i>Internet Protocol</i>
IT.....	<i>Information Technology</i>
MFA.....	<i>Multi Faktor Authentifizierung</i>
NFC.....	<i>Near Field Communication</i>
NIST.....	<i>National Institute of Standards and Technology</i>
O365.....	<i>Office 365</i>
PDF	<i>Portable Document Format</i>
PIN	<i>Personal Identification Number</i>
RFID	<i>Radio Frequency Identification</i>
RSO.....	<i>Reduced-Sign-On</i>
SSO	<i>Single-Sign-On</i>
VKSS	<i>Verein Kooperative Speicherbibliothek Schweiz</i>
VoIP	<i>Voice over Internet Protocol</i>
VPN.....	<i>Virtual Private Network</i>
WLAN.....	<i>Wireless Local Area Network</i>

1 Problem, Fragestellung, Vision

1.1 Problemstellung

Nach einer Umfrage von Allianz Global Corporate & Speciality stellten Cyberangriffe im Jahr 2022 für Unternehmen erneut das grösste Geschäftsrisiko dar, nachdem diese im Vorjahr aufgrund der Unterbrechungen von Betriebsketten auf den zweiten Platz verdrängt worden waren. (Allianz Global Corporate & Speciality, 2021) Der Verein Kooperative Speicherbibliothek Schweiz (VKSS) ist für die effiziente und raumsparende Lagerung sowie Bewirtschaftung von Büchern und anderen Medien zuständig für die angeschlossenen Bibliotheken. (Speicherbibliothek, 2022) Nach einem persönlichen Gespräch mit der Geschäftsleitung sowie mit dem Information and Communication (ICT)-Verantwortlichen konnte evaluiert werden, dass der VKSS aufgrund eines durchgeführten Security Audits die Cybersicherheit mit einer zielgerichteten Security Awareness Kampagne erhöhen will.

1.2 Fragestellung

Für den VKSS soll zur Erhöhung der IT-Sicherheit eine Security Awareness Kampagne geplant, vorbereitet sowie initial umgesetzt werden. Die Konzipierung der Kampagne soll sich an den Empfehlungen des Critical Security Controls (CIS) v8, genauer Control 14, orientieren. Das CIS ist ein Framework mit 18 Schutzmassnahmen um die IT-Sicherheit zu erhöhen.

Initial soll ein Schulungskonzept erstellt werden, welches die Themenbereiche nach CIS Control 14 abdeckt sowie verschiedene Schulungskanäle und einen Zeitplan für die einzelnen Schulungen enthält. Die erste Schulung in einem Themenbereich soll im Rahmen der Bachelorarbeit erfolgen. Die Security Awareness Kampagne soll sämtliche Angestellte des VKSS erreichen.

1.3 Aufbau der Arbeit

Im Verlauf dieser Arbeit werden ein Schulungskonzept sowie Schulungsunterlagen für eine Security Awareness Kampagne nach dem Critical Security Control Nummer 14 erstellt. Zu Beginn wird ein Überblick über die theoretischen Grundlagen von «Security Awareness», relevanter Themengebiete sowie der Struktur und Umsetzung einer Security Awareness Kampagne geschaffen. In Kapitel 3 wird das methodische Vorgehen nach dem Critical Security Control vorgestellt. Das Kapitel 4 beschreibt die Ideen und Konzepte für die Schulungskanäle sowie die Eingrenzung der Themen der Security Awareness Kampagne. In Kapitel 5 wird die Realisierung der

Arbeit beschrieben. Diese umfasst das Auswählen von geeigneten Schulungskanäle für die einzelnen Themen, das Erstellen der Schulungsunterlagen sowie die Erstellung eines Zeitplans für die Kampagne. Das Kapitel 6 beschreibt die Evaluation und Validation des Critical Security Control, der Schulungskanäle, des Zeitplans, der Schulungsunterlagen, der Onlinetests sowie der initialen Schulung. Kapitel 7 beinhaltet die Reflexion der Arbeit und den Ausblick.

2 Stand der Technik

In diesem Kapitel werden die theoretischen Grundlagen und Begriffe für eine Security Awareness Kampagne dokumentiert.

2.1 Security Awareness

Die ‹Security Awareness› ist ein entscheidender Teil eines Informationssicherheitsprogramms, sei es auf persönlicher oder auf organisatorischer Ebene. Mangelndes Bewusstsein von Einzelpersonen kann unter anderem die Preisgabe persönlicher Informationen auf nicht vertrauenswürdigen Webseiten oder an Dritte zur Folge haben sowie die Installation gefährlicher Anwendungen. Informationssicherheitsprogramme müssen so ausgestaltet werden, dass sie das Verhalten und den Kenntnisstand der Benutzer beeinflussen. Ein Informationssicherheitsprogramm hat daher zahlreiche Definitionen. (Ao et al., 2017)

‹Security Awareness› kann sich auf die Gefahren im Umgang mit dem Internet beziehen. Ebenso kann sie in einem direkten Bezug zur IT-Sicherheit oder zu datenschutzrechtlichen Fragestellungen gesehen werden. Zudem kann sie im Rahmen der Informationssicherheit oder des Risikomanagements betrachtet werden. Die unternehmensindividuelle Realität spielt eine entscheidende Rolle, welche Themen unter den Begriff ‹Security Awareness› subsumiert werden. (Helisch & Beyer, 2010)

2.2 Social-Engineering

Social-Engineering ist eine Methode, die von Angreifern genutzt wird um die Schwächen der menschlichen Natur und die Naivität des Durchschnittsmenschen auszunutzen. (Aldawood & Skinner, 2019) Social-Engineering-Angriffe nehmen stark zu und schwächen die Cybersicherheitskette. Sie zielen darauf ab, Einzelpersonen und Unternehmen zu manipulieren, um an sensible Daten zu kommen. Dies stellt eine Herausforderung für die Sicherheit aller Netzwerke dar, unabhängig von der Robustheit der Firewall, der Kryptographie-Methoden, der Intrusion-Detection-Systeme und der Antivirensoftware. Menschen sind eher bereit, anderen Menschen zu vertrauen als Computern oder Technologien. Daher sind sie das schwächste Glied in der Sicherheitskette. Aktivitäten, welche durch menschliche Interaktionen ausgeführt werden, beeinflussen eine Person psychologisch, vertrauliche Informationen preiszugeben oder Sicherheitsverfahren zu umgehen.

Aufgrund dieser menschlichen Interaktion sind Social-Engineering-Angriffe die stärksten Angriffe, da sie alle Systeme sowie Netzwerke bedrohen. Software- oder Hardwarelösungen können solche Angriffe nicht verhindern, solange der Mensch nicht darin geschult ist, sie zu erkennen. Cyberkriminelle wählen diese Methode, wenn es keine Möglichkeit gibt, in ein System einzudringen. (Fatima Salahdine, Naima Kaabouch, 2019)

2.2.1 Klassifizierung

Social-Engineering-Attacken können in zwei Kategorien eingeteilt werden: menschenbasierte und computerbasierte. Dies wird in der Abbildung 1 aufgezeigt.

(L. Xiangyu, L. Qiuyang, S. Chandel, 2017)

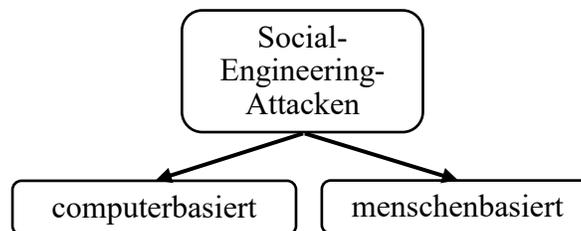


Abbildung 1 Social-Engineering-Attacks-Klassifikation (L. Xiangyu, L. Qiuyang, S. Chandel, 2017)

Bei menschenbasierten Social-Engineering-Attacks wird der Angriff vom Angreifer persönlich ausgeführt, indem er mit dem Ziel agiert, um an die gewünschten Informationen zu gelangen. Mit dieser Vorgehensweise kann nur eine begrenzte Anzahl von Opfern innerhalb einer bestimmten Zeit angegriffen werden. Die computerbasierten Angriffe werden mithilfe von Computern oder Mobiltelefonen durchgeführt, um Informationen von den Zielpersonen zu erhalten. Mit dieser Vorgehensweise können zahlreiche Opfer innerhalb weniger Sekunden angegriffen werden. (L. Xiangyu, L. Qiuyang, S. Chandel, 2017) Social-Engineering-Angriffe lassen sich je nach Art des Angriffs in drei Ansätze einteilen, in physische, soziale und technische wie aus der Abbildung 2 ersichtlich wird. (Koyun & Janabi, 2017)

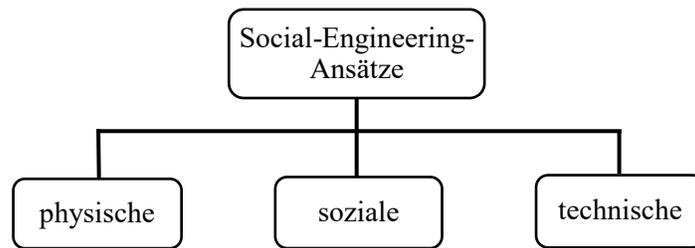


Abbildung 2 Social-Engineering-Ansätze (Koyun & Janabi, 2017)

Physische Ansätze sind eine Form von Aktion, welche der Angreifer durchführt, um Informationen über das Opfer zu sammeln. Eine häufig verwendete Methode ist hierbei das Durchsuchen von Müllcontainern (Dumpster Diving). Ein Müllcontainer kann somit eine wertvolle Quelle für diverse Informationen für Angreifer sein. (Koyun & Janabi, 2017)

Soziale Ansätze sind der wichtigste Aspekt einer erfolgreichen Social-Engineering-Attacke. Zur Erhöhung der Erfolgchance versuchen Angreifer oft, eine Beziehung zu ihren Opfern aufzubauen. Dies geschieht, indem sie sozialpsychologische Techniken wie Überredungsmethoden verwenden, um ihre Opfer zu manipulieren. Ein anderer Ansatz wäre die Ausnutzung der Neugierde des Opfers. (Koyun & Janabi, 2017)

Technische Ansätze werden hauptsächlich über das Internet durchgeführt. Oft werden dabei die Webseiten sozialer Netze als Informationsquellen verwendet. Die Angreifer nutzen Suchmaschinen, um persönliche Informationen über das Opfer zu sammeln. Zudem gibt es diverse Tools, welche Daten aus verschiedenen Webressourcen sammeln und aggregieren. Technische Ansätze sind insbesondere dienlich, um Passwörter von Benutzern auszuspähen. (Koyun & Janabi, 2017)

Oft kombinieren Social-Engineering-Angriffe mehrere der oben genannten Ansätze. Allerdings haben sozial-technische Angriffe die grössten Erfolgchancen. (Koyun & Janabi, 2017)

2.2.2 Kategorien von Angriffen

Social-Engineering-Angriffe können in mehrere Kategorien eingeteilt werden. Es kann wie oben beschrieben nach der beteiligten Einheit unterschieden werden (computerbasiert oder menschen-

basiert) sowie nach dem Ansatz, wie der Angriff durchgeführt wird (soziale, physische, technische). Ein Angriff kann zudem direkt oder indirekt stattfinden. Die Abbildung 3 zeigt die geläufigsten Attacken im Bereich Social-Engineering auf.

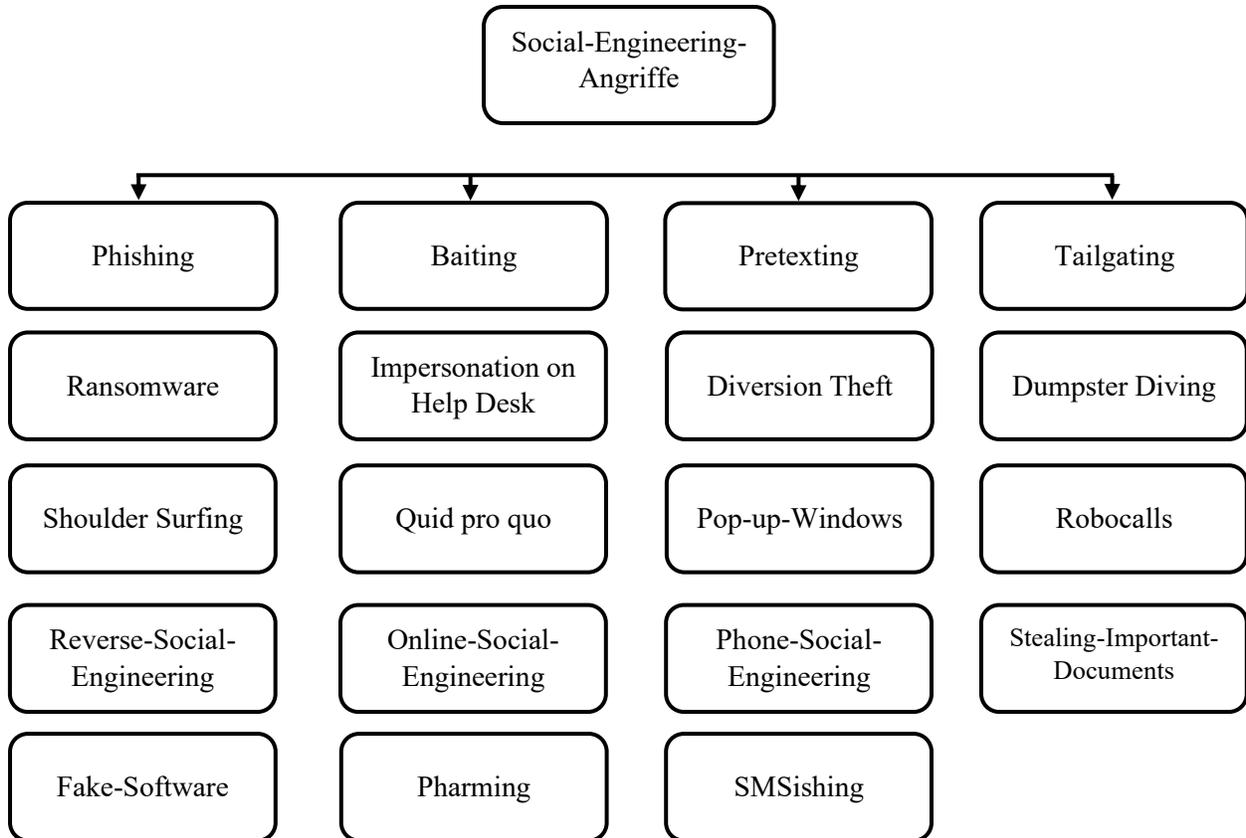


Abbildung 3 Social-Engineering-Angriffe (Fatima Salahdine, Naima Kaabouch, 2019)

2.2.2.1 Phishing-Attacken

Phishing-Attacken zielen darauf ab, auf betrügerische Weise private und vertrauliche Informationen über Telefonanrufe oder E-Mails zu erhalten. Dafür werden die Opfer in die Irre geführt und es werden gefälschte Websites, E-Mails, Anzeigen, Antivirenprogramme, Scareware, PayPal-Websites und kostenlose Angebote eingesetzt. Der Angriff kann beispielsweise durch einen Anruf oder ein E-Mail erfolgen mit falschen Versprechungen über einen Lotteriegewinn. Zur Auszahlung des Gewinns wird das Opfer aufgefordert, private oder sensitive Daten anzugeben oder auf einen Link zu klicken. Auf diese Weise werden etwa Kreditkarteninformationen, Versicherungsdaten, persönliche Angaben, physische Adressen, Haustiernamen, Jobangaben und andere Auskünfte gesammelt. Diese Angaben werden zu einem späteren Zeitpunkt verwendet, um sich bei sensitiven

Diensten anmelden zu können. Phishing-Attacken können in fünf Kategorien unterteilt werden: Spear-, Whaling-, Vishing-, Interactive-Voice-Response- und Business-E-Mail-Compromise-Phishing. (Fatima Salahdine, Naima Kaabouch, 2019)

Gemäss einer Umfrage in rund 600 Unternehmen weltweit, durchgeführt von Proofpoint, nahmen die Phishing-Angriffe im Jahr 2021 gegenüber dem Vorjahr zu. Wie aus dem Bericht zu entnehmen ist, betraf dies rund 86 % der Unternehmen, während 79 % Attacken auf konkrete Anwender erlebt haben. (State of The Phish 2022, 2022)

Spear-Phishing-Angriffe zielen auf bestimmte Personen oder ausgewählte Gruppen ab. Dabei werden die Namen der Personen genutzt, um Forderungen zu stellen oder Mitteilungen zu machen. Die Informationen über das Opfer werden online recherchiert. Es handelt sich um einen Angriff, welcher von innen aus dem Unternehmen heraus stattfindet. Somit ist es für die Opfer schwieriger, diesen zu erkennen. (Fatima Salahdine, Naima Kaabouch, 2019)

Whaling-Phishing ist ein Spear-Phishing-Angriff, welcher auf hochrangige Personen in einem Unternehmen gerichtet ist, während sich Vishing-Phishing auf Telefon-Phishing bezieht und die Opfer dazu verleitet werden, sensitive, persönliche Daten zur Überprüfung anzugeben. Die Zusammensetzung <Vishing> leitet sich von den englischen Wörtern <voice> und <phishing> ab und beschreibt somit Angriffe über das Voice over the Internet Protocol (VoIP). Beim Interactive Voice-Response-Phishing wird ein interaktives Voice-Response-System verwendet. Damit wird ein legitimes Unternehmen imitiert, um sensitive Informationen vom Opfer zu erhalten. Business-E-Mail-Compromise-Phishing imitiert die Whaling-Phishing-Methode. Ziel dieses Angriffs sind somit hochstehende Personen im Unternehmen, um Zugang zu deren E-Mails, Kalendern, Zahlungen oder zu Buchhaltungsinformationen und anderen privaten Informationen zu erhalten. (Fatima Salahdine, Naima Kaabouch, 2019)

2.2.2.2 Baiting-Angriffe

«Baiting» bedeutet auf Deutsch «ködern». Bei einem Baiting-Angriff werden Opfer geködert, indem deren Neugierde geweckt wird. Die Köder können physisch oder nichtphysisch sein. Erstere können USB-Sticks an einem allgemein zugänglichen Ort, wie an einem Parkplatz, sein. Sobald das Opfer den USB-Stick aus Neugierde an seinem Computer anschliesst, wird das Gerät automatisch mit Malware infiziert. Nichtphysische Köder sind beispielsweise illegale Torrents für Filme oder Musik. Nach dem Download des Films ist der Computer beim Öffnen der Datei mit Malware infiziert. (Chetioui et al., 2022)

2.2.2.3 Pretexting

Die populärste Nachahmungstechnik ist das Pretexting. Dabei werden im Vorfeld Nachforschungen über das Opfer angestellt. Unter Vorspiegelung falscher Tatsachen versucht der Angreifer, an sensitive Informationen zu gelangen. Beim Pretexting werden ein falsches Gefühl von Sicherheit und Vertrauen geweckt. Beispielsweise gibt sich der Angreifer als Vorstandmitglied aus, welches ein Datenleck im Unternehmen untersucht. (Ivaturi & Janczewski, 2011)

2.2.2.4 Tailgating

Tailgating bedeutet, dass eine unberechtigte Person einer Person mit Zugangsberechtigung in einen sicheren Bereich folgt. Diese Handlung kann als legal oder illegal betrachtet werden, ist im Allgemeinen aber negativ besetzt und wird als negative Handlung beschrieben. (Ivaturi & Janczewski, 2011) Bei dieser Form des Social-Engineering wird auf Onlinemedien verzichtet, um an Informationen zu gelangen. Der Angreifer verhält sich unauffällig und erweckt den Eindruck, dass er berechtigterweise Zugang zum geschützten Objekt hat. Er zeigt zudem Selbstvertrauen, erfindet eine Geschichte und überzeugt mit schauspielerischem Talent. (Chetioui et al., 2022)

2.2.2.5 Ransomware

Ransomware-Angriffe schränken den Zugriff auf Daten und Dateien des Opfers mithilfe einer Malware ein, indem die genannten Informationen verschlüsselt werden. Um die Dateien wiederherzustellen, wird meistens eine Lösegeldforderung (Ransom) gestellt, welche häufig in der unregulierten digitalen Währung Bitcoin beglichen werden muss. Die Bedrohung richtet sich gegen Einzelpersonen sowie gegen Unternehmen. Häufig sind die Folgen eines Ransomware-Angriffs teurer als die Lösegeldforderung. Gerade Unternehmen können jahrelang darunter leiden, wenn

ihr Geschäft sowie ihre Produktivität beeinträchtigt werden und Daten nicht mehr verfügbar sind. (Fatima Salahdine, Naima Kaabouch, 2019)

2.2.2.6 Impersonation on Help Desk

Bei dieser Attacke gibt sich der Angreifer als eine Autoritätsperson oder als Mitarbeiter des Unternehmens aus. Dabei kontaktiert er den Helpdesk, um Informationen oder Dienstleistungen anzufordern. (Fatima Salahdine, Naima Kaabouch, 2019)

2.2.2.7 Diversion Theft

Beim Diversion Theft versucht der Angreifer, Lieferungen von einem Transportunternehmen zu manipulieren. Er veranlasst, Ware von einem Kurier oder ein Paket an einen anderen Ort als den vorgesehenen liefern zu lassen, um diese zu stehlen. (Fatima Salahdine, Naima Kaabouch, 2019)

2.2.2.8 Dumpster Diving

Beim Dumpster Diving sammelt der Angreifer sensible Daten aus Müllcontainern oder ausrangierten Geräten von Unternehmen. Diese Informationen können von Papierdokumenten, alten Computern, Laufwerken, CDs oder DVDs stammen. (Fatima Salahdine, Naima Kaabouch, 2019)

2.2.2.9 Shoulder Surfing

Bei einem Shoulder-Surfing-Angriff wird das Opfer bei der Eingabe sensibler Informationen wie beispielsweise von Passwörtern beobachtet. (Fatima Salahdine, Naima Kaabouch, 2019)

2.2.2.10 Quid pro quo

Quid pro quo beinhaltet ein Dienstleistungsversprechen im Austausch für sensible Informationen. Im Gegensatz zum Baiting handelt es sich nicht um eine Ware wie beispielsweise ein Film oder eine App. Eine häufige Vorgehensweise bei Quid pro quo beinhaltet, dass der Betrüger sich als IT-Berater oder Kundendienstmitarbeiter gegenüber seinen Opfern ausgibt. Dies wird solange fortgesetzt, bis eine Person gefunden wird, welche tatsächlich ein IT-Problem hat und dementsprechend auf einen Anruf vom IT-Berater wartet. Die Lösung des Problems verlangt in der Regel die Preisgabe sensibler Informationen wie Passwörter. (Chetioui et al., 2022)

2.2.2.11 Pop-up-Windows

Pop-up-Windows-Angriffe verwenden Anzeigefenster, welche auf dem Bildschirm des Opfers erscheinen. Diese werden von einem bösartigen Programm generiert, welches mit dem Erscheinen des Fensters installiert wurde. Der Benutzer reagiert häufig auf die angezeigte Meldung, indem er

seine Anmeldeinformationen eingibt. Diese werden direkt an den Angreifer weitergeleitet. Pop-up-Anzeigefenster können auch Warnmeldungen sein, welche bei Onlinewerbung erscheinen. Häufig verbreitet sind Pop-ups über einen Virenfund auf dem Gerät des Opfers. Damit wird dem Opfer vorgeschlagen, eine bestimmte Antivirensoftware für die Beseitigung des Virus herunterzuladen und zu installieren. (Fatima Salahdine, Naima Kaabouch, 2019)

2.2.2.12 Robocalls

Robocalls-Angriffe sind Anrufe von Computern an bekannte Telefonnummern von Zielpersonen. Diese gehen sowohl auf Handys als auch auf Privat- und Arbeitstelefone. Bei einem Robocall handelt es sich um ein Gerät, welches automatisch eine Liste von Telefonnummern anruft und aufgezeichnete Nachrichten übermittelt. Der Angriff basiert auf dem VoIP, um verschiedene Funktionen wie die interaktive Sprachausgabe und Text-to-Speech nutzen zu können. Die Anrufe dienen dazu, Dienstleistungen oder Problemlösungen anzubieten oder zu verkaufen. Die Hilfe bei Steuerlösungen ist ein bekanntes Beispiel für diesen Angriff. Sollte das Opfer den Anruf annehmen, wird seine Telefonnummer automatisch in der Datenbank des Angreifers gespeichert. Ein Blockieren der Nummer ist nur selten zielführend, da das System des Angreifers über mehrere Nummern verfügt. Die einzige Möglichkeit, solche Angriffe abzuwenden, ist auf Anrufe von unbekanntem Nummern nicht zu reagieren. (Fatima Salahdine, Naima Kaabouch, 2019)

2.2.2.13 Reverse-Social-Engineering

Reverse-Social-Engineering-Angriffe starten häufig mit der Behauptung seitens des Angreifers, dass ein Netzwerkproblem gelöst werden muss. Dabei geht der Angreifer nach den drei folgenden Schritten vor: Ein Netzwerkproblem wird im Netzwerk des Opfers verursacht, der Angreifer gibt vor, dass er der Einzige ist, der es beheben kann und dies dann auch tut, anschliessend Informationen stiehlt und unbemerkt verschwindet. (Fatima Salahdine, Naima Kaabouch, 2019)

2.2.2.14 Online-Social-Engineering

Bei einem Online-Social-Engineering-Angriff gibt der Betrüger vor, ein interner Netzwerkadministrator des Unternehmens zu sein, und fragt das Opfer über Benutzernamen sowie Kennwörter aus. (Fatima Salahdine, Naima Kaabouch, 2019)

2.2.2.15 Telefon- und E-Mail-Angriffe

Bei Telefon- oder E-Mail-Angriffen wird das Opfer per Telefon oder E-Mail kontaktiert. Dabei versucht der Angreifer, an bestimmte Informationen zu gelangen, oder verspricht kostenlose

Dienstleistungen und Waren. Somit wird das Opfer verleitet, Sicherheitsregeln zu brechen oder persönlicher Informationen preiszugeben. Handybasierte Angriffe können als Anrufe oder als Textnachrichten erfolgen, wobei Letztere als SMSishing-Angriffe bezeichnet werden und eine Ähnlichkeit mit den Phishing-Angriffen haben. Jedoch werden sie auf unterschiedliche Weise ausgeführt. SMSishing-Angriffe bauen auf der Erkenntnis auf, dass die Opfer ihre Mobiltelefone überall und jederzeit bei sich tragen. Die gesendeten Textnachrichten können Malware enthalten. Die Malware arbeitet im Hintergrund und installiert Hintertüren, um Zugang zu persönlichen Informationen wie Kontakten, Nachrichten, E-Mails, Fotos, Notizen, Anwendungen und Kalender zu ermöglichen. Der Angreifer kann auch ein Root-Kit installieren, um die vollständige Kontrolle über das Mobiltelefon zu erlangen. (Fatima Salahdine, Naima Kaabouch, 2019)

2.2.2.16 Stealing-Important-Documents

Beim Stealing-Important-Documents-Angriff handelt es sich um eine physische Attacke. Dabei werden beispielsweise Akten von einem Schreibtisch gestohlen und für die persönlichen Zwecke des Angreifers verwendet. (Fatima Salahdine, Naima Kaabouch, 2019)

2.2.2.17 Fake-Software

Bei einem Fake-Software-Angriff wird vorgespielt, dass es sich um bekannte und vertrauenswürdige Software oder Webseiten handelt. Das Opfer verwendet echte Anmeldedaten auf der Webseite, die direkt dem Angreifer übermittelt werden. Beispiele dafür sind beliebte Webseiten wie Onlinebanking, Facebook oder Twitter. Der Angreifer nutzt das Vertrauen aus, welches die Opfer in die genannten Webseiten haben. (Fatima Salahdine, Naima Kaabouch, 2019)

2.2.2.18 Pharming

Beim Pharming stiehlt der Angreifer den Datenverkehr von einer bestimmten Webseite und leitet diesen auf eine andere gefälschte Seite um. Somit erhält er mitgeführte Informationen. Bei diesem Angriff wird der DNS-Server gehackt und die (IP)-Adresse des Host-Rechners und -Servers geändert. (Fatima Salahdine, Naima Kaabouch, 2019)

2.4 Authentifizierung

Als Authentifizierung wird der Prozess bezeichnet, welcher gewährleistet, dass nur bestimmte Benutzer Zugriff auf ein System haben. Authentifizierung ist eines der Hauptziele von Systemsicherheit. (Dowland & Furnell, 2009) Notwendig ist dafür die Bestätigung einer Identität. Die Bandbreite von Authentifizierungsmethoden ist gross und kann in vielerlei Hinsicht variieren. Nachfolgend sind die gängigsten Authentifizierungsmethoden aufgelistet:

- Identifikation mit einem Passwort
- Verwendung einer Personal Identification Number (PIN)
- Radio-Frequency-Indentification (RFID)-Karte
- Fingerabdruck
- Gesichtserkennung
- USB-Token
- One-Time-Passwort-Token

Jede der Authentifizierungsmethoden hat einen spezifischen Nutzen sowie Nachteile. Token könnten beispielsweise gestohlen und Gesichtserkennungssysteme können durch Vorlage eines Fotos unterlaufen werden. Folglich besteht das Ziel der Authentifizierung darin, die Identität einer Entität mit einem bestimmten Mass an Vertrauen überprüfen zu können. Wenn eine Authentifizierungsmethode nicht komplett vertrauenswürdig ist, kann die angebotene Verifizierung ebenfalls nicht vertrauenswürdig sein. (Idrus et al., 2013)

2.4.1 Passwort

Ein Passwort ist ein Sicherheitsmechanismus und wesentlicher Bestandteil der Computersicherheit. Das Passwort ist die häufigste Form der Authentifizierung. (Wash & Rader, 2021) Zahlreiche Passwortregeln, welche bei Benutzern angewendet werden, fallen in zwei Kategorien: Regeln, welche die Passwortstärke festlegen, sowie Regeln für die sichere Passwortverwaltung.

Folgende Regeln sind massgebend für die Passwortstärke:

1. Passwortlänge

Eine Passwortregel verhindert, dass der User ein zu kurzes Passwort verwendet. Typische Passwortregeln verlangen mindestens sechs bis acht Zeichen, allerdings manche Systeme auch weniger und andere mehr. (Leah Zhang-Kennedy, Sonia Chiasson, Paul van Oorschot, 2016)

2. Zusammensetzung des Passwortes

Eine Richtlinie zur Zusammensetzung verhindert, dass zu einfache Passwörter gewählt werden. Dabei ist es relevant, welche Art von Zeichen verwendet werden müssen. Dies können Zeichen aus einer oder mehreren der folgenden Gruppen sein: (Leah Zhang-Kennedy, Sonia Chiasson, Paul van Oorschot, 2016)

- Grossbuchstaben
- Kleinbuchstaben
- Basis-10-Ziffern
- Nichtalphanumerische ASCII-Zeichen

Die Passwortstärke ist abhängig davon, welche Zusammensetzung von den verschiedenen Gruppen erzwungen wird.

3. Blacklist

Die Verwendung von Wörterbuchwörtern kann verboten sein, da von Menschen gewählte Passwörter anfällig sind für Angriffe mit Wörterbuchpasswörtern. Diese Regel kann auch umgesetzt werden, indem die gebräuchlichsten Passwörter untersagt werden, was beispielsweise durch geleakte Datensätze vorgenommen werden kann. (Leah Zhang-Kennedy, Sonia Chiasson, Paul van Oorschot, 2016)

Die Richtlinien können zum Schutz vor Rätselangriffen beitragen, aber nicht verhindern, dass die Passwörter durch Malware, Social-Engineering oder physische Beobachtung abgegriffen werden.

Folgende Regeln sind für die Verwaltung von Passwörtern massgebend:

1. Passwortwechsel

Eine Richtlinie, die verlangt, dass Passwörter in einem bestimmten Intervall geändert werden. Die Änderung von Passwörtern wird vom National Institute of Standards and Technology (NIST) empfohlen, damit die Benutzer vor einer Passwort-Kompromittierung über einen längeren Zeitraum geschützt werden. Je länger das gleiche Passwort für eine Authentifizierung verwendet wird, desto höher ist die Wahrscheinlichkeit, dass es von einem Angreifer missbraucht wird. (Leah Zhang-Kennedy, Sonia Chiasson, Paul van Oorschot, 2016)

2. Passwort-Wiederverwendung

Die Passwortanzahl, welche ein einzelner Benutzer in Gebrauch hat, steigt bei jeder Neuankündigung für Onlineservices. Werden Passwörter in mehreren Konten wiederverwendet, ist ein Angreifer in der Lage, das kompromittierte Passwort für die Anmeldung auf anderen Diensten einzusetzen. Es wurde festgestellt, dass Dienste mit geringem Wert in der Regel schlecht abgesichert sind und Dienste mit hohem Wert durch die Wiederverwendung von Passwörtern gefährdet sind. Passwortrichtlinien können die Wiederverwendung erschweren, verhindern sie aber nicht direkt. Sie sind je nach Dienst unterschiedlich und nur für den Dienst relevant, welcher sie durchsetzt. (Leah Zhang-Kennedy, Sonia Chiasson, Paul van Oorschot, 2016)

3. Aufschreiben von Passwörtern

Den Benutzern wird empfohlen, dass sie ihre Passwörter niemals aufschreiben. Der Sicherheitszweck dieser Regel besteht darin, lokale Angriffe von Freunden, Kollegen, der Familie oder anderen Drittpersonen zu vermeiden. Obwohl Klartextpasswörter nicht auf ungeschützten Computern mit Netzwerkzugang gespeichert werden sollen, stellt das Aufschreiben von Passwörtern auf Papier kein ernsthaftes Sicherheitsrisiko dar. (Leah Zhang-Kennedy, Sonia Chiasson, Paul van Oorschot, 2016)

4. Teilen von Passwörtern

Den Benutzern wird empfohlen, Passwörter niemals mit anderen Personen zu teilen. Der Sicherheitsgrund ist offensichtlich, die Praxis zeigt aber, dass Passwörter vielfach mit dem engen Familienkreis und mit Kollegen geteilt werden. Sicherheitsexperten argumentieren, dass die

Weitergabe von Passwörtern unter bestimmten Umständen angemessen sein kann. Beispiele dafür wären Notsituationen oder zur Wiederherstellung eines Kontos. (Leah Zhang-Kennedy, Sonia Chiasson, Paul van Oorschot, 2016)

2.5.1 Multi-Faktor-Authentifizierung

Durch die Erkenntnis, dass die Authentifizierung lediglich mit einem Faktor, beispielsweise Benutzername und Passwort, keinen ausreichenden Schutz mehr bietet, wurde die Zwei-Faktor-Authentifizierung eingeführt. Dabei werden Daten wie Benutzername und Passwort mit dem weiteren Faktor des persönlichen Besitzes zum Beispiel einer Smartcard oder eines Telefons verwendet.

Es gibt drei Arten von Faktorgruppen, um eine Person mit den etablierten Anmeldeinformationen in Verbindung bringen zu können:

1. Wissensfaktor

Dabei handelt es sich um etwas, was der Benutzer kennt, beispielsweise ein Passwort oder ein Geheimnis.

2. Besitz

Dabei handelt es sich um etwas, was der Benutzer besitzt, beispielsweise eine Karte, ein Smartphone oder ein Token.

3. Biometrischer Faktor

Dabei handelt es sich um etwas, was der Benutzer ist. Dazu zählen biometrische Daten oder Verhaltensmuster.

In der Folge wurde die Multi-Faktor-Authentifizierung (MFA) vorgeschlagen, um ein höheres Mass an Sicherheit zu erreichen. Durch sie kann ein kontinuierlicher Schutz von Computergeräten und anderen kritischen Diensten vor dem Zugriff unberechtigter Drittpersonen erreicht werden. Grösstenteils basiert die MFA auf der Biometrie und somit auf der Grundlage verhaltensbezogener und biologischer Merkmale des Benutzers. Daraus resultiert eine höhere Sicherheit, da der Benutzer den Nachweis der Identität erbringen muss, welcher sich auf zwei oder mehr Faktoren stützt. Aktuell wird die MFA in Szenarien eingesetzt, bei welchen die Sicherheitsanforderungen höher als üblich sind. (Ometov et al., 2018)

2.5.2 Verwaltung der Zugangsdaten

Für die Verwaltung von Passwörtern setzen zahlreiche Unternehmen Lösungen ein, um die Benutzerkontoerkennung und die Passwörter zu vereinfachen. Auch unternehmensweite und lokale Passwortverwaltungsprogramme können für die Speicherung der Passwörter verwendet werden, um den Aufwand für den Benutzer im Zusammenhang mit Passwortänderungen und -rücksetzungen zu verringern. Die Wahrscheinlichkeit, dass Passwörter kompromittiert werden, da sie über eine Tastatur eingetippt oder schwach gesetzt werden, kann durch eine Passwortverwaltungslösung verhindert werden. In Unternehmen werden häufig zwei Arten eingesetzt: Single Sign-on (SSO) und Passwortsynchronisierung sowie lokale Passwortverwaltungstechnologien. (Scarfone & Souppaya, 2009)

2.5.2.1 Single-Sign-on-Technologie

Die SSO-Technologie ermöglicht es den Benutzern, sich einmalig zu authentifizieren und danach auf alle Ressourcen zuzugreifen, zu deren Nutzung sie berechtigt sind. Für die einzelnen Ressourcen wird die Authentifizierung in transparenter Weise durchgeführt. Das SSO erstellt ein eindeutiges, starkes Benutzerpasswort für jede Ressource und ändert die Passwörter regelmässig. Im Normalfall kennt der Benutzer die Ressourcenkennwörter nicht, sondern lediglich das SSO-Passwort. Das SSO kann das Passwort so stark machen, wie es die jeweilige Ressource unterstützt. SSO-Lösungen unterstützen auch die Speicherung und Verwendung mehrerer Kennungen einzelner Benutzer auf einem System. In vielen Umgebungen ist es nicht möglich SSO einzusetzen, welches die Authentifizierung für alle Systeme und Ressourcen übernimmt. Die daraus resultierende reduzierte Anmeldung nennt sich Reduced Sign-on (RSO). Somit können nur einige Systeme und Ressourcen durch SSO abgedeckt werden. Auch eine SSO-Technologie, welche eine begrenzte RSO-Fähigkeit aufweist, kann dazu beitragen, die Anzahl von Benutzernamen und Passwörtern zu verringern, welche sich Benutzer merken müssen.

Die Benutzerauthentifizierung der SSO-Technologie ist wichtig. Wenn keine gegenseitige Authentifizierung durchgeführt wird, ist SSO anfällig für Man-in-the-Middle-Angriffe. Die Vertraulichkeit sowie Integrität aller sensiblen übertragenen Daten sollten durch eine Federal-Information-Processing-Standard (FIPS) geprüfte Kryptographie geschützt werden. Darum sollten Zeitstempel oder andere Mechanismen verwendet werden bei der Übertragung von Anmeldeinformationen, um Replay-Angriffe zu verhindern. Ein weiteres Problem der SSO-Technologie ist der

Diebstahl des Passwortes durch Social-Engineering, Phishing und Keylogging. Durch die Kompromittierung eines einzelnen Passwortes erhält ein Angreifer Zugang zu vielen Ressourcen. (Scarfone & Souppaya, 2009)

2.5.2.2 Passwortsynchronisierung

Die Passwortsynchronisierungslösung nimmt das Passwort eines Benutzers und ändert die Passwörter auf anderen Ressourcen, damit diese übereinstimmen. Dabei authentifiziert sich der Benutzer direkt bei jeder Ressource mit dem zuvor gesetzten Passwort. Ein zentrales Verzeichnis oder einen zentralen Server, welcher die Authentifizierung bei der Ressource durchführt, gibt es nicht. Der Vorteil dieser Lösung ist, dass die Anzahl der Passwörter verringert wird, welche sich der Benutzer merken muss. Somit können stärkere Passwörter gewählt und einfacher behalten werden. Die Passwortsynchronisierung verringert die Anzahl der Authentifizierungen nicht, welche der Benutzer vornimmt. Passwort-Synchronisations-Lösungen sind in der Regel einfacher und kostengünstiger zu implementieren als SSO-Technologien.

Die Passwortsynchronisierung birgt aber auch erhebliche Sicherheitsnachteile. Da dasselbe Passwort für viele Ressourcen verwendet wird und jede dieser Ressourcen das Passwort als Hash speichert, führt die Kompromittierung einer einzelnen Instanz zu einer Kompromittierung aller Ressourcen. Somit kann das Passwort für eine Ressource mit geringer Sicherheit relativ leicht kompromittiert und für die Authentifizierung bei einer Ressource mit hoher Sicherheit wiederverwendet werden. Ein weiteres Problem besteht darin, dass die Passwortstärke auf dem kleinsten gemeinsamen Nenner gehalten werden muss. Wenn insgesamt zehn Ressourcen verwendet werden, jedoch zwei keine Sonderzeichen erlauben und eine weitere lediglich sechs Zeichen, führt dies zu einem schwächeren Passwort, als die meisten Ressourcen unterstützen würden. Passwörter könnten zudem auch nicht mehr synchronisiert werden. Der Benutzer könnte das Passwort direkt bei der Ressource ändern, anstatt die Benutzeroberfläche für die Passwortsynchronisierung zu verwenden. Dies hat zur Folge, dass sich das Passwort von den anderen Ressourcen unterscheidet, was eine zukünftige Synchronisierung verhindert. Das Passwort könnte auch durch einen Ressourcenausfall nicht mehr synchron sein mit anderen Ressourcen, da beispielsweise ein Backup eingespielt werden musste. (Scarfone & Souppaya, 2009)

2.6.1.1 Lokale Passwortverwaltung

Bei der lokalen Passwortverwaltung wird eine Passwortverwaltungssoftware eingesetzt. Diese ist ein Dienstprogramm, mit welchem der Benutzer Passwörter, Benutzernamen und andere sensitive Informationen speichern kann. Durch deren Einsatz kann sich die Anzahl der Passwörter, welche sich ein Benutzer merken muss, erheblich reduzieren. Die Passwortverwaltungssoftware ist geschützt durch ein Masterpasswort, welches der Benutzer zuerst eingeben muss, um den Zugang zu den gespeicherten Informationen zu erhalten. Dieses schützt die Informationen vor dem Zugriff anderer Personen und ist das einzige Passwort, welches behalten werden muss. Einige Programme verwenden dabei Wechselmedien als Speicherort, was einen zusätzlichen Schutz bietet. Somit muss das Medium nur bei Bedarf an den Computer angeschlossen sein und kann ansonsten sicher und separat aufbewahrt werden.

Bei vielen Passwortverwaltungsprogrammen ist eine Liste vorhanden mit den gespeicherten Konten und den dazugehörigen Passwörtern. Der Benutzer kopiert den Benutzernamen sowie das Passwort und fügt diese anschliessend in die passenden Felder ein. Einige Programme ermöglichen es, dass das jeweilige Passwort automatisch in die entsprechende Anwendung oder das Webformular eingefügt wird.

Die nachfolgenden Punkte sind allgemeine Empfehlungen bei der Verwendung einer Passwortverwaltungssoftware:

- Einstellen der Timeout-Funktion, damit der Zugang nach einer bestimmten Leerlaufzeit gesperrt wird.
- Löschen des Puffers, nachdem das Passwort kopiert und eingefügt wurde.
- Backup der Passwortdatenbank, wenn ein Passwort geändert wurde. Sollte die Passwortdatenbank oder der Computer beschädigt werden, kann das Backup verwendet werden.
- Verwendung eines starken Masterpasswortes oder einer alternativen Form der Authentifizierung, welche stärker ist als ein Passwort.
- Die gespeicherten Passwörter sollten durch Federal Information Processing Standard (FIPS)-geprüfte Algorithmen und Implementierungen geschützt werden.

Eine Passwortverwaltungssoftware kann nicht alle Bedrohungen abwehren, welche es für Passwort-Angriffe gibt. Auf einem kompromittierten Computer könnte ein Angreifer beispielsweise einen Logger verwenden, um Zugriff auf die Passwortverwaltungssoftware zu bekommen.

Folgende weitere Nachteile sind ebenfalls bekannt. Die Passwortdatenbank muss jedes Mal manuell vom Benutzer aktualisiert werden, wenn ein Passwort neu angelegt wird. Die Passwortgenerierung muss zudem jedes Mal an die spezifischen Anforderungen der Anwendung angepasst werden. Dies führt oft zu menschlichem Versagen. Die Passwörter werden dann schwächer gewählt, da die Benutzer nicht alle Passwortstärkefunktionen nutzen. Einige Passwortverwaltungssoftwares werden zudem nicht zentral gesteuert, sodass die Anwendung nach der Installation nicht richtig konfiguriert ist. Ein Beispiel wäre, dass unverschlüsselte Passwörter über längere Zeit zwischen- oder unverschlüsselt gespeichert werden. Zudem kann eine nicht lokal verwaltete Software regelmäßig exportiert und mit den Passwortrichtlinien des Unternehmens verglichen werden. Anwendungen wie Webbrowser bieten in der Regel eine Passwortverwaltungsfunktion an, teilweise mit einem integrierten Dienstprogramm, welches Passwörter sicher speichert und den Zugriff durch ein vom Benutzer festgelegtes Masterpasswort kontrolliert. In anderen Fällen sind die Passwörter weniger sicher verwaltet und werden bei Bedarf automatisch und ohne Benutzerauthentifizierung bereitgestellt. Dies ermöglicht einem Angreifer mit physischer Kontrolle über einen Arbeitsplatz, die gespeicherten Passwörter ohne grossen Aufwand zu verwenden. Unternehmen sollten sich deshalb der Risiken bewusst sein, welche eine lokale Passwortverwaltung mit sich bringt, und nur die Speicherung von Kennwörtern mit geringem Schadenpotenzial auf diese Weise zulassen. (Scarfone & Souppaya, 2009)

2.7 Datenverarbeitung

Die Datenverarbeitung umfasst eine Vielzahl unterschiedlicher automatisierter oder manueller Verfahren. Inkludiert werden beispielsweise der Umgang, die Speicherung, die Anpassung oder die Veränderung sowie die Übermittlung und das Löschen oder die Vernichtung dieser Daten. (Europäische Kommission, 2022)

Für den Umgang mit sensiblen Daten sollten verbindliche Regelungen zur Klassifizierung erlassen und diese konsequent umgesetzt werden. Damit sollte festgelegt werden, wie diese klassifizierten Daten elektronisch gespeichert und übermittelt werden dürfen. Insbesondere sollte geregelt werden, welche unternehmensinternen Daten weitergegeben werden dürfen und welche nicht.

Viele Mitarbeiter benötigen keine Administratorenrechte auf Dateien. Auch hier ist zu beachten, dass nur so viele Rechte vergeben werden, wie für die Erledigung der Arbeit von Mitarbeitern tatsächlich benötigt werden. (NCSC, 2020)

Zum Schutz vertraulicher Dokumente und Daten gegen unbefugten Zugriff helfen Clean-Desk- oder Clear-Screen-Policys. Die Clean-Desk-Policy umfasst unter anderem, dass Mitarbeiter bei Abwesenheit vom Arbeitsplatz vertrauliche Dokumente und Unterlagen wegschliessen. Dies soll verhindern, dass unberechtigte Personen wie Kunden, Besucher, Reinigungspersonal oder andere Mitarbeiter Zugriff auf Dokumente mit sensiblen Inhalten erhalten. Damit wird ein ähnlicher Grundgedanke für das Arbeiten am Computer verfolgt wie mit der Clear-Screen-Policy, bei der der Computer beim kurzzeitigen Verlassen des Arbeitsplatzes vom Benutzer gesperrt werden soll. Entfernt sich der Mitarbeiter längere Zeit vom Arbeitsplatz, soll er sich vom Computer abmelden. (Wirtschaftskammer Österreich, 2017)

Die Entsorgung von Papier und Speichermedien ist die häufigste Ursache für einen unkontrollierten Abfluss von Unternehmensdaten. Die dabei bekannt gewordenen Fälle reichen von Patientenakten in Müllcontainern bis zu Entwicklungsdaten eines Automobilherstellers auf einer ersteigerten Festplatte. (Fox, 2009)

Bei Windows werden Daten im Normalfall durch das Löschen in den «Papierkorb» verlagert und erst entfernt, wenn der vorgegebene Speicherplatz belegt ist, also der «Papierkorb» voll ist, oder wenn der Benutzer die Löschung des «Papierkorbes» vornimmt. Dieser Vorgang entfernt die Verweise auf die Daten im Index und gibt den Bereich zur Überschreibung frei. Damit ist aber nicht sichergestellt, dass dieser Bereich überschrieben wird. Die Daten sind somit immer noch vorhanden, jedoch für den normalen Benutzer nicht mehr sichtbar.

Das Formatieren einer Festplatte gewährleistet ebenfalls nicht, dass vorhandene Daten komplett gelöscht werden. Die High-Level-Formatierung bewirkt lediglich, dass das Inhaltsverzeichnis der Festplatte gelöscht und durch ein Neues ersetzt wird. Die Daten sind noch auf der Festplatte vorhanden. Eine spezielle Software erlaubt das vollständige Überschreiben einer intakten Festplatte, sodass Daten nicht wiederherstellbar sind. Während dieses Vorgangs werden die Daten einmal oder mehrfach mit vorgegebenen Zeichen oder Zufallszahlen überschrieben. Moderne Festplatten erlauben die Ausführung der herstellereigenen Routine, welche durch den Befehl ATA-«Enhanced Security Erase» angestoßen wird. Damit soll die gesamte Festplatte inklusive defekter Speicherbereiche gelöscht werden. Dieser Vorgang wird vor allem für Solid State Drive (SSD)

sowie Solid State Hybrid Drive (SSHD) empfohlen. Die Anzahl der angebotenen Produkte, welche dieses Überschreibungsverfahren anbieten, ist vielfältig. Das BSI empfiehlt in dem Zusammenhang, Produkte zu verwenden, welche von einem bootfähigen Medium wie einem USB-Stick oder einer CD gestartet werden können. Speichermedium, die nicht überschreibbar sind oder einen Defekt aufweisen, sollten physisch beschädigt und zerstört werden. (BSI, 2022)

2.8 Datenexposition

Eine Datenexposition findet statt, wenn sensible Informationen durch unbeabsichtigtes Offenlegen Drittparteien zugänglich gemacht werden. Dies unterscheidet sich von einer Datenpanne, bei welcher unbefugte Angreifer private Informationen entwenden. Vielmehr resultiert die Gefährdung aus den Massnahmen oder Fehlern eines Unternehmens. Daten, welche dabei versehentlich in falsche Datenbanken oder in falsche Onlinesysteme hochgeladen werden, sind typische Beispiele für eine Datenexposition. (Nimrod Iny, 2022)

In Anbetracht der komplexen IT-Umgebung vieler Unternehmen ist es nicht überraschend, dass beim Schutz sensibler Informationen Mängel vorliegen. Daten, welche sich im Transit befinden, durchqueren das Netzwerk und das Internet sowie verschiedene Systeme. Dies ist beispielsweise der Fall, wenn sie per E-Mail versendet oder von einem lokalen System in die Cloud übertragen werden. Die Ursachen für eine Datenexposition während dieser Übertragung sind (Nimrod Iny, 2022):

- Fehlende Verschlüsselung von Daten während der Übertragung.
- Unzureichende Richtlinien sowie mangelnde Datentransparenz, wodurch Benutzer Daten auf nicht genehmigte oder nicht geprüfte Geräte herunterladen oder freigeben können.
- Die Benutzung unsicherer Verbindungen.

Mobile Endgeräte des Unternehmens sollten nie an Drittpersonen weitergegeben werden. Sollte von unterwegs gearbeitet werden, ist das Gerät so zu positionieren, dass der Bildschirminhalt nicht von Dritten eingesehen werden kann. (NCSC, 2022)

Beim Einwählen in ein öffentliches WLAN beispielsweise in Hotels oder an Bahnhöfen sollte Vorsicht geboten sein. Daten, welche dabei übermittelt werden oder auf dem Gerät gespeichert sind, können von unbefugten Dritten verfolgt und gestohlen werden. Es ist empfehlenswert, sich direkt über die Roaming-Option mit dem Internet zu verbinden. Prinzipiell sollten sämtliche un-

genutzte Verbindungen (WLAN, Bluetooth, NFC usw.) ausgeschaltet sein, wenn diese nicht benötigt werden. Dies ist essenziell, da offene Verbindungen von Angreifern missbraucht werden können. (NCSC, 2022)

2.9 Erkennen und Melden von Sicherheitsvorfällen

Zeichen zur Erkennung eines Befalls des IT-Systems mit Viren sind zahlreich. Ein erster Indikator für Schadsoftware auf dem Computer ist, dass das System langsamer als gewöhnlich arbeitet. Zudem sollte danach in einem zweiten Schritt überprüft werden, ob unbekannte Apps oder Programme installiert sind. Weitere Anzeichen für einen Befall mit Schadsoftware können unter anderem folgende sein (Kaspersky, 2022):

- Auf dem System tauchen unerwartete Meldungen, Bilder oder Tonsignale auf oder werden ausgegeben.
- Programme werden ohne Beteiligung des Users geöffnet oder es wird eine Verbindung zum Internet hergestellt.
- Kontakte erhalten E-Mails oder Instant-Messaging-Nachrichten, welche nicht vom User gesendet wurden.
- Im E-Mail-Postfach sind Nachrichten ohne Absender und Betreff vorhanden.
- Das System arbeitet langsamer als gewöhnlich und stürzt häufig ab.
- Beim Einschalten des Systems wird das Betriebssystem nicht gestartet.
- Inhalte oder gesamte Dateien und Ordner werden gelöscht oder geändert.
- Es werden Systemmeldungen über einen Fehler angezeigt.
- Der Internetbrowser reagiert nicht mehr oder bestimmte Registerkarten lassen sich nicht mehr schliessen.

2.10 Sicherheitsupdates

Aufgrund der sich schnell verbreitenden neuen Viren haben Sicherheitsupdates von Virenschutzprogrammen eine hohe Priorität. Auch Anwendungen wie Webbrowser, E-Mail-Programme und das Betriebssystem müssen regelmässig geupdatet werden. Andere Anwendungssoftware und teilweise Hardware-Komponenten müssen ebenfalls auf vorhandene Sicherheitsupdates überprüft werden. (BSI, 2017)

Zur Absicherung von IT-Systemen ist es notwendig, sich über neu aufgedeckte Schwachstellen sowie deren Beseitigung zu informieren. Diese Recherchen können anhand von Fachartikeln sowie Internetrecherchen vorgenommen werden. Neuere Versionen der Anwendungen beinhalten die Beseitigung sicherheitsrelevanter Schwachstellen, jedoch können diese wieder neue Schwachstellen bergen. (BSI, 2017)

Die hohe Anzahl relevanter Sicherheitsupdates sowie Patches erfordert in der Regel einen Auswahlprozess. Als Sofortmassnahme ist es häufig nicht möglich, sämtliche Updates zu installieren. Es sollten daher im Vorfeld Auswahlkriterien dahingehend definiert werden, welche Updates mit welchem Zeitverzug installiert werden müssen. (BSI, 2017)

Aus theoretischer Sicht sollte jede Änderung der Software an einem Produktivsystem vorgängig in einer Testumgebung überprüft werden. Dies garantiert die reibungslose Installation von Updates. Wie aus Praxisbeispielen bekannt ist, können Updates von Virenschutzprogrammen ganze Unternehmensnetzwerke lahmlegen, da interne Software nach einem Update als Virus identifiziert wird. Aufgrund des Zeitdrucks, welcher häufig bei Updates besteht, sollten Administratoren eine sorgfältige Abwägung von Sicherheitserfordernissen und den verfügbaren Ressourcen vornehmen. (BSI, 2017)

2.11 Unsichere Netzwerke

Jedes Routingprotokoll muss einen wesentlichen Satz von Sicherheitsmechanismen enthalten. Diese dienen zur Verhinderung, Erkennung sowie zur Reaktion auf Sicherheitsangriffe. Es gibt fünf Sicherheitsziele, welche berücksichtigt werden müssen, um eine zuverlässige Netzwerkumgebung gewährleisten zu können. (Jawandhiya et al., 2010)

- Vertraulichkeit: Der Schutz von jeglicher Information vor unbeabsichtigter Weitergabe an Dritte.
- Verfügbarkeit: Die Dienste sollten bei Bedarf jederzeit verfügbar sein.
- Authentifizierung: Die Gewissheit, dass das System oder der Ursprung einer Kommunikation das ist, was sie vorgibt zu sein.
- Integrität: Die übertragene Nachricht wird nicht verändert.
- Nichtabstreitbarkeit: Es wird sichergestellt, dass Absender und Empfänger niemals leugnen können, die Nachricht gesendet oder empfangen zu haben.

2.11.1 Externe versus interne Attacken

Ziel bei Angriffen von aussen ist es, eine Überlastung des Netzes zu verursachen, gefälschte Routinginformationen zu verbreiten oder Knotenpunkte bei der Bereitstellung von Diensten zu stören. Bei einem Angriff von innen will sich der Angreifer einen normalen Zugang zum Netz verschaffen und sich an der Netzwerkaktivität beteiligen. Dies kann erreicht werden durch einen Identitätswechsel oder durch das Kompromittieren eines bestehenden Knotens im Netzwerk. Die Angriffe, welche daraus resultieren, lassen sich in aktive sowie passive Angriffe unterteilen. (Jawandhiya et al., 2010)

2.11.2 Passive Attacken

Durch einen passiven Angriff wird der Betrieb des Netzwerks nicht gestört, der Angreifer beschafft sich dabei Informationen über ausgetauschte Daten, ohne dass diese verändert werden. Folglich wird die Vertraulichkeit verletzt. Die Erkennung eines solchen Angriffs ist schwierig. Eine Lösung ist die Verwendung von Verschlüsselungsmechanismen. Somit wird der Angreifer daran gehindert, Informationen zu erhalten. (Jawandhiya et al., 2010)

2.11.3 Aktive Attacken

Mit einem aktiven Angriff wird versucht, die ausgetauschten Daten im Netzwerk zu verändern, indem der Betrieb gestört wird. Aktive Angreifer können sich intern oder extern im Netzwerk befinden. Aktionen, welche intern ausgeführt werden, sind Identitätswechsel, Änderungen oder Fälschungen am Netzwerk sowie Replikationen. (Jawandhiya et al., 2010)

2.12 Struktur

Der Faktor Mensch wurde in den letzten Jahren vermehrt als Argument in der Security-Branche herangezogen. Einen Menschen zu verstehen, ihn zu erreichen, zu überzeugen und verändern zu können, wird als Erfolgsfaktor im Hinblick auf Informationssicherheit dargestellt und ist somit die primäre Aufgabe eines Security Awareness-Trainings. (Helisch & Beyer, 2010)

Zielgruppe eines Information-Security Awareness-Programms sind sämtliche Mitarbeiter und Mitarbeiterinnen eines Unternehmens, denen Grundwissen vermittelt werden soll. Dazu zählen die Dos und Don'ts betreffend Informationssicherheit, welche in den alltäglichen Arbeitstag integriert werden sollen. Dies wären Passwortsicherheit und der Umgang mit vertraulichen Informationen oder mit E-Mails. Vertiefungen sind nicht notwendig, sondern eine stetige Wiederholung simpler Kernbotschaften. (Aengenheyster & Dörr, 2019)

In einem nächsten Schritt soll zielgruppenspezifisches Wissen vermittelt werden, welches den jeweiligen Bedürfnissen gerecht wird. Die IT wäre hier eine Zielgruppe, welche in eine Security Awareness Kampagne einbezogen werden muss, da das Verständnis für Informationssicherheit in der IT-Abteilung zentral für eine sichere Umsetzung der Digitalisierung ist. Es sollten technische und prozessuale Inhalte vermittelt werden, welche die Informationssicherheit in IT-Projekten sicherstellen. (Aengenheyster & Dörr, 2019)

2.13 Umsetzung

Die Umsetzung eines Security Awareness Programms sollte multimedial durch eine Vielzahl von Kanälen sowohl digital als auch physisch erfolgen. Die wichtigsten medialen Komponenten sind nachfolgend in einer Grafik dargestellt.

Digital	Physisch
Computer based training	Informationsevents
Learning App	Poster
Intranet-Auftritt	Installationen
Learning games	Vorträge
Videos	
Online-Trainingsmaterialien (z. B. SharePoint)	

Abbildung 4 Mediale Komponenten

Wie aus der Abbildung 4 hervorgeht, ist die digitale Kommunikation wichtig. Die Wirkung physischer Kommunikationskomponenten darf aber nicht unterschätzt werden. Der direkte, persönliche Austausch sollte ein Bestandteil einer Security Awareness Kampagne sein. Für internationale Unternehmen ist relevant, dass lokale Gegebenheiten einbezogen werden. Ausschlaggebender Faktor ist primär die Sprache. Sämtliche Schulungsmaterialien sollten in der spezifischen Landessprache zur Verfügung stehen. Die Kommunikation und verwendete Tonalität sollten positiv sein. Bestrafungen von Mitarbeitern oder Mitarbeiterinnen sollten auf keinen Fall Bestandteil der Schulung sein. Trockene technische Fachbegriffe sollten auch vermieden werden. (Aengenheyster & Dörr, 2019)

3 Methoden

Die theoretischen Grundlagen wurden anhand einer Literaturrecherche erarbeitet. Die Methode für die Erstellung der Security Awareness Kampagne wurde durch den VKSS vorgegeben. Die Methode dieser Arbeit sind die Anforderungen im CIS Control 14 zur Erstellung einer Security Awareness Kampagne.

3.1 Critical Security Controls

Die Critical Security Controls sind eine Veröffentlichung von Best-Practice-Richtlinien für die Computersicherheit. Die Leitlinien bestehen aus 18 Controls, welche von Unternehmen umgesetzt werden sollen, um bekannte Angriffe zu blockieren oder abzuschwächen. Die einzelnen Controls sind dabei so konzipiert, dass Anforderungen an einzelne Schutzmassnahmen gestellt werden. Die Ziele sind, dass Menschen und Unternehmen unterstützt werden sollen, um ihre Aufmerksamkeit zu bündeln und Schritte zu unternehmen, um sich gegen Angriffe zu schützen. Das Ziel von CIS ist die Erhöhung der IT-Sicherheit. (CIS, 2021)

3.1.1 Critical Security Controls 14

Das Control 14 beinhaltet das Thema «Security Awareness and Skills Training». Es dient der Einführung und Aufrechterhaltung eines Programms zur Förderung des Sicherheitsbewusstseins und dazu, das Verhalten der Mitarbeiter zu beeinflussen, damit diese qualifiziert mit Cybersicherheits-themen innerhalb des Unternehmens umgehen können. (CIS, 2021)

Folgende neun Schutzmassnahmen sollen zur Erreichung der Anforderungen an ein effizientes Security Awareness- und Skills-Training nach Control 14 von CIS umgesetzt werden:

3.1.1.1 Schutzmassnahme 1

«Establish and maintain a security awareness Program.» (CIS, 2021) Es soll ein Programm eingeführt sowie gepflegt werden, welches das Sicherheitsbewusstsein fördert. Dessen Zweck ist die Schulung von Mitarbeitern, damit diese sicher mit Unternehmensressourcen und -daten umgehen können. Die Schulung sollte mindestens einmal jährlich stattfinden. Der Inhalt sollte jährlich überprüft und aktualisiert werden. (CIS, 2021)

3.2.1.1 Schutzmassnahme 2

⟨Train workforce members to recognize social engineering attacks.⟩ (CIS, 2021) Die Mitarbeiter sollen geschult werden, dass sie geläufige Social-Engineering-Attacken wie Phishing und Tailgating erkennen. (CIS, 2021)

3.2.1.2 Schutzmassnahme 3

⟨Train workforce members on authentication best practices.⟩ (CIS, 2021) Die Mitarbeiter sollten in bewährten Authentifizierungsverfahren geschult werden. Themen sind MFA, Passwortzusammensetzung sowie die Verwaltung von Anmeldeinformationen. (CIS, 2021)

3.2.1.3 Schutzmassnahme 4

⟨Train workforce on data handling best practices.⟩ (CIS, 2021) Die Mitarbeiter sollten in der Identifizierung und ordnungsgemässen Speicherung, der Übertragung, der Archivierung und der Vernichtung sensibler Daten geschult werden. Dies umfasst ebenfalls bewährte Praktiken wie Clean-Desk- und Clear-Screen-Policy. (CIS, 2021)

3.2.1.4 Schutzmassnahme 5

⟨Train workforce members on causes of unintentional data exposure.⟩ (CIS, 2021) Die Mitarbeiter sollten geschult werden, damit sie sich der Ursachen für eine unbeabsichtigte Datenexposition bewusst werden. Themen, welche hier aufgegriffen werden können, sind die falsche Übermittlung sensibler Daten, der Verlust eines Endgerätes oder die unbeabsichtigte Weitergabe von Daten. (CIS, 2021)

3.2.1.5 Schutzmassnahme 6

⟨Train workforce members on recognizing and reporting security incidents.⟩ (CIS, 2021) Die Mitarbeiter sollten geschult werden, damit sie einen möglichen Vorfall erkennen und melden können. (CIS, 2021)

3.2.1.6 Schutzmassnahme 7

⟨Train workforce on how to identify and report if their enterprise assets are missing security updates.⟩ (CIS, 2021) Die Mitarbeiter sollten geschult werden, wie sie veraltete Software oder Fehler

in automatisierten Prozessen oder Werkzeugen erkennen können. Zu dieser Schulung gehört ebenfalls die Information, dass das IT-Personal über solche Vorfälle informiert werden soll. (CIS, 2021)

3.2.1.7 Schutzmassnahme 8

«Train workforce on the danger on connecting to and transmitting enterprise data over insecure networks.» (CIS, 2021) Die Mitarbeiter sollten über die Gefahren unsicherer Netzwerke geschult werden. Dies betrifft das Verbinden von unternehmensinternen Endgeräten sowie die Übertragung von Firmendaten in unsicheren Netzwerken. Sollten Personen von zu Hause arbeiten, muss die Schulung eine Anleitung enthalten, welche sicherstellt, dass die Heimnetzwerkinfrastruktur sicher konfiguriert ist. (CIS, 2021)

3.2.1.8 Schutzmassnahme 9

«Conduct role-specific security awareness and skills training.» (CIS, 2021) Es sollten rollenspezifische Schulungen zum Sicherheitsbewusstsein und zu den Fähigkeiten von den Personen erstellt werden. Ein Beispiel wäre die fortgeschrittene Social-Engineering-Schulung für hochrangige Personen. (CIS, 2021)

4 Ideen und Konzepte

Im nachfolgenden Kapitel werden die Ideen und Konzepte dargelegt, anhand welcher die Schulungsunterlagen für die Security Awareness Kampagne erstellt werden.

4.1 Schulungskanäle

Anhand der in Kapitel 2 erarbeiteten Grundlagen sowie nach einer Diskussion mit den Ansprechpersonen des VKSS ergaben sich folgende Schulungskanäle, welche sinnvoll sind.

4.1.1 Präsentation

Die Präsentationen werden mit PowerPoint umgesetzt. PowerPoint-Präsentationen werden mit Folien durchgeführt, welche vor Ort bei dem VKSS genutzt werden. Dies soll den Aspekt des persönlichen Austausches fördern. Fragen bezüglich der Themengebiete können mit den Mitarbeitern besprochen und direkt beantwortet werden.

4.1.2 Video

Videos werden als Aufnahme zur Verfügung gestellt. Dabei werden Folien zu einem Themengebiet präsentiert und erläutert. Videos haben den Vorteil, dass Inhalte seitens der Mitarbeiter im Selbststudium erarbeitet werden können. In Absprache mit dem VKSS wurde beschlossen, dass ein Video die Zeitdauer von zehn Minuten nicht überschreiten sollte.

4.1.3 Blogpost

Blogposts beinhalten Bilder und Text zu einem Themengebiet. Sie werden als Word Dokument dem VKSS zur Verfügung gestellt. Zu einem späteren Zeitpunkt können sie im zukünftigen Intranet aufgeschaltet werden. Ein Blogpost soll höchstens aus ein bis zwei Wordseiten bestehen.

4.1.4 Plakate

Plakate beinhalten Bilder und Text zu einem Themengebiet. Sie werden nach Rücksprache mit dem VKSS im Querformat und als Word Dokument zur Verfügung gestellt. Sie können in Umkleiden oder Büroräumlichkeiten aufgehängt und für das Selbststudium der Mitarbeiter verwendet werden.

4.1.5 Onlinetest

Die Onlinetests werden mit Microsoft Forms erstellt. Mit Forms können Umfragen oder Onlinetests erstellt werden. Die Teilnahme an der Umfrage kann zu einem späteren Zeitpunkt auch als Schulungsnachweis verwendet werden. Der Onlinetest beinhaltet fünf Fragen zum spezifischen Schulungsthema und wird eine Bearbeitungsdauer von zehn Minuten nicht überschreiten. Die Fragen werden so entworfen, dass Definitionen von Begriffen abgefragt und überprüft werden, um festzustellen, inwiefern der geschulte Themenbereich verstanden wurde und noch gegenwärtig ist. Die Resultate werden für den ICT-Verantwortlichen sowie die Geschäftsleitung ersichtlich sein. Eine kurze Besprechung der Resultate mit den Mitarbeitern kann falsch beantwortete Fragen sowie Unklarheiten beseitigen.

4.2 Themen

Die nachfolgenden Themenbereiche werden auf Basis der in Kapitel 3 definierten Schutzmassnahmen geschult.

4.2.1 Social-Engineering

Der Themenbereich Social-Engineering wird mit einer Phishing-Kampagne gestartet, um den Awareness-Stand der Mitarbeiter zu ermitteln. Die Social-Engineering-Schulung beinhaltet nach einer Diskussion mit den Verantwortlichen des VKSS folgenden Inhalt: Vorwort zur aktuellen Bedrohung bezüglich Social-Engineering, Definition von Social-Engineering, Klassifizierung sowie Ansätze der Angriffe, Auflistung und Beschreibung geläufiger Social-Engineering-Angriffe, Ablauf des Phishing, Auswertung der durchgeführten Phishing-Kampagne, Fallbeispiele zu den Angriffen, Schutzmassnahmen und Erkennung von Social-Engineering.

4.2.2 Authentifizierung

Die MFA ist bei dem VKSS bereits teilweise, wo notwendig, im Einsatz. Für die Verwaltung von Anmeldeinformationen ist Passwork als Passwortmanagertool in Gebrauch. Aus der Diskussion mit den Zuständigen des VKSS resultierte, das anhand von Best-Practice-Beispielen aufgezeigt werden soll, wie sichere Passwörter gesetzt werden können unter Berücksichtigung der aktuellen Passwort-Policy des VKSS. Demnach müssen Passwörter mindestens acht Zeichen lang sein und drei der folgenden Voraussetzungen erfüllen:

- Sonderzeichen (Bsp.: !,\$*#)
- Zahlen (0 bis 9)
- Grossbuchstaben (A bis Z)
- Kleinbuchstaben (a bis z)

Zudem soll den Mitarbeitern die Benutzung des Passwortmanagertools Passwork aufgezeigt werden.

4.3.1 Datenverarbeitung

Der Fokus des Themenbereichs Datenübertragung bei der Schulung soll das Senden und Empfangen von Daten mit Externen sein. Die Archivierung wird in einer separaten Schulung durch den VKSS abgehandelt. Eine Clean-Desk-Policy oder eine Clear-Screen-Policy sind nicht vorhanden. Das Thema Datenverarbeitung soll die Grundgedanken der beiden Richtlinien vermitteln.

4.3.2 Datenexposition

Die Schulung bezüglich Datenexposition soll das Bewusstsein für eine unbeabsichtigte Datenexposition fördern. Themenbereiche, welche hier behandelt werden, sind sensible Datenübermittlung, Verlust des Endgerätes sowie die unbeabsichtigte Weitergabe von Daten an Dritte.

4.3.3 Sicherheitsvorfälle

Der Themenbereich Sicherheitsvorfälle soll die Mitarbeiter schulen, damit sie Sicherheitsvorfälle erkennen können und wissen, wie sie reagieren sollen. Anhand von Best-Practice-Tipps wird ihnen aufgezeigt, welche Anhaltspunkte auf eine Infektion mit Schadsoftware hinweisen können. Ansprechpersonen des VKSS, welche bei verdächtigem Verhalten der Computer informiert werden müssen, sind die Folgenden: Der ICT-Verantwortliche sowie in Kopie die Geschäftsführung, wenn die Meldung per E-Mail erfolgt. Der ICT-Verantwortliche ist Hauptansprechpartner, falls die Meldung über andere Kanäle erfolgt.

4.3.4 Updates

Den Mitarbeitern soll aufgezeigt werden, woran sie erkennen können, dass Updates auf den Systemen erforderlich sind. Folgende Punkte sollen angesprochen werden: Das Thema Updates der Computer soll allgemein behandelt werden, damit diese konsequent auf den Systemen durchgeführt werden. Ein weiterer Punkt ist, dass Updates auch im Homeoffice erfolgen sollen. Zudem

wird kommuniziert, dass bei allfälligen Problemen mit Updates der ICT-Verantwortlich in Kenntnis gesetzt werden muss.

4.3.5 Unsichere Netzwerke

Der VKSS verwendet für das Homeoffice bereits den VPN-Client von Sophos. Die Mitarbeiter sind dementsprechend darin geübt, wie dieser verwendet wird. Ihnen soll aufgezeigt werden, weshalb eine VPN-Verbindung wichtig ist für die sichere Datenübermittlung.

Zudem soll ein Verständnis geschaffen werden, wie mit Geschäftsgeräten im privaten Umfeld oder in öffentlichen Netzwerken umgegangen werden soll. Zusätzlich soll der Umgang mit privaten Geräten im Netzwerk des VKSS abgehandelt werden.

4.3.6 Rollenspezifische Skills

Aus der Diskussion mit den Ansprechpersonen des VKSS resultierte, dass kein individuelles Training stattfinden soll mit der Begründung, dass im Geschäftsalltag keine klaren abgrenzbaren Abteilungen vorhanden sind, da der Betrieb nur über wenig Personal verfügt. Diese Schutzmassnahme soll somit nicht umgesetzt werden.

5 Realisierung

Im folgenden Kapitel wird erläutert, wie die in Kapitel 3 definierten Schutzmassnahmen in einer Security Awareness Kampagne realisiert werden. Zuerst werden die verwendeten Schulungskanäle bestimmt. Danach erfolgt die Dokumentation der Erstellung der Schulungsunterlagen. In einem letzten Schritt wird für die Schulung ein Zeitplan erstellt und aufgezeigt, wie die Kampagne weitergeführt werden kann.

5.1 Schulungskanäle für einzelne Themen

Anhand der nachfolgenden Abbildung wird aufgezeigt, über welche Schulungskanäle die Themenbereiche behandelt werden.

Tabelle 1 Schulungskanäle

	Präsentation	Video	Blogpost	Plakate	Onlinetest	Phishing Simulation
Social-Engineering	X				X	X
Authentifizierung	X	X			X	
Datenverarbeitung			X		X	
Datenexposition				X	X	
Sicherheitsvorfälle			X		X	
Updates	X				X	
Unsichere Netzwerke			X		X	

Wie aus der Tabelle 1 ersichtlich ist, wurde der Themenbereich Social-Engineering folgendermassen vermittelt: Vor dem Start der Schulung wurde eine Phishing-Simulation durchgeführt, welche sämtliche Mitarbeiter des VKSS inkludierte. In einem weiteren Schritt fand eine Vor-Ort-Schulung mit einer PowerPoint-Präsentation statt, da dieser Themenbereich initial im Rahmen der Bachelorarbeit geschult wurde. Der Lernerfolg wurde nach der erfolgten Schulung anhand einer Forms-Umfrage, wie bei allen Themenbereichen, überprüft. Das Thema Authentifizierung wurde mit einem Video behandelt, da die Funktionen des Tools Passwork somit am besten aufgezeigt werden konnten. Das Video beinhaltete ebenfalls PowerPoint-Folien, um die Theorie besser vermitteln zu können. Das Thema Datenverarbeitung wurde mit einem Blogpost abgehandelt. Dieser bot sich an, damit zukünftige Richtlinien zum Datenschutz oder zur Clean-Desk- bzw. Clear-Screen-Policy direkt verlinkt werden können. Die Datenexposition wird mit verschiedenen Plaka-

ten geschult. Dafür wurden insgesamt drei Poster erstellt, welche die drei Themenbereiche abdecken. Plakate boten sich an, da der Inhalt der Schulung unverändert bleibt. Der Themenbereich Sicherheitsvorfälle wurde ebenfalls mit einem Blogpost abgehandelt, da er die Möglichkeit bot, aktuelle Sicherheitsvorfälle direkt zu verlinken. Das Thema Updates wurde anhand einer Power-Point-Präsentation geschult. Dies ermöglicht das einfache Austauschen und Ergänzen von Folien, um auf aktuelle Updates hinzuweisen. Unsichere Netzwerke werden einmalig bei der ersten Durchführung für alle Mitarbeiter anhand eines Blogposts behandelt. Ansonsten wird der Blogpost nur für Mitarbeiter aufgeschaltet, welche einen VPN-Zugriff erhalten.

5.2 Dokumentation der Schulungsunterlagenerstellung

In diesem Kapitel wird dokumentiert, wie die Schulungsunterlagen für die einzelnen Themenbereiche erstellt wurden. Die Unterlagen werden als ZIP-Datei der Bachelorarbeit beigelegt.

5.2.1 Social-Engineering

Der Themenbereich Social-Engineering besteht aus den drei nachfolgenden Teilen.

5.2.1.1 Phishing-Simulation

Die Erstellung sowie der Versand wurden mit Sophos Phish Threat realisiert, da Erfahrungen im Umgang mit der Anwendung bereits vorhanden waren. Vorgängig wurde eine Liste sämtlicher Mitarbeiter mit Vornamen, Nachnamen sowie E-Mail-Adresse erstellt. Die Mitarbeiter des VKSS konnten dadurch im Sophos Phish Threat Tool als User erfasst werden. Für die Erstellung einer Phishing-Kampagne in Sophos müssen insgesamt sechs Schritte konfiguriert werden.

- 1 Im ersten Schritt wurde ein Kampagnenname benötigt, welcher wie folgt gewählt wurde: «Office Phishing Kampagne». Auf derselben Seite trifft man eine provisorische Auswahl, welche Art von Kampagne erstellt werden soll. Zur Verfügung stehen Phishing, Credential Harvesting, Attachment und Training. Der Typ der Kampagne wurde auf Phishing festgelegt. Die Bestimmung der Sprache, in welcher die Kampagne erfolgen soll, befindet sich weiter unten und wurde auf Deutsch eingestellt.
- 2 Im zweiten Schritt wählt man die Attacke aus. Dabei handelt es sich um vorgefertigte E-Mail-Templates von Sophos. Diese können nach Schwierigkeitsgrad der Erkennung der Attacke gefiltert werden. Nach einer Diskussion mit dem VKSS wurde entschieden, dass

ein Office-365-Phishing-E-Mail-Template die höchste Chance auf Erfolg bei den Mitarbeitern hat, weil Office-Meldungen in unregelmässigen Abständen bereits bei den Mitarbeitern im Postfach eingehen.

- 3 Im dritten Schritt kann ausgewählt werden, wie die Mitarbeiter geschult werden sollen, falls Links oder angehängte Dateien im E-Mail geöffnet werden. Folgende Möglichkeiten werden angeboten: «Phish Threat Training» von Sophos, «Use my own training» oder «No Training». Da die Schulung bezüglich Social-Engineering für die Mitarbeiter erst nach dem Phish Threat stattfindet, wurde hier «No training» ausgewählt.
- 4 Im nächsten Schritt kann das ausgewählte Template individualisiert werden. Dieses ist in Abbildung 5 ersichtlich. «From Name» wurde dabei mit «Microsoft» angegeben und die «From Email» ebenfalls. Für die Auswahl der Domäne ist eine Liste vorhanden. Da «it-supportdesk.com» in Verbindung mit Microsoft Sinn ergibt, wurde diese ausgewählt. Das «Email Subject» wurde auf einen Betreff angepasst, welcher tatsächlich bei Fehlermeldungen von Microsoft verschickt wird. Der Text im E-Mail wurde ebenfalls komplett überarbeitet, um Bezug zu nehmen auf die gemeinsam genutzten Endgeräte des VKSS.

From Name*

Microsoft

From Email*

microsoft @ it-supportdesk.com

Use a sub-domain on phishing URL replacements

Email Subdomain*

support

Email Subject*

Kontohinweis: Es ist ein Problem mit Ihrem Microsoft 365-Konto aufgetreten

Edit

Hallo {FirstName}

Es ist ein Problem mit Ihrem Microsoft 365-Konto aufgetreten, und wir benötigen Ihre Hilfe, um das Problem zu beheben. Dieses Problem kann durch einen Wechsel des Endgerätes ausgelöst werden und kann zur Sperrung des Kontos führen.

Um das Problem zu beheben melden Sie sich bitte [hier](#) bei Ihrem Office 365-Konto an. Durch die erneute Anmeldung, kann Ihr Gerät wieder mit dem Office 365-Konto verbunden werden.

Mit freundlichen Grüssen

Das Microsoft Office 365 Team

 Microsoft Office 365

Um Ihre Benachrichtigungseinstellungen zu ändern, wechseln Sie zu [Planner für Web](#), wählen Sie oben rechts die Schaltfläche „Einstellungen“ und dann „Benachrichtigungen“ aus [Weitere Informationen](#).

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 USA

 Microsoft

Abbildung 5 Entwurf Phishing-E-Mail in Sophos

- 5 Als Nächstes werden die zu Beginn erfassten User der Kampagne hinzugefügt. In diesem Schritt wurden alle zwölf Mitarbeiter des VKSS berücksichtigt.

- 6 Im letzten Schritt wird der geplante Zeitpunkt der Kampagne bestimmt, indem ein Start- sowie Enddatum der Kampagne festgelegt wird. Die Phishing-E-Mail kann gestaffelt an die einzelnen Empfänger verschickt werden oder an alle gleichzeitig. Der Startzeitpunkt wurde auf den 1. Dezember um 08:00 Uhr festgelegt, das Enddatum auf den 5. Dezember um 17:00 Uhr. Da viele Mitarbeiter des VKSS in einem Teilzeitpensum beschäftigt sind, wurde durch den angegebenen Zeitraum abgedeckt, dass alle während der Dauer der Kampagne arbeiten. Der Versand der E-Mail erfolgte für alle gleichzeitig um zu verhindern, dass die Mitarbeiter sich untereinander austauschen oder warnen können.

5.2.1.2 Schulungspräsentation

Die Schulungspräsentation wurde mit PowerPoint erstellt und beinhaltet folgende Agenda.

Vorwort

Im Vorwort werden zwei aktuelle Beispiele für Cyberangriffe vorgestellt, welche mit Social-Engineering-Methoden durchgeführt wurden. Es handelt sich dabei um den Uber-Hack sowie den Twilio-Hack, welche beide aus dem Jahr 2022 stammen. Dies soll veranschaulichen, dass Social-Engineering ein gefährliches Werkzeug von Angreifern ist und auch angewandt wird.

Definition, Klassifizierung, Social-Engineering-Attacke, Angriffe

Der Inhalt dieser Folien wird mittels der in Kapitel 2 erarbeiteten Literatur abgebildet.

Fallbeispiele

Folgende Social-Engineering-Angriffe wurden nach einer Diskussion mit den Verantwortlichen des VKSS genauer angeschaut: Phishing, Ransomware, Dumpster Diving, Phone-Social-Engineering, Fake-Software. Für jeden Angriff wurde eine Folie mit der Definition vorbereitet mit einem oder mehreren Fallbeispielen sowie eine Folie mit Schutzmassnahmen, welche sich aus den Fallbeispielen ableiten. Für die Fallbeispiele beim Phishing wurden privat erhaltene Phishing-E-Mails verwendet. Das Fallbeispiel für Ransomware wurde im persönlichen Rahmen getestet. Für die Fallbeispiele Dumpster Diving sowie Phone-Social-Engineering wurden mit dem VKSS Beispiele erarbeitet, welche effektiv auf den VKSS zutreffen könnten. Die Fake-Software-Beispiele stammen von persönlichen Screenshots verdächtiger Software sowie von einer Fake Website.

Schlussfolgerung

Auf der letzten Folie werden alle Schutzmassnahmen aus den Fallbeispielen zusammengefasst.



Schlussfolgerung

- Keine Preisgabe von sensiblen Daten an Drittpersonen
- Kritisch sein und sich bewusst sein was man tut
 - Absender überprüfen, Inhalt überprüfen, Grammatik
 - URL/Link prüfen
 - Soziale Medien
- Im Zweifelsfall vier Augen Prinzip anwenden
- IT-Verantwortlichen/Geschäftsleitung informieren

33

Abbildung 6 Schlussfolgerung Präsentation Social-Engineering

Wie aus der Abbildung ersichtlich wird, sind auf der Folie die wichtigsten Erkenntnisse dargestellt, welche die Mitarbeiter von der Schulung mitnehmen sollen.

5.3.1.1 Onlinetest

Die Fragen sowie die korrekten Antworten sind im Anhang C ersichtlich.

5.4.1 Authentifizierung

Der Themenbereich Authentifizierung besteht aus zwei Teilen. Diese sind das Video mit PowerPoint-Präsentation zur Schulung sowie der Onlinetest.

5.4.1.1 Schulungspräsentation

Die Schulung erfolgt als Video und beinhaltet zudem eine PowerPoint-Präsentation mit folgender Agenda: Vorwort, Passwort-Policy VKSS, Erstellung sicherer Passwörter, Passwork, MFA und Schlussfolgerung.

Zu Beginn des Videos, im Vorwort, wird die Frage beantwortet, warum sichere Passwörter wichtig sind. Dies wird mit einem Zitat von Prof. Dr. Dirk Labudde, Dozent und Entwickler im Bereich digitale Forensik erreicht.

Ein Passwort ist wie ein Schlüssel für virtuelle Daten. Für unsere Wohnung, die Haustür oder den Keller haben wir unterschiedliche Schlüssel, um zu verhindern, dass Fremde eintreten können. Und wenn mal ein Schlüssel gestohlen wird, kann nicht direkt alles geöffnet werden. – Prof. Dr. Dirk Labudde (Janina Raeder, 2021)

Nach dem Vorwort wird die gesetzte Passwort-Policy des VKSS vorgestellt. Damit soll das Grundwissen darüber vermittelt werden, welche Länge und welche Komplexität ein Passwort beim VKSS haben muss. In einem nächsten Schritt wird die Theorie aus Kapitel 2 angewendet, um aufzuzeigen, welche Fehler häufig bei der Passwortsetzung begangen werden. Anhand eines selbst erstellten Fallbeispiels wird im weiteren Verlauf aufgezeigt, wie man ein sicheres Passwort erstellen kann unter Berücksichtigung der Komplexität sowie auch der Länge. Mit Verweis auf Abschnitt 4.2.2 wird auf Verlangen des VKSS die Verwendung des Passwortmanagers Passwork erläutert. Es wird anhand von Screenshots aufgezeigt, wie mit dem Tool gearbeitet und insbesondere wie ein neuer Eintrag erstellt, ein Passwort generiert und geteilt sowie das Plugin verwendet werden kann.

Die nächste Folie bildet das Thema MFA. Die erarbeitete Theorie aus Abschnitt 2.3.2 Multi-Faktor-Authentifizierung wird anhand eines kurzen Überblickes vermittelt. Den Abschluss des Videos bildet die Schlussfolgerung, mit der die wichtigsten Erkenntnisse aus der Schulung nochmals aufgezeigt werden. Diese werden aus der nachfolgenden Abbildung 7 ersichtlich.

Schlussfolgerung

- Starke Passwörter sind wichtig um persönliche und sensiblen Daten zu schützen
- Starke Masterpasswörter können anhand eines einprägsamen Satzes erstellt werden
 - Ansonsten Verwendung eines Passwortmanagers
- MFA erweitert den Zugriffsschutz um einen weiteren Faktor und stärkt somit die Sicherheit

13

Abbildung 7 Schlussfolgerung Themenbereich Authentifizierung

5.4.1.2 Onlinetest

Die Fragen sowie die korrekten Antworten sind im Anhang C ersichtlich.

5.4.2 Datenverarbeitung

Der Themenbereich Datenverarbeitung besteht aus den nachfolgenden zwei Teilen. Unter Anwendung der zuvor in Abschnitt 4.2.3 definierten Einschränkungen wurden die Unterlagen wie folgt erstellt.

5.4.2.1 Blogpost

Der Blogpost wurde in drei Abschnitte unterteilt. Der erste umfasst die Massnahmen, welche die Mitarbeiter konkret am Arbeitsplatz treffen sollten, um die sensiblen Daten zu schützen. Dabei wurde die Theorie aus Abschnitt 2.4.2 angewandt, um Massnahmen zu definieren, welche den Grundgedanken beider Richtlinien entsprechen.

Im zweiten Abschnitt wurden nach einer Diskussion mit dem VKSS die Speicherung und Übertragung von Daten thematisiert. Dabei wird vermittelt, dass nur interne Dienste sowie Speichermedien für das Speichern von Daten verwendet werden sollen. Sollten sensible Daten per E-Mail übermittelt werden, müssen diese als vertraulich gekennzeichnet werden. Die Verwendung portabler Speichermedien für die Übertragung sensibler Daten soll vermieden werden.

Der letzte Abschnitt umfasst die Vernichtung sensibler Daten. Es wird aufgezeigt, wie die verschiedenen Medien, digitale Speichermedien sowie physische Dokumente vernichtet werden können. Bei den digitalen Medien wird darauf verwiesen, dass die Verschiebung von Dateien in den Papierkorb keine Löschung bewirkt. Bei der Formatierung von Festplatten wird erwähnt, dass spezielle Software nötig ist, welche ein komplettes Überschreibungsverfahren anwendet, um die gespeicherten Daten unwiderruflich zu löschen. Sollte dies nicht möglich sein, müssen die Speichermedien physisch zerstört werden. Physische Dokumente mit sensiblen Daten müssen für eine effektive Vernichtung immer geschreddert werden.

Da das Intranet seitens des VKSS für die Blogposts noch nicht eingerichtet ist, können an dieser Stelle keine Abbildungen gezeigt werden.

5.4.2.2 Onlinetest

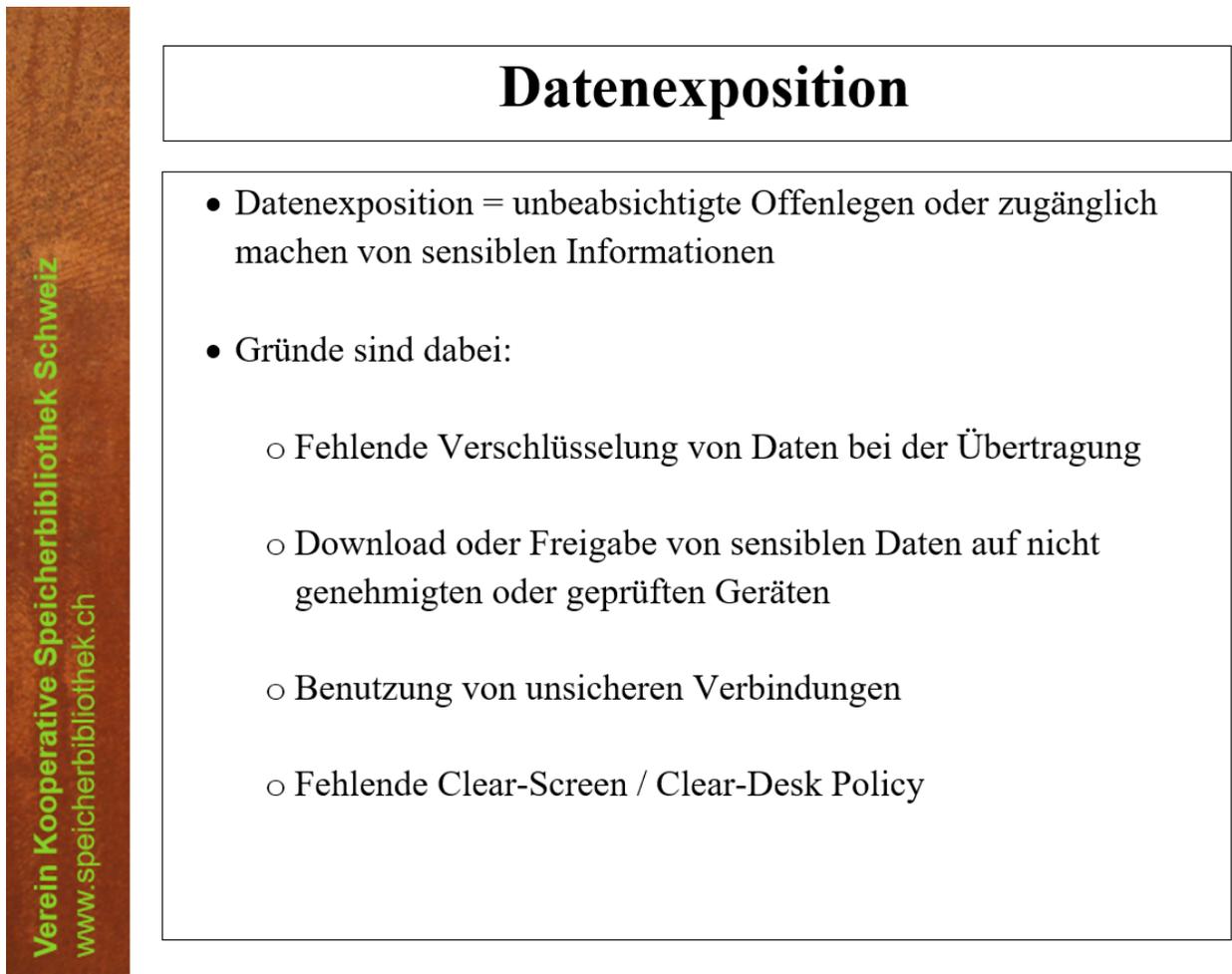
Die Fragen sowie die korrekten Antworten sind im Anhang C ersichtlich.

5.4.3 Datenexposition

Der Themenbereich Datenexposition besteht aus zwei Teilen, aus den Plakaten, welche zu Schulungszwecken erstellt wurden, sowie dem Onlinetest zur Überprüfung des Schulungserfolgs. Zur Erstellung der Plakate wird auf Abschnitt 2.5 verwiesen.

5.5.1.1 Plakate

Insgesamt wurden drei Plakate für die Schulung erstellt. Das erste Plakat behandelt die Datenexposition und ist in der Abbildung 8 ersichtlich.



The image shows a poster titled "Datenexposition". On the left side, there is a vertical orange bar with the text "Verein Kooperative Speicherbibliothek Schweiz" and the website "www.speicherbibliothek.ch". The main content of the poster is enclosed in a black border and contains the following text:

Datenexposition

- Datenexposition = unbeabsichtigte Offenlegen oder zugänglich machen von sensiblen Informationen
- Gründe sind dabei:
 - Fehlende Verschlüsselung von Daten bei der Übertragung
 - Download oder Freigabe von sensiblen Daten auf nicht genehmigten oder geprüften Geräten
 - Benutzung von unsicheren Verbindungen
 - Fehlende Clear-Screen / Clear-Desk Policy

Abbildung 8 Plakat Datenexposition

Zuerst wird der Begriff definiert, um den Mitarbeitern verständlich zu machen, was eine Datenexposition ist. In einem zweiten Teil werden die Ursachen für eine Datenexposition dargelegt. Das zweite Plakat betrifft die Datenübermittlung und ist in der Abbildung 9 ersichtlich.

Datenübermittlung

- Keine Übermittlung oder Zugriff auf sensible Daten über ein öffentliches WLAN
- Aktivierung von VPN bei Zugriff auf interne Daten
- Bei vertraulichen E-Mails (Outlook):
 - Vertraulichkeit > Vertraulich setzen und Betreff:
VERTRAULICH
 - Verschlüsseln > Nicht weiterleiten
 - dies verhindert, dass die Nachricht weitergeleitet oder kopiert/gedruckt werden kann
- Benutzen von VKSS internen Diensten und Medien für eine Datenübermittlung (SwissTransfer.ch, OneDrive, SharePoint, E-Mail)

Abbildung 9 Plakat Datenübermittlung

Es werden stichwortartig Verhaltensregeln und -anweisungen aufgezählt, welche für eine sichere Datenübertragung notwendig sind. Stichworte sind dabei, dass keine Übermittlung und kein Zugriff auf sensible Unternehmensdaten über ein öffentliches Netzwerk erfolgen darf. Die Mitarbeiter werden zudem angewiesen, das VPN zu aktivieren, falls kein internes Netzwerk vorhanden ist. Nach einer Diskussion mit den Verantwortlichen des VKSS wird zudem kurz erklärt, wie E-Mails in Outlook als vertraulich gekennzeichnet werden können und wie die Weiterleitung verhindert werden kann. Zudem werden die VKSS-internen Dienste und Medien aufgezeigt, welche für die Datenspeicherung sowie die Übermittlung verwendet werden sollen.

Das dritte Plakat befasst sich mit dem Verlust des Endgerätes und ist in der Abbildung 10 ersichtlich.

Verlust Endgerät

- Der Verlust/Diebstahl eines Endgerätes (Notebook, Tablet, Smartphone, Datenträger) ist umgehend an den ICT-Verantwortlichen und die Geschäftsleitung zu melden.
- Auch der Verlust von Schlüsseln oder geschäftlichen Akten sind mitzuteilen.

Abbildung 10 Plakat Verlust Endgerät

Es wird darauf aufmerksam gemacht, dass der Verlust eines Endgerätes schnellstmöglich an den ICT-Verantwortlichen sowie an die Geschäftsleitung zu melden ist. Nach Absprache wurde der Verlust von Schlüsseln oder geschäftlichen Akten noch hinzugefügt.

5.5.1.2 Onlinetest

Die Fragen sowie die korrekten Antworten sind im Anhang C ersichtlich.

5.5.2 Sicherheitsvorfälle

Der Themenbereich Sicherheitsvorfälle besteht aus zwei Teilen. Diese sind der Blogpost sowie der Onlinetest. Zur Erreichung der in Abschnitt 3.1.1.6 sowie Abschnitt 4.2.5 definierten Anforderungen wird die in Abschnitt 2.6 erläuterte Theorie angewendet.

5.5.2.1 Blogpost

Der Blogpost ist in zwei Teile untergliedert. Im ersten wird aufgezeigt, wie man erkennen kann, ob das Endgerät mit Schadsoftware befallen ist. Dabei wird auf den Windows Defender verwiesen zur Überprüfung des Systems sowie auf das manuelle Untersuchen ungewöhnlicher Software, welche installiert wurde. Zudem werden typische Anzeichen sowie typisches Systemverhalten verdeutlicht, welche bei einem Befall mit Schadsoftware auftreten können. Im zweiten Teil wird der Meldeablauf gemäss Absprache definiert sowie die Anordnung seitens des VKSS weitergegeben, dass die Verbindung zum Internet getrennt werden soll. Meldungen erfolgen dabei primär an den ICT-Verantwortlichen, bei Meldung per E-Mail soll die Geschäftsführung ins <cc> genommen werden.

Da das Intranet seitens des VKSS für die Blogposts noch nicht eingerichtet ist, können an dieser Stelle keine Abbildungen gezeigt werden.

5.5.2.2 Onlinetest

Die Fragen sowie die korrekten Antworten sind im Anhang C ersichtlich.

5.5.3 Updates

Der Themenbereich Updates besteht aus zwei Teilen. Dies sind die PowerPoint-Präsentation für die Schulung sowie der Onlinetest.

5.5.3.1 PowerPoint

Die PowerPoint-Präsentation weist folgende Agenda auf: Vorwort, Updates, Updates mit Windows, Updates von Software, Updates O365 sowie Meldungen. Im Vorwort werden die Titel

von drei aktuellen Beispielen eingeblendet. Die Artikelnamen sind dabei wie folgt: ‹Codeschmuggel möglich: Microsoft stuft Sicherheitslücke auf kritische herauf› (Dirk Knop, 2022), ‹Webbrowser: Chrome-Update dichtet acht Sicherheitslecks ab› (Dirk Knop, 2022) sowie ‹US-Cyberaufsichtsbehörde warnt vor Angriffen unter anderem auf Veeam› (Dirk Knop, 2022). Damit soll vermittelt werden, dass täglich neue Sicherheitslücken bekannt werden und Updates von Betriebssystemen sowie Software von Bedeutung sind. Dies wird mit der Abbildung 11 vermittelt.



Updates

- Wieso sind Updates wichtig?
 - Täglich neue & schnell verbreitende Viren, welche Sicherheitslücken ausnutzen
 - Updates sind essenziell um vorhandene Sicherheitslücken im Betriebssystem sowie in Software zu schliessen
- Im VKSS werden Updates von Windows und Office prinzipiell automatisch verteilt.
- Updates sind im Homeoffice sowie auf privaten Geräten (Computer, Tablets, Smartphones, etc.) unverzichtbar!

Abbildung 11 Folie Updates

Es wird erwähnt, dass der VKSS Windows- sowie O365-Updates automatisch verteilt. Die darauffolgende Folie ‹Update Windows› zeigt auf, wie überprüft werden kann, ob Betriebssystemupdates notwendig sind und wie diese vorgenommen werden können unter Windows 10 und Windows 11. Auf der nächsten Folie ‹Updates von Software› wird zusammengefasst, wo die Update-Einstellungen für Software häufig zu finden sind. Dabei wird erwähnt, dass Updates von Software nur vom ICT-Verantwortlichen durchgeführt werden dürfen. Die nächste Folie zeigt anhand von O365 als

Software auf, wie es möglich ist, nach Updates zu suchen. Die letzte Folie bildet die Meldungen. Dort wird definiert, was gemeldet werden soll und an welche Person.

5.5.3.2 Onlinetest

Die Fragen sowie die korrekten Antworten sind im Anhang C ersichtlich.

5.5.4 Unsichere Netzwerke

Die Schulung «Unsichere Netzwerke» besteht aus zwei Teilen. Zur Vermittlung der Theorie wird ein Blogpost erstellt. Die Überprüfung des Lernerfolgs geschieht anhand einer Onlineprüfung.

5.5.4.1 Blogpost

Der Blogpost besteht aus vier Abschnitten. Im ersten Teil wird auf den Sophos VPN Client aufmerksam gemacht und darauf, weshalb dieser verwendet werden soll. Zugleich wird auf die Anleitung zur Installation verlinkt. Im zweiten Abschnitt «Private Geräte» wird nach einer Diskussion mit den Verantwortlichen des VKSS zusätzlich geregelt, was die Mitarbeitenden beachten müssen, wenn sie private Geräte zur Arbeit mitbringen und verwenden. Im dritten Abschnitt «Sicherheitsziele» wird die Theorie aus Abschnitt 2.8 vorgestellt. Im vierten Teil «Gefahren» werden die konkreten Angriffe auf Netzwerke dargelegt und wie diese die Sicherheitsziele beeinflussen. Dafür wird die Theorie von Abschnitt 2.8.1 verwendet.

Da das Intranet seitens des VKSS für die Blogposts noch nicht eingerichtet ist, können an dieser Stelle keine Abbildungen gezeigt werden.

5.5.4.2 Onlinetest

Die Fragen sowie die korrekten Antworten sind im Anhang C ersichtlich.

5.7 Zeitplan

Abbildung 12 veranschaulicht, wie der zeitliche Ablaufplan der Security Awareness Kampagne initial umgesetzt wird. Dabei wird das erarbeitete Wissen aus Kapitel 2 und aus der Beschreibung des CIS-Frameworks für die Planung der Schulungen angewendet. Die Schulungen sollten über das Jahr verteilt stattfinden. Da keine Betriebsferien beim VKSS vorgesehen sind, werden die Schulungen ungefähr in Zweimonatsabständen durchgeführt.

Bereich/Monat	Januar	Februar	März	April	Mai	Juni	Juli	August	September	Oktober	November	Dezember
Authentifizierung												
Datenverarbeitung												
Datenexposition												
Sicherheitsvorfälle												
Updates												
Unsichere Netzwerke												
Social-Engineering												

Abbildung 12 Zeitplan Schulung

5.7.1 Social-Engineering:

Die Social-Engineering-Schulung startete am 1. Dezember 2022, in der Kalenderwoche 48. Das Versenden von Phishing-E-Mails an sämtliche Mitarbeiter dauerte bis zum 5. Dezember. Der Theoretische Teil der Schulung erfolgte am 14. Dezember 2022, in der Kalenderwoche 50, in den Räumlichkeiten des VKSS. Der Onlinetest mit Microsoft Forms wurde am 19. Dezember 2022, in der Kalenderwoche 51, für die Mitarbeiter aufgeschaltet und war bearbeitbar bis zum 20. Dezember 2022.

5.7.2 Authentifizierung

Die Schulung betreffend den Themenbereich Authentifizierung startet am 1. Februar 2023, in der Kalenderwoche 5. Dann wird das Video im Intranet für die Mitarbeiter freigeschaltet und diese werden per E-Mail informiert, dass ein neuer Schulungsblock beginnt. Am 15. Februar 2023, in der Kalenderwoche 7, wird der Link zum Onlinetest an alle Mitarbeiter per E-Mail versendet und der Onlinetest aufgeschaltet. Ab dem 24. Februar 2023, in der Kalenderwoche 8, wird der Onlinetest ausgewertet und kurze persönliche Besprechungen bezüglich der Resultate finden anschließend mit den einzelnen Mitarbeitern statt.

5.7.3 Datenverarbeitung

Die Schulung betreffend Datenverarbeitung startet am 3. April 2023, in der Kalenderwoche 14. Der Blogpost wird im Intranet aufgeschaltet und die Mitarbeiter werden darüber per E-Mail informiert. Der Link zum Onlinetest steht am 17. April 2023, in der Kalenderwoche 16, im Intranet zur Verfügung und wird per E-Mail an alle Mitarbeiter versendet. Ab dem 28. April 2023, in der Kalenderwoche 17, wird der Onlinetest ausgewertet und eine Besprechung mit den einzelnen Mitarbeitern bezüglich der Resultate findet statt.

5.7.4 Datenexposition

Am 5. Juni 2023, in der Kalenderwoche 23, startet die Schulung zum Themenbereich Datenexposition. Die Plakate werden in Umkleidekabinen und Büroräumlichkeiten aufgehängt. Die Mitarbeiter werden per E-Mail über den Beginn der Schulung und die Standorte der Plakate informiert. Am 19. Juni 2023, in der Kalenderwoche 25, wird der Onlinetest per E-Mail oder Aufschaltung im Intranet den Mitarbeitern zur Bearbeitung freigegeben. Die Auswertung sowie die Besprechung der Resultate finden dabei ab dem 26. Juni 2023, Ende der Kalenderwoche 26, statt.

5.7.5 Sicherheitsvorfälle

Am 7. August 2023, in der Kalenderwoche 32, startet die Schulung des Themenbereichs Sicherheitsvorfälle. Dazu wird der Blogpost im Intranet aufgeschaltet und die Mitarbeiter werden per E-Mail informiert, dass ein neuer Schulungsblock beginnt. Am 21. August 2023, in der Kalenderwoche 34, wird der Onlinetest per E-Mail oder Aufschaltung im Intranet den Mitarbeitern zur Bearbeitung freigegeben. Ab dem 28. August 2023, in der Kalenderwoche 35, kann der Onlinetest ausgewertet werden und die persönlichen Besprechungen mit den Mitarbeitern können stattfinden.

5.7.6 Updates

Ab dem 2. Oktober 2023, in der Kalenderwoche 40, findet die Schulung bezüglich Updates statt. Dazu wird ein Termin vereinbart, an welchem alle Mitarbeiter des VKSS vor Ort sind. Die Aufschaltung des Onlinetests erfolgt am 16. Oktober 2023, in der Kalenderwoche 42. Die Besprechung der einzelnen Resultate des Onlinetests findet ab dem 23. Oktober 2023, Ende der Kalenderwoche 43, statt.

5.7.7 Unsichere Netzwerke

Am 1. November 2023, in der Kalenderwoche 44, startet die Schulung ‹Unsichere Netzwerke› für alle Mitarbeiter. Der Blogpost wird im Intranet aufgeschaltet und die Mitarbeiter werden über den Beginn der neuen Schulung per E-Mail informiert. Am 20. November 2023, in der Kalenderwoche 47, wird der Onlinetest per E-Mail oder Aufschaltung im Intranet den Mitarbeitern zur Bearbeitung freigegeben. Die Auswertung sowie die Besprechung mit den Mitarbeitern können Ende der Kalenderwoche 47 am 23. November 2023 erfolgen.

5.8 Weiterführung der Kampagne

Zur Aufrechterhaltung der Security Awareness Kampagne und zur Erfüllung der ersten Schutzmassnahme wurden Kalenderwochen für die Termine angegeben (siehe Abbildung 13). Diese dienen als Orientierungshilfe, um die Kampagne in den kommenden Jahren wiederholen und planen zu können.

Kalenderwoche	Thema	Aktion
5	Authentifizierung	Aufschaltung Video
7		Aufschaltung Onlinetest
8		Auswertung Onlinetest
14	Datenverarbeitung	Aufschaltung Blogpost
16		Aufschaltung Onlinetest
17		Auswertung Onlinetest
23	Datenexposition	Aufhängen Plakate
25		Aufschaltung Onlinetest
26		Auswertung Onlinetest
32	Sicherheitsvorfälle	Aufschaltung Blogpost
34		Aufschaltung Onlinetest
35		Auswertung Onlinetest
40	Updates	Präsentation
42		Aufschaltung Onlinetest
43		Auswertung Onlinetest
44	Unsichere Netzwerke	Aufschaltung Blogpost
47		Aufschaltung/Auswertung Onlinetest
48	Social-Engineering	Start Phishing
50		Präsentation
51		Aufschaltung/Auswertung Onlinetest

Abbildung 13 Jahreszyklus der Schulungen

Die Unterlagen zu den Themenbereichen können für zukünftige Schulungen durch den VKSS angepasst oder erweitert werden. Ausnahme bildet lediglich das Schulungsvideo ‹Authentifizierung›, welches aufgrund des gewählten Schulungskanal schwer anzupassen ist. Die Materialien werden in Dateiformaten abgegeben, welche durch den VKSS bearbeitet werden können. Ziel ist es, dass der VKSS die Schulungsunterlagen auf dem neusten Stand der Technik hält und die Mitarbeiter zeitgemäss geschult werden können.

6 Evaluation und Validation

In diesem Kapitel werden die Ergebnisse ausgewertet. Es wird überprüft, inwiefern durch die Realisierung die Ziele erreicht werden konnten.

6.1 Erstellung Schulungskonzept

Ziel war es, ein Schulungskonzept für eine Security Awareness Kampagne nach dem CIS Control 14 zu erstellen auf unterschiedlichen Schulungskanälen sowie einen entsprechenden Zeitplan. In die Realisierung konnten einzelne Teile des Schulungskonzepts übernommen werden. Dies betraf die Schulungskanäle für die einzelnen Themen (Abschnitt 5.1), den Zeitplan (Abschnitt 5.3) sowie die Weiterführung der Kampagne (Abschnitt 5.4).

6.1.1 Critical Security Controls 14

Ziel war es, eine Security Awareness Kampagne zu erstellen, welche die Schutzmassnahmen im Control 14 erfüllt. Die Schutzmassnahme 1 wird durch die die Erstellung der Security Awareness Kampagne sowie durch die Erstellung des Zeitplans erfüllt. Für die Schutzmassnahmen 2 bis 8 wurden Schulungsunterlagen erstellt. Da der VKSS eine zielgerichtete Security Awareness Kampagne erwartete, war mit Abweichungen von den einzelnen Anforderungen zu rechnen. Die Schutzmassnahme 9 wurde nach Absprache nicht umgesetzt. Die Begründung dazu befindet sich in Abschnitt 4.2.8. Dies steht in keinem Widerspruch zum CIS-Framework, dessen alleiniges Ziel die Erhöhung der IT-Sicherheit ist.

6.1.2 Schulungskanäle

Ziel war es, verschiedene Schulungskanäle für die Security Awareness Kampagne zu verwenden. Als Grundlage für die Evaluierung von Schulungskanälen wurde eine Literaturrecherche vorgenommen. Die gewonnen Erkenntnisse wurden verwendet, um anhand der Grösse und Komplexität der verschiedenen Themenbereiche einen geeigneten Schulungskanal auszuwählen. Die Schulungskanäle wurden nach Rücksprache mit dem VKSS genehmigt. Insgesamt wurden sechs verschiedene Schulungskanäle eingesetzt.

6.1.3 Zeitplan

Ziel war es, einen Zeitplan sowie einen Zyklus für die Security Awareness Kampagne zu erstellen. Für jeden der sieben Themenbereiche wurde ein Zeitplan für das Jahr 2022 festgelegt. Auf diesem

ist ersichtlich, wann die Schulung jedes Themenbereichs beginnt, die Onlinetests aufgeschaltet werden und die Nachbesprechungen stattfinden. Zur Weiterführung der Kampagne wurde zudem eine Tabelle erstellt mit der Angabe der Kalenderwochen, anhand derer ersichtlich wird, welches Thema wann geschult wird und welche Aktion seitens des VKSS erforderlich ist.

6.2 Schulungsunterlagen

Ziel war es, Schulungsunterlagen anhand der Schutzmassnahmen von Control 14 zu erstellen, welche in Themenbereiche aufgeteilt werden. Aufgrund der Anforderung der Schutzmassnahme 1, welche darin besteht, dass der Inhalt jährlich überprüft und gegebenenfalls angepasst werden soll, wurden die Schulungsunterlagen in Dateiformaten erstellt, welche leicht abänderbar sind.

6.3 Onlinetests

Ziel war es, Onlinetests zu erstellen, um den Erfolg der einzelnen Schulungen messen zu können. Die Onlinetests sind im Anhang C ersichtlich. Diese wurden anhand der Schulungsunterlagen ausgerichtet und nach einer Diskussion mit den Verantwortlichen des VKSS genehmigt.

6.4 Initiale Schulung

Ziel war es, eine initiale Schulung der Mitarbeitenden des VKSS durchzuführen. Diese umfasst den Themenbereich Social-Engineering. Der Beginn der Phishing-Kampagne war am 1. Dezember 2022, welche bis zum 5. Dezember 2022 dauerte.



Abbildung 14 Ergebnisse Phishing-Simulation

Abbildung 14 zeigt die Ergebnisse der Phishing-Simulation. Daraus wird ersichtlich, dass kein Mitarbeiter des VKSS auf den Link im Phishing-E-Mail geklickt hat. Lediglich 25 % der Mitarbeiter öffneten die E-Mail. Nach Rücksprache mit dem ICT-Verantwortlichen meldeten mehrere Personen den Erhalt einer Phishing-E-Mail. Darunter auch zwei der drei Mitarbeitenden, welche die E-Mail geöffnet hatten. Somit öffneten nur eine Person die Phishing-E-Mail und meldete diese

nicht an den ICT-Verantwortlichen. Daraus lässt sich folgern, dass die Mitarbeiter des VKSS bezüglich Phishing E-Mails sensibilisiert sind.

Die Schulung vor Ort nach der Phishing-Kampagne fand am 14. Dezember 2022 statt und dauerte ungefähr eine Stunde. Der Onlinetest wurde am 19. Dezember online geschaltet und an die Mitarbeiter versandt. Der Test war bearbeitbar bis zum 23. Dezember aufgrund von Abwesenheiten und Ferien einzelner Mitarbeiter.

6.4.1 Ergebnisse Onlinetest

Die Frage 1 sowie das Ergebnis ist in der Abbildung 15 ersichtlich.

1. Was sind die Ziele von Social Engineering? (2 Punkte)

100% der Antwortenden (10 von 10) haben diese Frage richtig beantwortet.

- Diebstahl von wertvollen & sens... 10 ✓
- Sozialwissenschaftliche Studien ... 0
- Manipulation von Einzelpersone... 10 ✓
- Informationsverarbeitung mit Bi... 0



Abbildung 15 Ergebnis Frage 1

Die Frage 2 sowie die Antworten sind in der Abbildung 16 ersichtlich.

2. In welche Kategorien können Social Engineering Attacken eingeteilt werden? (___ und ___) (2 Punkte)
 20% der Antwortenden (2 von 10) haben diese Frage richtig beantwortet.

● computerbasiert und menschen...	3	✓
● Menschenbasiert und Computer...	2	✓
● Computerbasiert und menschba...	1	
● Phishing, Dumpster Diving	1	
● Maschinen- und Menschenbasiert	1	
● Computer und Menschen	1	
● menschenbasiert + computerba...	1	
● 0 weitere Optionen	0	

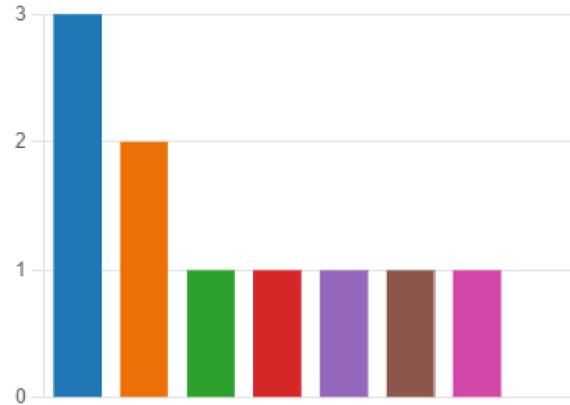


Abbildung 16 Ergebnis Frage 2

Das Ergebnis der Frage 3 ist in der Abbildung 17 ersichtlich.

3. Das Durchsuchen von Müllcontainern gehört in folgende Kategorie: (2 Punkte)
 90% der Antwortenden (9 von 10) haben diese Frage richtig beantwortet.

● Soziale Attacke	1	
● Technische Attacke	0	
● Physische Attacke	9	✓



Abbildung 17 Ergebnis Frage 3

Die Antworten sowie das Ergebnis der Frage 4 sind in der Abbildung 18 ersichtlich.

4. Welches sind Schutzmassnahmen um Social Engineering vorzubeugen? (2 Punkte)
90% der Antwortenden (9 von 10) haben diese Frage richtig beantwortet.

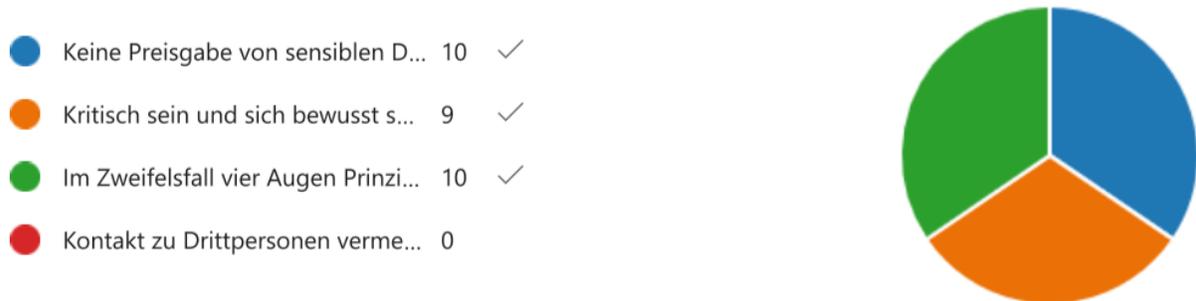


Abbildung 18 Ergebnis Frage 4

Die Frage 5 enthält das Feedback der Teilnehmenden, dieses war ausschnittsweise wie folgt:

- ‹Ich finde Frage 1 und 4 irrelevant›
- ‹Sehr gute Präsentation. Vielleicht müsste etwas weniger ‹Computerdeutsch› gesprochen werden (Ausdrücke, die auch jeder versteht) oder erklären, was die Ausdrücke bedeuten. Wir sind Laien und haben keine oder nicht viel Fachwissen›
- ‹Etwas eintönig, zu viele Fachbegriffe. Wäre schön etwas ‹menschlicher› statt fachlich. So wäre es auch weniger eintönig, sondern packender›
- ‹Für mich massgeblich sind die Schlussfolgerungen am Ende der PP-Präsentation.›
- ‹Die Schulung war gut und verständlich.›
- ‹War eine bisschen zu trockene Präsentation›
- ‹Ergänzend zur Präsi dann jeweils den spezifischen Input, wie wir das handhaben.›
- ‹Kurs war super informativ. ‹Vermittlungssprache› war auf angenehmer Stufe, nicht zu hoch. Praktische Beispiele waren gut. Merci.›

6.4.2 Auswertung Onlinetest Social-Engineering

Aufgrund von Abwesenheiten konnten zwei Mitarbeitende des VKSS den Onlinetest nicht absolvieren. Wie aus den Abbildungen im Abschnitt 6.4.1 ersichtlich wird, wurde die Mehrheit der Fragen mit rund 90 % richtig beantwortet. Ausnahme bildet dabei die Frage 2. Nach genauerem Betrachten ist erkennbar, dass aufgrund der Schreibweise, richtige Antworten als falsch erkannt wurden. Eine nachträgliche Überprüfung der Antworten ergab, dass auch diese Frage mit rund

90 % richtig beantwortet wurde. Aus dem Feedback wird ersichtlich, dass einzelne Mitarbeitende mit den Fachbegriffen von Social-Engineering-Attacken überfordert waren.

7 Ausblick

Ziel der vorliegenden Arbeit war es, eine Security Awareness Kampagne für den VKSS zu planen, vorzubereiten sowie initial umzusetzen. Die Erstellung der Kampagne soll dabei nach den Vorgaben von CIS Control 14 umgesetzt werden. Dazu soll ein Schulungskonzept mit verschiedenen Schulungskanälen sowie einem Zeitplan für die Schulungen erstellt werden. Eine initiale Schulung eines Themenbereichs, soll dabei im Rahmen der Bachelorarbeit stattfinden.

7.1 Reflexion der Arbeit

In der vorliegenden Arbeit befasste ich mich mit der Erstellung einer Security Awareness Kampagne. Dabei lag der Fokus auf der Sensibilisierung der Mitarbeiter des VKSS unter Verwendung des Control 14. Mit dem Ergebnis der Arbeit bin ich zufrieden und hoffe dadurch einen Mehrwert bezüglich der IT-Sicherheit des VKSS erreicht zu haben.

Aufgrund der Vorgabe des CIS Control 14 hatte ich anfängliche Schwierigkeiten bei der Literaturrecherche zur Erfüllung der Anforderungen. Literatur war teilweise ausreichend auffindbar, jedoch eignete sich diese nicht als wissenschaftliche Quellen.

Die Methodik konnte relativ schnell abgehandelt werden, da das Framework mit CIS bereits vorgegeben war, gut dokumentiert ist und Beispiele zu den einzelnen Schutzmassnahmen geboten werden. Die Erstellung des Konzepts mit den einzelnen Schulungskanälen sowie Themen, welche eingeschränkt wurden, beanspruchte mehr Zeit als eingeplant. Dies lag vor allem am regen Austausch und an den Diskussionen mit dem VKSS, damit die Themenbereiche optimal auf die Schulung ihrer Mitarbeiter abgestimmt werden konnten. Es stellt sich hierbei als positiv heraus, dass mehr Zeit in diese Kapitel investiert wurde, da die Schulungskanäle sowie Themen in das Schulungskonzept für den VKSS übernommen werden konnten. Zudem erleichterte es die Erstellung der Schulungsunterlagen im nächsten Kapitel.

Die Realisierung umfasste positive sowie negative Aspekte. Für die Erstellung der Schulungsunterlagen konnte ich meine eigenen Ideen einbringen und diese gemäss meinen Vorstellungen umsetzen. Da der VKSS aber momentan noch über kein ausgebautes Intranet verfügt, konnte ich die Blogposts lediglich in Word ausarbeiten. Es wäre besser gewesen, wenn ich diese direkt im Intranet hätte erstellen können, beispielsweise mit der Verwendung von SharePoint. Somit wäre es möglich gewesen, in die Materialien eine Corporate Identity hineinzubringen. Die Festlegung

des Zeitplans verlief reibungslos. Da keine terminlichen Einschränkungen wie Betriebsferien seitens des VKSS vorhanden sind, konnten die Schulungen einfach über das Jahr verteilt werden. Der Jahreszyklus für die einzelnen Themenbereiche konnte ebenfalls problemlos erstellt werden.

Die Auswertung des Onlinetests der initialen Schulung bezüglich des Themas Social-Engineering zeigte auf, dass die Mitarbeiter das vermittelte Wissen weitgehend verstanden haben. Das Feedback zeigte aber auch auf, dass in zukünftigen vor Ort Schulungen, die Vermittlungssprache angepasst werden muss.

Die Ausarbeitung eines Schulungskonzepts sowie die Erstellung von Schulungsunterlagen nach dem Control 14 von CIS war für mich persönlich eine neue und lehrreiche Erfahrung. Dabei konnte ich vor allem viel lernen, da ich von der Konzeption bis hin zur Realisierung der Kampagne alles ausarbeiten konnte. Die in die Umsetzung des Auftrages des VKSS investierte Zeit hat sich meiner Ansicht nach somit gelohnt.

7.2 Ausblick

Der Auftrag umfasste eine initiale Schulung für eine der im CIS-Framework definierten Schutzmassnahmen. Aufgrund der zeitlichen Begrenzung der Bachelorarbeit finden die weiteren Schulungen nach der Abgabe statt. Die Ergebnisse der Onlinetests der kommenden Schulungen sind somit noch abzuwarten. Interessant wäre die Auswertung der kommenden Onlinetests zu analysieren. Die Ergebnisse können einerseits verwendet werden, um die Security Awareness Kampagne für die kommenden Jahre anzupassen und den Lernerfolg der Mitarbeiter zu maximieren. Andererseits kann anhand der Resultate abgeleitet werden, bei welchen Themengebieten noch Handlungsbedarf besteht und nachgeschult werden muss.

Bei mehrfach wiederholter Durchführung der Kampagne kann ebenfalls eruiert werden, inwiefern der vermittelte Lernstoff der einzelnen Themenbereiche bei den Mitarbeitern noch präsent ist. Dies wäre interessant, um zu ermitteln, inwiefern die «Security Awareness» der Mitarbeiter durch die Kampagne gesteigert werden konnte.

8 Anhang

A. Aufgabenstellung

Ausgangslage und Problemstellung

Um die IT-Sicherheit der Speicherbibliothek zu erhöhen, soll eine Security Awareness Kampagne geplant, vorbereitet und initial umgesetzt werden.

Ziel der Arbeit und erwartete Resultate

Konzipierung einer für die Speicherbibliothek massgeschneiderten Security Awareness Kampagne. Erstellung eines Zeitplans für Schulungen und Tests. Bereitstellung benötigter Unterlagen. Durchführung einer initialen Schulung.

Gewünschte Methoden, Vorgehen

Die Konzipierung der Kampagne soll sich an den Empfehlungen des CIS Controls v8 (Control 14) orientieren.

Kreativität, Varianten, Innovation

Frei. Angemessen an Tagesbetrieb und Teilzeitarbeit (z.B. Self-Learning). Orientierung an / Integrierung von bestehender Kampagne (z.B. s-u-p-e-r.ch) ist denkbar.

Starttermin: 19. September 2022

Abgabetermin: 3. Januar 2023

B. Schulungsunterlagen und Schulungskonzept

Die Dateien im Anhang B wurden in einer separaten ZIP-Datei abgegeben.

Anhang_B_Schulungsunterlagen

Anhang_B_Schulungskonzept

C. Onlinetests

Authentifizierung

* Required

1. Wieso sind sichere Passwörter wichtig? * (2 Points)

- Schutz persönlicher Daten
- Schutz öffentlicher Daten
- Schutz sensibler Daten
- Schutz vor Phishing

2. Welche der folgenden Passwörter gelten als sicher? * (2 Points)

- Itsi16JabrKmM!
- AAAAAAAAAAAAA
- Passwort123456
- 95JlaisiDFS.
- Speicherbibliothek2022
- !NwluED

3. Wie werden Passwörter korrekt mit anderen Benutzern geteilt? * (2 Points)

- Passwort auf Zettel schreiben und Benutzer geben
- Verknüpfung erstellen im Passwort-Manager
- Mit der Funktion an Benutzer senden im Passwort- Manager

4. Was sind die Vorteile von MFA? * (2 Points)

- Starke Passwörter sind nicht mehr wichtig
- Die Identität des Benutzers stützt sich auf mehrere Faktoren
- Das Login wird vereinfacht

5. Feedback / Verbesserungsvorschläge *

Enter your answer

Submit

Datenverarbeitung

...

* Required

1. Wie sollen geschäftliche Daten gespeichert werden? * (2 Points)

- SharePoint
- Google Drive
- OneDrive
- Dropbox

2. Sind Daten im Papierkorb unwiderruflich gelöscht? * (2 Points)

- Ja
- Nein

3. Welche Medien können sensible Daten beinhalten? * (2 Points)

- Post-it Zettel
- Ausgedruckte Dokumente
- Fotos und Filme
- defekter USB-Stick
- Festplatte eines Computers

4. Was sollte beim Verlassen des Arbeitsplatzes beachtet werden? * (2 Points)

- Sperren des Computers
- Ausschalten des Bildschirms
- Abmelden vom Computer (bei längerer Abwesenheit)
- Wegschliessen sensibler Daten
- Keine der genannten

5. Feedback / Verbesserungsvorschläge *

Submit

Datenexposition

...

* Required

1. Wie kann eine Datenexposition entstehen? * (2 Points)

- Benutzung unsicherer Verbindungen
- Benutzung des VPN
- Fehlende Verschlüsselung von Daten bei der Übertragung
- Download oder Freigabe von sensiblen Daten auf nicht genehmigte oder geprüfte Geräte
- Alle Optionen treffen zu

2. Welche der genannten Dienste sind VKSS intern? * (2 Points)

- Swisstransfer
- OneDrive
- Google Drive
- SharePoint
- Dropbox
- Amazon Web Services AWS
- E-Mail

3. Dürfen sensible Dokumente über ein öffentliches Flughafen WLAN ohne VPN verschickt werden? * (2 Points)

- Ja
- Nein
- Keine der genannten Optionen trifft zu

4. Das setzen von *Vertraulich* im Betreff von E-Mails hat folgende Auswirkungen: * (2 Points)

- Daten werden verschlüsselt
- Das Weiterleiten von der Nachricht ist nicht mehr möglich
- Das Ausdrucken/Kopieren der Nachricht ist nicht mehr möglich
- Keine der genannten

5. Feedback / Verbesserungsvorschläge *

Enter your answer

Submit

Sicherheitsvorfälle

...

* Required

1. Ordnen Sie die folgenden Aktionen, die bei Verdacht auf Schadsoftware vorgenommen werden müssen, in die richtige Reihenfolge. * (2 Points)

Geschäftsführung kontaktieren

Verbindung zum Internet trennen

ICT-Verantwortlichen kontaktieren

Antivirus Scan durchführen

2. Welches sind typische Anzeichen für einen Befall mit Schadsoftware? * (2 Points)

- Programme öffnen und schliessen sich selbständig
- Das Betriebssystem startet nicht
- Keine Netzwerkverbindung
- Systemmeldungen mit Fehlern erscheinen

3. Wer ist primärer Ansprechpartner bei Verdacht von Schadsoftware? * (2 Points)

- ICT-Verantwortliche
- Geschäftsführung
- Swisscom
- Externer IT-Dienstleister

4. Im Posteingang des E-Mails befinden sich Nachrichten ohne Absender und Betreff. Was ist zu tun? * (2 Points)

- Ich kontaktiere zuerst den ICT-Verantwortlichen.
- Ich deaktiviere zuerst die Internetverbindung.
- Ich starte zuerst einen Virensan.
- Ich erkundige mich bei Mitarbeitern, ob sie auch solche E-Mails im Posteingang haben.

5. Feedback / Verbesserungsvorschläge *

Enter your answer

Submit

Updates

...

* Required

1. Wieso sollten regelmässig Updates gemacht werden? * (2 Points)

- Damit man immer die aktuellsten Funktionalitäten hat.
- Um vorhandene Sicherheitslücken zu schliessen.
- Damit die Software kompatibel zum Betriebssystem bleibt.

2. Wie oft muss auf dem Geschäftscomputer in Windows Update überprüft werden, ob neue Updates vorhanden sind? * (2 Points)

- Täglich
- 1x in der Woche
- 1x im Monat
- Die Updates werden vom VKSS automatisch verteilt

3. Wenn eine Software meldet, dass ein neues Update zur Verfügung steht, darf ich dieses umgehend installieren? * (2 Points)

- Ja
- Nein

4. Was muss ich genau an den ICT-Verantwortlichen melden? * (2 Points)

- Wenn ein Update fehlgeschlagen ist (Windows)
- Wenn neue Updates verfügbar sind (Software)
- Wenn neue Updates verfügbar sind (Windows)
- Wenn länger als 2 Tage keine Updates erscheinen (Windows)

5. Feedback / Verbesserungsvorschläge *

Enter your answer

Submit

Unsichere Netzwerke

...

* Required

1. Darf ich mein privates Smartphone mit dem internen WLAN des VKSS verbinden? * (2 Points)

- Ja
- Nein

2. Welche der folgenden Begriffe sind Sicherheitsziele eines sicheren Netzwerkes? * (2 Points)

- Vertraulichkeit
- Verfügbarkeit
- Verschwiegenheit
- Integrität
- Autonomisierung
- Abstreitbarkeit
- Least Privilege
- Authentifizierung

3. Könnte ein Angreifer von mir übermittelte Anmeldeinformationen vom Smartphone, welches sich im Starbucks WLAN befindet, abgreifen? * (2 Points)

- Ja
- Nein

4. Warum stellen unsichere Netzwerke ein Problem dar? Notieren Sie die wichtigsten Punkte. * (2 Points)

Enter your answer

5. Feedback / Verbesserungsvorschläge *

Enter your answer

Submit

Social-Engineering

...

* Required

1. Was sind die Ziele von Social-Engineering? * (2 Points)

Please select 2 options.

- Sozialwissenschaftliche Studien zu erarbeiten
- Diebstahl von wertvollen & sensiblen Daten
- Informationsverarbeitung mit Big Data
- Manipulation von Einzelpersonen & Unternehmen

2. In welche Kategorien können Social-Engineering-Attacks eingeteilt werden? (___ und ___) * (2 Points)

Enter your answer

3. Das Durchsuchen von Müllcontainern gehört in folgende Kategorie: * (2 Points)

- Technische Attacke
- Soziale Attacke
- Physische Attacke

4. Welches sind Schutzmassnahmen um Social-Engineering vorzubeugen? * (2 Points)

Please select 3 options.

- Kontakt zu Drittpersonen vermeiden
- Kritisch sein und sich bewusst sein was man tut
- Im Zweifelsfall vier Augen Prinzip anwenden
- Keine Preisgabe von sensiblen Daten an Drittpersonen

5. Feedback / Verbesserungsvorschläge *

Enter your answer

Submit

D. Ergebnisse Onlinetest Social-Engineering

Social Engineering

10
Antworten

6.6
Durchschnittliche Bewertung

Aktiv
Status

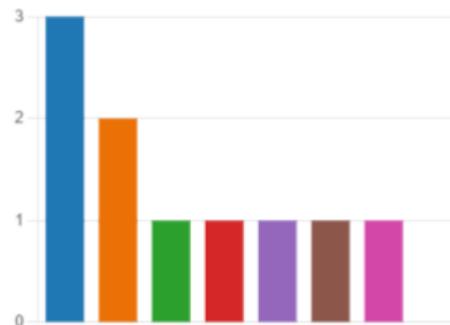
1. Was sind die Ziele von Social Engineering? (2 Punkte)
100% der Antwortenden (10 von 10) haben diese Frage richtig beantwortet.

- Diebstahl von wertvollen & sens... 10 ✓
- Sozialwissenschaftliche Studien ... 0
- Manipulation von Einzelpersone... 10 ✓
- Informationsverarbeitung mit Bi... 0



2. In welche Kategorien können Social Engineering Attacken eingeteilt werden? (___ und ___) (2 Punkte)
20% der Antwortenden (2 von 10) haben diese Frage richtig beantwortet.

- computerbasiert und menschen... 3 ✓
- Menschenbasiert und Computer... 2 ✓
- Computerbasiert und menscha... 1
- Phishing, Dumpster Diving 1
- Maschinen- und Menschenbasiert 1
- Computer und Menschen 1
- menschenbasiert + computerba... 1
- 0 weitere Optionen 0



8 Befragten (80%) antworteten **Computer** für diese Frage.

Phishing **Computer** Menschen
Dumpster Diving

3. Das Durchsuchen von Müllcontainern gehört in folgende Kategorie: (2 Punkte)
 90% der Antwortenden (9 von 10) haben diese Frage richtig beantwortet.

- Soziale Attacke 1
- Technische Attacke 0
- Physische Attacke 9 ✓



4. Welches sind Schutzmassnahmen um Social Engineering vorzubeugen? (2 Punkte)
 90% der Antwortenden (9 von 10) haben diese Frage richtig beantwortet.

- Keine Preisgabe von sensiblen D... 10 ✓
- Kritisch sein und sich bewusst s... 9 ✓
- Im Zweifelsfall vier Augen Prinzi... 10 ✓
- Kontakt zu Drittpersonen verme... 0



5. Feedback / Verbesserungsvorschläge (0 Punkt)

9
Antworten

Neueste Antworten

"Kurs war super informativ. "Vermittlungssprache" war auf angenehmer Stuf...

"Vortragsgeschwindigkeit zu schnell. Kapital Angriffe. Kaum Zeit zum Verarb...

" "

3 Befragten (30%) antworteten Frage für diese Frage.

Word cloud containing feedback terms: Kapital Angriffe, angenehmer Stufe, PP-Präsentation, Ausdrücke, halben Jahr, Praktische Beispiele, schützenswerte" Information, Frage, Ende, Präsi, viel Fachwissen, viele Fachbegriffe, trockene Präsentation, PowerPoint Präsentation, Z.B., Sehr gute Präsentation, Büchern, Rückschluss, normalen Abfall, spezifischen Input.

9 Abbildungs-, Tabellen-, Literaturverzeichnis

Abbildungsverzeichnis

Abbildung 1 Social-Engineering-Attacken-Klassifikation (L. Xiangyu, L. Qiuyang, S. Chandel, 2017)	4
Abbildung 2 Social-Engineering-Ansätze (Koyun & Janabi, 2017).....	5
Abbildung 3 Social-Engineering-Angriffe (Fatima Salahdine, Naima Kaabouch, 2019).....	6
Abbildung 4 Mediale Komponenten.....	25
Abbildung 5 Entwurf Phishing-E-Mail in Sophos.....	35
Abbildung 6 Schlussfolgerung Präsentation Social-Engineering	37
Abbildung 7 Schlussfolgerung Themenbereich Authentifizierung.....	39
Abbildung 8 Plakat Datenexposition	41
Abbildung 9 Plakat Datenübermittlung	42
Abbildung 10 Plakat Verlust Endgerät	43
Abbildung 11 Folie Updates	45
Abbildung 12 Zeitplan Schulung	47
Abbildung 13 Jahreszyklus der Schulungen	49
Abbildung 14 Ergebnisse Phishing-Simulation	52
Abbildung 15 Ergebnis Frage 1	53
Abbildung 16 Ergebnis Frage 2	54
Abbildung 17 Ergebnis Frage 3	54
Abbildung 18 Ergebnis Frage 4	55

Tabellenverzeichnis

Tabelle 1 Schulungskanäle	33
---------------------------------	----

Literaturverzeichnis

- Aengenheyster, S., & Dörr, K. M. (Hrsg.). (2019). *Praxishandbuch IT-Kommunikation*. Springer Berlin Heidelberg. <https://doi.org/10.1007/978-3-662-57965-7>
- Aldawood, H., & Skinner, G. (2019). Challenges of Implementing Training and Awareness Programs Targeting Cyber Security Social Engineering. *2019 Cybersecurity and Cyberforensics Conference (CCC)*, 111–117. <https://doi.org/10.1109/CCC.2019.00004>
- Allianz Global Corporate & Speciality. (2021). *The most important global business risks for 2022*. <https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html>
- Ao, S.-I., Gelman, L., Hukins, D. W. L., Hunter, A., & Korsunsky, A. M. (Hrsg.). (2017). *World Congress on Engineering: WCE 2017 : 5-7 July, 2016, Imperial College London, London, U.K.* Newswood Limited.
- BSI. (2017). *Leitfaden Informationssicherheit*. Bundesamt für Sicherheit in der Informationstechnik.
- BSI. (2022). *Daten auf Festplatten und Smartphones endgültig löschen*. https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Daten-sichern-verschluesseln-und-loeschen/Daten-endgueltig-loeschen/daten-endgueltig-loeschen_node.html
- Chetioui, K., Bah, B., Alami, A. O., & Bahnasse, A. (2022). Overview of Social Engineering Attacks on Social Networks. *Procedia Computer Science*, 198, 656–661. <https://doi.org/10.1016/j.procs.2021.12.302>
- CIS. (2021). *CIS Critical Security Controls Version 8*.
- Dirk Knop. (2022). *US-Cybersicherheitsbehörde warnt vor Angriffen unter anderem auf Veeam*. <https://www.heise.de/news/US-Behoerde-CISA-warnt-vor-Angriffen-etwa-auf-Veeam-7394722.html>
- Dirk Knop. (2022). *Webbrowser: Chrome-Update dichtet acht Sicherheitslecks ab*. <https://www.heise.de/news/Webbrowser-Chrome-Update-dichtet-acht-Sicherheitslecks-ab-7394554.html#:~:text=Neue%20Versionen%20des%20Webrowsers%20Chrome,keine%20weiteren%20Informationen%20dazu%20liefern.>
- Dirk Knop. (2022). *Codeschmuggel möglich: Microsoft stuft Sicherheitslücke auf „kritisch“ herauf*. <https://www.heise.de/news/Codeschmuggel-moeglich-Microsoft-stuft-Sicherheitsluecke-auf-kritisch-herauf-7396879.html#:~:text=auf%20%22kritisch%22%20herauf-,Codeschmuggel%20m%C3%B6glich%3A%20Microsoft%20stuft%20Sicherheitsl%C3%BCke%20auf%20%22kritisch%22%20herauf,Angreifen%20ohne%20Anmeldung%2C%20Schadcode%20einzuschleusen.>
- Dowland, P., & Furnell, S. (2009). *Advances in communications, computing, networks and security. Volume 6, Proceedings of the MSc/MRes programmes from the School of Computing, Communications and Electronics, 2007-2008*. School of Computing, Communications & Electronics, University of Plymouth.
- Europäische Kommission. (2022). *Datenverarbeitung*. https://commission.europa.eu/law/law-topic/data-protection/reform/what-constitutes-data-processing_de
- Fatima Salahdine, Naima Kaabouch. (2019). *Social Engineering Attacks: A Survey*.
- Fox, D. (2009). *Sicheres Löschen von Daten auf Festplatten*. 4.
- Helisch, M., & Beyer, M. (Hrsg.). (2010a). *Security awareness: Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung* (korr. Nachdruck). Vieweg + Teubner.

- Helisch, M., & Beyer, M. (Hrsg.). (2010b). *Security awareness: Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung* (korr. Nachdruck). Vieweg + Teubner.
- Idrus, S. Z. S., Cherrier, E., Rosenberger, C., & Schwartzmann, J.-J. (2013). *A Review on Authentication Methods*. 14.
- Ivaturi, K., & Janczewski, L. (2011). A Taxonomy for Social Engineering attacks. *2011*, 12.
- Janina Raeder. (2021). *Passwortsicherheit—Warum wir mehr darauf achten sollten*. <https://www.hs-fresenius.de/blog/wissen/passwortsicherheit-warum-wir-mehr-darauf-achten-sollten/#:~:text=%E2%80%9EEin%20Passwort%20ist%20wie%20ein,werden%E2%80%9C%2C%20veranschaulicht%20Dirk%20Labudde>.
- Jawandhiya, P. M., Ghonge, M., Ali, M. S., & Deshpande, J. S. (2010). A Survey of Mobile Ad Hoc Network Attacks. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3451027>
- Kaspersky. (2022). *Computervirus*. <https://www.kaspersky.de/resource-center/threats/how-to-get-rid-of-a-computer-virus>
- Koyun, A., & Janabi, E. A. (2017). *Social Engineering Attacks*. 4(6), 6.
- L. Xiangyu, L. Qiuyang, S. Chandel. (2017). *Social Engineering and Insider Threats*.
- Leah Zhang-Kennedy, Sonia Chiasson, Paul van Oorschot. (2016). *Proceedings of the 2016 APWG Symposium on Electronic Crime Research (eCrime) ; Jun 1-3, 2016, Toronto, Ontario, Canada*. IEEE.
- NCSC. (2020). *Merkblatt Informationssicherheit für KMUs*.
- NCSC. (2022). Mobil unterwegs -Ihre Aufmerksamkeit ist gefordert. 07.12.2022. https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/bundesinterne-kampagnen/mobil_unterwegs.html
- Nimrod Iny. (2022). *Sensitive Data Exposure*. <https://www.polar.security/post/sensitive-data-exposure>
- Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-Factor Authentication: A Survey. *Cryptography*, 2(1), 1. <https://doi.org/10.3390/cryptography2010001>
- Scarfone, K., & Souppaya, M. (2009). *Guide to Enterprise Password Management (DRAFT)*. 38.
- Speicherbibliothek. (2022). *Speicherbibliothek*.
- State of The Phish 2022*. (2022). 60.
- Wash, R., & Rader, E. (2021). Prioritizing security over usability: Strategies for how people choose passwords. *Journal of Cybersecurity*, 7(1), tyab012. <https://doi.org/10.1093/cybsec/tyab012>
- Wirtschaftskammer Österreich, B. I. und C. (2017). *Clear Desk / Clear Screen-Policy*. <https://www.onlinesicherheit.gv.at/Themen/Experteninformation/Sicherheitsmanagement/Personelle-Massnahmen/Clear-Desk-und-Clear-Screen-Policy.html>