Das Printmagazin des VersicherungsJournals

VJ spezial

Ausgabe 22 / Sommer 2023

CYBER-VERSICHERUNG

Das cyber'sche Florianiprinzip

Ein Schutzschild gegen digitale Gefahren

Existenzrisiko Cyberangriff

Cyberversicherungen müssen als Gesamtpaket angeboten werden

Österreichische Post AG I MZ 02Z041736 M I FinanzMedienVerlag Ges.m.b.H., Gentzgasse 15, 1180 Wien

Partnerschaft für den Erfolg

KMU in Österreich zu versichern gehört seit mehr als 12 Jahren zu unseren Stärken.

Werden auch Sie Teil davon, als R+V-Vertriebspartner!

www.ruv.at

Niederlassung Österreich

Sehr geehrte Leserin, sehr geehrter Leser!

Schätzungen gehen davon aus, dass Cybervorfälle jährlich mehr als sechs Billionen Euro Schaden verursachen. Und doch glauben viele kleinere und mittelgroße Unternehmen, dass sie für Angriffe uninteressant sind und dass ihnen „schon nichts passieren" wird. Grund genug für uns, sich in der vorliegenden Ausgabe des VersicherungsJournal Spezial mit der Risikosituation und der Versicherbarkeit von KMUs gegen Cyberrisiken zu beschäftigen.

In unserem Expertenpanel gehen wir den Fragen nach, welche Sicherheitslücken es gibt, wie es um das Risikobewusstsein steht und welche Möglichkeiten kleinere Unternehmen haben, Risiken vorzubeugen. Und wir haben versucht herauszufinden, wie sich die Schadensituation tatsächlich darstellt.

Natürlich beschäftigen wir uns auch damit, wie sich KMUs versichern können und ob es ausreichende Möglichkeiten für sie gibt, Deckung zu erhalten, welche Voraussetzungen sie dafür erfüllen müssen und wie sie zu einer entsprechenden Beratung kommen. Und schließlich wollten wir auch wissen, ob die Prämien für KMUs überhaupt leistbar sind.

Dass Cyberattacken ihre geschäftliche Existenz bedrohen können, ist vielen Unternehmen mittlerweile bewusst. Die meisten rechnen auch damit, dass Angriffe zunehmen werden. Klar ist ebenfalls, dass die Täter immer professioneller werden. In unserem Beitrag „Existenzrisiko Cyberangriff" lassen wir dazu Fakten sprechen: Wie sich die Zahl der Angriffe in Österreich entwickelt, welche Folgen erfolgreiche Cyberattacken haben und welche Maßnahmen Experten empfehlen.

Weil Cyberkriminalität keine nationalen Grenzen kennt, ist zu ihrer Bekämpfung eine EU-weite Zusammenarbeit essenziell. Aktuell befinden sich mehrere neue europäische Rechtsakte in Planung oder Umsetzung. Einen Überblick über die Aktivitäten, die es derzeit auf Unionsebene im Zusammenhang mit digitaler Sicherheit gibt, finden Sie ab Seite 12 in dieser Ausgabe.

Abschließend lesen Sie, welche Entwicklungen Branchenexperten für die Cyberversicherung erwarten. Denn die steigende Zahl der Schadensfälle, immer höhere Schadensummen und die Zunahme von Kumul-Attacken stellen Versicherer vor große Herausforderungen. 2021 haben Cyberversicherer erstmals in Deutschland Verluste erlitten, häufig fehlen noch gesamtheitliche Produktangebote, und der Fachkräftemangel lässt die Branche an ihre Grenzen stoßen.

Ich darf Ihnen wieder eine interessante Lektüre wünschen.

MARIUS PERGER, HERAUSGEBER

IMPRESSUM

Herausgeber und Verleger: FinanzMedienVerlag Ges.m.b.H., 1180 Wien, Gentzgasse 15 **Für den Inhalt verantwortlich:** Marius Perger und Klaus Schweinegger; für namentlich gekennzeichnete Artikel der jeweilige Autor **Produktion:** FinanzMedienVerlag Ges.m.b.H., 1180 Wien, Gentzgasse 15 **Druck:** Print Alliance HAV Produktions GmbH, 2540 Bad Vöslau, Druckhausstraße 1 **Anzeigenpreise:** Es gilt der Werbetarif 2023 **Offenlegung nach §25 Mediengesetz:** Medieninhaber FinanzMedienVerlag Ges.m.b.H. **Blattlinie:** VersicherungsJournal Spezial, kurz VJ, ist ein österreichweites Fachmedium für die Versicherungswirtschaft. Die unabhängige Redaktion berichtet vierteljährlich über branchenrelevante Themen. Zum Zielpublikum gehören – ähnlich dem digitalen Pendant VersicherungsJournal.at – Mitarbeiter von Versicherungskonzernen sowie der freie und gebundene Versicherungsvertrieb **Bilder:** S.1: 9dreamstudio (AdobeStock), S.3: VÖZ/Woody, S.4: Hans und Christa Ede (Adobe Stock), S.5 ganz oben: Wefox Österreich, S.5 zweites von oben: Cogitanda Dataprotect, S.5 Mitte: Infinco GmbH, S.5 zweites von unten: Daniel Gressler, S.5 ganz unten: Helmut Tenschert, S.6: lumerb (AdobeStock), S.8: Leo Lintang (AdobeStock), S.10: patcharin (AdobeStock), S.12: peterschreiber.media (AdobeStock), S.14: your123 (AdobeStock), S.16: arrow (AdobeStock), S.18: Tobias (AdobeStock), S.19: Cmon (AdobeStock)

Das cyber'sche Florianiprinzip

Berufsunfähigkeits- und Cyberversicherer haben offenbar eines gemeinsam. Viele aus ihrer Zielgruppe glauben: Wenn was passiert, dann eher bei jemand anderem. Cyberversicherungen gehören entsprechend selten zum Inventar von KMUs. Die Absicherungsnotwendigkeit wäre aber groß, meint man im Expertenpanel.

Von Emanuel Lampert

Alles (oder fast alles) wird immer „digitaler". Werden Klein- und Mittelunternehmen auch immer „digital-fitter"? Wo sind ihre größten Sicherheitslücken? Risikomanagementexperte Helmut Tenschert sieht die größte im Menschen selbst, „und das sowohl in kleinen wie auch in größeren Betrieben". An Prävention mangle es zwar auch öfters, „aber auch die besten Vorkehrungen nützen nichts, wenn die handelnden Personen sorglos mit eingehenden Informationen umgehen".

Aus Sicht von Infinco-Geschäftsführer Joe Kaltschmid reißen organisatorische, aber auch IT-Security-technische Defizite die größten Lücken in die Sicherheit, etwa durch Ausführung von Malware über manipulierte E-Mail-Anhänge. Häufig würden auch Sicherheitsupdates viel zu spät eingespielt. Benjamin Schilling vom Underwriting Cyberrisk der R+V Allgemeine Versicherung AG betont: Datensicherungen müssen vor Angriffen geschützt sein, „Backups und Originaldaten sollten nicht

durch dieselbe Ursache unbrauchbar gemacht werden können".

Oft sei es allerdings gar nicht möglich, dem Cyberrisiko die nötige Aufmerksamkeit zu schenken, meint René Besenbäck, Managing Director bei Wefox Österreich. Gründe dafür seien in fehlenden Ressourcen, „horrenden Kosten" für Präventionsmaßnahmen und häufig fehlender Aufklärung über Schadenszenarien auszumachen.

Viele KMUs meinten auch immer noch, für Angreifer zu uninteressant zu sein, stellt Natascha Jäger, CEO Austria der Cogitanda Dataprotect AG, fest. „Dies äußert sich dann in einem manchmal schon fast fahrlässigen Umgang mit Datensicherungen, vernachlässigter Einspielung von Sicherheitsupdates und wenigen bis gar keinen Vorgaben im Umgang mit Passwörtern." Gerade in kleineren Unternehmen, sagt Kaltschmid, herrsche oft die Auffassung: Bei uns gibt es nicht viel zu holen, deshalb trifft es uns nicht. „Die Angreifer schauen jedoch meist bei der Auswahl ihrer Targets nur, wo sie mit wenig Widerstand in ein Unternehmen eindringen können."

Tenschert meint, dass das Risikobewusstsein in letzter Zeit zwar gestiegen ist; die wirtschaftlichen Folgen eines Zwischenfalls würden aber oft unterschätzt, was zur Vernachlässigung der Prävention führe. Auch Schilling befindet, die Folgen eines Stillstands der eigenen IT würden unterschätzt.

Wie vorbeugen?

Wie können KMUs vorbeugen? „Der in diesem Bereich meist wenig bewanderte Geschäftsführer ist überfordert, das aus eigener Kraft umfassend und richtig zu konzipieren", meint Tenschert. „Sie oder er wird gut beraten sein, hier externe Hilfe in Anspruch zu nehmen."

Jedes Unternehmen, rät Jäger, sollte sich seiner Risiken rasch bewusstwerden, um geeignete Maßnahmen zu definieren. „Der beste Einstieg dazu ist ein standardisiertes Audit, um festzustellen, welche Risikofelder im eigenen Unternehmen besonders kritisch sind und welche Möglichkeiten es zur Risikoreduzierung gibt". Für die Mitarbeiter als „die letzte ‚Verteidigungslinie' gegen Cyberangriffe" empfiehlt sie regelmäßige IT-Sicherheitsschulungen.

Schilling sieht als „grundlegende Absicherung" moderne Firewalls und Antivirensoftware, ebenso die Regelung, wer wie auf die IT-Systeme zugreifen darf. „Kostenintensiver, aber besser, sind sogenannte EDR-Lösungen, die alle Prozessaktivitäten eines Endpoints erfassen und im laufenden Betrieb analysieren." Kaltschmid unterstreicht: Sicherheitskritische Updates sollten

René Besenbäck
Managing Director
Wefox Österreich

Mag. Natascha Jäger
CEO Austria
Cogitanda Dataproject AG

Mag. (FH) Joe Kaltschmid
Geschäftsführer
Infinco GmbH & Co. KG

Mag. Benjamin Schilling
Underwriting Cyberrisk
R+V Allgemeine Versicherung AG

Dr. Helmut Tenschert
Risikomanagementexperte
und Bildungsanbieter

schnellstmöglich eingespielt werden, und auch komplexe Passwörter sind hilfreich. „Darüber hinaus empfehlen wir aber, dass Unternehmen einen IT-Security-Experten mit einem ‚Penetration Test' beauftragen sollen, um Sicherheitslücken identifizieren zu können."

Potenziell enorme Schäden

Wie stellt sich die Schadensituation bei KMUs nun tatsächlich dar? „Einen echten Überblick darüber gibt es eigentlich nicht", sagt Tenschert, „zu hoch sind die Dunkelziffern an Attacken, die erfolgreich sind, aber nicht bekannt werden". Die Schadenhöhe erreiche rasch sechsstellige Beträge, gibt Jäger zu bedenken, „denn der unverzügliche Einsatz von Experten aus den Bereichen IT, Daten und Recht ist kostspielig, aber notwendig, um noch größeren Schaden abzuwenden".

„Wir haben eine enorme Zunahme an Schäden insgesamt am österreichischen Markt verzeichnet", sagt Besenbäck und beziffert diese mit +32 Prozent gegenüber 2021. „Allerdings ist durchschnittlich die Schadenhöhe mit etwa 17.500 Euro seit gut eineinhalb Jahren stabil." Wie Schilling berichtet, treten in letzter Zeit „gehäuft Angriffe auf Social-Media-Accounts" auf. KMUs seien häufig von gezielten Ransomware-Attacken betroffen. Auch seien häufiger Fälle zu beobachten, in denen Angreifer durch Kompromittierung von E-Mail-Accounts Phishing-Mails an Dritte versenden.

Wie versichern?

Wie können sich KMUs versichern? Im Wesentlichen „ist die ‚Maßschneiderung' des Produkts auf das jeweilige Unternehmen die beste Lösung", sagt Tenschert. Cyberversicherung bedeute eine „Kombination an sich bekannter Versicherungssparten, wie etwa Betriebsunterbrechung oder Haftpflicht, mit spezifischer Ausrichtung". Für KMUs gebe es weitreichende Möglichkeiten, Deckung zu beschaffen, sagt Kaltschmid. „Die meisten Anbieter bieten ein Bausteinsystem an Deckungskomponenten, das stets aus einer Eigen- und Drittschadenkomponente und einer Dienstleisterkomponente besteht, die je nach Versicherungslösung First Response Services, Datenforensiker und Rechtsdienstleister zur Verfügung stellt."

„Grundsätzlich ist für jedes Unternehmen etwas dabei", beschreibt Besenbäck das Marktangebot: „So gibt es Anbieter, die mit geringen Versicherungssummen und attraktiven Prämien vor allem kostensensible Unternehmen ansprechen wollen. Manche bieten über sogenannte Antragsmodelle durch Beantwortung weniger Risikofragen einen erleichterten Zugang zum Versicherungsmarkt." Dann gebe es „Cyberdeckungen über Nischenproduktanbieter in anderen Produkten" wie etwa der Vertrauensschadenversicherung. Die auf Cyber spezialisierten Versicherer „bieten sehr weite Deckungen, fordern jedoch intensive Risikodialoge". Und schließlich gebe es mittlerweile auch Plattformanbieter, die die Möglichkeit des Vergleichs bieten.

Eine Sache für Spezialisten?

Sind für die Versicherungsberatung von KMU im Cyberbereich Spezialisten nötig? Wie können Versicherer Berater unterstützen? „Aufgrund der enormen Dynamik im Cyber-Risks-Bereich empfiehlt es sich jedenfalls, einen Berater zu konsultieren", im Optimalfall einen mit Erfahrung, so Besenbäck. Viele Versicherungsanbieter, sagt Tenschert, „geben wertvolle Unterstützung bei der Beratung, die zumindest bei den ersten Kundengesprächen in Anspruch genommen werden sollte". Es handle sich um eine doch „für viele Berater relativ neue Versicherungsform". Kooperation sei empfehlenswert, auch mit versierten Kollegen.

Wichtig sei das Bewusstsein, dass Cyberattacken auch kleine Unternehmen treffen und die Folgen weitreichend

sein können, merkt Schilling an. Hierfür seien „klare Statistiken und Umfragen wichtige Hilfsmittel“ in der Beratung. „Unser Ziel als Cogitanda ist es, dass jeder Versicherungsmakler, der Gewerbekunden betreut, künftig auch in Sachen Cyber professionell beraten kann“, sagt Jäger. Hierzu stelle man eine digitale Berechnungsplattform und persönliche Ansprechpartner zur Verfügung.

„Als Spezialmakler“, sagt Kaltschmid, „unterstützen wir die Vermittler bei ihren Kunden, die an Cyber interessiert sind, mit der notwendigen Beratung, worauf es in welcher Branche ankommt, und nehmen auch die Ausschreibung des Risikos vor sowie die Platzierung.“ Unterstützt werde auch „in der Prävention, im Screening und vor allem auch bei den Risikodialogen mit mehreren Versicherern“.

Marktdurchdringung und Potenzial

Wie steht es bei KMUs derzeit um die Marktdurchdringung? „Die flippige Marktdurchdringung von bis zu 30 Prozent, die von einigen Marktteilnehmern kolportiert wird, sehen wir nicht“, sagt Kaltschmid und siedelt sie eher bei etwas über zehn Prozent an. Dabei gelte: größere Unternehmen – größere Durchdringung. Das Wachstumspotenzial der Cyberversicherung sei also sehr hoch, die Realisierung sei aber „mühsam“ und werde „nur durch ständiges Ansprechen beim Kunden und durch einen stärkeren Fokus der Vermittler“ zu heben sein.

Ähnlich Tenschert: Einer „stark ausbaufähigen“ Durchdringung stehen viele Kundengespräche und Abschlüsse in geringem Umfang gegenüber. Gleichwohl sei die Beratung unabdingbar, „schon alleine wegen der denkbaren Haftungsfolgen für eine unterlassene Information der Betriebe“.

Das Bewusstsein für das eigene Risiko, so Schilling, müsste ebenso gestärkt werden wie jenes für die Pflichten der Leitungsorgane: „Diese sind gesellschaftsrechtlich verpflichtet, ein angemessenes Risikomanagement zu installieren, einen Teil davon stellt die Cyber Security dar.“

„Manche sprechen davon, dass Cyber ‚die Feuerversicherung des 21. Jahrhunderts‘ sei“, sagt Jäger. Schätzungen zufolge verursachten Cybervorfälle bereits jetzt weltweit jährlich über sechs Billionen Euro Schaden. „Entsprechend ist mit zunehmenden Abschlüssen seitens der Unternehmen, aber auch mit steigenden Prämien zu rechnen.“

Prämien heute und morgen

Was kostet Cyberversicherung für KMUs jetzt und in Zukunft? Aktuell sei diese in der Regel gut leistbar und oft einfach zu erhalten, solange die „Hausaufgaben“ erledigt sind, sagt Jäger. „Für eine Prämie von 610,70 Euro ist bereits eine Cyberrisk inklusive VSV-Deckung möglich“, so Schilling.

Wobei freilich mehrere Faktoren eine Rolle spielen, etwa, so Besenbäck, die Unternehmensart oder die Risikosituation. „Was man jedenfalls faktisch belegen kann“, fährt Besenbäck fort, „ist eine Reduktion der Kapazitäten um 20 Prozent und eine Anhebung der Prämien um 30 Prozent in den letzten zweieinhalb Jahren, damit ist eine Tendenz erkennbar.“ Tenschert: „Mit zunehmender Zahl an Schadenfällen wird mit einem Prämienanstieg zu rechnen sein, das liegt in der Natur der Sache.“

Die meisten Cyberversicherer tarifieren KMU unterschiedlich, hält Kaltschmid fest. Produktionsunternehmen würden meist höher bepreist als Dienstleistungsunternehmen. Aber: „Die Prämien für KMU sind durchwegs gut leistbar.“ Dies gelte auch für die Zukunft, „so die Unternehmen bereit sind, auch künftig in organisatorische und technische Security-Maßnahmen zu investieren“. ■

Existenzrisiko Cyberangriff

Die Hälfte der heimischen Unternehmen sieht laut einer Umfrage ihre geschäftliche Existenz durch Cyberattacken bedroht. Zwei von drei Unternehmen rechnen mit mehr Angriffen in den kommenden Monaten. Und es wird offenbar immer schwieriger, sie abzuwehren. Fachleute drängen zu Risikomanagement.

Von Emanuel Lampert

Jedes Jahr erfasst das Bundeskriminalamt (BK) in der „Polizeilichen Kriminalstatistik" die von der Polizei an die Justiz übermittelten Anzeigen wegen strafrechtlich relevanter Handlungen. Der Internetkriminalität ist darin ein eigenes Kapitel gewidmet.

„Cybercrime im engeren Sinn" sind Handlungen, bei denen Angriffe auf Daten oder Computersysteme unter Ausnutzung der Informations- und Kommunikationstechnik (IKT) begangen werden, erläutert das BK: „Die Straftaten sind gegen die Netzwerke selbst oder aber gegen Geräte, Dienste oder Daten in diesen Netzwerken gerichtet, wie zum Beispiel Datenbeschädigung, Hacking oder DDos-Angriffe." Cybercrime im weiteren Sinn benutzt IKT lediglich als Mittel, um „herkömmliche" Delikte wie etwa Betrug, Drogenhandel oder Cybermobbing zu begehen.

2022 erreichte die Anzahl der Anzeigen wegen Internetkriminalität mit insgesamt 60.195 einen neuen Höhepunkt, plus 30,4 Prozent gegenüber 2021. Der Teilbereich „Cybercrime im engeren Sinn" legte gar um 44,5 Prozent auf 22.376 zu.

Um ein Segment herauszugreifen: 3.424 Anzeigen erfolgten wegen Cybererpressung; die Aufklärungsquote ist gering: 4,6 Prozent im Jahr 2022. „In den letzten Jahren konnte beobachtet werden, dass die Täter von den Massenaussendungen tendenziell weg und hin zum Suchen einzelner Sicherheitslücken von Unternehmen gingen", so das BK. Besonders KMUs stünden im Fokus der Täter. Der erpresste Betrag richte sich dabei oft nach der Finanzkraft von Unternehmen und deren vorhandener IT-Infrastruktur oder Backup-Lösungen.

Deloitte: Angreifer immer professioneller

Mit der Cybersicherheit in österreichischen Unternehmen hat sich Deloitte zusammen mit den Marktforschern von Sora auseinandergesetzt. Für den im April erschienenen „Deloitte Cyber Security Report" wurden 350 Mittel- und Großunternehmen befragt. Dabei habe sich gezeigt, dass die Anzahl der Angriffe zwar annähernd auf Vorjahresniveau liege, die Abwehr aber immer schwerer falle.

Die Analyse mache deutlich, „dass sich Betriebe mit einer zunehmenden Professionalität der Angreifer auseinandersetzen müssen", kommentierte Sora-Geschäftsführer Christoph Hofinger. „Im Vergleich zum Vorjahr konnten um rund die Hälfte weniger Attacken durch technische Infrastrukturmaßnahmen verhindert und um knapp ein Drittel weniger Daten nach einem Angriff wiederhergestellt werden. Das sind alarmierende Zahlen – solche Sprünge erlebt man als Marktforscher nicht jeden Tag."

Angesichts der kritischen geopolitischen Lage spiele Risikomanagement eine zentrale Rolle für einen wirksamen Schutz, sagte Karin Mair, Managing Partnerin Risk Advisory und Financial Advisory bei Deloitte. „Zwar haben viele Unternehmen dies auch erkannt, gleichzeitig haben 47 Prozent aber noch kein Risikomanagement implementiert oder Maßnahmen getroffen – hier gibt es Investitionsbedarf."

Vor dem Hintergrund einer steigenden Professionalität der Angriffe seien „klare Pläne, wie im Fall des Falles zu reagieren ist", erforderlich, unterstrich auch Georg Schwondra, Partner Cyber Risk bei Deloitte. „Regelmäßige Tests und Evaluierungen dieser Pläne sind das Um und Auf." Eine Hürde stellt der Personalmangel dar. „Das Fehlen der Talente hat massive Auswirkungen auf die Cyber Security der Unternehmen", so Mair. Eine sichere IT-Landschaft bedürfe ausreichender, qualifizierter Personalressourcen.

KPMG: Hälfte sieht Angriffe als Existenzbedrohung

Im Mai folgte KPMG Austria mit der gemeinsam mit dem Sicherheitsforum Digitale Wirtschaft des Kompetenzzentrum Sicheres Österreich (KSÖ) veröffentlichten Analyse „Cybersecurity in Österreich 2023". Hierfür wurden im Februar und März 903 kleine, mittlere und große Unternehmen verschiedener Branchen befragt.

Hier fielen die Antworten hinsichtlich der Cyberangriffe drastischer aus: Gegenüber 2021 habe es um 201 Prozent mehr Attacken gegeben. Jedes einzelne der 903 Unternehmen sei 2022 von Phishing betroffen gewesen, gefolgt unter anderem von „Business-E-Mail-Compromise" und „CEO Fraud" (88 Prozent), „Social Engineering" (57 Prozent) sowie Angriffen auf die Lieferkette (39 Prozent). Angriffe auf die kritische Infrastruktur würden laufend zielgerichteter und komplexer, fügt Deloitte hinzu. Krankenhäuser, Windparks zur Stromerzeugung, Supermärkte und Handelsketten, aber auch IT-Dienstleister seien immer häufiger Ziele von Ransomware-Attacken.

Ähnlich wie in der Deloitte-Analyse klingt das Fazit von Robert Lamprecht, Director bei KPMG: Sei 2021 noch „vorsichtiger Optimismus" zu spüren gewesen, so habe sich in den letzten Monaten gezeigt, dass die Angreifer ihre (potenziellen) Opfer „abgehängt" haben. „Auch hybride Bedrohungen durch den Einsatz verschiedener Methoden der Einflussnahme wie beispielsweise gezielte Desinformationskampagnen werden immer häufiger zur Realität." So sehen 72 Prozent der Unternehmen staatliche oder staatlich unterstützte Angriffe als besondere Herausforderung an. 63 Prozent stufen „Social Engineering"

über Fake-Telefonanrufe mittlerweile sogar als normales Tagesgeschäft ein, teilt KPMG mit. Weitere Ergebnisse:

- 63 Prozent rechnen mit mehr Cyberangriffen auf ihr Unternehmen in den nächsten zwölf Monaten.
- 55 Prozent sehen durch Cyberangriffe ihre geschäftliche Existenz bedroht.
- 33 Prozent waren Opfer von Ransomware/Erpressung.
- Bei jedem Vierten ist es in privat genutzten sozialen Netzwerken zu Beeinflussungsversuchen gekommen, die auf das berufliche Umfeld abzielten.
- 22 Prozent waren in den letzten zwölf Monaten von „Deep Fakes", also echt wirkenden aber gefälschten Medieninhalten, betroffen.
- 43 Prozent benötigen durchschnittlich vier bis sechs Monate, um IT-Experten einzustellen.
- 47 Prozent haben sich mit der neuen EU-Cybersicherheits-Richtlinie „NIS 2" beschäftigt.

Schwerwiegende Folgen

Erfolgreich verlief 2022 rund jede zehnte Attacke (12 Prozent). „Beinahe jedes siebte Unternehmen (14 Prozent) musste aufgrund eines Ransomware-Angriffs Betriebsunterbrechungen von mehr als vier Wochen in Kauf nehmen, ein Drittel der Unternehmen immerhin von rund einer Woche", so KPMG-Partner Andreas Tomek. „Das kann eine klare Existenzbedrohung darstellen."

Nach einem Cyberangriff seien es neben Reputationsverlusten vor allem Betriebsstillstand und Aufarbeitung, die den finanziellen Schaden in die Höhe treiben, so KPMG. Knapp die Hälfte der Unternehmen habe einen finanziellen Schaden von bis zu 100.000 Euro erlitten. Bei 12 Prozent betrage er über eine Million Euro.

Die gute Nachricht sei, dass inzwischen eine Sensibilisierung eingetreten sei, die dazu geführt habe, dass technische Infrastruktur und Schutzmaßnahmen sukzessive ausgebaut werden. Gleichwohl betonen die Studienautoren den Faktor Mensch: Er sei zwar der Eintrittspunkt für viele Cyberangriffe, „gleichzeitig aber auch einer der wirksamsten Sicherheitsfaktoren, wenn es um die Prävention und Erkennung von Vorfällen geht". Daher sei „eine gelebte Cybersecurity-Kultur in den Unternehmen" nötig.

Cybercrime im Onlinehandel

Ebenfalls im Mai publiziert wurde die „Sicherheitsstudie 2023", die der Handelsverband zusammen mit dem Bundeskriminalamt erstellt hat. 150 Unternehmen quer durch die Handelsbranchen, vom EPU bis zum Konzern, haben im Februar und März teilgenommen.

64 Prozent (2020: 46 Prozent) der Onlinehändler haben nach eigenen Angaben schon „in irgendeiner Form Erfahrungen mit Betrug gemacht", 34 Prozent schon mehrmals. „61 Prozent aller Händler waren bereits Opfer von Phishing-Angriffen, bei denen z.B. Login-Informationen erbeutet wurden", heißt es in der Studie weiter. 52 Prozent haben Erfahrungen „mit Malware, also Schadsoftware aus Spam-Mails oder manipulierten Links" gemacht. Danach folgen Cybererpressung (32 Prozent), bei der Hacker Geld verlangen, um angeblich drohende Angriffe noch abzuwenden, und Ransomware, wobei Angreifer Daten verschlüsseln und Lösegeld fordern (28 Prozent).

Beim E-Commerce-Betrug häufen sich vor allem Bestellungen, bei denen die Käufer vorab wissen, dass sie nicht zahlen können (57 Prozent aller Händler). Häufig komme inzwischen auch die Angabe einer falschen Identität vor (51 Prozent) oder die Nutzung verfälschter Namens- bzw. Adressdaten (50 Prozent). 47 Prozent hatten laut Umfrage schon mit Kunden zu tun, die den Erhalt der Ware abstreiten, obwohl sie sie erhalten haben.

Bei den kleineren Betrieben beläuft sich die Mehrzahl der durch Onlinebetrug verursachten Schadensummen auf bis zu 500 Euro (30 Prozent) oder auf Beträge zwischen 500 und 10.000 Euro (ebenfalls 30 Prozent). „Unternehmen mit mehr als zehn Beschäftigten erlitten 2022 im Schnitt wesentlich höhere Verluste: 32 Prozent der entstandenen Schäden machten zwischen 5.000 und 10.000 Euro aus, bei 27 Prozent beliefen sich die finanziellen Einbußen auf 10.000 bis zu 100.000 Euro." ■

GARANTA
VERSICHERUNG

Unterwegs in Richtung Zukunft.

Mit viel Erfahrung und
klarem Blick für die Zukunft
bieten wir verlässlichen Schutz
für jede Lebenslage.

**Persönlich und vertrauensvoll –
gestern, heute, übermorgen.**

www.garanta.at

Ein Schutzschild gegen digitale Gefahren

Gegen Cybergefahren kann man mit technischen und mit organisatorischen Maßnahmen angehen – und mit Recht: Aktuell sind diverse europäische Rechtsakte in Planung oder Umsetzung. Ein Überblick über zentrale neue Gesetze und Vorhaben.

Von Emanuel Lampert

Cyberkriminalität kennt keine nationalen Grenzen, und mögliche Auswirkungen von Angriffen sind nicht unbedingt auf einen kleinen Raum beschränkt; sie können großflächige Folgen haben und Dominoeffekte auslösen.

In einer kürzlich veröffentlichten, von KPMG zusammen mit dem Kompetenzzentrum Sicheres Österreich (KSÖ) durchgeführten Umfrage erachteten denn auch 74 Prozent der befragten Unternehmen in Österreich eine verstärkte EU-weite Zusammenarbeit im Kampf gegen Cyberkriminalität als essenziell. „Wir müssen und werden uns mit der Frage der digitalen Souveränität in Europa auseinandersetzen", sagte KSO-Präsident Michael Höllerer anlässlich der Präsentation.

Auf Unionsebene gibt es diverse Aktivitäten im Zusammenhang mit digitaler Sicherheit – nicht erst seit heute, aber in den letzten Jahren wird dem Thema Cybersicherheit besondere Aufmerksamkeit gewidmet.

Ausweitung der Sicherheitsregeln für wichtige Sektoren

Eines der jüngsten Ergebnisse ist die sogenannte „NIS 2"-Richtlinie (http://data.europa.eu/eli/dir/2022/2555/oj). Sie ist die Nachfolgerin der 2016 beschlossenen Richtlinie über „Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union" (http://data.europa.eu/eli/dir/2016/1148/2016-07-19) und steht seit 27. Dezember 2022 im Amtsblatt der EU. Die Mitgliedstaaten haben nicht ganz zwei Jahre Zeit zur Umsetzung, spätestens ab 18. Oktober 2024 sind die Vorschriften anzuwenden.

Die derzeit geltende NIS-1-Richtlinie – in Österreich wurde sie durch das Netz- und Informationssystemsicherheitsgesetz (http://www.ris.bka.gv.at/eli/bgbl/I/2018/111) umgesetzt – verlangt von den „Betreibern wesentlicher Dienste", dass sie „geeignete und verhältnismäßige technische und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die sie für ihre Tätigkeiten nutzen, zu bewältigen". Sie statuiert auch bestimmte Meldepflichten. Erfasst sind eine Reihe von Betreibern aus den Schlüsselsektoren Energie, Verkehr, Finanzmarkt, Gesundheit und Trinkwasserversorgung, und digitale Infrastruktur, sofern bestimmte Kriterien auf sie zutreffen – unter anderem, dass es sich um einen Dienst handelt, der für die Aufrechterhaltung kritischer gesellschaftlicher und/oder wirtschaftlicher Tätigkeiten unerlässlich ist. Auch für Anbieter bestimmter digitaler Dienste gelten diesbezügliche Vorgaben.

Die NIS-2-Richtlinie soll nun der voranschreitenden Digitalisierung Rechnung tragen: Sie bezieht sich auf Betreiber aus einem künftig größeren Kreis an Wirtschaftssektoren, beispielsweise Postdienste, Lebensmittelproduktion oder weltraumgestützte Dienste. Ein Überblick über die Neuerungen der NIS 2, inklusive Webinar, ist auf der Website der Wirtschaftskammer (http://www.wko.at/service/innovation-technologie-digitalisierung/nis2-uebersicht.html) abrufbar.

Cybersicherheitsvorgaben für gesamten Produktlebenszyklus

Noch jüngeren Datums ist ein Vorschlag für eine Verordnung über Cybersicherheitsanforderungen an „Produkte mit digitalen Elementen", auch bekannt als „Gesetz über Cyberresilienz" (Cyber Resilience Act, CRA), den die Europäische Kommission im September 2022 vorgelegt hat (https://eur-lex.europa.eu/procedure/EN/2022_272).

Es wäre, so die Kommission, die „erste EU-weite Rechtsvorschrift ihrer Art", die verbindliche Cybersicherheitsanforderungen für den gesamten Lebenszyklus solcher Produkte festschreibt. Ziel sei, dass digitale Produkte – wie drahtlose und drahtgebundene Hardware sowie Software – für die Verbraucher sicherer werden. Hersteller würde eine Pflicht zu Support und Softwareupdates treffen, sodass sicherheitsrelevante Schwachstellen behoben werden. Zudem sollen Konsumenten ausreichend über die Cybersicherheit der Produkte, die sie kaufen und verwenden, Auskunft erhalten, „über das Ende der Lebensdauer der Produkte und die gebotene sicherheitsbezogene Unterstützung" informiert werden und Sicherheitsupdates und -unterstützung „über einen angemessenen Zeitraum" bekommen. Was diesen angemessenen Zeitraum angeht, ist in dem Vorschlag von der „erwarteten Produktlebensdauer oder einem Zeitraum von fünf Jahren" ab Markteinführung die Rede, je nachdem, welcher der beiden Zeiträume kürzer ist.

Angesichts einer zunehmenden Zahl „intelligenter und vernetzter Produkte" könne ein Cybersicherheitsvorfall bei einem Produkt Auswirkungen auf die gesamte Lieferkette haben „und möglicherweise wirtschaftliche und soziale Tätigkeiten im gesamten Binnenmarkt ernsthaft stören, die Sicherheit beeinträchtigen oder sogar Leben gefährden", argumentiert die Kommission.

Im Bereich der Cybersicherheit sei Europa „nur so stark wie sein schwächstes Glied – zum Beispiel ein gefährdeter Mitgliedstaat oder ein unsicheres Produkt in der Lieferkette", sagte Binnenmarkt-Kommissar Thierry Breton bei der Präsentation des Entwurfs letzten September.

„Computer, Handys, Haushaltsgeräte, virtuelle Hilfsgeräte, Autos, Spielzeug usw. – alle diese hunderte Millionen von vernetzten Produkten sind eine potenzielle Schwachstelle, über die Cyberangriffe erfolgen können." Für die meisten Hardware- und Softwareprodukte gälten heute noch keine Cybersicherheitsanforderungen. Beschlossen ist noch nichts, der Gesetzesentwurf ist derzeit in Diskussion.

Schutzschild und Notfallmechanismus

Ganz „frisch" ist noch ein Vorschlag, den die Kommission im April auf den Tisch gelegt hat: der Entwurf für ein „EU-Cybersolidaritätsgesetz" (EU Cyber Solidarity Act, https://ec.europa.eu/commission/presscorner/detail/de/QANDA_23_2244). Mit ihm sollen, in den Worten der Behörde, „ein europäischer Cyberschutzschild und ein umfassender Cybernotfallmechanismus" geschaffen werden.

Beim Schutzschild denkt die Kommission an eine EU-weite Infrastruktur aus „Sicherheitseinsatzzentren", also Stellen, die sich mit Hilfe künstlicher Intelligenz und „fortgeschrittener Datenanalyse" mit der Erkennung und Abwehr von Cyberbedrohungen befassen. Diese Zentren könnten schon Anfang 2024 einsatzbereit sein, meint man in Brüssel.

Im Rahmen des geplanten „Cybernotfallmechanismus" soll dreierlei unterstützt werden. Erstens: Vorsorgemaßnahmen – inklusive Tests zur Ermittlung potenzieller Schwachstellen bei Einrichtungen in besonders kritischen Sektoren wie etwa Gesundheitsversorgung, Verkehr und Energie usw. – auf Grundlage gemeinsamer Risikoszenarien und -methoden. Zweitens: der Aufbau einer neuen „EU-Cybersicherheitsreserve", die aus Sicherheitsvorfall-Notdiensten vertrauenswürdiger Anbieter besteht, die vorab unter Vertrag genommen werden und bei einem großen oder schwerwiegenden Cybersicherheitsvorfall auf Ersuchen der EU oder eines ihrer Staaten sofort eingreifen können. Drittens: die finanzielle Förderung der gegenseitigen Unterstützung der Mitgliedstaaten.

Außerdem ist ein „Überprüfungsmechanismus für Cybersicherheitsvorfälle" vorgesehen, der die nachträgliche Überprüfung und Bewertung von Cybersicherheitsvorfällen zum Gegenstand hat. Sein Sinn und Zweck besteht darin, Erkenntnisse zu gewinnen und gegebenenfalls Empfehlungen zur Verbesserung der Cyberabwehr zu formulieren.

Eine neue „Akademie für Cybersicherheitskompetenzen" wiederum soll „private und öffentliche Initiativen bündeln, die darauf abzielen, die Cybersicherheitskompetenzen auf europäischer und nationaler Ebene zu verbessern und sichtbarer zu machen". Sie ist als Informationsplattform zu Ausbildungsangeboten, Schulungen und Zertifizierungen aus der gesamten Union zu verstehen, mit dem Ziel, sich zu einem „gemeinsamen Raum für Hochschuleinrichtungen, Schulungsanbieter und die Branche" zu entwickeln. Mit der Akademie, sagte Kommissionsvizepräsident Margaritis Schinas, „soll unsere Kompetenzbasis gestärkt werden, damit wir auch die Fachkräfte haben, die wir dafür brauchen". ■

COGITANDA® - DER CYBER SPEZIALIST
IMMER AN IHRER SEITE!

Bevor etwas passiert,
sprechen Sie mit uns!

Umfassende
Cyber Risiko Prävention

Maßgeschneiderte
Cyber Versicherung

Hochprofessionelles
Cyber Schadenmanagement

COGITANDA®
CYBER SIND WIR.

www.cogitanda.at • +43 (0)1 206093-080 • austria@cogitanda.com

COGITANDA ACADEMY

DIE E-LEARNING-PLATTFORM
FÜR SIE UND IHRE MITARBEITER:INNEN

COGITANDA®
CYBER SIND WIR.

www.cogitanda.at • +43 (0)1 206093-080 • austria@cogitanda.com

Cyberversicherungen müssen als Gesamtpaket angeboten werden

Genau so wie die digitalen Angriffsmethoden muss sich auch das Angebot der Cyberversicherer weiterentwickeln – und das geht nur, wenn die Branche selbst Fachkräfte ausbildet. So ein Fazit des Insurance Forum Austria Anfang Mai in Wien.

Von Barbara Ottawa

Cyberkriminalität sei inzwischen eine „extrem entwickelte ‚Branche'" gab Markus Orth, Leiter des Industriesegments Schaden/Unfall bei der Gothaer Allgemeinen Versicherung, in seinem Vortrag zu bedenken. Dennoch ist er überzeugt, dass man diese Risiken weiter konventionell abdecken kann – aber nur mit „den richtigen Antworten".

Markus Niederreiner, Managing Director Deutschland beim Spezialversicherer Hiscox, lieferte Zahlenmaterial, um das wachsende Gefahrenpotenzial zu illustrieren: „Mittlerweile geben 46 Prozent aller befragten Unternehmen im deutschsprachigen Raum an, in den letzten 12 Monaten Opfer mindestens einer Cyberattacke geworden zu sein." Aber auch das Bewusstsein der Unternehmen für diese Risiken erhöhe sich weiter: Die „Investitionen in Cybersicherheit seit 2019 sind international um 250 Prozent gestiegen", sagte Niederreiner. Mittlerweile macht dieser Posten im Schnitt 24 Prozent des IT-Budgets einer Firma aus.

Mit den Schadenfällen erhöht sich auch die Schadensumme, was dazu geführt hat, dass die Cyberversicherer 2021 erstmals Verluste erlitten. Dazu wurde der Gesamtverband der Deutschen Versicherer (GDV) zitiert: „Unter dem Strich betrug die Schaden-Kostenquote fast 124 Prozent nach 65 Prozent ein Jahr zuvor".

Besonderer Schadentreiber war die „Ransomware", also erpresserische Hackerangriffe. Beispielhaft führte hier Christian Berger, Geschäftsführer der Marsh Austria, Zahlen aus dem Kundenportfolio seiner Unternehmensgruppe an, wo Ransomware der „Schadentreiber Nummer 1" war und 60 Prozent aller Schäden ausmachte. Allerdings sei der Anstieg der Fälle in den letzten Jahren deutlich zurückgegangen. Im Jahr 2019 sei noch eine Steigerung der Fallzahlen von 299 Prozent im Vergleich zum Vorjahr zu verzeichnen gewesen, 2021 lag der Anstieg nur mehr bei 19 Prozent. Das liege vor allem daran, dass die Unternehmen besser vorbereitet sind.

Orth zeichnete für die Gothaer ein ähnliches Bild wie bei Marsh, betonte aber, dass es bei Ransomware „nicht um die Frequenzproblematik, sondern um die Schadenhöhe" gehe.

Neue Anbieter kommen nach Bereinigung

„Aufgrund der gestiegenen Bedrohungslage" erwartet Orth „weiterhin ein substanzielles Beitragswachstum für die kommenden Jahre" im Bereich Cyberversicherung. Mit der steigenden Nachfrage werden auch „weitere Anbieter in den Markt eintreten".

Allerdings werden diese andere Geschäftsmodelle und Lösungsansätze liefern müssen als jene, die auf der ersten Neugeschäftswelle 2019 mitgeschwommen sind. Viele dieser Quereinsteiger in die Cyberversicherungsbranche haben sich mit den exponentiellen Anstiegen von Schadenfällen zwischen 2019 und 2022 wieder vom Markt verabschiedet.

Was es jetzt braucht, sind gesamtheitliche Produktangebote, darüber waren sich alle Panelteilnehmer beim IFA einig. Niederreiner warnte, dass „Cyberversicherer riskieren, perspektivisch die Relevanz im Markt zu verlieren, wenn es ihnen nicht gelingt, die wachsende Nachfrage nach Cyberdeckungen mit markt- und risikogerechten Lösungen zu beantworten". Denn einige Unternehmen überlegen sich aufgrund der extrem aufwändigen Risikoprüfungen, die Cyberversicherer (insbesondere Industriekunden) abfragen, „ob sie hohe Prämien zahlen oder das Geld stattdessen in die Cyber-Resilienz-Technologie investieren sollen".

Aber Orth sieht hier die Chance, als Versicherer ein Gesamtpaket zu liefern. Einerseits müsse ein „umfangreicheres Underwriting bei Risikozeichnung und Vertragsverlängerungen" angeboten werden, dabei wird die Entwicklung von digitalisierten Underwriting- und Verarbeitungsprozessen „immer wichtiger", wie auch die Anbindung an Vertriebs-Plattformen. Darüber hinaus müssten immer mehr externe Dienstleister, wie Risk-Assessment, Quality-Check, Prävention oder Schadenmanagement, mit ins Boot geholt werden.

Auch Makler suchen „nach weiteren Differenzierungsmerkmalen, wie zum Beispiel IT-Security-Beratung, Risk-Assessment und Policierung". Orth verglich die Cyber mit einer Feuerversicherung, die mittlerweile auch zum Standard gehöre und wo Prävention genauso wichtig sei wie Reaktion im Schadenfall.

Ausbilden für den großen Teich

Aber das alles ist eine Ressourcenfrage. Und genau hier stößt die Versicherungsbranche an ihre Grenzen – vor allem, was die Fachkräfte betrifft. Die Versicherungsbranche sei noch immer für viele wenig attraktiv – obwohl sich alle Vortragenden darüber einig waren, dass Cyberversicherung „sexier" ist als der Rest der Branche.

Orth betonte, dass der Informationsbedarf der Versicherer in dem Bereich stetig steige. Aber die Fachkräfte, die man braucht, seien am Markt „nicht leistbar" zu finden. Deshalb werde die Gothaer vermehrt auf interne Weiterbildung setzen. Niederreiner dazu: „Als kleiner Spezialversicherer haben wir schon lange auf eigene Ausbildung gesetzt, aber wir waren uns auch immer bewusst, dass wir für den Teich ausbilden", also

für den Rekrutierungs-Pool, in dem andere Versicherer fischen.

Viele Fachkräfte sind in den letzten Jahren von Unternehmen übernommen worden, aber hier zeigt der Hiscox Cyber Readiness Report 2022 einen etwas gegenläufigen Trend auf: In Deutschland weisen nur mehr drei Prozent der befragten Unternehmen eine „Cyberexpertise" aus, 2021 waren es noch 21 Prozent. „Zwar nehmen wir eine steigende Sensibilität für Cyberschutzmaßnahmen in Unternehmen war. Die vergangenen Wochen und Monate haben jedoch gezeigt, wie anspruchsvoll es ist und bleiben wird, dieses Risiko kontrollierbar zu halten," so Niederreiner.

Kumulrisiken und Vorbereitung

Ein Grund für die stark zurück gegangene Selbsteinschätzung was die Expertise betrifft, ist laut Hiscox-Umfrage unter anderem die große Zahl an Kumul-Attacken. Diese sind, so Niederreiner, ein von einigen Versicherern „weitgehend ausgeblendetes Risiko". Diese Anbieter würden von „zukünftigen Cybergroßschäden besonders hart getroffen werden".

Auch Orth betonte, dass „der Kumulversicherungsschutz und seine Beherrschung für die Versicherungsbranche langfristig wichtig ist". Er wies aber auch darauf hin, dass die „Modellierung und Bemessung" solcher Ereignisse „noch nicht gelöst sind" und sich noch in der Entwicklung befinden. „Versicherer müssen dafür auch die richtige Rückversicherung für die eigene Bilanz finden – und Rückversicherungen sind endlich". Letztendlich sei ein solcher Schaden, der dann mehrere Kunden betreffe, vor allem aber wieder eine Ressourcenfrage.

Vorbeugende Maßnahmen können aber schon in den Unternehmen getroffen werden und alle Umfragen

zeigen, dass die Angst vor Hackerangriffen und damit verbundenen Betriebsunterbrechungen derzeit in allen Branchen als größter Risikofaktor identifiziert wird. Dennoch gibt es laut Berger Firmen, die relativ einfache Sicherheitsmaßnahmen noch nicht getroffen haben. Und Unternehmen, die etwa noch keine Multifaktor-Authentifikation für externe Systemzugriffe haben, „tun sich schwer, eine Cyberversicherung zu bekommen".

„Cyber Incident Management", also die Erstellung eines Notfallplanes, der regelmäßig überprüft und auch durchgespielt wird, sei „das Gebot der Stunde" für Unternehmen, so Berger. Ein gut eingespieltes Cyber Incidence Team könne Datenverletzungskosten deutlich reduzieren, indem Angriffsstellen rasch gefunden und geflickt werden sowie die richtigen Behörden und Kunden zum richtigen Zeitpunkt informiert werden. Er betonte, dass bei Vorfällen nicht auf die Dokumentation vergessen werden darf. „Denn das braucht der Versicherer dann für die Abwicklung", so Berger.

Besonders wichtig werde das Cybermanagement bei Firmenzusammenlegungen und -übernahmen, aber auch bei internen Organisationsänderungen sowie bei großen neuen IT-Anschaffungen. Oft vergessen werde auf alte Systeme, die weiterlaufen müssen, für die es aber keine Updates mehr gibt. Für diese rät Berger, sie vom internen Netzwerk zu nehmen und gesondert laufen zu lassen.

Die Frage, ob Unternehmen, die alle Vorkehrungen getroffen haben, dann überhaupt noch eine Versicherung brauchen, bejahte Berger. Aber umgekehrt sei eine Cyberversicherung allein auch nicht die Lösung. „Denn die hilft nicht bei allen Problemen," so Berger. ■

höhere Erträge

Weiterbildung

bessere Produkte

persönlicher Support

IT-Komplettsystem

Bestandssicherheit garantiert

Alles dreht sich um dich

#360°servicelösung

Viele Versicherungsmakler:innen und Agent:innen in ganz Österreich haben sich bereits für eine wefox Partnerschaft entschieden. Wie auch du von unserem 360° Serviceangebot profitieren kannst, zeigen wir dir gerne persönlich.

Buche jetzt deinen **Beratungstermin** und profitiere noch heute von einer Partnerschaft mit wefox.

Überzeuge dich selbst von unserem einzigartigen Konzept

wefox

Insurance. But simple.