Zürcher Hochschule
für Angewandte Wissenschaften

School of
Management and Law

Cyberrisiken und Schweizer KMU

Eine Untersuchung der Einstellungen von Mitarbeitenden und verhaltensbedingter Anfälligkeiten

Carlo Pugnetti, ZHAW Institut für Risk & Insurance
Carlos Casián, Allianz Suisse

In Zusammenarbeit mit:

Allianz

Herausgeber
ZHAW School of Management and Law
St.-Georgen-Platz 2
Postfach
8401 Winterthur
Schweiz

Institut für Risk & Insurance
www.zhaw.ch/de/sml/institute-zentren/iri/

Autor/Kontakt
Dr. Carlo Pugnetti
carlo.pugnetti@zhaw.ch

Januar 2021

Editorial

Die Weiterentwicklung von Technologien und ihre verbreitete Anwendung eröffnen neue und interessante Möglichkeiten, unser Leben durch bessere Produkte und Dienstleistungen sowie bessere und häufigere menschliche Kontakte zu optimieren. Leider bieten diese Veränderungen auch neue Gelegenheiten für Kriminelle. Aus Erfahrung wissen wir, dass diese Gegenspieler intelligent, gut ausgerüstet und kreativ sein können, und sie finden in unserer Abwehr technische und menschliche Schwachstellen, die sie ausnutzen. Diese Entwicklungen sind auch signifikant für Versicherer, die derartige Risiken zeichnen.

Das Problem ist besonders kritisch für kleine und mittlere Unternehmen (KMU) in der Schweiz, die häufig Pioniere im Marktentwicklungs- und Innovationsbereich sind, jedoch nur über begrenzte Ressourcen verfügen, die sie der Cybersicherheit widmen können. Die letzten Jahre haben gezeigt, wie sehr diese Unternehmen ins Visier von Cyberkriminellen geraten sind. Wir bei Allianz Suisse haben unsere Kunden immer mit exzellenten Produkten, massgeschneiderten Dienstleistungen und bahnbrechenden Lösungen unterstützt, und diese neue Studie steht in Einklang mit unserer Innovationshistorie.

Die Einstellung von Mitarbeitenden gegenüber Cyberrisiken ist eine kritische Komponente des allgemeinen Schutzes und des Reaktionsmechanismus eines Unternehmens. Die Zürcher Hochschule für Angewandte Wissenschaften (ZHAW) hat mit dem Thema «Kundenverhalten in der Versicherungswirtschaft» einen spannenden Forschungsschwerpunkt entwickelt, und wir freuen uns, in diese Forschungsarbeit mit eingebunden zu sein. Insbesondere hat diese Studie interessante verhaltensbezogene und kulturelle Erkenntnisse zu den Einstellungen von Mitarbeitenden bei KMU gewonnen und klare und aussagekräftige Empfehlungen sowohl für die Unternehmen selbst als auch für ihre Technologielieferanten und Versicherungsträger entwickelt.

Ich hoffe, dass Sie diese Publikation informativ finden werden und sie Ihnen zugleich Denkanstösse gibt.

Severin Moser

CEO, Allianz Suisse

Management Summary

Cyberangriffe sind ein zunehmend signifikantes Problem für Schweizer KMU. Etwa ein Drittel von ihnen war bereits Opfer von Cyberangriffen, und vier Prozent wurden infolgedessen erpresst. Die meisten dieser Probleme begannen mit Phishing-Angriffen, wobei Kriminelle durch Ausnutzung eines Fehlers oder Versehens seitens eines Mitarbeitenden Zugang zum IT-System gewannen. Wir haben mehrere Mitarbeitende von Schweizer KMU befragt, um zu verstehen, wie ihre Einstellungen zu Cyberangriffen diese Anfälligkeit beeinflussen können, und um praktische Verbesserungsvorschläge zu entwickeln. Die Interviews wurden mit Hilfe des «Tiefen-Metaphern»-Ansatzes durchgeführt, um die verborgenen kulturellen und emotionalen Antriebskräfte für ihr Verhalten, statt nur die rationalen und sichtbaren Komponenten zu verstehen. Dann entwickelten wir drei Empfehlungen, um die bei KMU herrschende proaktive Unternehmenskultur zu nutzen und ihre Abhängigkeit von externen Lieferanten zu reduzieren: Bewusstsein schärfen, Mitarbeitende befähigen und den Wiederherstellungsmodus üben.

Inhaltsverzeichnis

Einleitung

1.1. CYBERRISIKEN UND SCHWEIZER KMU

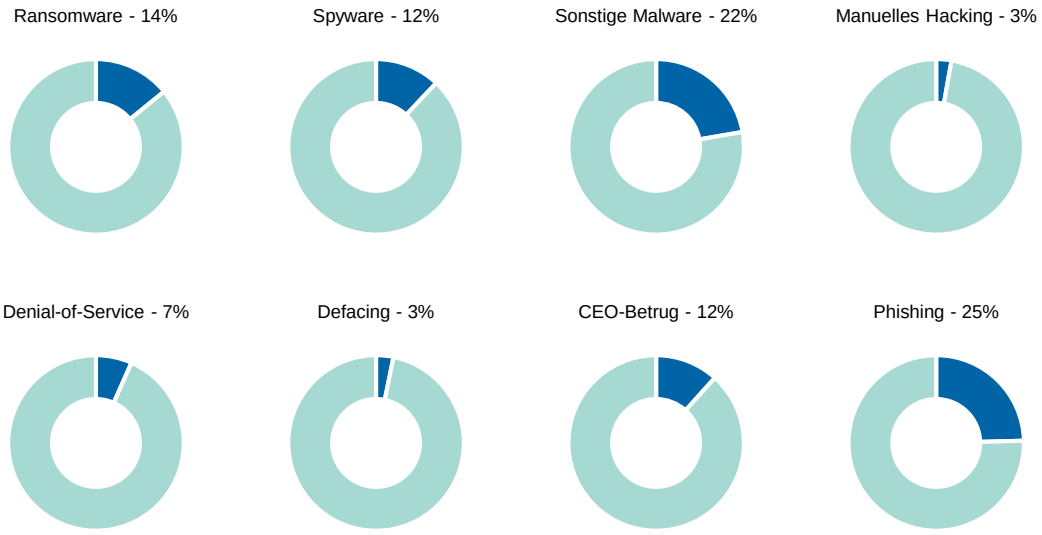
Datenschutz- oder Sicherheitsverletzungen, Spionage, Hackerangriffe, Ransomware, Denial-of-Service-Angriffe und Fehler von Mitarbeitenden sind die Hauptursachen für Cybervorfälle, und sie werden immer verbreiteter und kostspieliger. Diese Entwicklung spiegelt sich im Allianz Risk Barometer (2020) wider, bei dem mehr als 2‘700 Risikoexperten weltweit befragt wurden: Cybervorfälle haben Betriebsunterbrechungen als Risiko Nummer eins verdrängt. Die zunehmende Vernetzung der Wirtschaft bedeutet, dass die Unternehmen immer anfälliger für Cyberangriffe werden, und Berichte über spektakuläre Hackerangriffe und Datendiebstähle liest man immer häufiger. Den Unternehmen drohen Schäden in Millionenhöhe, Imageverlust und sogar Betriebsunterbrechungen, die ihre Existenz bedrohen, wenn Cyberkriminelle Daten stehlen, Schadprogramme in die Netzwerke einschleusen oder Server blockieren (Allianz, 2020). Severin Moser, CEO der Allianz Suisse, schätzt, dass die Folgen der Cyberkriminalität die Weltwirtschaft jährlich mehr als 600 Milliarden USD kosten (NZZ, 2019). Es ist jedoch schwierig, die Entwicklung genau zu quantifizieren, da es an zuverlässigen Zahlen mangelt und viele Fälle nicht gemeldet werden. Die Arbeitsgruppe Cyber Risk beim Schweizerischen Versicherungsverband schätzt die jährlichen Kosten alleine in der Schweiz auf 9.5 Milliarden CHF, und diese Zahl steigt weiter (SVV, 2018).

Kleine und mittlere Unternehmen (KMU), unter denen man Betriebe mit bis zu 250 Arbeitnehmern versteht, machen mehr als 99 Prozent der Unternehmen aus und stellen zwei Drittel aller Arbeitsplätze in der Schweiz zur Verfügung (Bundesamt für Statistik, 2020). Sie spielen eine wesentliche Rolle für die Schweizer Wirtschaft und sind stark betroffen von Cyberangriffen. Etwa ein Drittel der Schweizer KMU war bereits Opfer von Cyberangriffen, und vier Prozent wurden infolge dieser Angriffe erpresst (Mändli Lerch und Repic, 2017). Selbst wenn die Daten kleinerer Betriebe für Cyberkriminelle weniger interessant sind, bleiben diese Unternehmen für sie aus zwei Gründen attraktive Ziele: Erstens, um Lösegeld mit Hilfe von Ransomware zu erpressen, und zweitens, um sie als Einfalltor für Angriffe auf grössere Unternehmen zu nutzen, die mit diesen KMU zusammenarbeiten (Heer, 2020). Über ein gestiegenes Risiko von Ransomware-Angriffen berichtete Anfang 2020 die Melde- und Analysestelle Informationssicherung (MELANI, 2020a), die im Juli 2020 in das Nationale Zentrum für Cybersicherheit (NCSC) integriert wurde. Diese Bedrohung wächst weiter, und nachdem sie sich 2019 vervierfacht hat, ist sie heute der am häufigsten beobachtete Cybervorfall (Trustwave, 2020). Es gibt zahlreiche Beispiele von Schweizer Unternehmen, die Opfer von Ransomware-Angriffen geworden sind, und vier von ihnen werden im folgenden Kapitel behandelt.

Aktuellere Untersuchungen haben sich erstmals ausführlicher mit Cyberangriffen auf KMU in Nachbarländern befasst. Dreissigacker et al. (2020) schätzen, dass beispielsweise in Deutschland jedes Jahr 40 bis 50 Prozent der KMU mit mehr als 10 Mitarbeitenden einem Cyberangriff ausgesetzt sind, auch wenn die meisten dieser Attacken neutralisiert werden und keinen Schaden anrichten. Diese Zahl ist – wenn auch nicht in signifikanter Weise – kleiner als die bei grossen Unternehmen, die jährlich mit einer Rate von 50 bis 60 Prozent angegriffen werden. Diese Studie untersucht zudem die jährliche Rate in jeder wesentlichen Cyberangriffskategorie – siehe Zusammenfassung in Abbildung 1. KMU müssen alle vier Jahre mit einem Cyberangriff und alle sieben Jahre mit einem Ransomware-Angriff rechnen, was grob den Raten bei grösseren Unternehmen entspricht. Andererseits sind CEO-Betrugsfälle und manuelles Hacking bei KMU signifikant seltener, was möglicherweise mit der praxisnaheren Rolle des CEO bei kleineren Unternehmen und der potenziell geringeren Beute zusammenhängt. Studien in anderen europäischen Ländern nennen ähnliche Ergebnisse. Sie weisen jedoch teilweise signifikante Abweichungen auf, wobei ein direkter Vergleich aufgrund unterschiedlicher Forschungsmethoden und Meldemechanismen schwierig ist. In der Regel bestätigen sie jedoch eine wesentliche allgemeine Bedrohung für KMU durch Cyberangriffe.

Abb. 1: Geschätzte jährliche Rate der Cyberangriffe auf KMU

GESCHÄTZTE JÄHRLICHE RATE DER CYBERANGRIFFE AUF KMU IN DEUTSCHLAND 2018/2019, UNTERGLIEDERT NACH KATEGORIEN



Quelle: Dreissigacker et al. (2020)

Böswillige Cyberakteure passen regelmässig ihre Social-Engineering-Angriffe, insbesondere Phishing, an aktuelle Grossereignisse wie Sportveranstaltungen oder die derzeit herrschende COVID-19-Pandemie an. Doch praktisch alle üblichen Schadsoftware-Familien wurden mit einem an COVID-19 anknüpfenden Vorwand verbreitet: Am häufigsten werden dazu E-Mails mit einem infizierten Anhang oder einem Link zu einer infizierten Website verwendet (MELANI, 2020b). Die Anzahl der Phishing-E-Mails ist während der Pandemie sprunghaft gestiegen; so haben sich Betrüger als Mitarbeitende der Weltgesundheitsorganisation (WHO) ausgegeben und Soforthilfeprogramme für COVID-19-Geschädigte ins Visier genommen und Benutzer mit Hilfe gefälschter Werbebanner auf schädliche Websites gelockt (de Moura et al., 2020). Phishing-Angriffe zielten insbesondere auf das veränderte Arbeitsumfeld ab. Viele Benutzer waren anfangs nicht vertraut mit Konferenz- und Kooperationssoftware und den von diesen Plattformen versandten Mitteilungen, sodass Phishing-E-Mails für sie schwerer zu erkennen waren (MELANI, 2020b). Mehrere Artikel erwähnen die Anfälligkeiten von Unternehmen aufgrund menschlicher Fehler und die Bedeutung von Phishing-Angriffen. Auch wenn die technische Infrastruktur weiterhin ein kritischer Faktor ist, fallen Mitarbeitende häufig clever angelegten Plänen zum Opfer und setzen ihr Unternehmen Betrug und Schadsoftware aus (Pugnetti et al., 2019). Schweizer KMU sind in der Regel unzureichend gegen Cyberrisiken geschützt, insbesondere in Bezug auf Dienstleistungen für Schadenminderung und für die Wiederinbetriebnahme der Geschäftstätigkeit (Pugnetti und Schneebeli, 2020).

Diese Untersuchung zielt darauf ab, die potenziellen Anfälligkeiten aufgrund der Wahrnehmung der Cyberkriminalität durch die Mitarbeitenden und der Unternehmenskultur der KMU zu verstehen. Im Anschluss sollen Empfehlungen für Bewältigungsstrategien der Unternehmen sowie für Schulungen und Dienstleistungen, die von Dritten erbracht werden können, entwickelt werden.

1.2. BEISPIELE FÜR PROMINENTE CYBERANGRIFFE IN DER SCHWEIZ

In den Medien wurde über zahlreiche Fälle von Cyberangriffen gegen Schweizer Unternehmen berichtet. Vier Angriffe waren besonders relevant für die im Rahmen dieser Studie befragten Unternehmen; daher werden sie nachstehend genauer beschrieben.

1.2.1. OFFIX AG, 2019

Die OFFIX AG, die im Büroausstattungssektor tätig ist, hat 250 Mitarbeitende und einen Umsatz von 300 Millionen CHF (Papedis, n. d.). Dieses Unternehmen wurde am 15. Mai 2019 Opfer eines Ransomware-Angriffs (Jochum, 2019). Es wird angenommen, dass ein Hacker die E-Mail-Korrespondenz mit einem Kunden abfing und im E-Mail-Verkehr die Stelle des Kunden einnahm. Ein Mitarbeitender des Unternehmen erhielt dann eine Bestätigungsanfrage und klickte auf den beigefügten Link, woraufhin das Virus das IT-System des Unternehmens infizierte. Die ersten Unregelmässigkeiten wurden einen Tag später sichtbar, und am 17. Mai wurde auf der IT-Ebene klar, dass «alles weg war»: Datenbanken waren gelöscht und zahlreiche Server auf die Werkseinstellungen zurückgesetzt worden. Viele Kundenschnittstellen für die Auftragserteilung waren ebenfalls gelöscht worden, und OFFIX verlor die Kontrolle über Auftragseingänge und Verkäufe. Ein Lösegeld von 45 Bitcoins (zum damaligen Zeitpunkt 350‘000 CHF wert) wurde für die Entschlüsselung verlangt. Ein externer Cybercrime-Experte wurde beauftragt, und die Melde- und Analysestelle Informationssicherung (MELANI) sowie die Polizei wurden informiert. Man bat dann die Kunden, weitere Aufträge per Telefon, Fax oder über neu eingerichtete E-Mail-Adressen zu erteilen, bevor das gesamte Unternehmen offline ging. Glücklicherweise hatte der Hacker einen Fehler gemacht, und ausserdem war eine wichtige Applikation durch einen IT-Experten nur wenige Wochen vorher auf einer externen Festplatte gespeichert worden. Daher gelang es OFFIX, einen Teil seiner Datenbank wiederherzustellen und anschliessend die IT-Systeme wieder neu aufzubauen (Severin, 2019). Laut Martin Kelterborn, dem CEO des Unternehmens, konnte der finanzielle Schaden nicht quantifiziert werden, jedoch war der Angriff «sehr, sehr teuer» (Jochum, 2019).

1.2.2. Swisswindows, 2019

Im Mai 2019 hatte Swisswindows, ein Fensterbauer mit rund 170 Mitarbeitenden (Borkert, 2020), einen Produktionsausfall von mehr als einem Monat infolge eines Ransomware-Angriffs zu verkraften. Wahrscheinlich hatten Hacker durch eine harmlos wirkende E-Mail Zugang zum Netzwerk des Unternehmens erhalten und alle Unternehmensdaten verschlüsselt. Die Aufträge waren nicht mehr sichtbar, und die Mitarbeitenden hatten keinen Zugang mehr zu Kunden- und Maschinendaten. Das Unternehmen war lahmgelegt. Ein externes IT-Unternehmen hatte täglich Daten-Backups durchgeführt, doch die Backup-Dateien waren mit dem Server des Unternehmens verbunden, und daher waren auch sie nicht mehr zugänglich. Obwohl die Cyberkriminellen ein hohes Lösegeld in Bitcoins verlangten, um die Daten wieder freizugeben, entschied sich das Unternehmen, das Lösegeld nicht zu zahlen, sondern die Summe zu verwenden, um die IT-Infrastruktur zu ersetzen, deren Erneuerung sowieso notwendig war (Klein, 2020). Doch im Februar 2020 wurde das Personal überraschend in Kenntnis darüber gesetzt, dass das Unternehmen insolvent war. Der Cyberangriff hatte einen fortschreitenden Rückgang des Kerngeschäfts des Unternehmens noch verschärft und trug so zu seinem Untergang bei (SRF, 2020).

1.2.3. Meier Tobler, 2019

Meier Tobler, eine Gebäudetechnologiefirma mit einem Umsatz von 500 Millionen CHF und rund 1‘300 Mitarbeitenden (Meier Tobler, 2020) wurde im Juli 2019 Opfer eines Ransomware-Angriffs (Luzerner Zeitung, 2019). Die Angreifer erhielten über ein mit Schadsoftware infiziertes E-Mail-Attachment Zugang zum Unternehmen (Schäppi, 2020). Das zentrale SAP-System, das Lagerverwaltungssystem, der Festnetztelefonanschluss, die Website und alle E-Mail-Adressen funktionierten nicht mehr (Lüscher und Niedermann, 2019). Laut Pressemitteilung des Unternehmens hatte dies erhebliche Auswirkungen auf Umsatz und Gewinn:

> Obwohl die vorbereiteten Notfallprozeduren in Kraft traten und eine provisorische Infrastruktur innerhalb kürzester Zeit eingerichtet werden konnte, war es nicht möglich, eine zeitweise Unterbrechung der Auslieferungen zu verhindern. Dies führte im Handelsgeschäft zu einem sofortigen Umsatzrückgang von rund 5 Millionen CHF. Im Wärmeerzeugungs-geschäft kam es aufgrund der Nichtverfügbarkeit der IT-Systeme später zu einem weiteren Umsatzverlust in gleicher Grössenordnung.

Die direkten Zusatzkosten der Bewältigung dieses Angriffs minderten den Jahresgewinn 2019 um eine Million CHF. Seitdem hat das Unternehmen seine IT-Infrastruktur im Einklang mit den neuesten Sicherheitskriterien umstrukturiert (Meier Tobler, 2020).

1.2.4. Stadler Rail, 2020

Stadler Rail stellt Schienenfahrzeuge her und erzielt mit 11‘000 Mitarbeitenden einen Umsatz von weltweit mehr als 3,2 Milliarden CHF (Stadler Rail, 2020a). Es handelt sich also nicht um ein KMU. Dieser Cyberangriff wurde jedoch von den für diese Studie befragten Personen erwähnt und ist daher von Relevanz. Am 7. Mai 2020 wurde «das IT-Netzwerk von Stadler mit einer Schadsoftware attackiert. Das Unternehmen leitete sofort die erforderlichen Sicherheitsmassnahmen ein und bezog die zuständigen Behörden mit ein. Eine ausführliche Untersuchung der Angelegenheit ist noch in Arbeit.» (Stadler Rail, 2020). Die Täter erpressten Stadler mit der Drohung, gestohlene Daten zu veröffentlichen, und verlangten die Zahlung von sechs Millionen USD in Bitcoins. In einer Erklärung bestätigte das Unternehmen gegenüber inside-it.ch, dass «es sich dabei um vertrauliche Dokumente und Daten handelt, die durch kriminelle Aktivitäten aus dem Besitz von Stadler gestohlen wurden» (Anz, 2020). Stadler lehnte die Lösegeldzahlung ab, und einige Datensätze wurden veröffentlicht, um den Druck zu erhöhen. Nachdem das Unternehmen weiterhin die Zahlung verweigerte, folgte die Veröffentlichung von weiteren Datensätzen (Griesser Kym, 2020). Doch Stadler war zu keinem Zeitpunkt bereit, auf die Forderungen der Erpresser einzugehen und Zahlungen zu leisten, und «wird dies auch weiterhin nicht tun» (Anz, 2020).

1.3. SCHUTZ FÜR IHR UNTERNEHMEN

Alle Unternehmen müssen im Rahmen ihres Risikomanagement-Entscheidungsprozesses bestimmen, welche Risiken sie vermeiden, mindern, übertragen oder selbst tragen wollen. In diesem Zusammenhang ist es von entscheidender Bedeutung zu verstehen, welche Versicherungslösungen ihnen zur Verfügung stehen und ihnen in den oben beschriebenen Fällen einen gewissen Grad an Schutz geboten hätten. Cyberangriffe können Eigenschäden verursachen, etwa Wiederherstellungskosten für Daten, und die Unterbrechung des normalen Geschäftsbetriebs. Gängige Sachversicherungspolicen decken Sachschäden und die daraus resultierende Betriebsunterbrechung, wenn die Schadenursache (z. B. ein Feuer) versichert ist. Bei einem Cyberangriff kommt es jedoch nicht notwendigerweise zu einem Sachschaden, und daher kommt es selten vor, dass eine Sachversicherung zum Zug kommt. Zudem können Unternehmen nach einem Cyberangriff mit Haftpflicht-ansprüchen Dritter konfrontiert werden, wenn beispielsweise Kundendaten geleakt oder gelöscht werden. Eine herkömmliche Haftpflichtversicherung deckt die Haftpflichtansprüche aus Personen- und Sachschäden sowie daraus resultierenden Vermögensschäden. Haftpflichtversicherungen, die reine Vermögensschäden decken, sind in der Regel nur für bestimmte Berufsgruppen vorgesehen und daher nicht weit verbreitet.

Die etablierten, klassischen Geschäftsversicherungen haben eines gemeinsam: Sie adressieren Cyberrisiken nicht gezielt. Unter bestimmten Umständen sind der Schaden und die Auswirkungen eines Cyberangriffs durch derartige Produkte versichert, doch sie sind nicht explizit darauf ausgelegt, Cyberrisiken für Unternehmen kontrollierbar zu machen. Es ist zu beachten, dass Cyberrisiken erst im Zeitalter des Internets entstanden sind, und die ersten Cyberriskdeckungen wurden um die Jahrtausendwende entwickelt, um auf diese neue Bedrohung zu reagieren. In der Schweiz wurden die ersten Cyberriskversicherungen durch internationale Versicherer für Grossunternehmen im Jahr 2015 eingeführt, und umfassende Versicherungslösungen für KMU wurden erstmals im Jahr 2017 präsentiert. Üblicherweise decken sie Haftpflicht- und Eigenschäden sowie Krisenmanagementauslagen; ausserdem enthalten sie die Bausteine Cyber Crime / Social Engineering und Cyberrisk-Rechtsschutz. Der Schwerpunkt dieser Produkte liegt auf Cyberangriffen sowie Fehlverhalten des Personals und Datenschutz-verletzungen. Neben der Entschädigungszahlung für den entstandenen Schaden erhalten die Unternehmen Zugang zu einem Netzwerk von Experten für IT, Krisenkommunikation und Rechtsschutz, um den Schadenumfang zu bestimmen, die Schadenbehebung zu beschleunigen und eine Reputationsschädigung des Unternehmens zu verhindern oder zu mindern. Tabelle 1 gibt einen Überblick über die aktuell angebotenen üblichen Cyberversicherungsdeckungen (Pugnetti et al., 2019).

Tabelle 1: Marktübliche Cyberversicherungsdeckungen

MARKTÜBLICHE CYBERVERSICHERUNGSDECKUNGEN

Haftpflicht Ansprüche und Forderungen Dritter	- Datenschutzverletzungen - Datenverlust - Zweckentfremdung und Ausfall der Funktionalität - Digitale Kommunikation - E-Payment / Vertragsstrafen - Weitergabe von Schadsoftware
Eigenschäden Schäden des Versicherungsnehmers	- Wiederherstellungskosten - Betriebsunterbruch - Diebstahl durch Cyberangriff - Cybererpressung - Datenschutzverfahren
Krisenmanagement Dienstleistungen im Schadenfall	- Forensische Dienstleistungen - Informationskosten - Krisenkommunikation - Notfallkosten
Rechtsschutz Streitigkeiten im Zusammenhang mit Cyberrisiken	- Vertragsrecht - Persönlichkeitsverletzung - Identitätsmissbrauch - Missbrauch von Kreditkarten und Kontodaten - Internet-Domain
Cyber Crime - Social Engineering Finanzielle Schäden infolge von Täuschung durch einen Dritten	- Betrug durch Vorspiegelung einer falschen Identität - Betrug durch Umleitung von Zahlungsströmen - Betrug durch Nutzung einer fremden Identität

1.4. INTERVIEWS MIT TIEFEN METAPHERN

Die Konsumentenforschung hat sich lange auf das Verstehen kognitiver Strukturen konzentriert – d. h. «Belief Systems» und die Betonung von Struktur anstelle von Inhalt (Olson und Reynolds, 1983). Ein besserer Begriff zur Beschreibung und Darstellung von Konsumenten ist jedoch das mentale Modell, das auch Belief-unabhängige Darstellungen ermöglicht, einschliesslich Einstellungen, Gefühlen, Bildern, Erinnerungen, Werten usw. (Christensen und Olson, 2002). Dies entspricht eher der heutigen kognitiven neurowissenschaftlichen Sichtweise, die Gedanken als bildbasiert ansieht (Damasio, 1994). Die Forschungs- und Erhebungsverfahren wurden weiterentwickelt, um zu versuchen, die zusätzliche Komplexität mentaler Modelle zu erfassen. Eine dieser Methoden ist die Zaltman Metaphor Elicitation Technique (ZMET). Die der ZMET zugrundeliegende Annahme ist insbesondere die Bedeutung unbewusster, stillschweigender Inhalte, d. h. verdeckten Wissens, und die Kenntnis und Bedeutung von Bildern in mentalen Modellen. Die ZMET verwendet Bilder, um den Informanten zu helfen, Inhalte zu identifizieren und mitzuteilen (Zaltman, 1997). Sie wurde benutzt, um tiefere emotionale Verhaltens- und Auswahlfaktoren bei Konsumenten aufzudecken (Zaltman und Zaltman, 2008).

Die Methode basiert auf drei Phasen. Zunächst werden die Probanden gebeten, über ein Thema nachzudenken und Bilder auszuwählen, die ihre Gedanken und Gefühle in Bezug auf dieses Thema darstellen. Dann werden sie befragt, um die Bedeutungen zu verstehen, die sie den Bildern zuordnen, und es werden Verbindungen mit übergeordneten Vorstellungen mit Hilfe von «Laddering»-Fragen entwickelt. Schliesslich werden durch die Anlage von Consensus Maps zentraler Konstrukte und breiter Bedeutungsthemen die Ergebnisse entwickelt (Christensen und Olson, 2002). Das Endergebnis besteht aus einer Reihe von Themen, welche die Probanden mit dem Untersuchungsgegenstand assoziieren. Dabei wird nicht versucht, statistisch signifikante Ergebnisse zu erzielen; vielmehr ist der Fokus darauf gerichtet, nicht offensichtliche Erkenntnisse aufzudecken. Die Technik wurde in mehreren Studien, so auch von den Autoren der vorliegenden Studie, für Beratungsprojekte und in einer veröffentlichten Studie verwendet, um die Erfahrung neuer Versicherungskunden zu untersuchen. So signalisierten beispielsweise in dieser Studie Neukunden deutlich ihre Frustration in Bezug auf den branchenüblichen Fachjargon und ihre mangelnde Vertrautheit mit Versicherungsmarken (Pugnetti und Bekaert, 2018).

1.5. METHODIK

Wir rekrutierten drei KMU, die in der Wärme- und Fertigungsbranche tätig sind, und führten Interviews nach dem Ansatz der «Tiefen-Metaphern» mit 17 Freiwilligen durch, die einen breiten Querschnitt an Mitarbeiterprofilen in ihrem Unternehmen repräsentierten, einschliesslich Management, Verwaltungs-, Werks- und Montagepersonal. Die Befragten wurden gebeten, drei bis fünf Bilder auszuwählen, die beschreiben, wie sie sich fühlten, als sie Berichte über Cyberangriffe hörten (Tabelle 2). Danach wurden sie über die Bedeutung der ausgewählten Bilder befragt.

Tabelle 2: Forschungsfrage

Forschungsfrage	Wie fühlen Sie sich, wenn Sie über Cyberangriffe hören?

Die Interviews wurden im September 2020 gemeinsam von beiden Autoren jeweils am Firmenstandort durchgeführt. Je nach Anzahl der verwendeten Bilder und der durch das Gespräch ausgelösten nachfassenden Fragen dauerten sie jeweils rund eine Stunde lang. Die Ergebnisse wurden dann in einer Reihe von Workshops besprochen und konsolidiert, um Consensus Maps zu entwickeln und daraus die Themen abzuleiten. Diese Themen werden in den folgenden Abschnitten anhand der Originalbilder und des Originalwortlauts aus den Interviews besprochen. Aufgrund von Lizenzierungsproblemen wurden die Originalbilder in einigen Fällen durch ähnliche Bilder ersetzt.

Die Interviewpartner beschrieben sich selbst wie in Tabelle 3 zusammenfassend dargestellt:[1]

Tabelle 3: Eigenbeschreibung der Interviewpartner

EIGENBESCHREIBUNG DER INTERVIEWPARTNER

1	Hilfsbereit, niemand muss wegen mir leiden	10	Fröhlich, sorgt sich um das Wohl anderer
2	Positiv eingestellter Mensch	11	Offen, jedoch vorsichtig
3	Ruhig und nachdenklich	12	Bodenständig, jedoch offen für Neues
4	Zufrieden mit dem Leben	13	Eher vorsichtiger
5	Ruhig, sucht keinen Streit	14	Gutmütig, flexibel und kann zuhören
6	Loyal, höre gut zu	15	Weltoffener und konservativer Familienmensch
7	Positiver Mensch	16	Ist der Kopf der Familie
8	Aufgestellte und zielstrebige Person	17	Kommunikativ und wissbegierig
9	Ruhig und belastbar		

[1] Um Vertraulichkeit zu wahren, entspricht die Reihenfolge nicht der Reihenfolge der Interviews.

Ergebnisse

Die Interviews enthüllten einige gemeinsame Nenner. Ein wiederkehrendes Thema war die geopolitische Natur der Cyberangriffe, Verbindungen zum organisierten Verbrechen und die finanzielle Motivation. Die Hacker wurden als «Profis» mit Expertenkenntnissen sowie exzellenter Ausrüstung und nicht notwendigerweise immer als «Bösewichte» angesehen. In der Regel fühlten sich die Befragten hilflos, wenn es darum ging, Cyberangriffe zu erkennen oder sich selbst zu schützen. Infolgedessen fühlten sie sich anfällig, waren sich jedoch der Gefahren bewusst, die von Phishing-Angriffen ausgingen, und konnten die potenziell katastrophalen Folgen von Cyberangriffen ermessen. Viele erwähnten den unlängst bei Meier Tobler eingetretenen Fall. Zugleich meinten sie, dass weder sie wichtig genug noch ihr Unternehmen gross genug seien, um zum Angriffsziel zu werden. Im Notfall würden sie sich auf externe Dienstleister verlassen, um das Problem zu lösen. Schliesslich zeigten sie sich lösungsorientiert, mit dem Willen, eigenständig nach Lösungen zu suchen, bei Bedarf auch einschliesslich altmodischer Arbeitsweisen.

Tabelle 4: Abgeleitete Themen und Bildbezeichnungen

	THEMA	BILDBEZEICHNUNG
1	**Internationale Politik und organisiertes Verbrechen**	Geheimdienst Schattenmann Beute
2	**Der Hacker-Mythos**	Der Hacker Top Arbeitsplatz Übel- oder Wohltäter?
3	**Sich hilflos fühlen**	Datenmagnet Soziale Manipulation Lauter Fragen
4	**Sich anfällig fühlen**	Überwachung Sei vorsichtig! Phishing
5	**Katastrophale Folgen**	Modernes Einbrechen und Eindringen Angriff auf unseren Lieferanten Hoffentlich nicht!
6	**Das betrifft mich nicht**	Die ganze Welt verknüpft Angst Persönliche Unterstützung
7	**Proaktiv und engagiert**	Nebel Planung Wie früher

Diese nuancierten und facettenreichen Antworten auf eine relativ direkte Frage deuten auf eine differenzierte Denkweise hin. Dies ermöglichte die Identifikation mehrerer Verbesserungsbereiche und die Entwicklung klarer Empfehlungen für die Schweizer KMU und ihre Dienstleister.

2.1. INTERNATIONALE POLITIK UND ORGANISIERTES VERBRECHEN

Cyberangriffe wurden als Muster internationaler Intrigen und globaler politischer Ränkespiele mit hohen Einsätzen angesehen. Obwohl mehrere Befragte Cyberangriffe benennen konnten, die sich in ihrer Nähe oder sich in ihrem Unternehmen ereignet hatten (vor allem bei Meier Tobler, wie oben erwähnt), sahen sie Cyberangriffe in der Regel im Kontext internationaler politischer Konfrontationen. Die Wahlen in den USA und die vermutete russische Einmischung wurden ebenso wie der Terrorismus häufig als Beispiele zitiert. Die Schweiz wurde jedoch als «sicherer Hafen» mit einem stabileren politischen System angesehen. Doch war den Probanden bewusst, dass das organisierte Verbrechen eine starke und koordinierende Kraft ist, die hinter den Cyberangriffen steckt. Erfolgreiche Angriffe bedürfen über längere Zeit der breiten Koordination mehrerer Spezialisten und Datenquellen, was wiederum Organisation erfordert. Finanzieller Gewinn wurde als einen Treiber von Cyberangriffen benannt, wobei gelegentlich ausserdem Machtstreben erwähnt wurde. Während die politische Komponente Cyberkriminalität als relativ weit weg erscheinen lässt, rücken finanzielle und kriminelle Motive dieses Phänomen stärker ins Blickfeld, so dass es besser erkennbar und daher relevanter für die Befragten wird.

Abb. 2: Geheimdienst

GEHEIMDIENST

Es gibt starke Verschiebungen der internationalen Machtstruktur, und es ist nicht so wichtig, wenn einige Menschen sterben. In der Schweiz sehen die Dinge jedoch anders aus; das ganze System ist sicherer.

Abb. 3: Schattenmann

SCHATTENMANN

Es ist nicht bekannt, wer diese Person ist, aber es handelt sich eindeutig um organisiertes Verbrechen, die Mafia. Man kann die Polizei anrufen oder ihm aus dem Weg gehen, aber es ist zu gefährlich, ihm direkt entgegenzutreten.

Abb. 4: Beute

BEUTE

Geld, viel Geld. Letztendlich geht es doch immer nur um Geld.

Die Tendenz, Cyberkriminalität mit starken geopolitischen Kräften zu assoziieren und zugleich anzunehmen, dass die Schweiz ein «sicherer Hafen» sei, kann die Schweizer KMU anfällig machen. Die Mitarbeitenden sind dann möglicherweise nicht so auf der Hut, wie sie es sein sollten. Doch das Erkennen der Rolle des organisierten Verbrechens und der damit verbundenen finanziellen Motive ist ein positives Zeichen.

2.2. DER HACKER-MYTHOS

Die Person, die tatsächlich den Angriff durchführte, wurde oft mit dem englischen Begriff «Hacker» bezeichnet und als Hoodie-Träger dargestellt. Alle Befragten gaben an, dass ein Hacker eigentlich sehr wahrscheinlich nicht so aussehen würde und dass es sich um eine männliche oder auch weibliche Person handeln könne. Von Hackern wurde angenommen, dass sie über beträchtliche technische Fachkenntnisse verfügen und gut ausgerüstete Arbeitsplätze nutzen, die sogar besser sind, als die ihrer geplanten Opfer. Hacker wurden nicht allgemein als Kraft des Bösen angesehen. Häufig wurden sie als potenziell Gutes bewirkend bezeichnet – z. B. durch Aufdeckung von Pädophilennetzwerken und/oder Korruption. Diese differenzierte Betrachtung des Hackings öffnet ethisch gesinnten Hackern die Türen, um die Verteidigungsmechanismen eines Unternehmens gegen Bezahlung zu testen.

Abb. 5: Der Hacker

DER HACKER

Vernetzt mit mehreren Personen in mehreren Ländern. Anonym und angsteinflössend.

Abb. 6: Top Arbeitsplatz

TOP ARBEITSPLATZ

Ich weiss nicht, warum er so viele Geräte hat, aber er benutzt sie alle. Er kann sogar Unternehmen hacken, die vorbereitet und gut geschützt sind.

Abb. 7: Übel- oder Wohltäter?

ÜBEL- ODER WOHLTÄTER?

Ich sehe das neutral. Könnte ein Krimineller oder ein Whistleblower sein.

Die Antworten der Befragten bestätigten, dass ihnen die komplizierte Natur sowie die Antriebskräfte von Cyberangriffen und der mögliche Nutzen von Whistleblowing-Aktivitäten bewusst waren. Doch durch die Verknüpfung der Angriffe mit grösseren geopolitischen Kräften laufen sie Gefahr, Cyberangriffe in einen Kontext zu verweisen, in dem sie und ihre Unternehmen zu «unbedeutend» sind, um unerwünschte Aufmerksamkeit zu erregen, was wiederum automatisch ihre Anfälligkeit erhöht.

2.3. SICH HILFLOS FÜHLEN

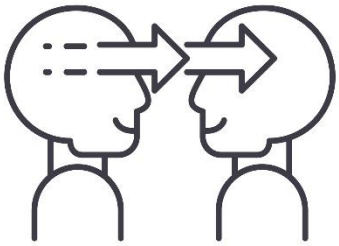
Die Befragten sprachen offen über die Undurchsichtigkeit von Cyberangriffen und erwähnten, dass sie ihre Dynamik nicht verstehen. Daten können unbemerkt entwendet werden, wie mit einem Magneten, der eisenhaltige Metalle anzieht. Die Einstellungen gegenüber Cyberangriffen können unbemerkt im Laufe der Zeit beeinflusst und manipuliert werden. Mehrere Fragen bleiben offen: wer hinter den Angriffen steckt und warum, und wie man während oder nach einem Angriff reagieren sollte. Das aktuell herrschende allgemeine Gefühl ist von Hilflosigkeit gegenüber Cyberangriffen geprägt. Das ist kein positives Zeichen, denn es hält von aktivem Engagement und dem Ergreifen sinnvoller Abwehrmassnahmen ab. Andererseits dürften Informationskampagnen und Schulungsprogramme zur Verbesserung der Kenntnisse und zur Bewusstmachung der Risiken ein interessiertes und motiviertes Publikum finden.

Abb. 8: Datenmagnet

DATENMAGNET

Daten können wie mit einem Magneten, der alles zu sich hinzieht, aus einem Netzwerk herausgezogen werden.

Abb. 9: Soziale Manipulation



SOZIALE MANIPULATION

Vertrauen wird missbraucht. Wenn Mitarbeitende unaufmerksam sind, können sie einen Fehler machen und ihre Stelle verlieren.

Abb. 10: Lauter Fragen

LAUTER FRAGEN

Warum hat er das getan? Was können wir tun? Wir können selbst keine Antworten geben oder Lösungen finden.

Unglücklicherweise löst ein Gefühl von Hilflosigkeit Passivität sowohl bei der Vorbereitung als auch der Reaktion auf einen Cyberangriff aus. Die Verantwortung für die Cybersicherheit wird dann an kenntnisreichere spezialisierte Dritten delegiert, statt den Fokus auf die Rolle jedes einzelnen Mitarbeitenden im Hinblick auf die Absicherung des Unternehmens zu richten. Es müssen spezifische Weiterbildungsprogramme entwickelt werden, um das Bewusstsein für riskantes Verhalten zu schärfen und das Wissen über die Tools zu verbessern, die verfügbar sind, um die Mitarbeitenden proaktiver zu machen.

2.4. SICH ANFÄLLIG FÜHLEN

Die Befragten wissen, dass sie beobachtet werden, wenn sie online sind. Sie mögen dieses Gefühl nicht und sie schätzen es auch nicht, dass sie nicht in der Lage sind, sich vor dem Beobachtetwerden zu schützen. Sie wissen, dass ihr Vertrauen missbraucht werden kann, um die Unternehmen, für die sie arbeiten, zu schädigen, und dass sie direkt oder indirekt darunter leiden können. Eine Befragte verglich dies mit einer unbekannten Person, der man die Tür öffnet und die dann das Gebäude betreten und Geräte stehlen kann. Darüber hinaus haben wir alle ein Privatleben und Verhaltensweisen, auf die wir nicht stolz wären, wenn sie öffentlich bekannt und einem breiteren Publikum mitgeteilt würden. Dies macht uns anfällig und unfähig, uns gegen einen Angriff zu wehren. Hacker nutzen unsere Anfälligkeit aus und erhalten unbefugten Zugang durch Phishing-Angriffe, die uns in einem Moment der Unaufmerksamkeit überraschen sollen.

Das Gefühl der Anfälligkeit ist unangenehm, und eine übliche Reaktion von Menschen besteht darin, den Gedanken daran zu verdrängen. Oder wie einer der Befragten es ausdrückte: «Wenn wir an alles denken würden, was passieren kann, würden wir niemals online gehen.» Das Bewusstsein für die Ernsthaftigkeit von Phishing-Angriffen ist jedoch ein ermutigender Indikator für den Wissensstand der Mitarbeitenden in Bezug auf Cyberangriffe und damit ein brauchbarer Ansatzpunkt für Schulungsprogramme.

Abb. 11: Überwachung

ÜBERWACHUNG

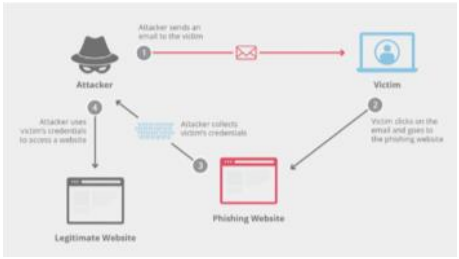
Jemand schaut über die Schulter dieser jungen Frau. Sie kann es nicht verhindern. Ich mag es nicht, wenn ich dieses Gefühl habe.

Abb. 12: Sei vorsichtig!

SEI VORSICHTIG!

Diese Person wird erpresst – etwas aus ihrer privaten Vorgeschichte wurde veröffentlicht. Sie hat einen Fehler auf einer Social-Media-Plattform gemacht.

Abb. 13: Phishing



PHISHING

Daten werden mittels Phishing-Angriffen gestohlen. Man kann versuchen, sich mit Hilfe von Antivirus- und sonstigen Programmen zu schützen, doch das schützt einen nicht vor Profis.

Wenn einem bewusst ist, dass man beobachtet wird, ist das ein gutes Zeichen, das einen zu genauerem Achten auf Risiken und einer vorsichtigeren Herangehensweise motivieren kann, wenn man online ist. Das Verstehen der spezifischen Bedrohung durch Phishing ist von wesentlicher Bedeutung und wirkt ermutigend. Phishing ist die

heimtückischste Art und Weise, um Schwachstellen von Menschen auszunutzen. Dabei werden Informationen gesammelt und die Angreifer können unbemerkt und ziemlich lange operieren, bevor sie zuschlagen. Wirksame Massnahmen zur Bekämpfung von Phishing-Angriffen müssen darin bestehen, Mitarbeitende zu schulen, so dass sie auf Online-Anfragen mit angemessener Vorsicht reagieren.

2.5. KATASTROPHALE FOLGEN

Die Interviewpartner sahen Cyberangriffe einfach nur als eine andere Form von Einbruch und Eindringen an, wobei – wie beim physischen Einbruch – selbst ein erfolgloser Versuch Schaden anrichtet und beunruhigend ist. Der Vorfall, der den Lieferanten Meier Tobler lahmlegte, schärfte das Bewusstsein für die potenziell katastrophalen Folgen eines derartigen Angriffs. Auch wenn das Unternehmen letztendlich die Betriebstätigkeit wiederherstellen konnte, war der Vermögensschaden erheblich, und die Befragten waren selbst in ihrer tagtäglichen Arbeit betroffen. Interessanterweise zeigten sie zwar volle Unterstützung und Verständnis für die Probleme ihres Geschäftspartners, waren aber offensichtlich irritiert und reagierten ungeduldig darauf, dass die Probleme nicht früher gelöst werden konnten. In der Regel war ihnen sehr bewusst, dass IT-Systeme lahmgelegt werden könnten und welche katastrophalen Auswirkungen dies auf das Geschäft haben würde.

Abb. 14: Modernes Einbrechen und Eindringen

MODERNES EINBRECHEN UND EINDRINGEN

Ein Cyberangriff ist einfach nur eine moderne Form des Einbruchs in eine Privatwohnung. Der normale Schutz reicht nicht aus, um Einbrecher zu stoppen: Schäden gibt es in jedem Fall, und wenn es nur ein eingeschlagenes Fenster ist.

Abb. 15: Angriff auf unseren Lieferanten

ANGRIFF AUF UNSEREN LIEFERANTEN

Unser Lieferant, der voll automatisiert ist, wurde angegriffen. Er konnte sein Geschäft nicht mehr betreiben und hat einen Millionenverlust erlitten. Das könnte auch uns passieren.

Abb. 16: Hoffentlich nicht!

HOFFENTLICH NICHT!

Das Ganze kann uns um die Ohren fliegen.

Das Bewusstsein für die möglichen Folgen von Cyberangriffen bietet einen klaren Ansatzpunkt für Schulungsprogramme. Es wurde auch deutlich, dass der gute Wille gegenüber den von Cyberangriffen betroffenen Handelspartnern begrenzt war. Das lässt vermuten, dass das Zeitfenster für die Wiederherstellung, bevor es zu einer langfristigen Beeinträchtigung der Geschäftsbeziehungen kommt, relativ klein sein kann. Im Falle eines Angriffs ist es daher entscheidend, den Geschäftsbetrieb so schnell wie möglich wiederherzustellen.

2.6. DAS BETRIFFT MICH NICHT

Die Befragten erkannten zwar ihre individuellen Anfälligkeiten, schrieben sich jedoch zugleich einen geringen Stellenwert zu und hielten es daher für unwahrscheinlich, dass sie unerwünschte Aufmerksamkeit erregen würden. In einem gewissen Umfang galt diese Denkweise auch für das Unternehmen, in dem sie arbeiten. Im Vergleich zu multinationalen Unternehmen wurden die KMU als zu klein angesehen. Die Interviews enthüllten auch das unterschwellige Gefühl, dass die Gefahren überbewertet werden könnten und dass die Angst vor Angriffen unter Umständen unnötige und möglicherweise schädliche Schutzmassnahmen nach sich zieht. Sollte das Unternehmen jedoch angegriffen werden, würden externe Dienstleister Lösungen und Fachkenntnisse bereitstellen, um das Problem zu beheben – so wie eine gute Krankenschwester in einem gut ausgestatteten Krankenhaus Patienten behandelt. Vor allem dieser Vergleich deutet auf eine potenzielle systemische Schwachstelle hin. Wir begeben uns bereitwillig in die Obhut von Ärzten und Krankenschwestern und würden uns nicht selbst medikamentös behandeln, wenn es uns ernsthaft schlecht geht. Ebenso können wir annehmen, dass es automatisch besser ist, Cybersicherheit ausschliesslich in die Hände von Spezialisten zu legen.

Abb. 17: Die ganze Welt verknüpft

DIE GANZE WELT VERKNÜPFT

Sobald wir online sind, sind wir mit der ganzen Welt verbunden und haben Zugang zum gesamten Wissen. Ein sehr positiver Wandel.

Abb. 18: Angst

ANGST

Unbegründete Angst, online könnte etwas passieren, obwohl es relativ sicher ist. Übermässiger Schutz ist unnötig.

Abb. 19: Persönliche Unterstützung

PERSÖNLICHE UNTERSTÜTZUNG

So fühlt sich ein Unternehmen, wenn es angegriffen wird: wie jemand, der krank ist und zur Behandlung externe Experten und Spezialgeräte benötigt.

Die Vorstellung, zu klein und unbedeutend zu sein, um ins Visier von Cyberkriminellen zu geraten, ist vielleicht der beunruhigendste Aspekt der Denkweise vieler KMU-Mitarbeitenden. Auch wenn Einzelpersonen nicht das eigentliche Ziel eines Angriffs sind, können sie unwissentlich das schwächste Glied in der Kette sein, wenn Cyberkriminelle über sie auf die Systeme eines Unternehmens zugreifen können. Kleine KMU befinden sich vielleicht nicht in der direkten Schusslinie, aber sie können dennoch das Ziel von Kriminellen werden. Verlässt man sich zu sehr auf die Fachkenntnisse Dritter, so kann dies das Problem und seine Lösung auch aus der individuellen Verantwortung verbannen. Dies wiederum führt zu weiteren Einschränkungen des Wahrnehmens von Cyber-angriffen und zur Verschlechterung der Reaktionsfähigkeit im Fall eines Angriffs.

2.7. PROAKTIV UND ENGAGIERT

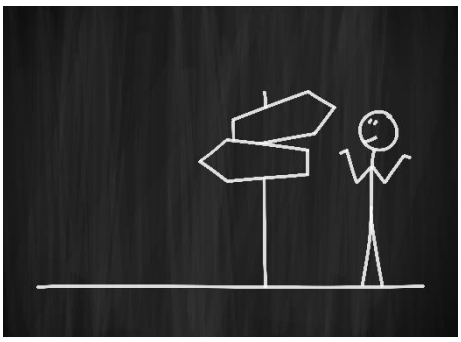
Bei der Diskussion über mögliche Angriffe und Betriebsstörungen zeigten die Befragten eine bemerkenswerte Bandbreite an Reaktionen. Anstatt sich lähmen zu lassen, äusserten sie Begeisterung für die Problembewältigung und eine vorwärts gerichtete Haltung. So wurde eine «nebelige Strasse», die für begrenzte Informationen stand, zu einer Metapher für das Bestreben, trotz aller Widrigkeiten den richtigen Weg zu finden. Und ein leeres Strassenschild wurde zum Symbol für die Notwendigkeit, eine Lösung zu entwickeln. Zahlreiche Tools, die auf älteren Technologien und Workflows basieren, können verwendet werden, um den Betrieb des Unternehmens auch im Falle einer Störung aufrechtzuerhalten.

Abb. 20: Nebel

NEBEL

Bei Cyberangriffen ist alles unklar, aber ich will diesen Weg weiterverfolgen und zu einer Lösung finden. Ich habe keine Angst vor dem, was sich im Nebel verbirgt, aber ich muss mich vorsichtig bewegen, um auf dem Weg zu bleiben.

Abb. 21: Planung



PLANUNG

Man muss das Schild selbst beschriften, und dafür gibt es keine Standardlösung. Die Schilder weisen in verschiedene Richtungen, da man immer verschiedene Lösungen für das Problem haben kann. Vielleicht muss ich mein privates Mobiltelefon benutzen, wenn die Unternehmenssysteme ausser Betrieb sind.

Abb. 22: Wie früher

WIE FRÜHER

Während des Angriffs auf unseren Lieferanten haben wir wie in alten Zeiten wieder zu Telefon, Kugelschreiber und Papier gegriffen. Das funktionierte relativ gut, obwohl alle Buchhaltungsinformationen im System gespeichert waren.

Dieser proaktive Denkansatz und der Wunsch, weiterzumachen, sind ein Trumpf für KMU, der vorteilhaft eingesetzt werden kann. Statt auf externe IT-Dienstleister zu warten, um den Normalbetrieb wiederherzustellen, wollten die Mitarbeitenden helfen, den Betrieb aufrechtzuerhalten. Mit etwas Planung und Training dürften Schweizer KMU in der Lage sein, einen Offline-Workflow zu entwickeln, der sich auf die Zusammenarbeit, Energie und Motivation der Mitarbeitenden stützt. Dies würde plötzliche und kritische Unterbrechungen in ihren Interaktionen mit Kunden vermeiden und ihre Fähigkeit erhöhen, den möglichen Folgen eines Cyberangriffs zu widerstehen.

Diskussion

Die von uns befragten Mitarbeitenden vermittelten ein nuanciertes und differenziertes Spektrum an Gefühlen, wenn sie an Cyberangriffe dachten und darüber diskutierten. Es war wenig verwunderlich, dass diese vielfältigen Emotionen inkonsistent, jedoch in den Köpfen der Gruppe gleichzeitig vorhanden waren. Sie lassen sich zu sieben Hauptthemen gruppieren, die in gewissem Masse für alle Befragten gelten. Jedes dieser Themen wurde einzeln in Abschnitt 2 besprochen. Einige Probleme lassen sich weiter nach spezifischen Merkmalen von Mitarbeitenden differenzieren, die im folgenden Abschnitt besprochen werden. Zudem waren wir auch in der Lage, umsetzbare Empfehlungen für KMU und ihre Dienstleister zu entwickeln.

3.1. AUSWIRKUNG NACH MITARBEITERKATEGORIE

Während der Interviews bemerkten wir in Abhängigkeit von der Mitarbeiterkategorie einige weitere Anzeichen für unterschiedliche Einstellungen. Sowohl die Kategorien als auch die Unterschiede sind rein anekdotisch und spiegeln eher unsere Beobachtungen wider, als dass es sich um theoretische oder fundamentale Erkenntnisse handelt. Nichtsdestoweniger denken wir, dass sie unsere Diskussion bereichern können.

3.1.1. Verwaltungspersonal gegenüber Produktionspersonal

Der erste Unterschied wurde zwischen Mitarbeitenden in der Verwaltung und jenen beobachtet, die in der Produktion oder an Kundenstandorten arbeiten. Typischerweise hat das Produktionspersonal nur begrenzten Zugang zu IT-Systemen, meist nur jenen, die mit Fertigungssystemen vernetzt sind. Daher fühlt es sich in der Regel weniger von Cyberangriffen betroffen. Dagegen sind sich die Mitarbeitenden in der Verwaltung der Folgen derartiger Probleme lebhaft bewusst. Sie können sich an Fälle erinnern, in denen ihre Systeme längere Zeit ausgefallen waren, oder an die Auswirkung des Angriffs auf Meier Tobler auf ihre eigene Arbeit. Infolgedessen dürfte das Verwaltungspersonal bereitwillig die Entwicklung von Notfallprozessen unterstützen und diese regelmässig üben.

3.1.2. Alt gegenüber jung

Ein weiterer möglicher Unterschied, auf den von mehreren Befragten hingewiesen wurde, besteht zwischen jüngeren und älteren Mitarbeitenden, wobei impliziert wird, dass ältere Menschen anfälliger für Angriffe sind als jüngere Personen. Jüngere Mitarbeitende sind klar vertrauter mit digitaler Technologie und aktiver auf Social-Media-Plattformen. Ältere Mitarbeitende berichteten, dass sie nicht mit der Technologie aufgewachsen seien und sich noch immer nicht mit ihr vertraut fühlten. Infolgedessen waren sie vorsichtiger in ihrem Ansatz – unter Umständen bewusster im Umgang mit verdächtigen Mitteilungen, zurückhaltender bei der Befolgung von Aufforderungen und eher bereit, um Rat zu fragen, wenn sie unsicher waren, insbesondere in einem geschäftlichen Kontext. Auch wenn es im Rahmen dieser Studie nicht möglich ist, das tatsächliche relative Risikoprofil zu erkennen, deuten die Antworten der Befragten darauf hin, dass die Unterschiede nicht signifikant sind. Jüngere Mitarbeitende sind vertrauter mit der Technologie und sich daher der Risiken bewusster, doch ältere Mitarbeitende zeigen eine Tendenz, die mangelnde Vertrautheit durch grössere Vorsicht auszugleichen.

3.1.3. Experten gegenüber Neulingen

Eine vergleichbare, jedoch abweichende Kategorisierung ist auf der Basis des Niveaus der digitalen Fachkenntnisse möglich. Dabei ergab sich eine gewisse Korrelation mit dem Alter, jedoch wich das Niveau der Fachkenntnisse bei der jüngeren Kohorte vollkommen von der Selbsteinschätzung ab. Je kenntnisreicher die Mitarbeitenden waren, desto zuversichtlicher waren sie auch bezüglich ihrer Fähigkeit, Cyberangriffe zu entdecken und die Systeme wiederherzustellen. Sie neigten zudem dazu, mögliche Schäden als gering einzuschätzen. Weniger kenntnisreiche Mitarbeitende neigten dazu, sich durch Beschränken ihrer Online-Kontakte zu schützen und nur bestimmte Plattformen (z. B. e-Banking) zu benutzen, bei denen ihrer Meinung nach ein Dritter für angemessene Sicherheit sorgte. Es ist schwierig, die tatsächlichen Auswirkungen dieser Unterschiede zu bestimmen. Daher ist nicht klar, ob sich grössere Vertrautheit in Form einer geringeren potenziellen Anfälligkeit

auswirkt. Mitarbeitende, die sich subjektiv für kenntnisreicher halten und daher zuversichtlicher sind, können weniger risikoscheues Verhalten an den Tag legen und sich grösseren Gefahren aussetzen.

3.1.4. Berufliches gegenüber persönlichem Verhalten

Eine weitere Differenzierung betrifft das individuelle Verhalten und scheint durch das Umfeld beeinflusst zu werden (z. B. Arbeit im E-Mail-Umgebung des Unternehmens oder auf einem privaten Gerät). Die Befragten erklärten, dass sie in einer beruflichen Umgebung vorsichtiger seien – teilweise aufgrund externer Kontakte / Interaktionen mit Kunden und teilweise weil sie meinten, dass das Schadenpotenzial grösser sei. Berufliche Umgebungen wiesen zudem eine Tendenz zu mehr Komplexität auf. In den Unterhaltungen fielen häufig die Namen unbekannter Kunden und Partner, was wiederum grössere Sorgfalt auslöste. Mehrere Mitarbeitende erwähnten betrügerische E-Mails von Fake-Kunden oder -Lieferanten, sodass die Abwehrmechanismen eher stark waren. Die Interviews deuteten darauf hin, dass der Ansatz in einer privaten Umgebung weniger wachsam ist. Grund dafür ist zumindest zum Teil, dass die Befragten meinten, sie könnten verdächtige Namen oder Nachrichten leichter erkennen. Zudem hielten sich die meisten Befragten selbst nicht für wichtig genug, um einen Cyberangriff zu rechtfertigen. Diese Unterscheidung kann eine Bedrohung darstellen, wenn diese lockere Einstellung auf eine berufliche Umgebung übertragen wird oder private Geräte gehackt und benutzt werden, um Unternehmenssysteme zu schädigen. Die Wahrscheinlichkeit dieser Bedrohung nimmt noch weiter zu, wenn Mitarbeitende regelmässig von zu Hause aus arbeiten müssen, wie dies beispielsweise während der derzeitigen Corona-Pandemie der Fall ist.

3.2. VERBESSERUNGSVORSCHLÄGE

Unsere Empfehlungen für Verbesserungen basieren auf einigen eindeutigen Beobachtungen aus den Interviews. In der Regel sind Mitarbeitende motiviert und proaktiv; häufig sehen sie Cyberbedrohungen als Problem für Spezialisten an. Spezialisten sind in der Tat erforderlich, doch kann sich jeder an der Entwicklung von Lösungen und der Systemwiederherstellung nach einem Angriff beteiligen. Zudem ist nicht klar, in welchem Masse sich Mitarbeitende des Risikos und der möglichen Folgen für ihre Organisation bewusst sind. Vor diesem Hintergrund empfehlen wir drei Schlüsselfelder für Verbesserungen. Diese Verbesserungen können autonom durch Unternehmen oder Dienstleister im Rahmen ihres Angebots durchgeführt werden. Die Empfehlungen verstehen sich ergänzend zum Standardhinweis an Unternehmen, ihre Infrastruktur und den aktuellen Arbeitstand abzusichern, um den Schweregrad möglicher Angriffe zu mindern. Die Infrastruktur sollte durch angemessene Firewalls sowie physische und Passwortsicherheit gestärkt werden. Zudem sollten Notfallreaktions- und Wiederherstellungspläne entwickelt werden. Die Folgen eines Angriffs können durch Ermitteln und Schützen der wertvollsten Vermögensgegenstände des Unternehmens, die sogenannten «Kronjuwelen», vermindert werden. Bei diesen handelt es sich meist um selbst entwickelte Daten, Kundeninformationen und Produktionsanlagen. Die in dieser Studie genannten Empfehlungen sollen diesem allgemeinen Hinweis mehr Wirkung verleihen, insbesondere für KMU.

3.2.1. Bewusstsein schärfen

Die Mitarbeitenden scheinen sich sowohl der potenziell katastrophalen Folgen von Cyberangriffen als auch ihrer eigenen Anfälligkeit bewusst zu sein, insbesondere im Zusammenhang mit Phishing-Versuchen. Zugleich sehen sie ihr Unternehmen als zu unbedeutend an, um einen Angriff zu rechtfertigen. Cyberangriffe werden auch als Element in einem globalen Kampf angesehen, statt sie näher am eigenen Standort einzuordnen. Natürlich ist diese Einstellung gefährlich, und es gibt nationale Statistiken und verschiedene hinreichend publizierte Fälle, die als Warnung dienen können. Derartige Informationen müssen den Mitarbeitenden direkt und konsistent mitgeteilt werden. Darüber hinaus sollten die Mitarbeitenden regelmässig über die Anzahl misslungener Angriffe auf die IT-Infrastruktur des Unternehmens informiert werden. Zugleich sollten sie daran erinnert werden, was das Unternehmen tut, um sich zu schützen (z. B. durch Upgrading der Firewalls). Die Mitarbeitenden sollten ausserdem an einfache Gewohnheiten erinnert werden, die sie verinnerlichen sollten, um das Risiko zu reduzieren, einem Phishing-Versuch zum Opfer zu fallen. Zudem sollten die Unternehmen die Abwehrmechanismen ihrer Systeme und die Anfälligkeit von Personen testen. Dies ist beispielsweise durch den Einsatz von «Ethical-Hackers» möglich, wenn sich das Unternehmen diese Ausgaben leisten kann, da die Mitarbeitenden mit Hackern sympathisieren, die sich für das Gemeinwohl engagieren. Diese Erkenntnisse sollten dann den Mitarbeitenden mitgeteilt werden, um den Stellenwert ihrer Rolle beim Schutz des Unternehmens zu unterstreichen.

3.2.2. Mitarbeitende befähigen

Es gibt die verbreitete Ansicht, dass Hacker ausgesprochen kenntnisreich und gut ausgerüstet sind, dass die Cyberwelt komplex ist und dass spezialisierte Dienstleister die «Hauptverteidigungslinie» bilden. Auch wenn dies in gewissem Masse zutrifft und professionelle Dienstleister ein Element eines wirksamen Schutz- und Reaktionssystems sind, können sie nicht isoliert arbeiten. Das Outsourcing der Verantwortung für Cybersicherheit an Dritte begünstigt eine gewisse Gleichgültigkeit auf Seiten der Mitarbeitenden, deren Online-Verhalten eine entscheidende Verteidigungslinie gegen Angriffe darstellt. Mitarbeitende von KMU neigen zudem zu proaktivem Handeln und wollen mitkämpfen. Neben dem Schärfen des Bewusstseins für ihre Rolle, sollten die Mitarbeitenden ermutigt werden, sich an der Aufdeckung und Mitteilung von Angriffen zu beteiligen, und in die Entwicklung von Lösungen eingebunden werden (siehe Abschnitt 3.2.3 unten). Externe Dienstleister sollten gebeten werden, die Mitarbeitenden anzuleiten und so intensiv wie möglich zu beteiligen.

3.2.3. Wiederherstellungsmodus üben

Im Fall eines Angriffs oder – was häufiger vorkommt – bei einer Systemstörung wissen die Mitarbeitenden unter Umständen nicht, wie sie reagieren sollen. Ihre Reaktionen sollten jedoch nicht improvisiert sein oder ad-hoc erfolgen. Derartige Szenarios sollten im Voraus geplant werden, wobei hilfreiche Tools bereitgestellt und vorher festgelegte Trigger für Notfallprozeduren klar definiert werden. Unsere Interviews deuteten darauf hin, dass insbesondere der Zugang zu Kunden-, Rechnungs- und technischen Produktdaten unter Umständen nur schwer möglich ist, wenn offline gearbeitet wird. Dieses Problem muss sorgfältig behandelt werden. Die Entwicklung eines Nicht-IT-Szenarios kann auch eine Gelegenheit für Teambildungsarbeit und den optimalen Einsatz der Fachkenntnisse jedes Mitarbeitenden sein. So können Unternehmen beispielsweise einen Workshop initiieren, in dessen Rahmen Mitarbeitende versuchen, ihre tagtäglichen Arbeiten ohne die üblichen IT-Tools zu erledigen. Auf diese Weise werden sie schnell erfahren, welche Informationen entscheidend sind und über Offline-Systeme bereitgestellt werden müssen, welche Aufgaben auf privaten Geräten erledigt werden können und was auf Papier aufbewahrt werden muss. Derartige Tools können im Normalbetrieb entwickelt und regelmässig unter realen Notfallbedingungen getestet werden, für den Fall, dass das Geschäft ohne die Standard-IT-Infrastruktur auskommen muss. Der Betrieb im Wiederherstellungsmodus sollte exakte, vorher festgelegte Trigger haben, die vom betroffenen System und der Ausfalldauer abhängen.

Abb. 23: Verbesserungsvorschläge

VERBESSERUNGSVORSCHLÄGE

VORBEREITEN

BEWUSSTSEIN SCHÄRFEN

MITARBEITENDE BEFÄHIGEN

WIEDERHERSTELLUNGSMODUS ÜBEN

Fazit

Cyberangriffe sind ein signifikantes und wachsendes Problem, und die Schweizer KMU sind von dieser Entwicklung nicht ausgenommen. In den letzten Jahren ist die Zahl der gezielten Ransomware-Angriffe gewachsen. Schweizer KMU waren ausserdem zunehmend von anderen Schadsoftware-Angriffen betroffen. Neben einer gut geplanten und auf dem neusten Stand gehaltenen IT- Infrastruktur sind das Bewusstsein und aufmerksames Online-Verhalten der Mitarbeitenden kritische Elemente jedes Abwehrmechanismus, da Cyberangriffe typischerweise mit einer Infiltration der IT-Systeme durch Phishing-Angriffe beginnen. Diese Angriffe nutzen menschliche Schwächen aus, um an Passwörter und sonstige kritische Informationen zu gelangen. Phishing ist fast ein Dauerphänomen, und es können mehrere Monate zwischen einem erfolgreichen Phishing-Versuch und dem tatsächlichen Angriff vergehen, was das Rückverfolgen und die Rückmeldung an die Mitarbeitenden erschwert. Das «normale» Niveau des Bewusstseins und des Online-Verhaltens von Mitarbeitenden ist daher der signifikanteste Indikator für Anfälligkeiten gegenüber Phishing-Angriffen.

Für diese Studie haben wir mehrere Mitarbeitende aus drei Schweizer KMU befragt, um ihre Ansichten zu Cyberangriffen zu verstehen. Unsere Untersuchung stützte sich auf den «Tiefen-Metaphern»-Ansatz, um die Gefühle und versteckten Antriebskräfte von Mitarbeitenden im Hinblick auf die Bedrohung durch Cyberkriminalität an die Oberfläche zu bringen. Die Antworten wurden zu allgemeinen Themenkomplexen gebündelt, die das breite Spektrum an Gedanken und Gefühlen im Zusammenhang mit der digitalen Welt hervorheben. Die Mitarbeitenden sahen Cyberangriffe im breiteren Kontext der internationalen Politik und erkannten zugleich die rein finanziellen, kriminellen Motive hinter den meisten Angriffen. Sie sahen Hacker als geschickte und gut ausgerüstete Computernutzer an, nahmen sie jedoch nicht immer als negative Kraft wahr. Sie fühlten sich anfällig und hilflos gegenüber Cyberangriffen und erkannten den möglichen Schaden, den sie verursachen können. Zugleich neigten sie dazu, ihr Unternehmen und sich selbst als zu klein anzusehen, um zum Ziel zu werden, und vertrauten auf Dritte, wenn es um den Schutz im Fall eines Angriffs ging. Grundsätzlich zeigten sie sich jedoch proaktiv und interessierten sich für die Mitarbeit an der Entwicklung praktischer Lösungen.

Wir haben drei umsetzbare Empfehlungen für KMU unterbreitet, um die bisherigen allgemeinen Empfehlungen für Cybersicherheit zu optimieren. Diese dienen dazu, die positiven Elemente der vorherrschenden KMU-Kultur optimal zu nutzen und die riskanteren Elemente in den Griff zu bekommen. Weitere Informationen zur Schärfung des Bewusstseins sind notwendig; dies gilt auch für die Bereitstellung geeigneter Tools, um den Übergang zu einer direkteren Verantwortung der Mitarbeitenden für die Probleme und ihre Lösungen zu begleiten. Zudem müssen die Unternehmen Massnahmen für den Fall eines Systemausfalls planen und einüben. Weiterführende Untersuchungen sollten prüfen, ob es Unterschiede zwischen Mitarbeitenden gibt, die auf Phishing-Angriffe reagieren, und solchen, die dies nicht tun, ob Mitarbeitende grosser Organisationen ähnliche Verhaltensweisen im Hinblick auf Cybersicherheit aufweisen und ob die von uns hier empfohlenen Massnahmen die Bedrohung durch Cyberangriffe mindern.

Literaturverzeichnis

Allianz (2020). *Allianz Risk Barometer 2020*. (zuletzt aufgerufen am 25. November 2020) https://www.agcs.allianz.com/news-and-insights/news/allianz-risk-barometer-2020-de.html

Anz P. (2020). *Daten aus Cyber-Attacke auf Stadler Rail veröffentlicht*. (zuletzt aufgerufen am 25. November 2020) https://www.inside-it.ch/de/post/daten-aus-cyber-attacke-auf-stadler-rail-veroeffentlicht-20200529

Borkert S. (2020). *Bankrott auch mit Cyberangriff begründet: Wurde Mörschwiler Swisswindows in den Ruin gehackt?*. (zuletzt aufgerufen am 25. November 2020) https://www.tagblatt.ch/wirtschaft/bankrott-auch-mit-cyberangriff-begruendet-wurde-moerschwiler-swisswindows-in-den-ruin-gehackt-ld.1198956

Christensen G.L. and Olson J.C. (2002). Mapping Consumers' Mental Models with ZMET. *Psychology and Marketing*, Band 19 (6): 477-502. doi: 10.1002/mar.10021

Damasio A. R. (1994). Time-locked multiregional retroactivation: A systems level proposal for the neural substrates of recall and recognition. In P. D. Eimas & A. Galaburda (Eds.), *Neurobiology of cognition* (Seiten 24–62). Cambridge, MA: MIT Press.

De Moura G. et al. (2020) *Cybersecurity Leadership Principles Lessons learnt during the COVID-19 pandemic to prepare for the new normal*. World Economic Forum (zuletzt aufgerufen am 25. November 2020) https://www.weforum.org/reports/cybersecurity-leadership-principles-lessons-learnt-during-the-covid-19-pandemic-to-prepare-for-the-new-normal

Dreissigacker A., von Skarczinski B. und Wollinger G.R. (2020).*Cyberangriffe gegen Unternehmen in Deutschland*. Kriminologisches Forschungsinstitut Niedersachsen e.V., Forschungsbericht 152

Bundesamt für Statistik (2020). *KMU in Zahlen*. (zuletzt aufgerufen am 25. November 2020) https://www.kmu.admin.ch/kmu/de/home/fakten-trends/zahlen-und-fakten%20/kmu-in-zahlen/firmen-und-beschaeftigte.html

Griesser Kym T. (2020). *Nach Cyberangriff: Erpresser erhöhen Druck auf Stadler*. Tagblatt. (zuletzt aufgerufen am 25. November 2020) https://www.tagblatt.ch/wirtschaft/erpresser-erhoehen-druck-auf-stadler-ld.1235844

Damasio A. R. (2020). *So greifen Cyberkriminelle Unternehmen an*. (zuletzt aufgerufen am 25. November 2020) https://www.swisscom.ch/de/magazin/datensicherheit-infrastruktur/cyberangriffe-unternehmen-malware-phishing/

Jochum K. (2019). *Offix von massivem Hacker-Angriff getroffen*. (zuletzt aufgerufen am 25. November 2020) https://www.inside-it.ch/de/post/offix-von-massivem-hacker-angriff-getroffen-20190703

Damasio A. R. (2020). *Schweizer Fensterfirma Swisswindows AG geht nach Ransomware-Angriff pleite*. (zuletzt aufgerufen am 25. November 2020) https://dataloft.ch/security/schweizer-fensterfirma-swisswindows-ag-geht-nach-ransomware-angriff-pleite/

Lüscher A., und Niedermann M. (2019). *Hacker legen Schweizer Grossunternehmen lahm*. SRF (zuletzt aufgerufen am 25. November 2020) https://www.srf.ch/news/wirtschaft/geht-es-um-loesegeld-hacker-legen-schweizer-grossunternehmen-lahm

Luzerner Zeitung (2019). *Cyberattacke gegen Meier Tobler legt Betrieb weitgehend lahm*. (zuletzt aufgerufen am 25. November 2020) https://www.luzernerzeitung.ch/wirtschaft/cyberattacke-gegen-meier-tobler-legt-betrieb-weitgehend-lahm-ld.1138900

Mändli Lerch K. und Repic, A. (2017). *Cyberrisiken in Schweizer KMUs*. (zuletzt aufgerufen am 25. November 2020) https://gfs-zh.ch/wp-content/uploads/2017/12/Schlussbericht_CyberriskKMU_12122017.pdf

Meier Tobler(2020). *Geschäftsbericht 2019 Meier Tobler Group AG*. (zuletzt aufgerufen am 25. November 2020) https://www.meiertobler.ch/de/content/download-file/6534/file/25.02.20%20Gesch%C3%A4ftsbericht%202019.pdf

MELANI (2020a). *Vorsicht: Weiterhin erhöhtes Sicherheitsrisiko durch Ransomware gegen KMUs*. (zuletzt aufgerufen am 25. November 2020) https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/sicherheitsrisiko-durch-ransomware.html

MELANI (2020a). *Halbjahresbericht 2020/1*. (zuletzt aufgerufen am 25. November 2020) https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/semi-annual-report-2020-1.html

Moser S. (2019). Cyberrisiken – die unterschätzte Gefahr. *Neue Zürcher Zeitung*. 22.05.2019.

Olson J. C., und Reynolds, T. J. (1983). Understanding consumers' cognitive structures: Implications for advertising strategy. In L. Percy & A. G. Woodside (Eds.), *Advertising and consumer psychology* (Seiten 77–90). Lexington, MA: Lexington Books.

Papedis (n. d.). *OFFIX Gruppe*. (zuletzt aufgerufen am 25. November 2020) https://www.papedis.ch/de/unternehmen/offix-gruppe/#:~:text=Mit%20einem%20Jahresumsatz%20von%20gegen,und%20Lieferanten%20in%20der%20Schweiz.

Pugnetti C. und Bekaert X. (2018). *A Tale of Self-Doubt and Distrust. Onboarding Millennials: Understanding the Experience of New Insurance Customers*. ZHAW School of Management and Law

Pugnetti C. und Schneebeli M. (2020). Kundenbedürfnisse und Marktpenetration. Schweizer KMUs unterschätzen die Bedeutung von Dienstleistungen und Versicherungsdeckungen gegen Cyberrisiken. *Schweizer Versicherung*, Januar 2020.

Pugnetti C., Casián C., Staub N. und Ellenberger T. (2019). Cyber-Resilienz steigern. *Schweizer Versicherung*, Januar 2019.

Schäppi M. (2020). *Cyberattacke auf Meier Tobler, Dienstleister der Gesundheitsbranche*. (zuletzt aufgerufen am 25. November 2020) https://www.infosec-health.ch/_Resources/Persistent/77d3731325caf3cb4a5060a02fea716d543be3c3/K_Ref2_Sch%C3%A4ppi_Cyberangriff%20auf%20DL%20der%20Gesundheitsb.pdf

Severin C. (2019). *Wie ein Schweizer KMU ohne Lösegeld, dafür mit Militärtaktik einen Hackerangriff überlebt hat*. (zuletzt aufgerufen am 25. November 2020) https://www.offix.ch/media/cms/Offix/Media/NZZ_Cyber-Angriff%20auf%20KMU_OFFIX-Gruppe.pdf

SIA (2018). *Grundlagenpapier des SVV zu Cyber-Risiken*. Arbeitsgruppe Cyber-Risk, Swiss Insurance Association (zuletzt aufgerufen am 25. November 2020) https://www.svv.ch/sites/default/files/2018-04/Grundlagenpapier%20CyberRisiken_DE.pdf

SRF (2020). *Offenbar zwang eine Cyberattacke Swisswindows in die Knie*. (zuletzt aufgerufen am 25. November 2020) https://www.srf.ch/news/regional/ostschweiz/konkurs-fensterhersteller-offenbar-zwang-eine-cyberattacke-swisswindows-in-die-knie

Stadler Rail (2020a). *Geschäftsbericht 2019*. (zuletzt aufgerufen am 25. November 2020) https://www.stadlerrail.com/media/pdf/web_stadler_rail_gb19_de.pdf

Stadler Rail (2020b). *Cyber-attack against Stadler IT network*. (zuletzt aufgerufen am 25. November 2020) https://www.stadlerrail.com/media/pdf/2020_0507_media%20release_cyber-attack_en.pdf

Trustwave (2020). *2020 Trustwave Global Security Report*. (zuletzt aufgerufen am 25. November 2020) https://www.trustwave.com/en-us/resources/library/documents/2020-trustwave-global-security-report/

Zaltman G. (1997). Rethinking Marketing Research: Putting People Back In. *Journal of Marketing Research*, Vol. 34, 4. https://doi.org/10.1177/002224379703400402.

Zaltman G. und Zaltman L. (2008). *Marketing Metaphoria: What Deep Metaphors Reveal about the Minds of Consumers*. Harvard Business Press.

Tabellen

Abbildungen

Autoren

Dr. Carlo Pugnetti ist Dozent am Institut für Risk & Insurance an der Zürcher Hochschule für Angewandte Wissenschaften. Schwerpunkt seiner Forschung ist das Verhalten von Assekuranz-Kunden, insbesondere Veränderungen, die durch Technologie oder Generationswechsel entstehen. Er untersucht dabei auch die Verbindung zwischen Innovation und Risikomanagement.

Vor seiner Tätigkeit an der ZHAW war Carlo Pugnetti CEO der Allianz Global Assistance in der Schweiz, nachdem er verschiedene Funktionen innerhalb der Allianz Gruppe innehatte: die Restrukturierung der Schadensabteilung bei der Tochtergesellschaft Fireman's Fund in den USA, die Leitung strategischer Projekte für die Konzernentwicklung in München und die Leitung eines internationalen Geschäftsfelds aus Paris. Zuvor hatte er seine Karriere als Berater bei Oliver Wyman gestartet.

Carlo Pugnetti hat einen Ph.D. in Risikoanalyse und einen Master's in Elektroingenieurwesen erworben, beide von der Stanford Universität.

Carlos Casián ist Sach und Cyber Risk Underwriter bei Allianz Suisse. Er führt regelmässig interne und externe Schulungen durch und nimmt an Podiumsdiskussionen teil. Er ist Sprecher der Allianz Suisse in Sachen Cyber Risk und vertritt das Unternehmen in der Arbeitsgruppe Cyber Risk beim Schweizerischen Versicherungs-verband.

Carlos hat das Assekuranzgeschäft von der Pike auf gelernt und begann seine berufliche Laufbahn vor mehr als einem Jahrzehnt bei Allianz Suisse. In den letzten Jahren beschäftigte er sich vertieft mit Cyberrisiken und ihren Auswirkungen auf die Risikoprofile von Unternehmen.

Carlos hält einen BSc in Business Administration mit Vertiefung in Risk & Insurance der ZHAW.

Partner

Unser aufrichtiger Dank gilt unseren Partnerunternehmen, die uns Zugang zu ihren Mitarbeitenden gewährten und die Studie unterstützten.

Kurt Wyss, Partner
VTL Insurance + Partner AG

www.vtl.ch

Sokol Prendi, Head of Sales
Dätwyler Fertigungs-Technologie AG

www.daetwylerag.ch

Manuel Fischer, CEO
Fischer Wärmetechnik AG

www.heizprofi.ch

Terence Iseli, CEO
ISELI ENERGIE AG

www.iseli-energie.ch

Xavier Bekaert, Partner
Benthurst & Co.

www.benthurst.com

School of Management and Law

St.-Georgen-Platz 2
Postfach
8401 Winterthur
Schweiz

www.zhaw.ch/sml

AACSB ACCREDITED

swissuniversities