Cybersecurity in der unternehmerischen Praxis des Mittelstandes

Andreas Beyer

A. Cyberangriffe und -risiken in mittelständischen Unternehmen

„There is no glory in prevention.", sagte der Virologe Christian Drosten im März 2020 im Zusammenhang mit der Verbreitung des Coronavirus. Der Grundsatz, dass man durch die Vermeidung von Risiken keinen Ruhm erlangt, trifft – wie dieser Beitrag zeigen wird – auch auf den bisherigen Umgang von kleinen und mittelständischen Unternehmen mit dem Thema Cybersecurity zu. Doch ist eine langfristige Strategie zur Risikominimierung sowohl in der Coronapandemie als auch für eine sichere IT-Infrastruktur erfahrungsgemäß der Schlüssel zum Erfolg.

Die fortschreitende Digitalisierung birgt Gefahren und potenzielle Risiken für Unternehmen. So drohen Unternehmen weltweit innerhalb eines Zeitraums von fünf Jahren gigantische Mehrkosten und Umsatzverluste durch Cyber-Angriffe in Höhe von rund 5,2 Billionen Dollar.[1] Dementgegen erscheint das Bewusstsein insbesondere von kleinen und mittelständischen Unternehmen[2] für Cybersecurity und die damit verbundene Vermeidung von Risiken für die IT-Infrastruktur und den fortlaufenden Betrieb eines Unternehmens oftmals noch nicht ausgeprägt genug. Zwar erkennen bereits ca. zwei Drittel der mittelständischen Unternehmen die Gefahr und das Risiko von Cyberkriminalität grundsätzlich an, jedoch sehen lediglich ca. ein Drittel ein solches Risiko für ihren eigenen Betrieb.[3]

---

1 *Abbosh/Bissel*, Accenture Studie "Securing the digital economy", S. 16, https://www.accenture.com/us-en/insights/cybersecurity/_acnmedia/Thought-Leadership-Assets/PDF/Accenture-Securing-the-Digital-Economy-Reinventing-the-Internet-for-Trust.pdf#zoom=50 (abgerufen am 29.12.2020).

2 Im Folgenden: KMU.

3 Gesamtverband der deutschen Versicherungswirtschaft (GDV): Cyberrisiken im Mittelstand, 2020, S. 6, https://www.gdv.de/resource/blob/61466/0456901217b39a5893bc6829b8d7d156/report-cyberrisiken-im-mittelstand-2020-data.pdf (abgerufen am 12.04.2021).

Dieses mangelnde Bewusstsein ist problematisch, weil gerade KMU zunehmend von Cyberangriffen betroffen sind.[4]

Um auf dem Markt wettbewerbsfähig zu bleiben, können sich KMU der fortschreitenden Digitalisierung nicht entziehen. Dabei nimmt die Abhängigkeit der KMU von IT-Systemen und -strukturen stetig zu.[5] Gleichzeitig werden Angriffe auf die Informationsstrukturen im Cyberraum zunehmend komplexer und umfangreicher.[6] Eine sichere IT-Infrastruktur und wirksame Maßnahmen zur Prävention von Cyberangriffen werden somit auch für diese Unternehmen immer wichtiger. Jedes vierte mittelständische Unternehmen war bereits von erfolgreichen Cyberangriffen betroffen.[7] Bei einer Forsa-Umfrage im Auftrag des Gesamtverbands der deutschen Versicherungswirtschaft e.V. (GDV) gaben mehr als die Hälfte (59 %) der betroffenen Unternehmen an, sie hätten in Folge der Cyberangriffe unter Betriebsausfällen gelitten.[8] Solche Unterbrechungen der Betriebsabläufe stellen gemeinsam mit den damit verbundenen Kosten für die Wiederherstellung der Daten und IT-Systeme die regelmäßige Folge von Cyberangriffen dar.[9]

Der Begriff der Cybersecurity umfasst vor allem die Einhaltung von technischen und organisatorischen Maßnahmen, die für den Schutz des Unternehmens, der Arbeitnehmer, der Kunden sowie der Lieferanten vor Angriffen von außen erforderlich sind.[10] Art. 32 DSGVO stellt dabei die zentrale gesetzliche Grundlage dar. Hiernach sind Unternehmen, die selbst oder im Auftrag eines Anderen personenbezogene Daten verarbeiten insbesondere dazu verpflichtet, die zum Schutz der Daten angemessenen

4 Bitkom-Studie Wirtschaftsschutz 2020, S. 8, https://www.bitkom.org/sites/default/files/2020-02/200211_bitkom_studie_wirtschaftsschutz_2020_final.pdf (abgerufen am 13.01.2021); *Meyer, Seitz*, Deloitte Studie: Cybersecurity im Mittelstand, Download unter: https://www2.deloitte.com/de/de/pages/mittelstand/contents/cyber-security-im-mittelstand-studie.html (abgerufen am 13.01.2021).

5 GDV: Cyberrisiken im Mittelstand 2020 (Fn. 3), S. 7.

6 *Schuster*, Cyberangriffe werden immer komplexer, https://www.it-business.de/cyberangriffe-werden-immer-komplexer-a-798881/ (abgerufen am 13.01.2021).

7 Gesamtverband der deutschen Versicherungswirtschaft (GDV): Cyberrisiken im Mittelstand, 2019, S. 5, https://www.gdv.de/resource/blob/48506/a1193bc12647d526f75da3376517ad06/cyberrisiken-im-mittelstand-2019-pdf-data.pdf (abgerufen am 20.04.2021).

8 GDV: Cyberrisiken im Mittelstand 2019 (Fn. 7), S. 5.

9 *Dreißigacker u.a.*, PWC Studie: Cyberangriffe gegen Unternehmen in Deutschland, S. 36 ff., https://www.pwc.de/de/cyber-security/cyberangriffe-gegen-unternehmen-in-deutschland.pdf (abgerufen am 13.01.2021).

10 *Wybitul*, Vermeidung von DS-GVO-Risiken nach Datenpannen und Cyberangriffen, NJW 2020, 2577.

technischen und organisatorischen Maßnahmen zu treffen. Eine wirksame Minimierung von Risiken im Zusammenhang mit Cyberattacken ist daher das wesentliche Element für eine sichere und unterbrechungsfreie IT-Infrastruktur. Hierbei stellen die Identifikation, die Beurteilung und der korrekte Umgang mit den jeweiligen Risiken die zentrale Herausforderung für kleine und mittelständische Unternehmen dar.

Der Verfasser leitet als Syndikusrechtsanwalt die Rechtsabteilung der Vimcar GmbH[11], einem mittelständisches Berliner Tech-Unternehmen, welches zu den 20 wachstumsstärksten Tech-Unternehmen Deutschlands zählt und auf dem Markt für digitale Flottenmanagementlösungen für Unternehmen tätig ist.[12] Zuvor leitete er die Rechtsabteilung der VAI Trade GmbH, einem Fintech-Startup und Tochterunternehmen der Berliner Volksbank eG. Die Erkenntnisse aus diesen Tätigkeiten und der damit einhergehenden juristischen Betreuung des Themas Cybersecurity sowie kontinuierlichem Austausch mit der Geschäftsführung und dem CTO von Vimcar, geben diesem Beitrag fachliche und praktische Relevanz.

Im Folgenden werden zunächst einige ausgewählte und häufig vorkommende Cyberangriffe und -risiken von außen und innen näher beleuchtet (I.). Anschließend werden Lösungsansätze und Präventionsstrategien dargelegt, die kleine und mittelständische Unternehmen dabei unterstützen können, mit dem wichtigen Thema der Cybersecurity umzugehen und die Risiken weit wie möglich zu minimieren (II.). Schließlich wird dieser Beitrag aufzeigen, dass der Umgang mit dem Thema Cybersecurity nicht nur Aufgabe der Rechts- oder IT-Abteilungen ist (III.). Vielmehr stehen insbesondere die Geschäftsleitungen der Unternehmen in der Pflicht, entsprechende Strukturen zu schaffen und Budgets freizugeben.

I. Cyberangriffe und -risiken von außen

Die Häufigkeit und Qualität der Cyberangriffe von außen hat in den letzten fünf Jahren enorm zugenommen. In den Jahren 2015 und 2017 waren circa 50 % der im Rahmen einer Bitkom-Studie zum Wirtschaftsschutz befragten Unternehmen von Angriffen wie Datendiebstahl, Industriespiona-

11 Im Folgenden: Vimcar.

12 Deloitte, Winners of the 2020 Technology Fast 50 Award, https://www2.deloitte.com/de/de/pages/technology-media-and-telecommunications/articles/fast-50-2020-germany-winners.html (abgerufen am 17.04.2021).

ge oder Sabotage betroffen; im Jahre 2020 waren es bereits 75 % der befragten Unternehmen.[13]

1. *Cyberangriffe durch Dritte*

Angriffe mittels einer Schadsoftware stellten im Jahre 2018 mit 53 % die häufigste Form von Cyberangriffen durch Dritte auf deutsche Unternehmen und Institutionen dar.[14] Unter den Begriff Schadsoftware oder Schadprogramme fallen alle Arten von Software, die schädliche Funktionen auf einem Computersystem verursachen können.[15] In 90 % der Fälle von Cyberangriffen durch Dritte mittels Schadsoftware dienten dabei schädliche Anhänge oder Links in E-Mails als Zugangsmöglichkeit.[16] Im Lagebericht des Bundesamts für Sicherheit in der Informationstechnik aus dem Jahre 2019 wurde das „Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware“ sowie die „Infektion mit Schadsoftware über Internet und Intranet“ als massive Risiken mit weiterhin zunehmender Tendenz identifiziert.[17]

a. Ransomware

Das Bundeskriminalamt bezeichnet *Ransomware* in einem aktuellen Report als „die primäre, existenzielle Bedrohung von Unternehmen”.[18] Unter dem Begriff der *Ransomware* sind Schadprogramme zu verstehen, die den Zugriff auf das eigene Computersystem oder die eigenen Dateien durch Datenverschlüsselung einschränken oder verhindern.[19] Die Freigabe der Daten oder des Systems erfolgt in der Regel erst dann, wenn ein vom

13 Bitkom-Studie Wirtschaftsschutz 2020 (Fn. 4), S. 7.
14 BSI, Die Lage der IT-Sicherheit in Deutschland 2019, S. 49, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2019.pdf?__blob=publicationFile&v=7 (abgerufen am 27.12.2020).
15 BSI, Die Lage der IT-Sicherheit in Deutschland 2019 (Fn. 14), S. 11.
16 BSI, Cyber-Sicherheitsumfrage der Allianz für Cybersicherheit 2018, S. 12, https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/ACS/cyber-sicherheits-umfrage_2018.pdf?__blob=publicationFile&v=9 (abgerufen am 20.04.2021).
17 BSI, Die Lage der IT-Sicherheit in Deutschland 2019, (Fn. 14), S. 11.
18 Bundeskriminalamt, Cybercrime, Bundeslagebild 2019, S. 56, zum Download unter: https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/cybercrime_node.html (abgerufen am 03.01.2021).
19 *Beukelmann*, NJW Spezial 2017, 376, 376.

Täter geforderter, als „Lösegeld" bezeichneter Geldbetrag, meist in Form von Kryptowährungen, bezahlt wurde.[20] Bei diesen Schadprogrammen handelt es sich in der Regel um Verschlüsselungstrojaner, die zufällig oder gezielt durch infizierte Anhänge in E-Mails oder durch das Besuchen von vorgetäuschten Websites Zugriff auf Systeme erhalten.[21] Mittlerweile übersteigt die Anzahl der existierenden Varianten von Schadsoftware die Milliardengrenze und täglich kommen durchschnittlich 320.000 neue Schadprogramme hinzu.[22] Der Modus Operandi der Cyberkriminellen besteht häufig aus gefälschten Bewerbungsmails auf tatsächlich vom betroffenen Unternehmen geschaltete Stellenanzeigen. Diese E-Mails enthalten als Bewerbungsunterlagen getarnte Anhänge, die beim Herunterladen und Öffnen der Dateien Verschlüsselungstrojaner aktivieren.[23] Der Umstand, dass das Unternehmen infolge eines erfolgreichen Angriffs bis zur möglichen Lösegeldzahlung keinen Zugriff auf gespeicherte Daten hat, kann im schlimmsten Falle enorme Auswirkungen auf die gesamte unternehmerische Existenz haben.[24] Potenzielle Folgen sind dabei Eigenschäden wie Betriebsunterbrechungen und Reputationsschäden sowie Fremdschäden, die infolge der Nichterfüllung vertraglicher Verpflichtungen gegenüber Dritten entstehen.[25] Seit dem Jahr 2016 ist ein eindeutiger Trend zu einem kontinuierlichen Anstieg der Risiken durch *Ransomware* zu beobachten.[26]

WannaCry ist wohl die weltweit bekannteste *Ransomware*, welche seit Jahren erhebliche Schäden anrichtet. Sie infizierte im Mai 2017 innerhalb weniger Stunden hunderttausende Computer und erreichte in den folgenden Monaten nach Einschätzung der europäischen Ermittlungsbehörde Europol weltweit ein „beispielloses Ausmaß".[27] Neben Verbrauchern sowie kleinen und mittleren Unternehmen waren auch Großkonzerne, wie

---

20 *Salomon*, MMR 2016, 575, 575; *Wabnitz/Janovsky,* WirtschaftsStrafR-HdB, 6. Kapitel. Geldwäsche, 5. Aufl. 2020 Rn. 29c.

21 *Siller*, Definition Trojaner, in: Gablers Wirtschaftslexikon, https://wirtschaftslexikon.gabler.de/definition/trojaner-53413 (abgerufen am 20.04.2021).

22 BSI, Die Lage der IT-Sicherheit in Deutschland 2020, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf?__blob=publicationFile&v=2 (abgerufen am 04.01.2020).

23 *Ceffinato*, NZWiSt 2016, 464, 467.

24 *Salomon* (Fn. 20), 575.

25 BSI, Ransomware Bedrohungslage, Prävention und Reaktion 2019, S. 8, zum Download unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware.html (abgerufen am 19.04.2021).

26 BSI, Die Lage der IT-Sicherheit in Deutschland 2019 (Fn. 14), S. 17.

27 *Dörner*, Was steckt hinter dem Wanny-Cry-Angriff?, https://t3n.de/news/wannacry-podcast-823684/ (abgerufen am 12.01.2021).

Renault oder FedEx, Regierungsbehörden, wie z.B. das russische Innenministerium oder der britische National Health Service mit seinen Krankenhäusern betroffen. Bei der Deutschen Bahn sorgte die Schadsoftware für einen Ausfall der Anzeigetafeln.[28] Auch 2019 noch soll *WannaCry* weltweit für 23,56 % aller *Ransomware*-Attacken verantwortlich gewesen sein und verursachte dabei Schäden in Höhe von ca. 4 Milliarden US-Dollar.[29] Rund zwei Drittel der betroffenen Nutzer fingen sich dabei die *Ransomware* über Spam- oder *Phishing*-E-Mails ein.[30] Die *WannaCry Ransomware* ist so programmiert, dass sie sich nach einer initialen Infektion ohne Zutun eines Nutzers in einem Netzwerk von einem Computer zum anderen ausbreitet und Systeme gezielt verschlüsselt. Dies kann insbesondere in Netzwerken von Unternehmen und Organisationen zu großflächigen Systemausfällen führen.[31]

Ein aktuelles Beispiel für Angriffe auf Unternehmen mittels *Ransomware* stellt der Cyberangriff auf die Funke-Mediengruppe im Dezember 2020 dar. Dabei verschlüsselte die Schadsoftware sämtliche IT-Systeme. Infolgedessen litt die Funke-Mediengruppe mehrere Wochen unter den Folgen der Attacke. Es konnten weder E-Mails empfangen werden, noch funktionierte die Telefonanlage. Daher mussten zunächst alle genutzten IT-Systeme bundesweit heruntergefahren werden.[32] Von den Angriffen waren alle großen Standorte der Funke-Mediengruppe betroffen. Zur Funke-Mediengruppe gehören insgesamt zwölf Regionalzeitungen, darunter die „Berliner Morgenpost" und das „Hamburger Abendblatt". Alle Ausgaben dieser Zeitungen konnten nur sehr eingeschränkt erscheinen.[33] Der Weg zu einer wieder störungsfreien IT stellte sich beinahe als Sisyphus-

28 *Briegleb*, WannaCry: Was wir bisher über die Ransomware-Attacke wissen, https://www.heise.de/newsticker/meldung/WannaCry-Was-wir-bisher-ueber-die-Ransomware-Attacke-wissen-3713502.html (abgerufen am 12.01.2021).

29 *Dörner*, Was steckt hinter dem Wanny-Cry-Angriff? (Fn. 27).

30 *Brien*, Ransomware reloaded: Wanna Cry verursacht immer noch Schäden in Milliardenhöhe, https://t3n.de/news/ransomware-reloaded-wannacry-1240246/ (abgerufen am 12.01.2021).

31 BSI, Weltweite Cyber-Sicherheitsvorfälle durch Ransomware, https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2017/PM_WannaCry_13052017.html (abgerufen am 12.01.2021).

32 Wilkens, Trojaner-Angriff auf Funke-Mediengruppe dauert an – Notausgaben am Kiosk, https://www.heise.de/news/Trojaner-Angriff-auf-Funke-Mediengruppe-dauert-an-Notausgaben-am-Kiosk-4999342.html (abgerufen am 12.01.2021).

33 Thier, Hacker greifen Funke-Mediengruppe an – Erpressungsversuch vermutet, https://www.nzz.ch/technologie/hacker-greifen-funke-mediengruppe-an-ld.1593670 (abgerufen am 04.01.2021).

Arbeit heraus, da 6000 potenziell infizierte Rechner infrage kamen, die jeweils einzeln sehr aufwändig überprüft werden mussten. Die kolportierten Meldungen zu einer Lösegeldforderung in Form von Bitcoin ließ sowohl die Funke-Mediengruppe als auch die Staatsanwaltschaft unkommentiert.[34]

Die Zahlung von Lösegeld im Rahmen eines Cyberangriffs mittels *Ransomware* stellt sich als nicht unproblematisch dar. Zum einen können Unternehmen nicht mit absoluter Sicherheit davon ausgehen, dass die Täter die Unternehmensdaten und -systeme nach Zahlung des Lösegelds tatsächlich entschlüsseln.[35] Zum anderen birgt die Zahlung des Lösegelds zumindest die Möglichkeit, sich gemäß § 129 Absatz 1 Satz 2 StGB wegen Unterstützung einer kriminellen Vereinigung strafbar zu machen. Nach der wohl herrschenden Meinung in Rechtsprechung und Schrifttum liegt eine Verwirklichung des Straftatbestandes durch die Lösegeldzahlung vor. Diese ist weder durch den rechtfertigenden Notstand gemäß § 34 StGB gerechtfertigt, noch ist sie gemäß § 35 StGB entschuldigt, weil durch die Cyberangriffe in aller Regel keine Gefahr für Leib, Leben oder Freiheit eines Menschen besteht. Die herrschende Meinung wendet bisher die sogenannte Mitläufer-Klausel gemäß § 129 Abs. 6 StGB an. Diese gibt vor, dass „bei Beteiligten, deren Schuld gering und deren Mitwirkung von untergeordneter Bedeutung ist, von einer Bestrafung [...] abgesehen werden kann." Die Voraussetzungen dieser Klausel sind in den Fällen verschlüsselter IT-Systeme von Unternehmen regelmäßig gegeben, da die finanzielle Unterstützung ebenso wie die Schuld durch die Drucksituation als vergleichsweise gering anzusehen ist.[36] Die Klausel verhindert allerdings nur die Bestrafung, nicht aber den Schuldspruch und die Kostenfolge des § 465 StPO. Parallel dazu eröffnet die Mitläufer-Klausel die Möglichkeit eines Absehens von der Verfolgung gem. § 153b StPO.[37] Allerdings ist dies für die o.g. Fallkonstellation nicht höchstrichterlich entschieden, sodass Unsicherheiten in Bezug auf die strafrechtliche Bewertung bestehen bleiben. Zudem laufen Unternehmen durch die Bereitschaft zur Lösegeldzahlung Ge-

34 *Linde/Renner*, Hackerangriff auf Funke-Mediengruppe "hält unvermindert an" – Lösegeldforderung soll eingegangen sein, https://www.handelsblatt.com/technik/it-internet/cyberkriminalitaet-hackerangriff-auf-funke-mediengruppe-haelt-unvermindert-an-loesegeldforderung-soll-eingegangen-sein/26753992.html?ticket=ST-2610008-2L4DLvqXCdDycWJOyICv-ap1 (abgerufen am 12.01.2021).

35 Wie z.B. bei der Ransomware *GermanWiper* vgl. Bundeskriminalamt (Fn. 18), S. 5.

36 *Salomon* (Fn. 20), 577.

37 *Salomon* (Fn. 20), 577.

fahr, sich für Cyberkriminelle attraktiv zu machen und in der Folge erneut Opfer eines solchen Angriffs durch *Ransomware* zu werden. Aus diesem Grund lässt sich bei von Cyberattacken betroffenen Unternehmen beobachten, dass Fragen der Medien zu etwaigen Lösegeldzahlungen für die Entschlüsselung von Daten regelmäßig unbeantwortet bleiben.[38]

b. Phishing

Unter *Phishing* versteht man Versuche, über gefälschte Websites, E-Mails oder Kurznachrichten an persönliche Daten eines Nutzers zu gelangen, um damit einen Identitätsdiebstahl zu begehen. Ziel dieses Vorgehens ist es, mit den persönlichen Daten beispielsweise Zugang zu unternehmensinternen Systemen zu erhalten, um die dort enthaltenen Daten auszuspähen, zu verschlüsseln oder zu löschen.[39] *Phishing*-Nachrichten werden meist unter dem Deckmantel vertrauenswürdiger Geschäftspartner oder Dienstleister per E-Mail oder Instant-Messaging versandt und fordern den Empfänger auf, auf einer nachgeahmten Webseite oder am Telefon geheime Zugangsdaten preiszugeben. Typisch ist dabei die Nachahmung des Internetauftritts einer vertrauenswürdigen Stelle, etwa der Website eines E-Mail-Dienstleisters, durch die Verwendung des bekannten Corporate Designs. Der Nutzer wird auf einer solchen gefälschten Website etwa dazu aufgefordert, in ein Formular die Passwörter, PINs oder ID-Kennungen für den E-Mail-Dienst oder andere Produkte externer Dienstleister einzugeben. Diese Daten erhalten anschließend die Ersteller der gefälschten Websites. Der jeweilige Nutzer ist sich oftmals auch nach Eingabe der Daten nicht darüber im Klaren, dass die Daten an unautorisierte Personen gelangt sind. Währenddessen können die Phisher die erhaltenen unternehmensinternen Zugänge für ihre Zwecke missbrauchen.[40]

c. Spear-Phishing

Emotet galt bisher als eine der schädlichsten *Ransomwares* weltweit und infizierte auch in Deutschland IT-Systeme zahlreicher Unternehmen und In-

38 *Linde/Renner* (Fn. 34).
39 Auer-Reinsdorff/Conrad IT-R-HdB, § 3 Technische Grundlagen des Internets, 3. Aufl. 2019, Rn. 274.
40 Grützner/Jakob, Compliance von A-Z, 2. Aufl. 2015, P – Phishing.

stitutionen.[41] Im Jahr 2019 waren zahlreiche Behörden und Unternehmen, darunter die Bundesanstalt für Immobilienaufgaben, eine Niederlassung des Industriekonzerns Norsk Hydro, das Kammergericht in Berlin sowie verschiedene Krankenhäuser und lokale Stadtverwaltungen von Angriffen mittels *Emotet* betroffen. BSI-Präsident Arne Schönbohm bezeichnete *Emotet* vor diesem Hintergrund als „König der Schadsoftware".[42]

Emotet war in der Lage, besonders authentisch aussehende *Phishing*-Mails zu verschicken. Dazu las die Schadsoftware Kontaktbeziehungen und E-Mail-Inhalte aus den Postfächern bereits infizierter Systeme aus. Diese Informationen nutzte sie automatisiert zur Weiterverbreitung, sodass die Empfänger fingierte E-Mails von Absendern erhalten, mit denen sie erst kürzlich in Kontakt standen.[43] Aufgrund der korrekten Angabe der Namen und E-Mail-Adressen des jeweiligen Absenders und Empfängers in Betreff, Anrede und Signatur wirkten diese Nachrichten auf viele Empfänger authentisch. In der Folge konnten die Angreifer nahezu perfekte *Phishing*-Mails versenden, die an das gängige Kommunikationsschema des Absenders angepasst waren.[44]

Dieses maßgeschneiderte Erstellen von *Phishing*-Mails wird als *Spear-Phishing* bezeichnet. Mittels *Emotet* und anderer *Spear-Phishing* Software sind Kriminelle bereits in hochgesicherte Netzwerke von Regierungen und Rüstungskonzernen eingedrungen.[45] Wenn diese maßgeschneiderten E-Mails mittels einer Software automatisiert erstellt und in sehr großer

41 BSI, Aktuelle Information zur Schadsoftware Emotet, https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/emotet.html (abgerufen am 05.01.2020); Bundeskriminalamt, Infrastruktur der Emotet-Schadsoftware zerschlagen, https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2021/Presse2021/210127_pmEmotet.html (abgerufen am 12.04.2021).

42 *Beuth*, Wer ist Mummy Spider, https://www.spiegel.de/netzwelt/web/trojaner-emotet-wer-ist-ivan-a-a8bf3c85-cac9-4cb4-8755-d350ff5850f7 (abgerufen am 05.01.2020).

43 BSI, Informationen zur Schadsoftware Emotet, https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Sonderfall-Emotet/sonderfall-emotet_node.html (abgerufen am 12.04.2021).

44 BSI, Maßnahmen zum Schutz vor Emotet und gefährlichen E-Mails im Allgemeinen, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Gefaehrdungen/Malware/Emotet/emotet_node.html (abgerufen am 12.04.2021).

45 *Wellbrock*, Spear Phishing mit Emotet, https://www.psw-group.de/blog/spear-phishing-mit-emotet/6665 (abgerufen am 05.01.2021).

Zahl versendet werden, wird auch von *Dynamit-Phishing* gesprochen.[46] Durch die maßgeschneiderten Inhalte werden Empfänger zum unbedachten Öffnen von schädlichen Dateianhängen oder der in den Nachrichten enthaltenen URLs verleitet. Ist der Computer erst infiziert, laden *Spear-Phishing* Softwares in der Regel weitere Schadsoftware nach, wie z.B. den Banking-Trojaner *Trickbot*. Diese Schadprogramme führen zu Datenabfluss oder ermöglichen den Cyberkriminellen die vollständige Kontrolle über IT-Systeme zu erlangen. In mehreren bekannten Fällen hatte dies große Produktionsausfälle zur Folge, da ganze Unternehmensnetzwerke neu aufgebaut werden mussten.[47] Im Januar 2021 gelang es einem internationalen Team von Strafverfolgungsbehörden schließlich die Infrastruktur, über die die *Emotet* lief, zu übernehmen und zu zerschlagen, wie das Bundeskriminalamt, welches maßgeblich an der Aktion beteiligt war, bekanntgab.[48] Andere *Spear-Phishing*-Softwares sind nach wie vor aktiv und richten nicht unerhebliche Schäden an.[49]

d. Whaling

Whaling ist eine Methode Cyberkrimineller, bei der sie sich als hochrangige Mitarbeiter in einem Unternehmen ausgeben und unternehmenseigene Führungskräfte oder andere wichtige Personen direkt angreifen, um Geld oder vertrauliche Informationen zu stehlen oder sich für kriminelle Zwecke Zugriff auf ihre Computersysteme zu verschaffen.[50]

Wie beim *Spear-Phishing* wird eine individuell angepasste E-Mail verfasst und zumeist an leitende Mitarbeiter eines Unternehmens gesendet. Die E-Mail soll den Eindruck vermitteln, es handele sich bei dem Absender um einen noch höherrangigen Mitarbeiter. Meist wird hierfür die Identität des jeweiligen CEO, CTO oder CFO vorgetäuscht. Die versendeten E-Mails enthalten oftmals Unternehmenslogos oder Links zu betrügerischen Web-

46 *Schmidt*, Achtung Dynamit Phishing: Gefährliche Trojaner-Welle Emotet legt ganze Unternehmen lahm, https://www.heise.de/security/meldung/Achtung-Dynamit-Phishing-Gefaehrliche-Trojaner-Welle-legt-ganze-Firmen-lahm-4241424.html?view=print (abgerufen am 05.01.2021).

47 BSI, Aktuelle Information zur Schadsoftware Emotet (Fn. 41).

48 BKA, Infrastruktur der Emotet-Schadsoftware zerschlagen (Fn. 41).

49 *Auer*, So erkennen Sie E-Mail-Betrüger, https://www.computerwoche.de/a/so-erkennen-sie-e-mail-betrueger,3549545 (abgerufen am 17.04.2021).

50 https://www.kaspersky.de/resource-center/definitions/what-is-a-whaling-attack (abgerufen am 18.12.2020).

sites, die authentisch erscheinen. Cyber-Kriminelle werten soziale Medien und öffentliche Unternehmensinformationen gezielt aus, um ein Profil und einen Angriffsplan zu erstellen. Außerdem nutzen sie in einigen Fällen *Ransomware* und *Rootkits*[51], um Netzwerke zu infiltrieren. Dadurch können sogar E-Mails vom echten E-Mail-Konto des jeweiligen CEO gesendet werden. Da Führungskräfte bzw. „Wale", auf die derartige Angriffe abzielen, innerhalb des Unternehmens hohes Vertrauen genießen und umfassende Zugriffsrechte haben, lohnt sich der Aufwand für Cyberkriminelle, den Angriff möglichst glaubwürdig zu gestalten. Dadurch kommt ein weiteres Element des Social Engineerings[52] ins Spiel: Mitarbeiter werden in aller Regel nur ungern eine Anfrage von jemandem ablehnen, den sie für wichtig halten. Dies kann erhebliche Folgen haben. So überwies ein Mitarbeiter einer Rohstofffirma aufgrund eines *Whaling*-Angriffs 17,2 Mio. US-Dollar in mehreren Tranchen auf ein Bankkonto in China. Er wurde zuvor in E-Mails, die den Anschein machten, als hätte sie sein CEO geschrieben, zu den Überweisungen aufgefordert. Das Unternehmen plante zu diesem Zeitpunkt, nach China zu expandieren, weshalb die Anfrage ausreichend plausibel wirkte.[53]

2. *Cybersecurity in Zeiten der Coronapandemie*

Noch kann keine exakte Prognose darüber getroffen werden, inwieweit eine Pandemie, wie wir sie seit Verbreitung von COVID-19 erleben, auch die Sicherheitskonzepte in Unternehmen in Bezug auf Cybersecurity nachhaltig beeinflussen wird. Eine Befragung von Bitdefender aus dem Jahr 2020 liefert dahingehend erste Erkenntnisse. Im Rahmen der Studie wurden über 6700 Information Security Professionals – Fachleute aus dem Be-

51 Der Begriff Rootkit beschreibt Schadprogramme, die Computer infizieren und dadurch Cyberkriminellen erlauben, verschiedene Programme darauf zu installieren, die ihnen dauerhaften Zugriff auf die jeweiligen Computer ermöglichen. Vgl. *Malenkowich,* Was ist ein Rootkit?, https://www.kaspersky.de/blog/was-ist-ein-rootkit/853/ (abgerufen am 17.01.2021).

52 Bei dieser Vorgehensweise wird das Opfer dazu gebracht, Daten von sich aus einer ihm unbekannten Person mitzuteilen. Mit den dadurch erlangten Daten werden in der Regel missbräuchliche Zahlungen veranlasst. Eine Manipulation des Rechners des Opfers findet dabei nicht statt.
Vgl. Auer-Reinsdorff/Conrad IT-R-HdB, 3. Aufl. 2019, § 27 E-Payment und E-Invoicing Rn. 14.

53 *Rahmati-Georges*, Was ist ein Whaling-Angriff, https://blog.varonis.de/was-ist-ein-whaling-angriff/ (abgerufen am 06.01.2021).

reich der Informationssicherheit – hinsichtlich ihres Umgangs mit der Coronakrise befragt. Dabei gaben 26 % der befragten „InfoSec Professionals" an, dass *Phishing*- und *Whaling*-Attacken aus ihrer Sicht am stärksten zugenommen hätten. Eine Zunahme von *Ransomware*-Angriffen wurde von 22 % der Befragten wahrgenommen. 67 % der im Rahmen der Studie befragten Führungskräfte gaben an, dass ihre Mitarbeiter kein spezielles Cybersecurity-Training für die Heimarbeit erhalten hätten. Dabei glaubt fast die Hälfte von ihnen (43 %), dass die Häufigkeit und Intensität der Cyber-Attacken weiter zunehmen wird.[54] Dennoch: mehr als die Hälfte der Führungskräfte (55 Prozent) in deutschen Unternehmen nutzt ihre privaten Endgeräte auch im beruflichen Umfeld.[55]

Bereits jetzt kann festgestellt werden, dass Cyberkriminelle durchaus kreativ auf die Pandemiesituation reagieren. So hat das BKA im Laufe des Jahres 2020 Informationen zu mehreren *Phishing*-Kampagnen mit Bezug auf die Pandemie gesammelt. Es existierte beispielsweise über mehrere Wochen eine Website, die sowohl im Design als auch der URL der Website der Investitionsbank Berlin stark ähnelte. Über eine darüber verlinkte *Phishing*-Website konnten die Nutzer ein Online-Formular für die Beantragung von finanziellen Soforthilfen des Landes Berlin für betroffene Unternehmen aufrufen. Ziel dieses Konstrukts dürfte die Erlangung von personen- und unternehmensbezogenen Daten gewesen sein, um damit Folgestraftaten zu begehen.[56] Ähnliche gelagerte Fälle, die mithilfe täuschend echt wirkender E-Mails und Websites verschiedener staatlicher Institutionen in Zusammenhang mit den Soforthilfen des Bundes und der Länder arbeiteten, wurden aus beinahe allen Bundesländern gemeldet.[57]

Laut einer Studie von Unit42, einem Kooperationspartner des European Cybercrime Centers von Europol, sind im Zeitraum Januar bis April 2020 insgesamt 116.357 neu registrierte Domains mit Bezug auf die Pandemie identifiziert worden. Seit dem 12.3.2020 werden täglich ca. 3.000 neue Do-

54 vgl. Bitdefender Study "The indelible impact of Covid-19 on Cybersecurity", https://www.bitdefender.com/files/News/CaseStudies/study/348/Bitdefender-10-IN-10-The-Indelible-Impact-of-COVID-19-on-Cybersecurity.pdf (abgerufen am 24.09.2020).

55 vgl. https://www.crowdstrike.com/blog/securing-a-remote-workforce-in-the-time-of-covid-19/ (abgerufen am 24.09.2020).

56 Bundeskriminalamt, Sonderauswertung, Cybercrime in Zeiten der Coronapandemie, S. 6, Download unter folgendem Link: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeSonderauswertungCorona2019.html (abgerufen am 04.01.2020).

57 BKA, Sonderauswertung, Cybercrime in Zeiten der Coronapandemie (Fn. 57), S. 7.

mains pro Tag registriert. Unit42 stufte dabei 1,74 % der Domains als eindeutig maliziös und über ein Drittel als hochriskant ein. Die Anzahl der maliziösen bzw. der „Hochrisikodomains" sei im Februar und März 2020 um ca. 569 % bzw. 788 % gestiegen. 16 % dieser Domains würden für *Phishing*-Attacken und 84 % für das Hosten verschiedener *Ransomware* genutzt.[58]

II. Cyberangriffe und -risiken von innen

Den größten Risikofaktor im Bereich von Cyberangriffen auf Unternehmen stellt der einzelne Mitarbeiter selbst dar. Cyberangriffe können in der Regel nur Erfolg haben und Schäden für das Unternehmen nach sich ziehen, wenn ein Mitarbeiter durch eigenes Fehlverhalten ermöglicht, dass der jeweilige Angriff zum Erfolg führt.

1. Disgruntled employees

Ist von Cyberangriffen die Rede, vermutet man zunächst unternehmensfremde Menschen oder Hacker im Staatsauftrag dahinter. Dabei geht laut BSI von Innentätern eine größere Gefahr aus, da ihre Angriffe größere Aussicht auf Erfolg hätten. Angreifer hätten „bereits Zugang zu internen Ressourcen einer Organisation und könnten so Schutzmaßnahmen und Schwachstellen über einen langen Zeitraum analysieren".[59] Daher können sich Mitarbeiter als ein großes Risiko für Unternehmen erweisen. Ein Drittel der im Rahmen einer Bitkom-Studie zum Wirtschaftsschutz im Jahr 2020 befragten Unternehmen gab an, bei Cyberattacken von früheren Mitarbeitern vorsätzlich geschädigt worden zu sein.[60] Doch nicht nur (Ex-)Mitarbeiter können ihren Unternehmen Probleme bereiten. Auch externe Dienstleister stellen ein Risiko dar, weil diese durch ihre Tätigkeit

58 *Szurdi, Chen u.a.*, Studying how Cybercriminals Prey on the Covid-19 Pandemic, https://unit42.paloaltonetworks.com/how-cybercriminals-prey-on-the-covid-19-pandemic/ (abgerufen am 04.01.2020).

59 BSI, Glossar der Cybersicherheit, Innentäter, https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/cyberglossar/Functions/glossar.html?cms_lv2=9817288 (abgerufen am 28.12.2020).

60 Bitkom-Studie Wirtschaftsschutz 2020 (Fn. 4), S. 26.

teilweise Einfluss oder direkten Zugang zu internen IT-Systemen des Unternehmens haben.[61]

2. *Cyberrisiken durch geteilte Zugriffsrechte und Remote Devices*

a. Zugriffsrechte

Ein weiteres Risiko liegt im Bereich der Zugriffsrechte für Dateien, Ordner und Festplatten. Häufig haben Mitarbeiter, insbesondere in kleinen Unternehmen, zwischen mehreren Arbeitskollegen geteilte Zugriffsrechte auf Daten und Informationen. Gründe hierfür können Kostenvorteile durch geteilte Zugänge bei externen Diensten, Steigerung der Effizienz von Arbeitsprozessen oder schlicht mangelndes Risikobewusstsein sein.[62] In der Praxis hat sich gezeigt, dass Mitarbeiter durch geteilte Zugriffsrechte auf eine Fülle an Daten zugreifen können, die sie für ihre Arbeit oftmals gar nicht benötigen. Dies erhöht das Risiko eines Missbrauchs dieser Daten erheblich.

b. Mobile Endgeräte

Auch mobile Endgeräte und die immer weiter fortschreitende Möglichkeit, von zuhause oder von verschiedenen Orten weltweit arbeiten zu können, spielen im Rahmen von Cyberangriffen von innen eine große Rolle.[63] Auch vor Beginn der Corona-Krise war ein leichter Trend zum Arbeiten im Homeoffice und zu *remote work* erkennbar; durch die Pandemie hat sich dieser Trend erheblich verstärkt.[64] Aufgrund des Infektionsgeschehens am Arbeitsplatz, haben viele Unternehmen die Notwen-

---

61 BSI, Glossar der Cybersicherheit, Innentäter (Fn. 59).

62 Voitiz, The Comodo Breach and the Dangers of Shared Accounts, https://dzone.com/articles/the-comodo-breach-and-the-dangers-of-shared-accoun (abgerufen am 18.04.2021).

63 BSI, Mindeststandard des BSI für Mobile Device Management, https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Mobile_Device_Management/Mobile_Device_Management_node.html (abgerufen am 19.04.2021).

64 *Rosenbach/Börsch*, Covid-19-Briefing: HomeOffice-Trends vor, während und nach Corona, https://www2.deloitte.com/de/de/blog/covid-19-briefings/2020/covid-19-briefing-homeoffice-trends-corona.html (abgerufen am 07.01.2021).

digkeit erkannt und zunehmend Maßnahmen ergriffen, um Homeoffice oder *remote work* zu ermöglichen. Um die kurzfristige Arbeitsfähigkeit des Unternehmens aufrechtzuerhalten, wurden dabei Sofortmaßnahmen vieler Unternehmen größtenteils ohne konzeptionelle Vorbereitungsmaßnahmen umgesetzt. Dass dies Sicherheitsrisiken mit sich bringt, ist dabei wenig überraschend. Je flexibler die Mitarbeiter hinsichtlich des Arbeitsortes sind, desto mehr Möglichkeiten für Missbrauch und Sicherheitslücken entstehen. Denn im Homeoffice sind Daten und IT-Technik der unmittelbaren Kontrolle des Arbeitgebers entzogen. Gleichzeitig steigt die Gefahr unberechtigter Zugriffe durch Dritte, etwa durch die Nutzung öffentlicher W-Lan-Netzwerke im Café um die Ecke oder im Co-Working-Space.[65]

B. Lösungsansätze und Präventionsstrategien

Um die zuvor genannten Risiken so gut es geht einzudämmen und als Unternehmen vorbereitet zu sein, empfehlen sich verschiedene Vorgehensweisen und Präventionsstrategien. Für die Geschäftsführung von Unternehmen ist es dabei unabdingbar, Maßnahmen zur Gewährleistung sicherer IT-Systeme zu ergreifen. Bei einer allzu stiefmütterlichen Behandlung der Cybersecurity begibt sich die Geschäftsführung in ein immanentes Haftungsrisiko, da sie von Dritten für die wirtschaftlichen Folgen eines Cyberangriffs in Anspruch genommen werden kann.[66] Gemäß § 93 AktG und § 43 I GmbHG haben die Vorstandsmitglieder und Geschäftsführer eines Unternehmens in den Angelegenheiten der Gesellschaft die Sorgfalt eines ordentlichen Geschäftsleiters bzw. -mannes anzuwenden. Zu diesem Pflichtenmaßstab zählt dabei auch die Einhaltung der in der DSGVO festgelegten Pflichten, so auch die in Art. 32 DSGVO verankerte Pflicht, zum Schutz der Daten angemessene technische und organisatorische Maßnahmen zu treffen. In diesem Zusammenhang wird die Gewährleistung eines einheitlichen Sicherheitskonzepts die zentrale Herausforderung der Geschäftsleitungen sein.

In der Praxis hat sich gezeigt, dass für eine erfolgreiche Einführung eines Sicherheitskonzepts an erster Stelle eine klare Definition der Verantwortlichkeiten für das Thema Cybersecurity im jeweiligen Unternehmen

---

65 *Schonschek*, Home Office fordert die Cybersecurity, https://www.computerwoche.de/a/home-office-fordert-die-cybersecurity,3549013 (abgerufen am 19.04.2021).

66 *Schmidt-Versteyl*, Cyber Risk – neuer Brennpunkt Managerhaftung?, NJW 2019, 1637, 1642.

entscheidend ist. Diese Zuständigkeit dürfte in den meisten kleinen und mittelständischen Unternehmen aufgrund der – wie oben beschrieben – oftmals unzureichenden Auseinandersetzung mit dem Thema Cybersecurity noch nicht abschließend geregelt sein. Es ist durchaus häufig zu beobachten, dass bereits mehrere Mitarbeiter für wichtige Einzelthemen aus dem Bereich Cybersecurity zuständig sind. An einer gebündelten ausschließlichen Verantwortlichkeit eines Mitarbeiters oder einer Abteilung für sämtliche IT-Sicherheitsfragen fehlt es jedoch zumeist. In mittelständischen Unternehmen könnte dabei einerseits die Rechtsabteilung und andererseits die IT-Abteilung ein Interesse daran haben, dass Maßnahmen im Bereich Cybersecurity getroffen und vor allem umgesetzt und eingehalten werden. Hier zeigt sich regelmäßig, dass Schwierigkeiten hinsichtlich der Abstimmung und der Arbeitsteilung entstehen können. Es empfiehlt sich, in Unternehmen eine Schnittstelle zwischen den Bereichen IT, Recht und Entwicklung zu bilden, die für die Entscheidungsprozesse bezogen auf die Datensicherheit zuständig ist. Denkbar ist auch die Gründung eines kleinen Teams, welches diese Aufgaben übernimmt. Entscheidend ist, dass die Kompetenzen gebündelt werden und, dass es mindestens einen Ansprechpartner gibt, der ausschließlich für den Bereich der Cybersecurity verantwortlich ist und die Entwicklungen des Unternehmens sowie die aktuelle Rechtslage im Blick behält.

Unternehmen sollten sich zudem die Frage stellen, welche Daten sensibel und somit besonders schützenswert sind und vor welchen Angriffen sie geschützt werden sollen.

Sind diese ersten Schritte vollzogen, sollte der Fokus daraufgelegt werden, einen soliden Schutz gegen die jeweiligen unternehmensspezifischen Risiken zu entwickeln.

I. Lösungsansätze für Risiken von außen

Insbesondere Tech-Unternehmen wie Vimcar sehen sich mit vielen Risiken von außen konfrontiert. Je mehr ein Unternehmen mit Software und digitalen Daten arbeitet, desto höher sind die Anforderungen an die technischen und organisatorischen Maßnahmen, die im gesamten Unternehmen implementiert und im Anschluss fortlaufend und konsequent umgesetzt werden sollten.

1. Prävention gegen Ransomware

Software wie Betriebssysteme, Antivirenprogramme und Browser, sowie darin enthaltene Plug-ins, sollten stets auf dem aktuellen Stand sein, um Sicherheitslücken vorzubeugen.[67] Dazu können Mitarbeiter regelmäßig erinnert werden, Updates zu installieren. In der Praxis hat sich die Nutzung einer Patch-Management-Software, die auf den Unternehmensrechnern installierte Software beständig auf Aktualität überprüft und an Updates erinnert, bewährt. Diese kann auch so konfiguriert werden, dass wichtige Updates automatisch installiert werden.

Es empfiehlt sich außerdem ein vom System abgetrenntes Backup einzurichten und regelmäßig zu aktualisieren.[68] Dies dient als Vorbereitung für den Schadensfall. Durch das Backup können betrieblichen Daten gesichert werden. Dadurch kann die oben beschriebene Bredouille in Hinblick auf etwaige Lösegeldzahlungen im besten Falle vermieden und möglichst bald zum Tagesgeschäft zurückgekehrt werden. Im Fall von Tech-Unternehmen, deren Fokus auf der Verarbeitung von Daten liegt, empfiehlt es sich, eine komplette Spiegelung des Hauptservers vorzunehmen.

Vimcar spiegelt beispielsweise sämtliche Daten in Echtzeit. Die Spiegelung erfolgt auf mindestens zwei völlig voneinander unabhängigen Servern in geografisch getrennten Rechenzentren in Frankfurt am Main. Für den Fall, dass bei einem Server Probleme auftreten, schaltet das System sofort auf einen der anderen Server um. Die Funktionalität dieser Spiegelung wird kontinuierlich überwacht und einmal im Quartal manuell überprüft. Von allen Servern werden täglich Backups erstellt. Die manuelle Wiederherstellung dieser Backups wird einmal im Quartal von Vimcar geprüft. Im Rahmen der Prüfung wird mit jeweils einem Backup ein Test durchgeführt, der den unwahrscheinlichen und zeitgleichen Ausfall aller redundant betriebenen Server nachstellt.

Da *Ransomware* in den meisten Fällen durch Anhänge von E-Mails auf Unternehmensrechner und -systeme eingeschleust wird[69], gelten die folgenden Ausführungen zum *Phishing* auch zur Prävention gegen *Ransomware*.

---

67 BSI, Ransomware: Bedrohungslage, Prävention und Reaktion 2019 (Fn. 25), S. 15.
68 BSI, Ransomware: Bedrohungslage, Prävention und Reaktion 2019 (Fn. 25), S. 11.
69 BSI, Ransomware, erpresserische Schadprogramme, https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/Ransomware.html (abgerufen am 09.01.2021).

2. Prävention gegen Phishing

Phishing-Attacken sind in aller Regel aufgrund von Unachtsamkeit oder mangelnder Vorbereitung der Mitarbeiter auf derartige Angriffe erfolgreich.[70] Daher ist es beinahe unerlässlich, Mitarbeiter für den Umgang mit *Phishing*-Attacken zu sensibilisieren. Hierzu können externe Experten für unternehmensweite Workshops engagiert werden. Alternativ können Mitarbeiter durch digitale *Phishing*-Trainings geschult werden. Einige digitale Anbieter auf dem Markt haben sich darauf spezialisiert, die notwendige Sensibilität der Mitarbeiter im Umgang mit *Phishing*-E-Mails zu trainieren. Teilweise bieten diese Anbieter darüber hinaus Tools zur *Phishing*-Simulation an. Zur Durchführung der *Phishing*-Simulation wird den Anbietern durch das jeweilige Unternehmen in der Regel zunächst eine Liste von Mitarbeitern und deren E-Mail-Adressen zur Verfügung gestellt. Der Anbieter simuliert im Anschluss mögliche *Phishing*-Attacken im Unternehmen, indem er den Mitarbeitern in unregelmäßigen Abständen Test-E-Mails zukommen lässt, ohne dass die Mitarbeiter darauf vorbereitet werden. Diese Test-E-Mails orientieren sich in Design und Inhalt an tatsächlich existenten *Phishing*-Mails. Sie können jedoch keinen Schaden anrichten, sondern dienen lediglich dazu, Sicherheitslücken ausfindig zu machen und unvorsichtige Mitarbeiter zu sensibilisieren. Sollten Mitarbeiter die Test-E-Mails und deren Anhänge öffnen, wird der jeweilige Administrator des Tools entweder vom Anbieter darüber informiert, oder er kann dies jeweils anhand eines Dashboards verfolgen. Ziel ist es, einen Überblick über den Umgang der Mitarbeiter mit solchen E-Mails zu erhalten.

Vimcar arbeitet beispielsweise zur *Phishing*-Prävention mit einem Anbieter, der im Rahmen seines cloudbasierten Services eine Mischung aus digitalen Mitarbeitertrainings und Phishing-Simulationen bietet. Sobald ein Mitarbeiter eine der simulierten *Phishing*-Mails oder deren Anhänge öffnet oder vertrauliche Daten auf einer gefälschten Login-Website angibt, gelangt er zu einer Lernseite. Diese bietet dann individuelle Hinweise und Tipps, die bei der Vermeidung solcher Fehler helfen. Dieses System funktioniert anonym und über das Jahr verteilt, sodass alle Mitarbeiter eine kontinuierliche Schulung erhalten. Der Anbieter stellt außerdem ein Dashboard mit allen wichtigen Kennzahlen und Statistiken zur Verfügung.

---

70 *Nollau*, Eigene Mitarbeiter sind größte Security-Schwachstelle, https://www.it-business.de/eigene-mitarbeiter-sind-groesste-security-schwachstelle-a-732202/ (abgerufen am 17.04.2021).

Dadurch können sich die für Cybersecurity zuständigen Mitarbeiter zügig einen Überblick über die bei den Mitarbeitern aktuell vorhandene Sensibilität im Umgang mit *Phishing*-Mails verschaffen.

Außerdem hat sich in der Praxis bewährt, Mitarbeiter dahingehend zu verpflichten, sich auf allen beruflich genutzten Endgeräten Dateierweiterungen, wie z.B. „.doc" oder „.xls", vollständig anzeigen zu lassen. Diese Dateierweiterungen werden von den gängigen Betriebssystemen ausgeblendet. Diese Tatsache nutzen Cyberkriminelle gezielt aus. Die Anzeige dieser Dateierweiterungen bewirkt eine weitaus bessere Erkennbarkeit von verdächtigen Dateien. Wenn beispielsweise der Anhang einer Bewerbungsmail anstatt "LebenslaufPDF" als "LebenslaufPDF.exe" angezeigt wird, ist schnell erkennbar, dass es sich nicht um einen echten Lebenslauf im PDF-Format handelt, sondern vermutlich um eine Schadsoftware. Die Anzeige der Dateierweiterung ist ein einfacher und kostenloser Weg, um *Phishing*-Risiken gezielt zu minimieren. Empfehlenswert ist außerdem die Implementierung einer Meldekette für potenzielle *Phishing*-Mails. Sie kann als Warnsystem fungieren, durch das alle Mitarbeiter für den Fall alarmiert werden, dass ein Mitarbeiter eine solche E-Mail erhalten hat.

3. Prävention gegen Whaling

Für eine erfolgreiche Prävention vor *Whaling*-Attacken als spezielle Form des *Phishings* sollten zunächst die oben genannten Grundsätze zur Sensibilisierung von Mitarbeitern vor *Phishing*-Attacken umgesetzt werden.

Außerdem hat es sich in der Praxis bewährt, alle E-Mails, die von Absendern außerhalb des Unternehmens stammen, zu kennzeichnen. So können Whaling-E-Mails, die oberflächlich betrachtet wie die einer unternehmensinternen Führungskraft aussehen, auf den ersten Blick erkannt werden.

4. Passwörter und Passwortmanager

Ein entscheidender Faktor im Rahmen der erfolgreichen Verhinderung von Cyberangriffen stellt die Verwendung sicherer Passwörter dar.[71] Cyberkriminelle haben Tools entwickelt, die vollautomatisch eine Vielzahl

71 *Dirscherl*, BSI gibt Tipps für sichere Passwörter, https://www.pcwelt.de/ratgeber/Datenschutz-BSI-gibt-Tipps-fuer-sichere-Passwoerter-1452884.html (abgerufen am 17.04.2021).

von Zeichenkombinationen ausprobieren können. Dabei werden ganze Wörterbücher einschließlich gängiger Kombinationen aus Worten und angefügten Zahlen getestet oder einmal im Internet veröffentlichte Zugangsdaten bei diversen anderen Diensten durchprobiert.[72] Um zu verhindern, dass sich Cyberkriminelle so Zugang zu Unternehmenssystemen verschaffen, sollten Passwörter gängige Qualitätsanforderungen[73] erfüllen und jeweils nur für einen Zugang genutzt werden. Dabei ist regelmäßig die Länge eines Passwortes wichtiger als die Kombination aus Groß- und Kleinbuchstaben sowie Sonderzeichen. Je länger das Passwort, desto länger braucht ein computergestützter Algorithmus im Rahmen eines Cyberangriffs, um dieses zu knacken.

In der Praxis hat sich die Verwendung eines Passwortmanagers als nützlich erwiesen. Dies gilt insbesondere dann, wenn Mitarbeiter eine Vielzahl an Tools und Zugängen nutzen. Passwortmanager sind Programme, die Passwörter und vertrauliche Informationen verwalten.[74] Die Nutzer können verschiedene Passwörter, Softwarelizenzen und weitere sensible Daten in einem virtuellen „Tresor" speichern, der nur durch die Eingabe eines Hauptkennwortes zugänglich ist.[75] Das Hauptkennwort dient dabei als Sicherheitsschlüssel für die im „Tresor" gespeicherten Informationen. Die meisten gängigen Passwortmanager akzeptieren nur Hauptkennwörter, die den Vorgaben an sichere Passwörter entsprechen. Es wird empfohlen, die Hauptkennwörter besonders lang und mit besonders vielen Sonderzeichen zu versehen. In dem Fall kann der jeweilige Nutzer zwar kein simples Passwort wie z.B. „123456" nutzen, welches seit Jahren das beliebteste Passwort in Deutschland ist.[76] Dafür muss er sich lediglich ein Passwort merken.

---

72 BSI, Empfehlungen: Sichere Passwörter erstellen, https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html (abgerufen am 10.01.2021).

73 Vgl. die jeweils aktuellen Vorgaben im IT-Grundschutzkompendium des BSI; BSI IT-Grundschutzkompendium 2021, Download unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html (abgerufen am 19.04.2021).

74 BSI, Passwörter verwalten mit dem Passwort-Manager, https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/Passwort-Manager/passwort-manager_node.html (abgerufen am 19.04.2021).

75 BSI, Empfehlungen: Sichere Passwörter erstellen (Fn. 74).

76 *Micijewic*, die beliebtesten Passwörter der Deutschen sind auch dieses Jahr die unsichersten, https://www.handelsblatt.com/technik/it-internet/it-sicherheit-di

Selbstverständlich ist auch die Nutzung von Passwortmanagern nicht vollkommen risikolos. Passwortmanager können selbst Opfer von Cyberangriffen werden. Außerdem ist bei der Nutzung eines cloudbasierten externen Dienstleisters zu bedenken, dass dieser theoretisch Zugang zu vertraulichen Informationen des jeweiligen Nutzers erhält. Deshalb sollte der jeweilige Anbieter sorgfältig überprüft werden. Dabei sollte insbesondere auf die AGB, die Datenschutzerklärung, die technischen und organisatorischen Maßnahmen und die Verschlüsselung der Passwörter geachtet werden.

Vimcar verwendet beispielsweise ein Passwortmanager-Tool, welches die Zugangsdaten und Passwörter grundsätzlich anhand einer AES-256-Bit-Verschlüsselung Ende-zu-Ende verschlüsselt. Bei dieser Verschlüsselungsmethode besitzt ausschließlich der jeweilige Nutzer den Schlüssel. Daher kann auch der Anbieter selbst nicht auf die gespeicherten Zugangsdaten und Passwörter zugreifen. Zur Einrichtung des Tools installiert der Nutzer auf seinem Rechner ein Programm bzw. ein Browser Plug-in. Um an die gespeicherten Daten heranzukommen, muss der Nutzer das Hauptkennwort eingeben. Das Tool enthält außerdem einen integrierten Passwortgenerator. Dieser ermöglicht es, spezifische Anforderungen an die verwendeten Passwörter zu stellen, wie z.B. Länge, Anzahl der Sonderzeichen etc. Somit können sichere Passwörter automatisch generiert und über das Tool gespeichert werden.

5. Zwei-Faktor-Authentisierung

Neben dem Verwenden sicherer Passwörter ist der Einsatz eines zweiten Authentisierungsfaktors ein sinnvoller Schutz gegen Cyberangriffe von außen. Bereits in vielen Bereichen elektronischer Geschäftsprozesse ist eine solche sichere Authentisierung erforderlich. Spätestens seit der verpflichtenden Verwendung der Zwei-Faktor-Authentisierung für das Online-Banking aufgrund der PSD2 Richtlinie der EU sollte dieses Verfahren beinahe jedem Bürger bekannt sein. Bei der Zwei-Faktor-Authentisierung kommt zu einem ersten Faktor in Form eines Passworts ein zweiter Faktor hinzu, der einer weiteren Kategorie und einem weiteren Endgerät zuzuordnen ist,

---

e-beliebtesten-deutschen-passwoerter-sind-auch-dieses-jahr-die-unsichersten/25347562.html?ticket=ST-1331496-v5t7mOPREcB6UtbWLiLT-ap6 (abgerufen am 10.01.2021).

wie z.B. das Generieren einer TAN mithilfe eines Mobiltelefons.[77] Dieser Identitätsnachweis eines Nutzers mittels der Kombination zweier unabhängiger Komponenten wird insbesondere vom BSI in seinen IT-Grundschutz-Kompendium empfohlen.[78] Entscheidend für die Implementierung einer Zwei-Faktor-Authentisierung ist, ob das jeweilige System eine solche überhaupt unterstützt und wer der jeweilige Administrator des Systems ist.

6. Firewall und Antivirenprogramme

Zur Absicherung der eigenen Netzwerkinfrastrukturen in Unternehmen ist die Verwendung einer gut konfigurierten Firewall unerlässlich.[79] Ergänzend sollte auf jedem Endgerät eine Antiviren-Software installiert und regelmäßig aktualisiert werden.[80] Diese Vorkehrungen gelten als unbedingte Grundausstattung und wurden von der überwiegenden Anzahl der kleinen und mittleren Unternehmen inzwischen umgesetzt.[81]

7. Haftung und Cyberversicherungen

Cyberangriffe weisen ein enormes Potenzial auf, Schäden in den Unternehmen zu verursachen. Gleichzeitig sind die Fragen der Haftung nicht abschließend geklärt.[82] Zwar haften die Unternehmen bei erfolgreichen Cyberangriffen grundsätzlich sowohl für eigene substanzielle Schäden als

---

77 BSI, Empfehlungen: Sichere Passwörter erstellen (Fn. 74).

78 BSI, IT-Grundschutz-Kompendium 2020, S. 11, Download unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2020.html (abgerufen am 10.01.2021).

79 BSI, Schutz vor dem Angriff von außen, https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Virenschutz-Firewall/Firewall/firewall_node.html (abgerufen am 19.04.2021).

80 BSI, Virenschutz und falsche Antivirensoftware, https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Virenschutz-Firewall/Virenschutzprogramme/virenschutzprogramme_node.html (abgerufen am 20.04.2021).

81 *Hildebrandt/Niederprüm u.a.*, WIK Report, Aktuelle Lage der IT-Sicherheit in KMU, S. 28, https://www.it-sicherheit-in-der-wirtschaft.de/ITS/Redaktion/DE/PDF-Anlagen/Studien/aktuelle-lage-der-it-sicherheit-in-kmu-langfassung.pdf?__blob=publicationFile&v=3 (abgerufen am 04.01.20219).

82 *Mehrbrey/Schreibauer*, MMR 2016, 75, 75.

auch für Schäden, die ihre Kunden und Dienstleister erleiden, selbst.[83] Jedoch wird das angegriffene Unternehmen in einigen Fällen versuchen, Dritte wie z.B. externe Dienstleister in Anspruch zu nehmen und eigene Ansprüche durchzusetzen. Das Abschließen einer sog. Cyberversicherung wird vor diesem Hintergrund für Unternehmen im Rahmen ihres Risikomanagements immer wichtiger werden. Eine solche Versicherung trägt dem Umstand Rechnung, dass übliche Versicherungen meist einen unzureichenden Schutz gegen Schäden bieten, die durch Cyberangriffe entstehen. Eine Cyberversicherung bietet dem Versicherten dabei die Möglichkeit, Eigen- und Drittschäden im Zusammenhang mit Cyberangriffen und Cyberkriminalität zu versichern. In den letzten Jahren hat sich das Angebot solcher Versicherungen stetig weiterentwickelt. Die Cyberversicherungen erstatten dabei, je nach individuell vereinbartem Versicherungsschutz, Kosten im Rahmen der Wiederherstellung von Daten und IT-Systemen, Kosten infolge eines Betriebsausfalls bzw. einer Betriebsunterbrechung sowie für die Inanspruchnahme spezialisierter Rechtsanwälte. Optional können zusätzlich Fremdschäden – zumeist in Form von Schadensersatzforderungen von Geschäftspartnern und Kunden – versichert werden.[84] Eine mögliche Orientierungshilfe geben die im April 2017 veröffentlichten Musterbedingungen für Cyberversicherungen des Gesamtverbands der Deutschen Versicherungswirtschaft.[85] Diese legen einen Versicherungsschutz für Vermögensschäden fest, die durch eine „Informationssicherheitsverletzung" entstanden sind. Der Umfang des Versicherungsschutzes ist dabei vom Verständnis der Bezeichnung des „informationsverarbeitenden Systems" abhängig.[86] Darunter dürften alle Systeme fallen, die infolge eines Angriffs infiziert werden können, wie z.B. die Unternehmensserver.[87] Allerdings ist vor Abschluss eines Versicherungsvertrages zu beachten, dass in den Versicherungsbedingungen häufig Haftungsausschlüsse für den Fall enthalten sind, dass die Absicherung der Unternehmensnetzwerke und -systeme nicht dem Stand der Technik entspricht.[88] Des Weite-

83 Mehrbrey/Schreibauer (Fn. 82), Rn. 80 ff.
84 *Fortmann*, r+s 2019, 429, 432.
85 Vgl. GDV, Allgemeine Versicherungsbedingungen Cyberversicherung 2017, https://www.gdv.de/resource/blob/6100/d4c013232e8b0a5722b7655b8c0cc207/01-allgemeine-versicherungsbedingungen-fuer-die-cyberrisiko-versicherung--avb-cyber--data.pdf (abgerufen am 09.09.2020).
86 GDV, Allgemeine Versicherungsbedingungen Cyberversicherung 2017 (Fn. 89), S. 6, Ziff. A1–2.1.
87 *Malek/Schütz*, r + s 2019, 421, 422.
88 BSI, Ransomware Bedrohungslage, Prävention und Reaktion 2019 (Fn. 25).

ren sollten Unternehmen, die eine Cyberversicherungen abschließen wollen, die gängigen Sicherheitsvorschriften, die bspw. in der DSGVO, dem BDSG und weiteren branchenspezifischen Gesetzen, wie dem TKG, enthalten sind, beachten. Die Bedingungen der Cyberversicherungen sind in der Regel so formuliert, dass Verstöße gegen diese Sicherheitsvorschriften ebenfalls zu einem Haftungsausschluss für die jeweilige Versicherungsgesellschaft führen.[89] Allgemein lässt sich unter deutschen Unternehmen ein Trend zum Abschluss von Cyberversicherungen erkennen. Allerdings sind große Unternehmen bisher dabei etwa doppelt so häufig gegen Cyberrisiken versichert, als kleine und mittlere Unternehmen.[90]

II. Lösungsansätze für Risiken von innen

1. Mitarbeiterschulungen und -sensibilisierungen

Laut einer Bitkom-Studie zum Wirtschaftsschutz aus dem Jahr 2020 waren es bisher gerade die aufmerksamen und gut geschulten Mitarbeiter des eigenen Unternehmens, die Cyberangriffe erkannt und damit zu ihrer Aufdeckung beigetragen haben.[91]

Neben Schulungen zum Datenschutz, die bereits häufig in Unternehmen durchgeführt werden, haben sich in der Praxis Schulungen zum Thema Datensicherheit als hilfreich erwiesen. Die Mitarbeiter sollten in diesem Rahmen hinsichtlich des Umgangs mit Hardware und der Ablage und Speicherung von Daten sensibilisiert werden. Dabei spielt neben der Sensibilisierung zur regelmäßigen Durchführung von Updates der Antivirensoftware außerdem die Vorsicht bei Downloads von Dateien von Websites oder als Anhänge von E-Mails eine große Rolle.

Unternehmen müssen für solche Schulungen nicht zwangsweise teure externe Experten beauftragen. Oftmals können die Schulungen in Form von kostengünstigen Online-Trainings erfolgen. Auch diese Online-Trainings können einen erheblichen Beitrag dazu leisten, Risiken aus den Reihen der eigenen Mitarbeiter zu verringern. Die Mitarbeiterschulungen sollten, aufgrund der stetig verbesserten und neu entwickelten Vorgehens-

89 *Fortmann* (Fn. 84), Rn. 437.

90 *Krößmann/Artz*, Industrie setzt zunehmend auf Cyberversicherungen, https://www.bitkom.org/Presse/Presseinformation/Industrie-setzt-zunehmend-auf-Cyberversicherungen.html (abgerufen am 11.01.2021).

91 Bitkom-Studie Wirtschaftsschutz 2020 (Fn. 4), S. 29.

weisen der Cyberkriminellen, mindestens jährlich stattfinden. Idealerweise sollten derartige Schulungen als Teil des „Onboardings" neuer Mitarbeiter implementiert werden, damit diese Mitarbeiter bereits bei Beginn ihrer Tätigkeit für drohende Gefahren im Bereich der Cyberkriminalität sensibilisiert werden. Online-Schulungen bieten zudem den Vorteil, dass sie jederzeit verfügbar sind und von Mitarbeitern daher genutzt werden können, wenn gerade Zeit zur Verfügung steht. So kann die Bindung aller Ressourcen über Stunden oder gar Tage vermieden werden, was in einigen Unternehmen einem Betriebsstillstand nahekommen kann. Des Weiteren enthalten einige Online-Schulungen Abschlusstests, um zu gewährleisten, dass die Inhalte der Schulungen tatsächlich bei den Mitarbeitern angekommen sind.

2. Clean-Desk-Policy

Die Clean-Desk-Policy gibt vor, dass alle Arbeitsplätze bei deren Verlassen aufgeräumt und frei von Arbeitsmitteln hinterlassen werden müssen.[92] Die Einführung einer solchen Policy hat sich in der Praxis als sinnvoll erwiesen. Dies gilt umso mehr, als viele Unternehmen zunehmend Homeoffice-Regelungen einführen und Mitarbeiter häufig wechselnde Arbeitsplätze innerhalb eines Büros besetzen. Die Clean-Desk-Policy kann entweder bereits im Arbeitsvertrag enthalten oder als Büro-Richtlinie ausgestaltet sein.

3. Weitere Policies

Weitere Policies können dazu beitragen, Mitarbeiter zu sensibilisieren, beispielsweise dahingehend, dass betriebliche Systeme, wie z.B. E-Mail-Konten nicht für private Zwecke genutzt werden dürfen. Die Ausgestaltung der Policies hängt dabei maßgeblich von der konkreten Arbeitsumgebung eines Unternehmens ab. In größeren Unternehmen kann es sinnvoll sein, spezifische Policies für die einzelnen Abteilungen zu entwickeln, die ihre jeweiligen Besonderheiten widerspiegeln.

Vimcar hat beispielsweise eine sog. Private-Use-Policy hinsichtlich der verwendeten Systeme implementiert. Dabei werden die Mitarbeiter angehalten, keine private Kommunikation über Unternehmenssysteme zu

92 *Pletke/Schrader* u.a., Rechtshandbuch Flexible Arbeit, 1. Aufl. 2017, B. Dimensionen der Flexibilisierung, Rn. 1040.

führen, keine privaten Daten auf der Hardware des Unternehmens zu speichern sowie keine privaten Informationen im elektronischen Terminkalender einzutragen. Diese Policy ermöglicht es Vimcar, bei Ausscheiden eines Mitarbeiters, die genutzten Accounts zu löschen bzw. an aktive Mitarbeiter zu übergeben. Bei der Übergabe der Accounts muss der neue Nutzer die Zugangsdaten ändern, um einen etwaigen Zugriff ausgeschiedener Mitarbeiter zu verhindern. Bleiben Zugriffsrechte bestehen, steigt die Gefahr, dass ein verärgerter Ex-Mitarbeiter unternehmenskritische Daten stiehlt oder vernichtet. Im Rahmen der Private Use Policy werden die Mitarbeiter auch hinsichtlich des Teilens und Freigebens von Dateien dahingehend sensibilisiert, Verantwortung für die eigenen Dokumente zu übernehmen.

Policies erfüllen allerdings nur ihren Zweck, wenn sich die Mitarbeiter an sie halten. Von Unternehmensseite her gibt es kaum Kontroll- oder Regulierungsmöglichkeiten um zu überprüfen, ob Mitarbeiter den Policies Folge leisten. Die Policies dienen vielmehr als Richtlinien bzw. Empfehlungen, die naturgemäß das Risiko mit sich bringen, nicht beachtet zu werden. Hier ist die Kette nur „so stark wie das schwächste Glied", da bereits im Falle, dass sich ein einzelner Mitarbeiter nicht an die jeweilige Policy hält, potenziell große Schäden eintreten können. Deshalb sollten zumindest stichprobenhafte Kontrollen hinsichtlich der Beachtung der Policies erfolgen, um Mitarbeiter bei Nichtbeachtung der Policies erneut auf deren Geltung aufmerksam machen zu können.

4. Zugriffsrechte

Der Grundsatz der *Least Privileges* ist die wichtigste Regel zur Vergabe von Benutzerrechten. Sie beinhaltet, dass Mitarbeiter genau die Rechte bekommt, die sie für die Erfüllung ihrer Arbeit unbedingt benötigen. Es geht weniger darum, die Rechte einzelner Mitarbeiter zu beschneiden, vielmehr stellt der Grundsatz sicher, dass vertrauliche Daten auch vertraulich bleiben.[93]

Bei Vimcar können Mitarbeiter beispielsweise grundsätzlich nicht auf Kundendaten zugreifen, vielmehr werden für jeden einzelnen Mitarbeiter spezifische bedarfsgerechte Zugriffsrechte festgelegt. Auch für externe Tools benötigt ein Mitarbeiter eigens zugewiesene Zugriffsrechte, um z.B.

93 BSI, Missbrauch von Berechtigungen, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/elementare_gefaehrdungen/G_0_32_Missbrauch_von_Berechtigungen.html (abgerufen am 13.01.2021).

überhaupt Kundendaten abrufen zu können. Grundsätzlich sind die Zugriffsrechte in Leserechte und Adminrechte zu unterteilen. Leserechte besitzen z.B. Mitarbeiter des First-Level-Kundensupports, um Kunden und deren Daten im System finden zu können und ihnen Unterstützung bei der Nutzung der Vimcar Produkte zu bieten. Adminrechte (Schreiberechte) besitzen beispielsweise ausgewählte Mitarbeiter der Operations-Abteilung, um Kontaktdaten oder Vertragsdetails von Kunden für den Fall einer Änderung dieser Daten im System bearbeiten zu können.

5. Equipment

Ein zunehmend wichtigeres Thema ist zudem die Gewährleistung von Datensicherheit bei der Nutzung mobiler Endgeräte und Hardware. Vimcar führt z.B. eine Liste darüber, welchem Mitarbeiter welches Equipment wann zur Verfügung gestellt wurde. Die Geräte sind mit Identifikationsnummern versehen. Grundsätzlich sollte bei Beendigung eines Arbeitsverhältnisses darauf geachtet werden, dass die erhaltene Hardware bis zum Ende der Tätigkeit zurückzugeben wird, damit Zugriffe auf Daten und Systeme nach Beendigung des Arbeitsverhältnisses unterbunden werden können.

C. Fazit

Die Relevanz des Bereichs der Cybersecurity für die fortlaufende, störungsfreie Unternehmertätigkeit wird auch den kleinen und mittleren Unternehmen zunehmend bewusst. Dieser Prozess beschleunigt sich aufgrund der digitalen Abbildung einzelner Unternehmensprozesse, aber auch wegen der pandemiebedingten Umstellung auf Home-Office-Lösungen. Allerdings verfügen eine nicht zu vernachlässigende Anzahl an Unternehmen nach wie vor nicht über eine hinreichend funktionsfähige IT-Infrastruktur und umfassende Sicherheitskonzepte.

Für alle Unternehmen gilt gleichermaßen, dass Cybersecurity kein Thema ist, das einmal erledigt wird und danach keines Einsatzes mehr bedarf. Vielmehr ist abzusehen, dass auf dem Gebiet der Datensicherheit kontinuierliche Entwicklungen bevorstehen werden. Da Cyberkriminelle unermüdlich neue Methoden entwickeln, um Sicherheitslücken auszunutzen, gleicht es einem Katz-und-Maus-Spiel, den neuen Methoden standzuhalten. Insbesondere die Geschäftsleitungen von Unternehmen sind dazu

angehalten, ein größeres Augenmerk auf das Thema Cybersecurity zu legen. Die Aspekte der Cybersecurity müssen dabei stets mit der Praktikabilität innerhalb des Unternehmens und den notwendigen Innovationen auf dem jeweiligen Markt abgewogen werden. Dies stellt einen schwierigen Balanceakt dar, denn ohne ein innovatives Produkt ist ein Unternehmen am Markt nicht attraktiv. Allerdings kann eine öffentlichkeitswirksame Cyberattacke, die aufgrund von unzureichenden Präventionsmaßnahmen erfolgreich ist, ein ebenso unkontrollierbares unternehmerisches Risiko darstellen. Im Rahmen einer Studie gaben vier von fünf Managern von 108 befragten deutschen Unternehmen mit mindestens einer Milliarde Dollar Jahresumsatz zu, neue Technologien einzusetzen, noch bevor die notwendigen Sicherheitskonzepte angepasst seien.[94] Dies dürfte sich für junge, wachstumsorientierte Unternehmen nicht anders darstellen. Daher sollte frühzeitig eine Risikoanalyse vorgenommen und Schritte eingeleitet werden, die dem jeweiligen Unternehmen nach einer erfolgten Abwägung im Einzelfall finanziell zumutbar sind. Dies gilt nicht nur aufgrund des Umstands, dass sich die Anzahl der Cyberangriffe auf kleine und mittelständische Unternehmen kontinuierlich erhöht.[95] Vielmehr bieten sich Unternehmen bei frühzeitiger Auseinandersetzung mit dem Thema Cybersecurity und der Implementierung von Sicherheitsstandards perspektivisch Kostensparpotenziale. Denn eine Implementierung solcher Standards erweist sich meist als aufwendiger, wenn die Unternehmensstrukturen bereits gefestigt sind. Zudem führt beinahe jeder zweite Cyberangriff, der in der Zwischenzeit erfolgen kann, zu Produktions- bzw. Betriebsausfällen.[96] Ungeachtet aller zu empfehlenden Maßnahmen bleibt der Mensch und somit der Mitarbeiter weiterhin der größte Risikofaktor, welchem nur mit regelmäßig wiederkehrenden Schulungen und Sensibilisierungen begegnet werden kann. Ein erfolgreicher Umgang mit Cybersecurity kann letztlich nur funktionieren, wenn mehrere Akteure innerhalb eines Unternehmens erfolgreich zusammenarbeiten und insbesondere die Geschäftsleitung, die IT- und Rechtsabteilung sowie die Belegschaft am selben Strang ziehen.

---

94 *Abbosh/Bissel* (Fn. 1), S. 7.

95 Bitkom-Studie Wirtschaftsschutz 2020 (Fn. 4), S. 7.

96 BSI, Cyber-Angriffe haben erhebliche Konsequenzen für die Wirtschaft, https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2018/Cyber-Angriffe_haben_erhebliche_Konsequenzen_fuer_die_Wirtschaft_31012018.html (abgerufen am 17.01.2021).