veb.ch

HWZ
Die Hochschule für Wirtschaft in Zürich

Cyber Security Awareness

Cyber Security Awareness –

Wie der Faktor Mensch bei Cybersicherheit trotz Hightech die wichtigste Rolle spielt

Ralph Hutter
Eidg. dipl. Inf., EMBA, Studiengangsleiter HWZ, CAS Cyber Risk & Security

Kai Dorner
MAS Digital Business

Abstract

Dieses Whitepaper liefert einen Überblick über

- die allgemeine Lage der Informationssicherheit
- die häufigsten Angriffsarten und die Anatomie eines Hacks am Beispiel eines CEO-Fraud-Angriffs
- ein Modell für kontinuierliche Mitarbeitendenschulung
- eine Checkliste mit Empfehlungen, wie man sich und sein Unternehmen mittels Sensibilisierung schützen kann

Keywords: Cyber Security, Awareness Training

Inhaltsverzeichnis

1 Vorwort

Sehr geehrte Damen und Herren

Besitzen Sie ein Smartphone? Haben Sie sich eine stabile Hülle und sogar Panzerglas für den Bildschirm gekauft, um es zu schützen? Bleibt Ihnen trotz aller Vorkehrungen jedes Mal das Herz für eine Millisekunde stehen, wenn es Ihnen aus den Händen rutscht? Ja?

Dann verstehen Sie sicher, was ich hier auszudrücken versuche: Der Anblick meines Mobiltelefons vermittelt mir ambivalente Gefühle. Sicherheit und Fragilität zugleich. Einerseits der Schutz auf Vorder- und Hinterseite zur Sicherung, andererseits das Wissen, dass mein Telefon nur ungeschickt auf den Boden prallen muss, um komplett beschädigt zu sein.

Ähnlich verhält es sich mit der Cyber Security: Ein professioneller Schutz gegen alle denkbaren Risiken vermittelt zwar Sicherheit. Trotzdem bleibt die Gefahr eines «Blind Spot», wie z.B. einer bislang unbekannten Sicherheitslücke. Grund genug, um das Thema Informationssicherheit in den Fokus dieses Whitepapers zu rücken. Auch die Umfrage Digital Switzerland (2019), welche in Kooperation zwischen der HWZ und veb.ch – dem Schweizer Verband für Rechnungslegung und Controlling – entstanden ist, hat ein fehlendes Bewusstsein für diese Thematik sichtbar gemacht. Aus diesem Grund hat das Institute for Digital Business zusammen mit veb.ch dieses Whitepaper entwickelt. Eine starke Partnerschaft, dank welcher die folgenden wichtigen Seiten entstehen konnten. Herzlichen Dank für die erfolgreiche Zusammenarbeit.

Sie, die Leserinnen und Leser, jedoch nur auf die Dringlichkeit der Thematik Cyber Security aufmerksam zu machen und dann im Regen stehen zu lassen, ist nicht unser Stil. Das Pünktchen auf dem i und Zückerli im Kafi dieses Projektes befindet sich am Ende dieses Werkes: die Cyber-Security-Awareness-Checkliste. Sie schafft Klarheit über den vorhandenen Grad an Sensibilisierung in Ihrem Unternehmen.

Der Mensch ist nach wie vor das schwächste Glied in der Kette der Cybersicherheit. Damit wird Cyber Security Awareness zum Pflichtprogramm für Unternehmen. Sie vermindert u.a. Risiken von Datenlecks, Phishing- und Social-Engineering-Attacken und noch viel wichtiger: Sie etabliert eine Kultur, in der Verdachtsmomente, Probleme und versehentlich angeklickte E-Mails aktiv adressiert werden dürfen – ohne Angst vor Sanktionen. Cyber Security geht alle etwas an. Die gesamte Belegschaft. So auch Sie. Cyber Security ist Chefsache.

Manuel P. Nappo
Leiter Institute for Digital Business

Sehr geehrte Damen und Herren

Spätestens seit vor mehr als zehn Jahren Smartphones Einzug in unseren Alltag gefunden haben, ist Digitalisierung ein verbreitetes Schlagwort. Eigentlich startete die Digitalisierung aber schon viel früher: Gerade im Rechnungswesen führte die EDV (elektronische Datenverarbeitung) bereits in den 80er-Jahren zu einer Revolution. Heute ist die Rede von IT (Informationstechnologie), deren Daten als das neue Gold oder Öl gelten.

Entsprechend entstand rund um diese Daten ein grosses Geschäft und die Cyberkriminalität wurde zu einem Milliarden-Business, welches nach neusten Studienergebnissen von McAfee weltweit jährlich 600 Milliarden Dollar umsetzt. Der Umfang dieser Kriminalität betrifft heute praktisch jede Lebenslage und entsprechend kann jede Firma und jede private Person plötzlich davon betroffen sein.

Aufgrund der Entwicklungsgeschichte der EDV ist die IT heute oft dem CFO angegliedert. Das macht auch durchaus Sinn, schliesslich trägt er die Verantwortung für alle Daten und die damit verbundenen Prozesse. Wichtig ist, dass sich ein CFO den Gefahren von Cyber Crime bewusst ist, sich vertieft mit diesen Themen auseinandersetzt und aktiv die Beteiligten sensibilisiert.

Mit diesem Booklet nimmt auch veb.ch seine Verantwortung wahr und möchte seine Mitglieder und Interessierte auf dieses Thema aufmerksam machen. Nur wer sich der Umstände und Entwicklungen bewusst ist, kann rechtzeitig die notwendigen Massnahmen ergreifen.

Herzlich

Peter Herger
Vorstandsmitglied veb.ch

1 Einleitung

Unternehmen investieren jedes Jahr Millionen in Firewalls, Back-Up-Systeme und Verschlüsselungstechnologien, aber viel weniger in die Mitarbeitenden und die innerbetriebliche Prävention und Kommunikation, dies obwohl eine Vielzahl an Cyberangriffen aktiv über Social-Engineering- und Phishing-Attacken über Mitarbeitende initialisiert werden.

Fakt ist, die Gefährdungen nehmen laufend zu. Cyberkriminalität ist zu einem Geschäftsmodell geworden, und es wird laufend professionalisiert. Dazu kommen neue Rechtsvorschriften, aufgrund deren Unternehmen Datenschutzverletzungen aktiv an die Behörden rapportieren müssen. Ein neues Risiko auf dem Radar, welches mit hohen Bussgeldern verbunden ist, ganz zu schweigen vom möglichen Reputationsverlust.

Eine besondere Rolle fällt dem Social Engineering zu. Social Engineering ist nach wie vor der Motor oder besser der Anlasser vieler Cyberangriffe [2]. Eine Mehrheit gezielter Angriffe beginnt zuerst mit Aufklärung, dem Auskundschaften der potenziellen Opfer via öffentliche Informationsquellen. Kriminelle nutzen Social Engineering, um beispielsweise an persönliche Daten zu gelangen, Zugangsinformationen zu erhalten, Identitäten zu stehlen oder auch Zahlungen einzuleiten.

Paradox: In der hoch technisierten Welt sind die Menschen das schwächste Glied in der Kette. Und dies gleich mehrfach. Über Social Engineering sind einerseits Informationen im Internet oder über Telefonanrufe in Erfahrung zu bringen und andererseits erfordert Phishing am Ende noch immer das manuelle Zutun eines Benutzers: ein Klick auf einen Link, Username und Passwort in eine gefälschte Login-Seite eingegeben oder eine Datei versehentlich aus einem E-Mail-Anhang geöffnet. Oft wird auch ausgeblendet, dass Gefahren nicht nur von Externen ausgehen, sondern auch von Internen. Oft assoziieren Menschen den Begriff «Insider-Bedrohungen» in der Cybersicherheit mit bösartig motivierten Mitarbeitenden, die beabsichtigen, dem Unter-

nehmen direkt zu schaden. Der Insider Threat Report 2018 [3] kommt zum Schluss, dass in Wahrheit Mitarbeitende oder Lieferanten unbeabsichtigt eine gleich hohe Anzahl von Sicherheitsverletzungen durch reine Fahrlässigkeit verursachen.

Ein Cyber-Security-Awareness-Programm ist der einzig vergleichsweise wirksame Schutz vor Social Engineering, für eine dauerhafte Veränderung des Verhaltens und die Basis für eine Unternehmenskultur, in welcher schnelles Melden von Sicherheitsvorfällen gefördert und nicht etwa sanktioniert wird.

2 Cyber Crime als Geschäftsmodell

Cyberkriminalität ist ein internationales Phänomen, es macht nicht an der Landesgrenze halt. In der jungen Vergangenheit finden zunehmend Berichte über Cyberangriffe auf Schweizer Unternehmen den Weg in die Medien; dies ist nur die Spitze des Eisbergs. Der Halbjahresbericht 2019/2 der Melde- und Analysestelle Informationssicherung (MELANI), neu Nationales Zentrum für Cybersicherheit (NCSC), beschreibt die verschiedenen Angriffsvektoren und vor allem die eindrückliche Breite der verschiedenen Cyberangriffe.

Cyberspionage – das Sammeln von Informationen und Diebstahl von geistigem Eigentum – ist an der Tagesordnung wie z.B. Angriffe auf Sport- und Anti-Doping-Organisationen [3].

Aber auch Angriffe auf industrielle Kontrollsysteme, Angriffe zur Beeinträchtigung eines Dienstes (DDoS-Attacken), Social Engineering und Phishing oder auch erfolgreiche Datenabflüsse von Patienten- oder Unternehmensdaten sind traurige Realität weltweit – eben auch in der Schweiz. Eine Studie der Universität Bern zeigt das wahre Ausmass: Bis zu einem Drittel der Schweizer Unternehmen wurde schon mindestens einmal Opfer von Wirtschaftsspionage.

Das Bundesamt für Polizei (Fedpol) listet Phishing, Hacking und Malware als die drei häufigsten Angriffsarten 2018 in der Schweiz [4]. Europol kommt im IOCTA (Internet Organised Crime Threat Assessment) Report [2] zu denselben Schlüssen. Ransomware bleibt die grösste Malware-Bedrohung. Insbesondere wird erwartet, dass Cryptomining-Malware zu einer regelmässigen, risikoarmen Einnahmequelle für Cyberkriminelle wird.

In den vergangenen Wochen und Monaten wurden zahlreiche Schweizer Unternehmen und Universitäten Ziel von Cyberattacken.

Der Thurgauer Schienenfahrzeughersteller Stadler Rail wurde Opfer eines Erpressungsversuchs mittels Ransomware. Auch die Industriegruppe Metall Zug hat bekannt gegeben, dass sie Opfer einer Cyberattacke geworden sei. Omya, ein international tätiger Schweizer Hersteller von Industriemineralien, musste den Betrieb in allen Werken nach Cyberattacken einstellen, und die ETH registrierte Angriffe auf ihre Hochleistungsrechner Euler und Leonhard.

Cyberkriminalität ist zu einem lukrativen, internationalen Geschäftsmodell geworden. Der folgende Abschnitt gibt Einblicke in den Aufbau eines Angriffs, um das Vorgehen und die Motivation der Angreifer besser verständlich zu machen.

3 Angriffsarten und die Anatomie eines Hacks

Es gibt zahlreiche Varianten, mit denen Angreifer versuchen, an die wertvollen Vermögenswerte ihrer Opfer zu gelangen, um diese zu stehlen, zu kopieren, zu verschlüsseln oder zu zerstören. Dies kann abhängig vom Unternehmen u.a. sensible Informationen (Kunden-, Finanz-, Personaldaten), Systeme, Prozesse, monetäre Güter, aber auch das Image betreffen. Nun sollte man meinen, dass die neutrale Schweiz nichts Schlimmeres zu befürchten hat, denn schliesslich enthält sie sich jeglicher Konflikte und Kriege. Sie scheint also auf internationaler Bühne nicht sonderlich exponiert zu sein.

Dies mag auf den ersten Blick wohl stimmen, bei genauerem Hinsehen fällt aber auf, dass sowohl international agierende Unternehmen, Hilfsorganisationen, NGOs als auch namhafte Sportvereine in der Schweiz angesiedelt sind. Darüber hinaus nennen fast 8,5 Millionen Menschen die Schweiz ihre Heimat [4] und machen sie 2018 erneut zum vermögendsten Land der Welt. Glaubt man dem Global Wealth Report von Credit Suisse, so besitzt jeder Erwachsene in der Schweiz ein durchschnittliches Vermögen von USD 530’240 [5]. Die Kombination des Anteils der Internetnutzung der Schweizer Bevölkerung, welcher mit 91% deutlich über dem europäischen Durchschnitt liegt (81%), mit dem geringen Umsetzungsanteil von Mitarbeitendentrainings im Bereich der IT von nur 36% [6], macht die Schweiz zu einem lohnenden Ziel für Internetkriminelle.

Data is no longer just an IT asset; it's a core strategic asset, and some types of data are more valuable than others. Confidential business information, which encompasses company financials along with customer and employee data, is a highly strategic asset and equally a high-value target. Again this year, confidential business information (57%) takes the top spot as most vulnerable to insider attacks, followed by privileged account information (52%), and sensitive personal information (49%). *[insiderthreatreport]*

4 CEO Fraud

CEO Fraud ist in der Schweiz angekommen

Der CEO Fraud, oder auch unter dem Namen Business E-Mail Compromise (BEC) bekannt, ist eine international verbreitete Betrugsmasche mit einem sehr hohen Verlustpotenzial für jegliche Unternehmen. Unter Vortäuschen falscher Tatsachen versuchen die Betrüger mittels gefälschter E-Mail, im Namen des Firmenchefs (CEO), des Finanzvorstands (CFO) oder anderer Führungsmitglieder Zahlungsaufträge an einen meist im Ausland ansässigen Dritten zu überweisen. Die Betrugsmasche erstreckt sich dabei nicht auf bestimmte Länder, Branchen oder Unternehmensgrössen – jedes Unternehmen kann beim CEO Fraud zum potenziellen Ziel werden. Jedoch scheinen grössere Unternehmen aufgrund ihrer Komplexität sowie ihrer höheren Finanzmittel exponierter zu sein, hingegen sind KMUs mit ihren nicht sehr strikten Prozessabläufen im Umgang mit Finanzmitteln leichter verwundbar. Aufgrund der zunehmenden Bekanntheit des CEO Fraud werden mittlerweile die gefakten E-Mails der Führungspersonen nicht nur für finanzielle Aspekte eingesetzt. Je nach Ziel können ganz unterschiedliche Organisationseinheiten innerhalb des Unternehmens von den Betrügern direkt kontaktiert werden. So kann bspw. das Rechnungswesen und Treasury (Finanz-)Transaktionen ausführen, die Personalabteilung sensible Mitarbeitendendaten weiterleiten, die Forschungs- und Entwicklungsabteilung geistiges Eigentum bekannt geben, das Lager und der Versand Dispositionen abändern und das Vorstandssekretariat und Compliance vertrauliche Unternehmensdaten (z.B. GL/VR-Protokolle oder Verträge) weiterleiten.

Durchschnittlicher Verlust liegt bei USD 159'469

Mit dieser Betrugsmasche konnten bereits weltweit Milliarden an Franken von gutgläubigen Unternehmen erbeutet werden. So beziffert die zentrale Sicherheitsbehörde der USA, das Federal Bureau of Investigation (FBI), den weltweiten Verlust durch CEO Fraud zwischen Oktober 2013 und Mai 2018 auf 12,5 Mrd. USD [7]. Aufgrund

der zu befürchtenden Reputationsschäden dürfte die Dunkelziffer der nicht angezeigten CEO Frauds noch viel höher liegen.

Die Cyber Kill Chain eines CEO Fraud

Um das zuvor spezifisch ausgewählte Unternehmen zu täuschen, gehen die Betrüger in der Regel wie folgt vor:

Schritt 1 – Auskundschaftung

Durch eine gezielte Recherche im Internet werden Informationen über das Zielunternehmen zusammengetragen. Sie bildet die Basis für das weitere Vorgehen. Neben den allgemeinen Unternehmensinformationen (u.a. Branche, Servicedienstleistungen/Produkte, Tochterfirmen/Filialen, Kunden etc.) werden vorwiegend spezifische Informationen (u.a. Kontaktdaten [Namen, E-Mail-Adressen und Berufsbezeichnung] der einzelnen Führungskräfte, Organigramm etc.) gesammelt. Hierbei kommen insbesondere frei zugängliche Quellen zum Einsatz. Um die Suche nach Informationen zu vereinfachen, werden des Öfteren von den Betrügern sogenannte Web Crawler eingesetzt, welche die Suche und das Sammeln von Daten automatisch durchführen.

Definition Angriffsvektor

Der **Angriffsvektor** (engl. attack vector) bezeichnet einen möglichen Angriffsweg und die Angriffstechnik, die ein unbefugter Eindringling, ganz gleich welcher Art, nehmen kann, um ein fremdes Computersystem zu kompromittieren, das heisst unbefugt einzudringen und es danach entweder zu übernehmen oder zumindest für eigene Zwecke zu missbrauchen.

Während man diese öffentlich einsehbaren Informationen seitens Unternehmen relativ einfach einschränken und, um verdächtige Suchaktivitäten aufzudecken, die Zugriffe auf Webseiten sowie

Server auswerten kann, gibt es darüber hinaus nicht öffentliche Informationen, welche naturgemäss für den Angreifer interessanter erscheinen. Um diese Informationen wie bspw. über Unternehmensprozesse, IT-Systeme, aber auch Informationen wie z.B. die (Ferien-)Abwesenheit des CEO oder dessen persönliche E-Mail-Adresse/Durchwahlnummer zu erfahren, nutzt der Angreifer eine spezielle Schwachstelle im Unternehmen aus, und zwar uns Mitarbeitende. Indem er unter falschem Vorwand (bspw. als Kunde, Servicetechniker oder IT-Provider) anruft, erfährt er aufgrund unserer Gutgläubigkeit meistens mehr, als er erfahren sollte.

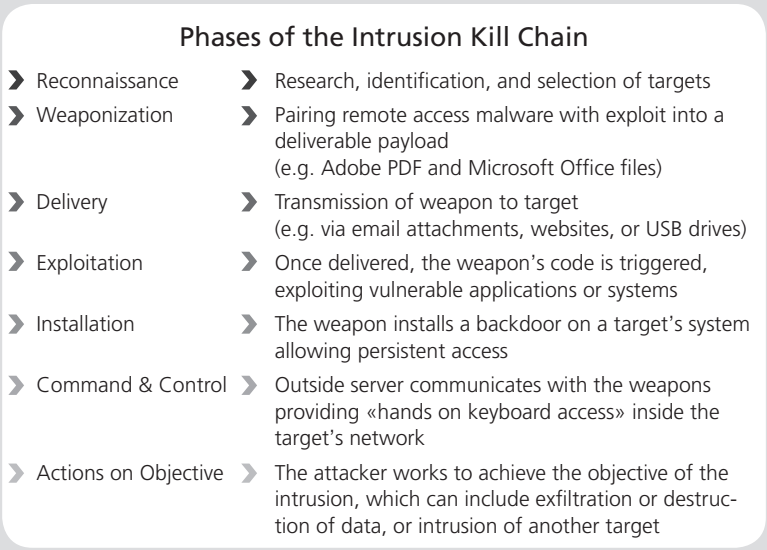

Abbildung 1: Cyber Kill Chain. Eigene Darstellung in Anlehnung an U.S. Senate Committee on Commerce, Science, and Transportation (2014)

Schritt 2 – Bewaffnung

Bei der Bewaffnung geht es um die Auswahl der passenden Angriffsroute und des geeigneten Werkzeugs. In der Regel kommt beim CEO Fraud eine auf den Mitarbeitenden angepasste Phishing-E-Mail zum Einsatz, da es die günstigste, risikoärmste und zugleich die erfolgversprechendste Form des Angriffs ist.

Um die Erfolgschancen zu erhöhen, sind der Inhalt und die Struktur der E-Mail von grösster Bedeutung. Ein wesentliches Element hierbei ist bspw. der suggerierte Zeitdruck, welcher negative Effekte auf die Leistung und die Entscheidungsfähigkeit von Mitarbeitenden hat. Auch der Absender der E-Mail spielt eine entscheidende Rolle. Führungspersonen spiegeln eine gewisse Autorität wider, was in der E-Mail fingiert wird. Feinheiten wie den richtigen Zeitpunkt abwarten (Abwesenheit des CEO) und ein plausibler Überweisungsgrund (z.B. Steuerzahlung, Firmenübernahme, Liquiditätsausgleich für eine Tochtergesellschaft) runden die Betrugsmasche erst richtig ab. Alle noch so guten Social-Engineering-Tricks funktionieren nur, wenn die Betrüger sich im Vorfeld über die Finanzkompetenzen zur Zahlungsfreigabe richtig informiert haben. So wählen sie im besten Fall eine Überweisungshöhe, welche unterhalb einer möglichen 4-Augen-Kontrolle liegt, sodass die Überweisung durch die alleinige Genehmigung des CEO ausgeführt werden kann.

Schritt 3 – Zustellung

Das ausgewählte Angriffswerkzeug, die Phishing-Nachricht, muss auf geeignete Weise an sein Ziel gelangen. In der Regel wird dabei auf die E-Mail als Transportmittel zurückgegriffen. Handelt es sich hierbei um keinen Massenversand von E-Mails, kann eine einzelne Nachricht nur sehr schwer als Phishing-E-Mail von der unternehmenseigenen Firewall identifiziert werden, und wird somit dem Empfänger zugestellt.

Schritt 4 – Aufspüren von Sicherheitslücken

Im Gegensatz zu anderen Cyberrisiken wird beim CEO Fraud klassischerweise der Mensch als wesentliche Sicherheitslücke angesehen und nicht das System. Es ist der Mitarbeitende, der am Ende die schädliche Handlung unwissentlich selbst ausführt bzw. in Auftrag gibt.

Schritt 5 – Installation

Wenn der Angreifer sich nicht blind auf die Mithilfe des Mitarbeitenden verlassen möchte, so sendet er in der Phishing-E-Mail eine Schadsoftware (Malware) mit, welche auf dem Zielsystem versteckt installiert und im späteren Zeitverlauf ausgeführt wird. Die Malware wird in Form einer Datei der E-Mail angehängt, dabei sind fast die Hälfte (45%) aller Malware-Anhänge Office-Dateien [8].

Schritt 6 – Steuerung und Kontrolle

Die zuvor installierte Schadsoftware ermöglicht es dem Angreifer, unter Umgehung der normalen Zugriffssicherung, per Fernsteuerung (Remote) Zugang zum Computer zu erlangen, um selbst die Zahlung auslösen zu können. Damit die Überweisung überhaupt getätigt werden kann, benötigt es neben den vorherigen Schritten vor allem eins: ein reales Empfängerkonto. Und genau dort kommt eine weitere Betrugsmasche ins Spiel. So muss der Angreifer nicht nur sein Opfer dazu bringen, ihm Geld zu überweisen, sondern er benötigt auch noch ein Bankkonto, welches nicht mit ihm in Beziehung gebracht werden kann. Wäre ja ansonsten ganz schön blöd, das zuvor aufwendig ergaunerte Geld an sich selbst zu überweisen und es damit den Ermittlungsbehörden ziemlich einfach zu machen. Da sich jedoch jede natürliche Person für eine Kontoeröffnung zweifelsfrei legitimieren muss, setzt der Angreifer einen oder mehrere Mittelsmänner, auch Money Mules genannt, als Geldwäscher ein. Die meist unwissenden Personen, welche im Vorfeld durch vermeintlich lukrative Jobangebote (hohes Gehalt bei geringem Arbeitsaufwand) geködert wurden, transferieren die illegalen Gelder sofort weiter. Meistens wird die Gesamtsumme in mehrere Beträge aufgeteilt und über Ländergrenzen hinweg weiterüberwiesen. Dies erschwert die Nachverfolgung seitens Vollzugsbehörden. Dass sich die Kontoinhaber dabei strafbar machen, ist ihnen des Öfteren gar nicht bewusst.

Schritt 7 – Durchführung

Der effektive Betrug findet statt. Die gefälschte E-Mail im Namen des CEO zur Ausführung einer hohen Zahlung wird ausgelöst. Dabei wird meistens der späte Nachmittag/Abend (optimal am Freitag vor dem Wochenende) gewählt, wenn nur noch wenige beim Arbeiten sind und die Chance auf mögliche Rückfragen bei Arbeitskollegen sinkt.

Informationen	**Quelle**
Standort	
Unternehmensstandort (Adresse)	Unternehmenshomepage (Impressum), Handelsregister
Gebäudeinfrastruktur (Nachbarn, Mieter, Vermieter)	Vor-Ort-Besichtigung, Suchmaschinen
Zutrittsmöglichkeiten (Haupt-, Neben-, Lieferanteneingang, Fenster, Tiefgarage)	Google Bilder, Google Maps, Google Street View, vor-Ort-Besichtigung
Zutrittsbeschränkungen, z.B. Kundenempfang, Vereinzelungsanlage (Personenschleuse), elektronisches Türschloss (Code, Badge, Schlüssel), Objektbewachung (Security), Alarmanlage, Überwachungskamera	Vor-Ort-Besichtigung
Unternehmensstruktur	
Branche Servicedienstleistungen/Produkte	Unternehmenshomepage, Handelsregister, Suchmaschinen
Organigramm (Vorstand, Führungskräfte, Mitarbeitende)	Unternehmenshomepage, Geschäftsbericht, alternativ über soziale Netzwerke (u.a. LinkedIn, Xing) herleiten
Kontakte (Namen, Positionen, E-Mail-Adressen, Hobbys und Interessen) Lieferanten	Unternehmenshomepage, soziale Netzwerke (u.a. LinkedIn, Xing, Facebook, Twitter) Suchmachinen

Abbildung 2: Beispiel-Checkliste zur Auskundschaftung.
Quelle: eigene Darstellung

5 Ransomware

Mit welcher Methode versuchen Kriminelle zulasten eines Dritten, unter Umständen sogar durch Gewaltandrohung, sich zu bereichern? Richtig, es handelt sich hierbei um Erpressung.

Was die meisten glücklicherweise nur aus Fernsehfilmen kennen, gibt es auch in der virtuellen Welt, und das nicht zu knapp. So wird geschätzt, dass es 2019 alle 14 Sekunden ein neues Opfer gab [9] [1]. Als Schadprogramm, auch Ransomware genannt, gelangt die Erpressungssoftware über diverse Kanäle (siehe Box «Mögliche Angriffsvektoren») auf den Computer und sperrt diesen oder verschlüsselt die darauf befindlichen Daten. Im Anschluss daran fordern die Täter von ihren Opfern eine gewisse Geldsumme, überwiegend in der Zahlungseinheit Bitcoin oder in Form von Guthaben- und Bezahlkarten, und versprechen, nach Eingang der Zahlung den Computer und die Daten wieder freizugeben. Der Schaden durch Ransomware wird 2019 auf 11,5 Milliarden USD geschätzt [9] [2].

Mögliche Angriffsvektoren im Schritt Durchführung

Spear Phishing / Whaling Im Gegensatz zum klassischen Phishing, bei dem willkürlich eine Vielzahl an Personen die gefakte Nachricht erhalten, geht es hierbei um einen gezielten Angriff. So wird beim Spear Phishing eine bestimmte Person oder Organisation ausgewählt und mittels individualisierter E-Mail attackiert. Hingegen sind beim Whaling nur Führungskräfte und die Geschäftsleitung (Top-Level Management) das Ziel. Auch sie erhalten in der Regel eine auf sie abgestimmte E-Mail.

Vishing setzt sich aus dem englischen Wort «Voice» (dt.: Stimme) und dem Kunstwort «Phishing» (siehe Erklärung unten) zusammen. Vishing bezeichnet Angriffe, die via Telefon stattfinden. Dabei kann es entweder zu automatisierten Telefonanrufen bspw. mittels Voice over IP (VoIP) kommen oder der Angreifer

sendet vorab eine Nachricht mit der Aufforderung, eine bestimmte Telefonnummer anzurufen. Das Ziel ist dasselbe wie beim Phishing: mittels ausgedachter Geschichten vertrauliche Informationen zu erfahren.

Pretexting ist die Nachahmung einer natürlichen Person durch einen Dritten. Unter Vorwand bzw. Missbrauch von (persönlichen) Daten gibt sich der Betrüger als jemand anderes aus, um sich in dessen Namen (Identitätsdiebstahl) missbräuchlich Zugang zu einer anderen Person, Informationen, Unternehmen oder IT-Systemen zu verschaffen.

Moralisches Dilemma: zahlen oder nicht zahlen?

Im Fall der amerikanischen Stadt Baltimore, bei der am 7. Mai 2019 Tausende von Computern durch eine Ransomware-Attacke verschlüsselt worden waren, entschied sich die Stadtverwaltung, die Lösegeldzahlung von 13 Bitcoin, was einem damaligen Gegenwert von ca. CHF 76’811 entsprach, nicht zu bezahlen [10][3].

Stattdessen setzte sie ihre gesamte Netzwerkinfrastruktur neu auf. Die Wiederherstellung wird dabei auf mehr als CHF 18’000’000 geschätzt [11][4]. Wäre es also nicht besser gewesen, der Erpressung nachzukommen und zu zahlen?

94% der Schadprogramme werden per E-Mail versandt [8][5]

Ähnlich erging es am 29. Mai 2019 der Stadt Riviera Beach in Florida. Auch sie wurde Opfer einer Ransomware-Attacke. Nachdem ein Mitarbeiter auf den Link in einer E-Mail klickte, wurde Malware auf den Computer geladen und diese verschlüsselte anschliessend das gesamte Netzwerk mitsamt den dort gespeicherten Daten. Im Gegensatz zum vorherigen Beispiel entschied sich diese Stadt zu zahlen, und zwar 65

Bitcoin, was in der Gesamtsumme etwa CHF 605'570 entsprach [12] [6]. Abgesehen vom moralischen Dilemma, ob man einer kriminellen Handlung klein beigeben soll, stellt sich vielmehr die Frage, ob man anonymen Erpressern überhaupt trauen kann? Erstaunlicherweise scheint dies tatsächlich der Fall zu sein. So erhielten stolze 93% der Betroffenen nach Bezahlung des Lösegelds ein Tool bzw. einen Schlüssel zum Wiederherstellen der Daten [13] [7]. Was aber, wenn nicht alle Daten wiederhergestellt werden, da im Schnitt 14% trotz Entschlüsselungstool verloren gehen [13] [8], oder was, wenn man sogar zu denjenigen gehört, die zahlen, aber keine Software erhalten? Und was, wenn der Erpressungsfall an die Medien gelangt? Können Sie dann noch zweifelsfrei sicher sein, dass Sie mit der tatsächlichen Person kommunizieren, die hinter der Erpressung steckt, oder eventuell nur mit einem Trittbrettfahrer? Wie würden Sie bei einer Ransomware-Attacke handeln?

Mögliche Angriffsvektoren

Baiting, auch Ködern genannt, zielt auf die Neugierde der Opfer ab. Dies geschieht insbesondere durch das absichtliche Liegenlassen eines präparierten USB-Sticks oder einer Speicherkarte. Auch Gewinnspiele, bei denen man ein Handy oder Laptop gewinnen kann, welche zuvor gezielt mit Schadsoftware infiziert wurden, dienen als lukrative Köder. Ziel ist wie beim Phishing, an vertrauliche Informationen zu gelangen oder sogar Sicherheitsfunktionen auszuschalten.

Phishing ist ein Kunstwort und setzt sich aus den englischen Wörtern «Password» (dt.: Kennwort), «Harvesting» (dt.: Ernte) und «Fishing» (dt.: Angeln) zusammen. Phishing bezeichnet Angriffe, bei denen versucht wird, Zugangsdaten (z.B. Benutzernamen und Passwörter für E-Mail-Konten, E-Banking, eBay, PayPal etc.), Kreditkartendaten oder andere vertrauliche Informationen (z.B. Personaldaten, Geheimnisse) von ahnungslosen Benutzern zu erfahren oder Malware auf dem Gerät zu installieren. Mittels

raffiniert formulierter Nachrichten per E-Mail, Instant-Messaging-Dienst (u.a. ICQ, WhatsApp, Skype), Social Media (u.a. Facebook, LinkedIn) oder SMS, letzteres auch «Smishing» genannt, wird die Ausübung einer Aktion vom Empfänger verlangt. Meistens soll dabei ein beigefügter Link oder Anhang geöffnet oder eine gefälschte Website besucht werden. Um die Glaubwürdigkeit einer solchen Phishing-Attacke zu unterstreichen, wird der tatsächliche Absender verschleiert («Spoofing»). Stattdessen geben sich die Angreifer als eine vertrauenswürdige Person aus oder ahmen das Corporate Design eines bekannten Unternehmens, einer Behörde oder Organisation in Form von Logo, Schriftart und Layout nach.

Drive-by-Download ist das unbewusste und unbeabsichtigte Herunterladen einer schädlichen Software. Durch das reine Besuchen einer gefakten Website mit einem in der Regel veralteten Browser gelingt die automatische Installation der Erpressungssoftware.

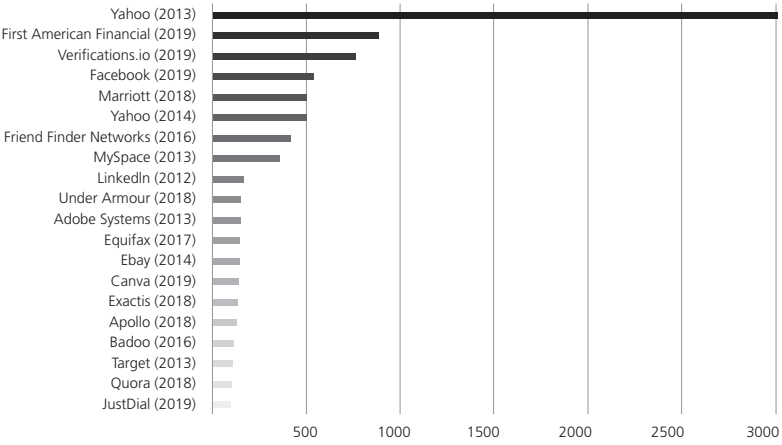

Abbildung 3: Grösste Datenmissbräuche. Quelle: eigene Darstellung

6 Data Breach

«Unbefugte Datenbeschaffung wird mit Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe bestraft» (Art. 143 Abs. 1 StGB)

Egal ob man von Datendiebstahl, Datenmissbrauch oder Datenklau spricht (engl. data breach), gemeint ist immer die unbefugte Beschaffung von sensiblen, vertraulichen oder anderweitig geschützten Daten. Die Ausprägungen können dabei von einzelnen Unternehmensgeheimnissen (z.B. Patente) bis hin zu mehreren Millionen von Kundendaten (z.B. Benutzeranmeldeinformationen) variieren. Die Daten werden zu missbräuchlichen Zwecken kopiert, allerdings nicht, wie der Name es vermuten lässt, gestohlen. Die Verfügbarkeit der Daten ist in der Regel weiterhin gegeben.

2018 wurden 33'000'000'000'000'000'000'000 Bytes an Daten produziert

Infolge der zunehmenden Digitalisierung werden immer mehr Daten produziert. So wird sich die jährliche Menge an neu generierten Daten, gemäss dem Whitepaper «The Digitization of the World», bis 2025 verfünffachen. Aufgrund dieses exponentiellen Zuwachses stellt sich die Frage neben der Sinnhaftigkeit dieser neuen Daten vor allem aber auch nach der Aufbewahrung und Sicherung der schier endlosen Datenmengen. Es ist also nicht verwunderlich, wenn wir in Zukunft mit noch mehr Datenmissbrauchsfällen konfrontiert werden.

Ein Jahr nach Inkrafttreten von GDPR gab es bereits europaweit 89'271 Datenverstösse [14][1]

Auch im Zuge von neuen bzw. angepassten Gesetzgebungsregelungen, wie bspw. dem europäischen GDPR (25. Mai 2018), dem australischen NDB Scheme (22. Februar 2018) oder dem aktuell in der Totalrevision befindlichen Bundesgesetz über den Datenschutz (DSG) der

Schweiz, werden Vorfälle voraussichtlich schneller und in grösserer Anzahl öffentlich, da sie nun einer gesetzlichen Offenlegungspflicht unterstehen.

65% der grössten Datenmissbrauchsfälle fanden erst in den letzten 5 Jahren statt

---

Mögliche Angriffsvektoren

Dumpster Diving oder auch Mülltauchen genannt ist das Suchen nach Schätzen in Abfallcontainern. Meistens geht es hierbei um weggeworfene Lebensmittel aufgrund von abgelaufenem Mindesthaltbarkeitsdatum, Form und Aussehen entsprechen nicht der Norm oder um Überschuss wegen mangelhafter Einkaufsplanung. Das Dumpster Diving kann man aber auch auf die Informationssicherheit anwenden, indem man im Müll nach sensitiven Informationen wie bspw. Kontoauszügen, Krankenakten, E-Mail-Adressen, Kalendereinträgen, Passwörtern etc. sucht. Die gefundenen Informationen können in den falschen Händen sehr wertvoll sein, indem sie für einen späteren Angriff gezielt eingesetzt werden, um bspw. das Vertrauen der Opfer zu gewinnen oder mehr über Unternehmensstruktur und -ablauf zu erfahren.

Shoulder Surfing wird gezielt eingesetzt, um Informationen zu erfahren. Indem man seinem Opfer über die Schulter schaut, wird versucht, bspw. an Zugangsdaten (Benutzername und Passwort) oder andere vertrauliche Informationen zu gelangen.

---

7 Insider Threat

Spricht man von Informationssicherheit, fällt den meisten Personen eine Vielzahl an Risiken ein, jedoch wird nur selten die Insider-Bedrohung als solche genannt. Dies liegt vermutlich daran, dass man Cyberattacken nur schwer visualisieren kann und sie damit nicht wirklich greifbar sind. Es ist also leichter, diese oft virtuellen Risiken einem anonymen Hacker zuzusprechen, als den Arbeitskollegen von gegenüber, mit dem man schon den einen oder anderen Kaffee in der Pause getrunken hat, zu verdächtigen. Allerdings muss man sich im Klaren sein, dass all diejenigen Personen, welche Einblick in das Unternehmen haben, potenzielle Insider-Informationen über Sicherheitspraktiken, Daten und Computersysteme der Organisation weiterleiten können. Das trifft sowohl auf den netten Mitarbeitenden aus der Personalabteilung, von dem man es am wenigsten vermutet hätte, als auch auf die ehemalige Kollegin aus dem Rechnungswesen, das langjährige Geschäftsmitglied, den externen Dienstleister und den namhaften Lieferanten zu. Dabei muss es sich nicht immer um einen bösartigen Insider, welcher bewusst und vorsätzlich dem Unternehmen schadet, handeln. Es gibt auch denjenigen, der versehentlich und auf fahrlässige Weise mit Daten und Informationen umgeht. Insbesondere eine E-Mail mit sensiblen Geschäftsinformationen oder Kundendaten in der Hektik an eine falsche Person versenden, geht schneller als man denkt. Aber egal um welche Art von Insiderbedrohung es sich handelt, es sollten stets alle Kommunikationskanäle und -möglichkeiten wie E-Mail, USB Ports, Instant-Messenger-Dienste (z.B. Skype-Chat, Slack, Thomson Reuters Messenger, Instant Bloomberg) und die Internetnutzung (z.B. Social Media, Chatforen) überwacht und geregelt werden.

> ***Mehr als die Hälfte der Unternehmen (53%) hatte in den vergangenen zwölf Monaten mindestens einen Insider-Vorfall [3][1***

Die Folgen eines Datenabflusses können für das jeweilige Unternehmen neben wirtschaftlichen Folgen, in Form von Umsatzverlusten und aufkommenden Kosten, auch Reputationsverlust oder gar rechtliche Konsequenzen bedeuten. Letzteres kann im Falle der Weitergabe von

personenbezogenen Daten an unberechtigte Dritte eine Datenschutzverletzung bedeuten und somit Sanktionen durch Aufsichtsbehörden oder des Gesetzgebers nach sich ziehen.

Mögliche Angriffsvektoren

Phishing: siehe Ransomware

Pretexting: siehe CEO Fraud

Quid pro quo ist eine auf Gegenleistung beruhende Vereinbarung. Das Opfer erhält etwas vom Angreifer, um in dessen Schuld zu stehen. Diese Schuld wird gemäss dem Sprichwort «Eine Hand wäscht die andere» ausgenützt.

Bestechung ist das illegale Anbieten, Versprechen oder Gewähren einer Leistung im Gegenzug für den Erhalt von Vorteilen (z.B. materielle Geschenke, Geld). Bei der Bestechung handelt es sich offiziell um eine strafbare Handlung (Art. 322 StGB).

8 Cyber-Security-Awareness-Programm

8.1. Einleitung

Während der Schutz durch Cyber-Sicherheitstechnologie objektiv betrachtet werden kann, bleibt der Faktor «Mensch» im Sicherheitssystem eine unberechenbare Komponente. Voraussetzung für einen erfolgreichen Schutz vor Cyberkriminalität ist, neben den technischen Komponenten (IT-Infrastruktur und Applikationen) die Kenntnis der Mitarbeitenden über die potenziellen Risiken auf dem Gebiet des Social Engineering. Die stetigen Veränderungen, aber auch die hohe fachliche Komplexität der Cyber Security fordern gerade im KMU-Bereich alles von den Unternehmen ab, um die Gefährdung richtig einschätzen und die Mitarbeitenden situations- und stufengerecht sensibilisieren zu können. So ist es nicht verwunderlich, dass zahlreiche Studien unabhängig voneinander zum Ergebnis kommen, dass der Mensch auf dem Gebiet der Informationssicherheit ein wesentlicher Risikofaktor ist. Dieses Risiko hat auch die Eidgenössische Finanzmarktaufsicht (FINMA) erkannt und als neuen Grundsatz in ihrem revidierten Rundschreiben 2008/21 «Operationelle Risiken – Banken» aufgenommen.

Mögliche Fehlverhalten seitens Mitarbeitende können zu einem grossen Risikofaktor im Umgang mit Cyberangriffen werden. Diese müssen nicht zwangsläufig unter kriminellem Vorsatz geschehen; meist führen fehlende Fachkenntnisse zu unbeabsichtigten Handlungen. Insbesondere KMU müssen im Zuge der Digitalisierung den Überblick, trotz beschränkter finanzieller und auch menschlicher Ressourcen, behalten. Sie müssen die Risikokultur ihrer Mitarbeitenden schärfen und ihnen mittels Schulungen sowohl ein angemessenes Risikobewusstsein vermitteln als auch die passenden Werkzeuge zur Verfügung stellen. Im Folgenden werden Fallbeispiele aufgezeigt, welche genau diese Risiken im Berufsalltag thematisieren.

Um Mitarbeitende zu sensibilisieren, welche zum Teil beruflich überhaupt nichts mit Informationsschutz am Hut haben, geschweige denn sich für dieses Thema interessieren, bedarf es einiger Tricks. Gerade in Zeiten, wo eine Schlagzeile auf die nächste folgt, wo die Lebenszeit von Nachrichten immer kürzer wird, wo Wissen allgegenwärtig abrufbar ist und man nicht mehr alles im Kopf speichern muss, ist es essenziell wichtig, auf geeigneter Weise Bildung zu vermitteln.

8.2. Lernen. Eine Terminologie

Lernen ist ein kontinuierlicher Prozess und die Bewusstseinsbildung stellt eine wichtige Schutzmassnahme im Bereich der Cybersicherheit dar. Dabei ist es wichtig, die verschiedenen Lernebenen [15][1] «Sensibilisierung», «Schulung» und «Ausbildung» zu kennen und voneinander abzugrenzen, um im späteren Verlauf ein auf den Mitarbeitenden zugeschnittenes Programm entwickeln zu können.

8.2.1. Sensibilisierung

Die erste Lernebene bildet die «Sensibilisierung». Sie lenkt die Aufmerksamkeit auf das ausgewählte Themengebiet der IT-Sicherheit innerhalb des Unternehmens. Das Bewusstsein für Informationssicherheit wird dabei bei allen Mitarbeitenden ohne jegliche IT-Vorkenntnisse im selben Umfang geschaffen, egal ob Management, Spezialisten oder Sachbearbeiter/-innen. Es zielt auf das Verhalten der Mitarbeitenden ab. Um dieses zu verändern, bedarf es einer langfristigen, meist über Jahre hinweg, wirksamen Sensibilisierung.

8.2.2. Schulung

Schulung ist die Vermittlung von wichtigen Fertigkeiten, grundlegendem Wissen und die Erweiterung der Fachkenntnisse. Im Gegensatz zur Sensibilisierung schränkt sich der Kreis der Anwender gemäss ihrem Aufgabengebiet ein.

8.2.3. Ausbildung

Die Ausbildung ist die oberste der drei Lernebenen und vervollständigt diese mit der Vertiefung von Fähigkeiten und Wissen. Spezifische Kenntnisse werden hierbei für die jeweiligen Fachaufgaben vermittelt. Mitarbeitende mit speziellen Rollen müssen weitergehend fachspezifisch geschult werden.

8.3. Modell für kontinuierliche Mitarbeiterschulung

Als wesentliche Grundlage für die Erarbeitung eines Modells für die ganzheitliche und auch kontinuierliche Mitarbeiterschulung wurde die wissenschaftliche Methode des PDSA-Zyklus von Deming (1993) gewählt, welche sich als Grundkonzept des Qualitätsmanagements [16][2] etabliert hat. Der PDSA-Zyklus wurde im Gegensatz zu anderen Modifikationen dieses Zyklus (z.B. PDCA) gewählt, da er den ursprünglichen Gedanken von Deming (1950 aufbauend auf Shewhart 1939) [17][3] hervorhebt, indem es nicht nur um einen Vergleich von Erfolg und Misserfolg geht, sondern vielmehr um einen kontinuierlichen Lernprozess. Die Buchstaben PDSA stehen für die vier Schritte

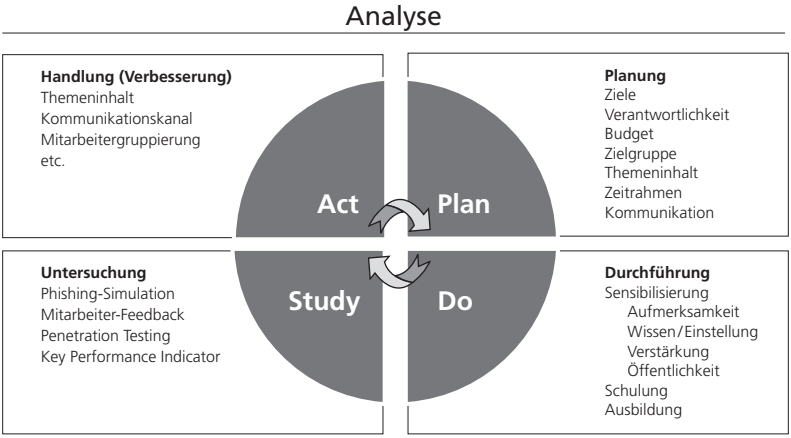

Abbildung 4: Modell für kontinuierliche Mitarbeiterschulung.
Quelle: in Anlehnung an Moen, R., & Norman, C. (2010, S. 27), eigene Darstellung

des Zyklus (Plan, Do, Study, Act) [17][4]. Folgende Schritte werden dabei kontinuierlich durchlaufen:

Am Anfang eines jeden Zyklus steht die sorgfältige Planung. Ausgangspunkt hierfür sind die Anforderungen seitens des jeweiligen Unternehmens, der Mitarbeitenden, der Aufsichtsbehörden (Gesetzgebung), der Kunden usw. Die Ziele sollten dabei klar definiert werden. Die Planung umfasst neben den erforderlichen Ressourcen (u.a. Mitarbeitende, Zeit, Budget), eine eindeutige Zuweisung der Verantwortlichkeiten und Bestimmung der Kommunikationswege, über welche die im Voraus definierten Themeninhalte mit den Mitarbeitenden ausgetauscht werden sollen. Die geplante Vorgehensweise wird über die dreistufige Lernebene («Sensibilisierung», «Schulung» und «Ausbildung») innerhalb der Durchführungsphase umgesetzt. Mittels geeigneter Überprüfung wie bspw. einer Phishing-Simulation und Befragung der Mitarbeitenden lassen sich anschliessend Rückschlüsse und wichtige Erkenntnisse auf die zuvor durchgeführten Massnahmen gewinnen, um daraus zu lernen. In der vierten Phase werden allfällige Verbesserungen geplant, um diese als Eingaben eines weiteren Zyklus einfliessen zu lassen.

Die Schnelllebigkeit und die Masse an Informationen lassen uns an unsere Grenzen stossen

Egal wo wir uns befinden, ob daheim, beim Arbeiten oder unterwegs, ständig werden wir mit neuen Informationen und Reizen überflutet. Es erschwert zunehmend, den Überblick zu behalten, was wirklich von Relevanz ist und was nicht. Wer schon einmal ein gewisses Thema recherchiert hat, der weiss, dass es eine Menge an (Lebens-)Zeit verschlingt, die relevanten Informationen zusammenzutragen, zu analysieren und zu bewerten.

Was also macht eine gute Schulung aus und wie sollte sie unter keinen Umständen sein?

8.4. Top 3 der häufigsten Fehler

8.4.1 Tick-The-Box Übung

Anstatt es als Pflichtveranstaltung anzusehen, kann eine Schulung im Bereich Informationsschutz auch interessant und spannend sein. Man muss aber den Mut haben, etwas Neues zu wagen und die etablierten Strukturen zu durchbrechen. Es muss jedem Einzelnen bewusst werden, dass gerade der Kampf gegen Cyberrisiken keine einmalige Aktion ist, sondern als Daueraufgabe implementiert werden muss.

8.4.2 Fehlende Motivation

Um sich nachhaltig gegen Cyberrisiken wehren zu können, sind motivierte Mitarbeitende elementar wichtig. Nur durch sie lässt sich eine positive Unternehmenskultur ernsthaft und nachhaltig realisieren, und sich dadurch effektiv vor gefährlichen Angriffen schützen. Allerdings gelingt es nicht immer, alle Mitarbeitenden zu motivieren. Zum einen liegt es daran, dass man ihre Anliegen und Wünsche nicht immer ernst nimmt, sondern eine Schulung nach seinen eigenen Ansichten erstellt und diese den Mitarbeitenden in gewisser Weise aufdrückt. Zum anderen liegt es vermutlich auch am unternehmensinternen Umgang mit Risiken, welche des Öfteren im Zusammenhang mit (rechtlichen) Konsequenzen genannt werden. Damit entsteht statt einer offenen, vielmehr eine geschlossene und kritische Kultur. Auswirkungen von falschem Verhalten müssen aufgezeigt werden, aber besonders im Bereich der Informationssicherheit wird vorschnell alles negativ dargestellt, «Mitarbeitende sind Risikofaktoren» oder «Konsequenzen für Fehlverhalten», aber man kann auch anders damit umgehen. Einfach mal wieder Mitarbeitende für ihr Verhalten loben, den Zusammenhalt stärken: «Bock darauf haben, den Detektiv in sich wecken». Gemeinsam gegen das Böse kämpfen.

8.4.3 Monotonie

Durch sich wiederholende Themeninhalte wird schnell Langeweile bei den Mitarbeitenden generiert. Die Empfänger müssen daher angesprochen und ernst genommen werden. Jedes Jahr dasselbe oder ähnliche Training führt zu einer Art Monotonie und verfehlt das gewünschte Ziel von optimal sensibilisierten Mitarbeitenden. Daher ist es zu empfehlen, die Schulung mit interessanten und spannenden Themen zu versehen. Untermauern kann man die Wichtigkeit mit aktuellen Szenarien aus dem realen Leben, welche spielerisch vermittelt werden.

9 Fazit

Die starke Dynamik im gesamten Bereich der Informationssicherheit und die Vielzahl an Phishing-Attacken, welche zunehmend an Qualität gewinnen, sind ein ernst zu nehmendes Problem. Aus diesem Grund ist die Prävention in Form von Sensibilisierungs- und Ausbildungsmassnahmen eine der wichtigsten Abwehrmassnahmen gegen Social-Engineering-Attacken. Denn was bringen einem die besten Systeme, wenn man diese durch den Faktor Mensch umgehen kann? So ist es essenziell wichtig, nicht nur regelmässig seine Systeme zu updaten, sondern auch die eigenen Mitarbeitenden auf laufendem Stand zu halten. Dies erfordert von jedem Einzelnen ein Umdenken in Sachen Schulung. Anstatt es als «Tick-the-box-Übung» anzusehen, muss es als Daueraufgabe mit wechselnden Themengebieten gelebt werden. Nur durch die Motivation aller Mitarbeitenden gelingt es, die Unternehmenskultur nachhaltig zu stärken und somit einheitlich den Bedrohungen entgegenzutreten.

Es gibt keine Allerweltslösung, wie eine Schulung optimal ausgestaltet werden muss. Dies hängt je nach Unternehmen, Branche und den Mitarbeitenden von ganz unterschiedlichen Faktoren und Umständen ab. Es gibt jedoch einige Grundelemente, welche zu beachten sind. Dabei gilt vor allem, den Empfängern der Schulung auf Augenhöhe zu begegnen und ihnen praxisnahes Wissen zu vermitteln, welches sie auch im Berufsalltag oder sogar zu Hause einsetzen können. Wichtig ist dabei auch, einmal die eigene Komfortzone zu verlassen, was Neues zu wagen. Fragen Sie sich selbst: Schenken Sie einem Thema, das Sie schon unzählige Male gehört und gesehen haben, Ihre volle Aufmerksamkeit oder lassen Sie sich von demselben Thema in einer anderen Darstellungsart und -weise eher faszinieren?

Unternehmen müssen sich auf die neue Risikosituation einstellen und sich der neuen Angriffsarten und -vektoren bewusst sein. Neben den klassischen technischen Möglichkeiten wird zunehmend der Mensch in den Fokus der Kriminellen geraten, da er sich naturgemäss irrationaler verhält als die Technik. Dagegen hilft nur, die Mitarbeitenden

fortlaufend zu sensibilisieren, zu motivieren und eine positive Unternehmenskultur zu schaffen. Die Unternehmen müssen sich aber auch von dem Gedanken lösen, dass sie den Kampf alleine bestreiten müssen. Es ist wichtig, sich einen Ruck zu geben und den aktiven Dialog mit anderen Unternehmen zu suchen sowie sich im Bereich Informationssicherheit auszutauschen.

10 Checkliste Cyber Security Awareness

Aktuelle Informationen und die Checkliste zur Selbsteinschätzung des vorhandenen Grads an Sensibilisierung im Unternehmen finden Sie unter

https://www.veb.digital/checklisten/

Quellenverzeichnis

[1] EJPD, Statistiken zum Jahresbericht fedpol 2018 (2018).

[2] Europol, IOCTA – Internet Organised Crime Threat Assessment, 2017. doi:10.2813/858843.

[3] Cybersecurity_Insiders, Insider Threat Report 2018 (2018).

[4] Bundesamt_für_Statistik, Bevölkerung: Ausgewählte Zahlen (2017).

[5] Credit_Suisse, Global Wealth Report 2018 (2018).

[6] K. M. Lerch, A. Repic, Cyberrisiken in Schweizer KMUs, Befragung von GeschäftsführerInnen Schweizer KMUs (2017).

[7] Federal_Bureau_of_Investigation, Business Email Compromise the 12 Billion Dollar Scam (2018).

[8] Verizon, Verizon: 2019 Data Breach Investigations Report (2019). doi:10.1016/s1361-3723(19)30060-0.

[9] S. Morgan, 2019 Official Annual Cybercrime Report (2019).

[10] BBC, Baltimore ransomware attack: NSA faces questions (2019).

[11] CBS_News, Florida city pays $600'000 to hackers who seized its computer system (2019).

[12] Finanzen.ch, Historische Kurse (2019).

[13] Coveware, Global Ransomware Marketplace Report Q4 2018 (2019).

[14] European_Commission, GDPR in numbers (2018).

[15] M. Wilson, H. Joan, Building an Information Technology Security Awareness and Training Program (2003).

[16] R. Lapschiess, PDSA- oder PDCA-Zyklus? (2016).

[17] R. Moen, C. Norman, Evolution of the PDCA Cycle (2006).

Institute for Digital Business

Das Institute for Digital Business ist ein schweizweites Kompetenzzentrum für digitale Transformation und neue Disziplinen in Wirtschaft und Gesellschaft. Es liefert relevante, anwendungsorientierte Inputs in Form von Weiterbildungen, Schulungen, Publikationen, Beratungen und Studien mit dem Ziel einen positiven Einfluss auf den digitalen Wandel der Schweiz zu haben.

Weitere Informationen finden Sie unter: **www.fh-hwz.ch/idb** und auf dem Blog **hwzdigital.ch**

veb.ch

Mit über 9000 Mitgliedern ist veb.ch der grösste Schweizer Verband in Rechnungslegung, Controlling und Rechnungswesen. Expertinnen und Experten in Rechnungslegung und Controlling sowie Inhaberinnen und Inhaber des Fachausweises im Finanz- und Rechnungswesen sind heute in der Schweiz die qualifizierten und staatlich geprüften Fachleute für alle Fragen des Rechnungswesens auf allen Ebenen des Unternehmens. Diese Fachleute und auch ausgewiesene Spezialisten des Rechnungswesens mit anderer Ausbildung können veb.ch beitreten. Als Mitglieder sind alle dem Verband verbundenen Personen willkommen.

Weitere Informationen finden Sie unter: **www.veb.ch**

ZERTIFIKATSLEHRGANG – Digital CFO

Gemeinsam mit der HWZ (Hochschule für Wirtschaft Zürich) hat veb.ch den Lehrgang Digital CFO entwickelt. In acht Kurstagen erarbeiten Sie eine individuelle Digitalisierungsstrategie, die Sie in der Praxis anwenden können. Zudem erfahren Sie alles Wichtige über Projektmanagement, Dokumentenmanagementsystem (DMS) und Business Intelligence (BI).

Erfahrene und praxisorientierte Dozenten unterstützen Sie dabei, vorhandene Lücken zu schliessen und Lösungen für Ihren beruflichen Alltag zu entwickeln.

Aktuelle Daten und weitere Informationen finden Sie unter: **www.veb.ch / Seminare und Lehrgänge**

veb.ch
Schweizerischer Verband der dipl. Experten in Rechnungslegung und Controlling und der Inhaber des eidg. Fachausweises in Finanz- und Rechnungswesen. Seit 1936

Talacker 34
8001 Zürich
Telefon 043 336 50 30
info@veb.ch

Lesen Sie unseren Blog unter
blog.veb.ch

Besuchen Sie unsere digitale Welt auf www.veb.digital
veb::digital

Folgen Sie uns auf:

EDUQUA
Schweizerisches Qualitätszertifikat für Weiterbildungsinstitutionen
Certificat suisse de qualité pour les institutions de formation continue
Certificato svizzero di qualità per istituzioni di formazione continua