

Gewappnet gegen Cybercrime

Jeder vierte Mittelständler wurde bereits Opfer von Cyberkriminellen

Eigene Website, Smartphone, Tablet, PC etc. Auch Handwerksbetriebe sind darauf angewiesen und damit für Cyberkriminelle ein lohnendes Ziel – egal wie groß oder klein sie sind. Technische Vorkehrungen und die Sensibilisierung von Mitarbeitern werden immer wichtiger. Cyberpolice decken das Restrisiko und helfen bei der Prävention.

Von den vielen Vorzügen des World Wide Web für das Wirtschaftsleben und seiner Unumgänglichkeit für das eigene Unternehmen dürfte inzwischen wohl fast jeder Elektro-Handwerksbetrieb überzeugt sein. Aus naheliegenden Gründen muss man jedoch auch über die Risiken reden. Denn ein „Wachstumsfeld“ im Zuge der immer stärkeren digitalen Vernetzung ist Cybercrime. „Ein Massenphänomen, das nicht nur Privatpersonen, sondern auch die Wirtschaft immer stärker trifft“, so Peter Henzler, Vizepräsident beim Bundeskriminalamt mit Bezug auf das aktuelle Lagebild „Cybercrime“ des BKA. Cyberangriffe sind nach seinen Worten für Kriminelle „ein lohnendes Geschäftsfeld“. Das widerspiegeln dann auch die Zahlen der jüngsten BKA-Analyse. Rund 87 000 Fälle von Cybercrime registrierte die Polizei demnach 2018, ein Prozent mehr als im Jahr zuvor. Einen Anstieg von rund fünf Prozent (271 864 Fälle) gab es auch bei der Anzahl der Straftaten mit dem Internet als Tatmittel.

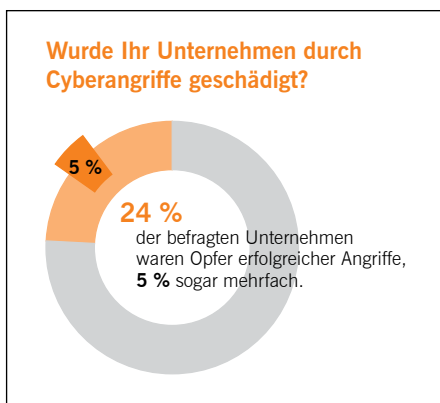
Großes Dunkelfeld

Cyberkriminelle müssen die Schadsoftware dabei nicht zwangsläufig selbst entwickeln. Auf Marktplätzen im Clearnet (sichtbares Web), Deepweb (nicht frei zugängliches Web) und im Darknet (abgeschlossenes Netzwerk) gibt es gegen Bezahlung eine Vielzahl illegaler Angebote, um beispielsweise Angriffe auf Firmennetzwerke und Webseiten zu starten oder Viren programmieren zu lassen. „Crime-as-a-Service“ nennt sich dieses Geschäftsmodell, bei dem neben Schadsoftware auch gestohlene Daten oder Anonymisierungsdienste verkauft werden.

fürchten einen Vertrauensverlust bei Partnern und Kunden.

Kleine Unternehmen werden häufig attackiert

Jeder vierte Mittelständler in Deutschland war bereits Opfer mindestens eines erfolgreichen Cyberangriffs, fasst der Gesamtverband der Deutschen Versicherungswirtschaft (GDV) das Ergebnis einer von ihm beauftragten Forsa-Studie zusammen (Bild 1). Die macht zudem deutlich: Gerade kleine Unternehmen werden besonders häufig – und mehrmals – Opfer von Cyberkriminellen. Die Befragung legt zudem folgenden Schluss nahe: Zu viele halten ihr Unternehmen schlicht für zu klein oder ihre Daten für nicht interessant genug, um angegriffen zu werden. Doch wer so denke, habe noch nicht wirklich verstanden, wie Cyberkriminelle vorgehen, so der GDV. Für massenhaft versuchte und ungezielte Attacken spielen demnach Umsatz- oder Mitarbeiterzahlen genauso wenig eine Rolle wie die Brisanz der gespeicherten Daten: Alle Unternehmen, die in irgendeiner Form am Netz hängen, werden angegriffen. „Und auch die vermeintlich langweiligsten Daten haben ihren Wert – mindestens für diejenigen, deren Daten nach einer Ransomware-Attacke plötzlich gesperrt sind.“



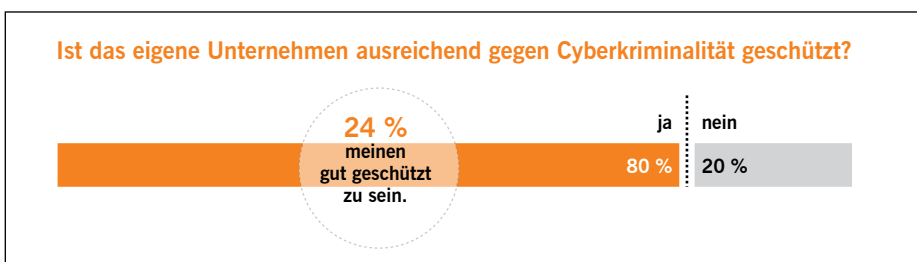
Quelle: GDV

1 Jedes vierte Unternehmen war schon von Cyberangriffen betroffen

Cybercrime verursachte 2018 einen Schaden in Höhe von über 60 Millionen Euro, ein Rückgang um rund 18 Prozent im Vergleich zum Vorjahr (2017: 71,4 Millionen Euro). Kein Widerspruch zu den wachsenden Risiken. Denn: Die Zahl bilde nur ab, was der Polizei bekannt geworden sei, so das BKA. Tatsächlich dürfte sich der Schaden für Unternehmen auf über 100 Milliarden Euro belaufen, so der BKA-Lagebericht unter Verweis auf Schätzungen aus der Wirtschaft im Betrachtungszeitraum 2018/2019. Die enorme Differenz erklärt sich laut Bundeskriminalamt auch durch das hohe Dunkelfeld in diesem Bereich. Insbesondere Unternehmen zeigen Fälle von Cybercrime und damit verbundene materielle Schäden nach wie vor vergleichsweise selten an. Grund: Sie

Prävention mit Lücken

Was aus Sicht der Assekuranz das Problem noch verschärft: Auf die Fehleinschätzung des Risikos folgen bei vielen kleinen Unternehmen Fehlentscheidungen bei der Prävention. Wer seinen Schutz an der gefühlten statt an der tatsächlichen Gefahr ausrichte, wähne sich schon mit Virenschanner und Firewall ausreichend geschützt. Zu oft seien kleine Unternehmer von ihren Sicherheitsmaßnahmen überzeugt (Bild 2). Ihre Bereitschaft, in Cybersicherheit zu investieren, sei gering. Infolgedessen seien sie für Cyberkriminelle ein leichtes Ziel. Sie können den Angreifern am wenigsten Widerstand entgegensetzen. Größtes Einfallstor sind dabei



Quelle: GDV

2 (Zu) hohes Vertrauen in den eigenen Schutz

Autorin

Carla Fritz arbeitet als freie Wirtschaftsjournalistin, Berlin.

E-Mails (Bild 3). „Elektronische Post samt Anhängen wird zu oft gedankenlos geöffnet“, kommentieren die Cyberexperten der Assekuranz das Geschehen. Darauf setzen Cyberkriminelle – und legen mit ihrer Schadsoftware nicht nur die IT-Systeme, sondern ganze Betriebe lahm. Das war in knapp 60 Prozent der betroffenen Unternehmen der Fall (Bild 4). Bis die IT-Systeme nach einem erfolgreichen Cyberangriff wieder laufen, vergehen bei den meisten Unternehmen mehrere Tage (Bild 5).

Angriff auf eigenen Wunsch

In Stresssituationen macht man Fehler. „Das nutzen die Angreifer aus. Es gibt aber technisch schon sehr gute Lösungen, die auch unbekannte Schadprogramme gut abwehren“, sagt Michael Wiesner, seit 25 Jahren IT-Sicherheitsexperte für den Mittelstand. Als sogenannter White-Hat-Hacker fühlt der Informatiker mittelständischen Unternehmen hinsichtlich ihrer IT-Sicherheit und in deren eigenem Auftrag auf den Zahn. Er deckt Sicherheitslücken auf, indem er versucht, in die Netzwerke der Auftraggeber einzudringen – so weit wie möglich. „Damit man dann auch weiß: Wie weit käme ein realer Angreifer denn tatsächlich?“ Unterwegs ist er quer durch alle Branchen – erst jüngst sehr intensiv in Krankenhäusern und im Bereich der Heilberufe. Was er dabei u. a. bei einem IT-Sicherheitstest von Arztpraxen – im Auftrag des GDV und mit Wissen der Ärzte – herausfand, dürfte so oder ähnlich auch anderswo ein Sicherheitsrisiko sein.

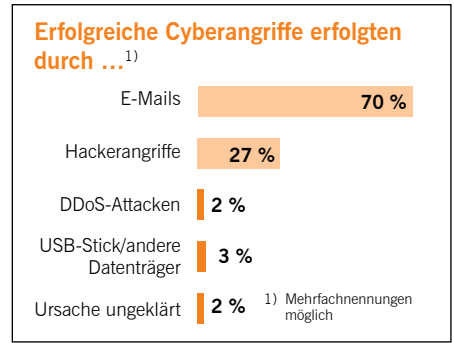
Simple Passwörter und fehlende Updates

Passwörter waren demnach das größte Problem bei der internen Sicherheit. Zu simpel, leicht zu knacken. „Tatsächlich konnten wir darüber die meisten Systeme übernehmen – außerdem dort, wo keine Updates eingespielt wurden. In solchen veralteten Systemen gibt es in der Regel immer Sicherheitslücken, die ich als Angreifer ausnutzen kann“, sagt der IT-Experte, der für die VdS Schadenverhütung maßgeblich an IT-Sicherheitsrichtlinien arbeitet. Dazu kommen teils ungeschützte, leicht zugängliche Server – ein großes Handicap, wenn Angreifer von innen kommen. Für den ständigen Zugriff auf das Netzwerk reicht nach Wiesners Worten schon eine Netzwerkdose, in die dann ein kleines Gerät gesteckt wird. „Das baut z. B. über Mobilfunk eine Verbindung

zum PC des Angreifers auf. So kann der von jedem Ort der Welt aus Daten abfischen.“

Plan B im Schubfach

Seine Empfehlung: Neben einer guten Prävention braucht man vor allem auch einen Plan B. Den arbeitet man dann ab – ohne noch lange nachdenken zu müssen: Was passiert, wenn es passiert ist? Wie kommt man wieder auf die Beine? Wie kann man Ausfallzeiten minimieren? „Früher nannte



Quelle: GDV

3 Die häufigsten Einfallstore sind E-Mails und Hackerangriffe

Tabelle 1 Rating Cyberversicherung für kleine und mittlere Unternehmen

Die aktuell besten Cyber-Policen (FFF und FF+) bieten: Tarif	Rating
Provinzial Nord Brandkasse AG Cyber-Versicherung mit Bausteinen Haftpflicht, Eigen-, Vertrauensschaden, Ertragsausfall, Stand 04.2019	FFF
Westfälische Provinzial Versicherung Aktiengesellschaft Cyber-Versicherung mit Bausteinen Haftpflicht, Eigen-, Vertrauensschaden, Ertragsausfall, Stand 04.2019	FFF
AIG EUROPE S.A. – Direktion für Deutschland CyberEdge online 3.0, Stand 08.2018	FF+
HISCOX CyberClear für Unternehmen bis € 10 Mio. Jahresumsatz, Stand 03.2019	FF+
Markel Insurance SE Pro Cyber (Antragmodell), Stand 04.2019 Cyber-Betriebsunterbrechung, Stand 04.2019 Cyber-Haftpflicht, Stand 04.2019 Cyber-Vertrauensschäden, Stand 04.2019	FF+
Ostangler Brandgilde VVaG Cyberversicherung, Stand 01.2019	FF+
Basler Sachversicherungs-AG Cyber-Police mit Betriebsunterbrechung wegen Ausfall des Dienstleisters und Sublimit-Anhebung, Stand 01.2019	FF+
Victor Deutschland GmbH CyberVlex, Stand 10.2019	FF+
ALTE LEIPZIGER Versicherung AG Cyberisiko-Versicherung für gewerbliche Risiken inkl. aller Zusatzmodule, Stand 09.2019	FF+
HDI Versicherung AG Cyberversicherung für Firmen und Freie Berufe, Stand 10.2018 Internet-Diebstahl, Stand 10.2018	FF+
ERGO Versicherung AG Cyber-Versicherung – Antragsmodell Branchentarif, „Vorschlag 3“, Stand 07.2019	FF+
Gothaer Allgemeine Versicherung AG Cyber-Versicherung für Gewerbetreibende, Stand 10.2018 Erhöhung der Sublimits auf 20% der Versicherungssumme, Stand 10.2018	FF+

Quelle: Franke und Bornberg, Stand: 06.02.2020

Das Franke-und-Bornberg-Rating ordnet Produkte sieben verschiedenen Ratingklassen zu: von FFF+/hervorragend, FFF/sehr gut, FF+/gut bis F-/ungenügend.

Hinweis: Teils sind Anbieter mit mehreren gleich benoteten Angeboten vertreten. In diese Tabelle wurde jeweils nur eines davon aufgenommen.

Das Rating wird ständig aktualisiert. Neueste Ergebnisse unter: <https://www.franke-bornberg.de/ratings/gewerbeversicherung/cyber-versicherung/cyberversicherung>

Cyberpolice für Unternehmen – Was die besten Tarife können müssen (Auszug):

- | **Betriebsunterbrechung:** Deckung von Ertragsausfällen
- | **Drittsschäden:** Deckung auch für immaterielle Schäden
- | **Mehrere Versicherungsverträge:** keine Subsidiarität der Cyber-Deckung (Im Schadenfall kommt zuerst die Cyberpolice zum Tragen, auch wenn Deckungsschutz noch über anderweitige Versicherungen besteht. So ist eine schnelle Reaktion gewährleistet.)
- | **Rückwärtsdeckung:** Deckungsausschluss nur für Ursachen / Schäden, die vor Vertragsabschluss bekannt waren (und nicht für solche, die hätten bekannt sein müssen)
- | **Wiederherstellung von IT-Systemen:** Zeitliche Befristung der Wiederherstellung auf mindestens 12 Monate nach Schadenfeststellung

Quelle: Franke und Bornberg

man das klassisch IT-Notfallmanagement, heutzutage neudeutsch Cyber-Resilienz. Das ist der wichtigste Punkt, weil man im Grunde immer damit rechnen muss, dass man angegriffen wird.“ Darüber hinaus empfiehlt der Cyberexperte, auch eine Cyberpolice in Erwägung zu ziehen, wenn sie noch nicht da ist. „Weil man sich eben nicht zu hundert Prozent technisch absichern kann.“

Cyberpolice im Rating – Mehrzahl im Mittelfeld

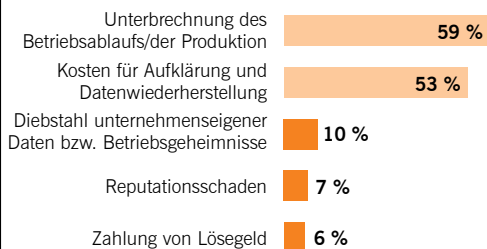
Im Kern tritt die Cyber-Versicherung ein für Schäden des versicherten Betriebs – sogenannter Eigenschaden – oder Dritter wie beispielsweise Kunden (Drittsschaden) durch ungewollte Einwirkungen, Zugriffe und Nutzung betrieblicher IT-Systeme sowie für Kosten, die im Zuge des Cyber-Schadens entste-

hen. Das Angebot von Cyberpolice auch für kleine und mittlere Betriebe hat sich in den letzten zwei bis drei Jahren deutlich erhöht, so dass es mittlerweile sogar für ein erstes Rating reichte. Das ist allerdings ernüchternd. Auf Anhieb schaffte kein Produkt in der Bewertung des Analysehauses Franke und Bornberg das Höchststufung FFF+. „Die Leistungsspitze ist noch dünn. Hier gibt es noch Luft nach oben“, kommentieren die Rating-Experten das Ergebnis. Die Mehrzahl der Tarife landete im Mittelfeld. Nur zwei Angebote erreichten die zweitbeste Note FFF (siehe Tabelle 1).

Als Standard hat sich nach Recherchen des Analysehauses dabei folgender Deckungsumfang bei gewerblichen Cyberpolice etabliert:

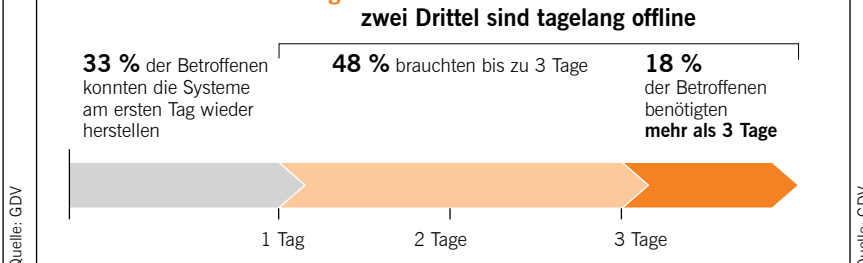
- | Wiederherstellung von Daten, Programmen & Systemen
- | IT-Forensik durch Sachverständige zur Feststellung von Ursache und Ausmaß des Schadens
- | Beratung zur Kommunikation im Krisenfall
- | Benachrichtigung von Betroffenen einer Datenschutzverletzung sowie
- | Rechtsberatung zu den Informationspflichten.

Welche Schäden sind im Unternehmen durch den Cyberangriff entstanden?



4 Die Unterbrechung der Betriebsabläufe und die Datenwiederherstellung sind kostspielig.

Wie lange hat es gedauert, die IT-Systeme wiederherzustellen und die Schadsoftware zu beseitigen?



5 Die IT-Systeme wieder zum Laufen bringen kann dauern

Produktlösungen

im Bereich Überspannungsschutz, Telekommunikation und Energieversorgung



- Blitz- und Überspannungsschutz für Gebäudeinfrastrukturen, eMobilität und erneuerbare Energien
- Schränke und Gehäuse für passive wie aktive Telekommunikationstechnik im Festnetz- und Mobilfunksektor
- Wärmeschrumpfsprodukte und Verbindungselemente für Nieder- und Mittelspannungsanwendungen



Die neusten Innovationen auf der Light+Building 8.-13. 3. 2020 Halle 12.0 Stand D10

Wie kann eine Cyberversicherung helfen?

So hilft eine Cyberversicherung bei Datendiebstahl

- IT-Forensik zur Aufklärung des Datendiebstahls
- Datenschutzrechtliche Beratung bei möglichem Kundendatenverlust
- Bezahlung gesetzlicher Haftungsansprüche aus dem Datenverlust
- Gegebenenfalls Übernahme der Vertragsstrafen an Zahlungsanbieter für Verlust von Daten
- Abwehr unberechtigter Schadenersatzansprüche
- Bezahlung von Krisenkommunikation

- Kostenübernahme für die Benachrichtigung geschädigter Kunden

So hilft eine Cyberversicherung bei Erpressungen

- Übernahme von Betriebsunterbrechungsschäden infolge von IT-Erpressungen
- Kostenerstattung für Datenwiederherstellung und Bereinigung der eigenen IT
- IT-Forensik zur Aufklärung und gegebenenfalls Bekämpfung der Erpresser
- Gegebenenfalls Übernahme der Vertragsstrafen an Zahlungsanbieter für Verlust von Daten

Quelle: GDV

Im Detail unterscheidet sich der Deckungsumfang je nach Anbieter dennoch erheblich. Das betrifft etwa die erste Hilfe durch IT-Forensiker, PR-Profis und spezialisierte Juristen bei einem Cybervorfall. Es macht dann schon einen Unterschied, ob das Management dieser Experten allein dem Betrieb überlassen bleibt – wie das in vielen Angeboten der Fall sei. Oder ob auch das Krisenmanagement mitversichert ist, unabdingbar für ein Top-Produkt. Darauf weisen die Experten von Franke und Bornberg hin.

Mitarbeitertraining mit abgedeckt

Ergänzend zu den Assistance- und sonstigen Leistungen im Schadenfall bieten neueste Tarife auch Unterstützung bei der betrieblichen Prävention – Stichwort Mitarbeitersensibilisierung, bekanntlich die größte Herausforderung für die allermeisten Unternehmen.

Das schließt z. B. in der Basisvariante von Pro Cyber 2019 des Versicherers Markel u. a. eine

einmalige IT-Sicherheitsüberprüfung ein, außerdem Online-Training Cybersicherheit für maximal drei Mitarbeiter, einen einmaligen Phishing-Test sowie einen Passwortgenerator und diverse Checklisten mit Anregungen für mögliche organisatorische und technische Maßnahmen im Unternehmen. In der Premiumvariante sind es u. a. laufende Phishing-Tests, Online-Training für eine unbegrenzte Mitarbeiterzahl, Online-Konten-Check, E-Mail-Scanner sowie Angriffsalarm.

Inzwischen gibt es auch erste branchenbezogene Versicherungskonzepte. Ein diesbezügliches Angebot macht mit CyberVlex beispielsweise der Assekuradeur Victor (Deutschland). „Wir beobachten deutliche Unterschiede in Aufbau und Umfang der Cyber-Bedingungen. Vom großen Komplettpaket über Baukastensysteme bis hin zu eng gefassten Kern-Deckungen ist alles vertreten“, konstatiert Michael Franke, geschäftsführender Gesellschafter der Franke und Bornberg Research GmbH.

Mit den Cyberschutz-Musterbedingungen des GDV für kleine und mittlere Unternehmen liegt zwar nunmehr ein verbindlicher Orientierungsrahmen vor. Doch längst nicht alle Anbieter greifen darauf zurück.

Kosten breit gefächert

Entsprechend breit gefächert sind auch die Kosten für den Cyberschutz. Je nach Branche und Geschäftsmodell ist nach Angaben von Franke und Bornberg ein Versicherungsschutz von einer Million Euro für unter 1 000 Euro Jahresprämie erhältlich. Der Online-Vermittler CyberDirekt etwa wirbt auf seiner digitalen Plattform mit einer Cyberabsicherung ab 400 Euro Jahresprämie. Die Ange-

bote der dort gelisteten Gesellschaften richten sich dabei an Firmen mit bis zu zehn Millionen Euro Jahresumsatz und einer Versicherungssumme bis zu zwei Millionen Euro.

Welches Angebot am besten zu welchem Handwerksbetrieb und seinem Geschäftsmodell passt, wäre möglichst mithilfe eines darauf spezialisierten Maklers herauszufinden. Erschwerend für eine fundierte betriebliche Risikoanalyse: Anders als bei den klassischen Gefahren Feuer, Wasser, Sturm, können sich Handwerksunternehmer bei digitalen Risiken bekanntlich nicht auf erprobte Basics und langjährige Erfahrungen stützen. Zumal sich die Cyber-Schadensszenarios fortlaufend ändern.

Alte Betrugsmaschen digital eingefädelt

Digitalisierung bringt zugleich auch vereinfachte Angriffswege für bekannte Betrugsdelikte: Falsche Chefs oder Lieferanten, die Zahlungen auf ihr Konto umleiten. Kriminelle, die sich als alte Firmenkunden ausgeben und Ware an Fake-Adressen ordern (Tabelle 2). Bei einer Kommunikation, die vorrangig über Internet und Intranet sowie häufig unter Zeit-

Versicherungsarten

Cyberversicherung

Tritt nach Angriffen auf die Daten oder die IT-Systeme eines Unternehmens ein („Informationsschutzverletzung“). Übernimmt Kosten durch Datendiebstähle, Betriebsunterbrechung und für den Schadenersatz an Dritte, schickt und bezahlt Experten, die nach einem Cyberangriff weiterhelfen.

Vertrauensschadenversicherung

Entschädigt Unternehmen, wenn sie Opfer von kriminellen Vertrauenspersonen geworden sind. Wenn z. B. Mitarbeiter eines Unternehmens Geld unterschlagen, das Unternehmen sabotieren, Geschäftsgeheimnisse verraten oder sich der Untreue schuldig machen. Als Mitarbeiter zählen dabei auch Zeitarbeiter oder Dienstleister. Vermögensschäden durch vorsätzlich begangene Taten von fremden Betrügnern (etwa bei Fake-Präsident-Fällen) sind üblicherweise ebenfalls im Rahmen einer Vertrauensschadenversicherung abgedeckt.

Anzeige



INDEXA®

Funk-Alarmanlage System 9000

- Einbruch-, Gefahrenmelde- und Notrufsystem
- Warni per App, E-Mail, SMS, Anruf
- Steuern über Smartphone/Tablet
- Scharfschalten vier einzelner Bereiche
- Hohes Sicherheitsniveau (EN 50131 Grad 2)

INDEXA GmbH · Tel. 071 36/98 10-0 · www.indexa.de

**Tabelle 2 Falsche Führungskräfte, falsche Lieferanten, falsche Geschäftspartner
Wirtschaftskriminalität 4.0 – ausgewählte Angriffswege im Überblick**

Kriminalitätsform	Angriffswege	Szenario/Täter...	Schäden	Versicherungsschutz
Betrugsdelikte	Fake President	... geben sich als Führungskräfte aus, hoher Druck auf Angestellte, um dringende Zahlungen auf Täterkonten zu veranlassen	Vermögensverluste durch falsche Überweisungen	Vertrauensschadenversicherung
	Payment Diversion	... geben sich als Lieferanten aus und ändern – zur Umleitung des Zahlungsstroms – die Bankverbindung		
	Fake Identity Fraud	... geben sich als Geschäftspartner aus und lassen sich Waren an falsche Lieferadressen senden		
Cyberkriminalität	Ransomware	... schleusen Schadsoftware in Unternehmens-IT ein, sperren so Zugriff auf Unternehmensdaten, verlangen Lösegeld	IT-Ausfall Datenverlust Betriebsunterbrechung Haftungsansprüche	Cyberversicherung
	DDoS-Attacke	... überlasten mithilfe eines Botnetzes gezielt IT-Systeme des Unternehmens: überfluten IT mit Anfragen		
	Datendiebstahl	... verschaffen sich Zugriff auf Unternehmensdaten und entwenden Kunden- und Zahlungsdaten, Betriebsgeheimnisse		
	Sabotage	... dringen in vernetzte Produktionssysteme ein und manipulieren die Maschinen	(bei Sabotage ggf. Maschinenschäden)	(bei Sabotage ggf. auch Technische/Vertrauensschadenversicherung)

Quelle: GDV

druck läuft, haben sie leichtes Spiel. Die Grenzen zwischen Cyber- und Wirtschaftskriminellen sind dabei fließend – wie dann häufig auch der Versicherungsschutz in diesem Bereich. Wer fragt heutzutage schon telefonisch nach, wenn er es doch „Schwarz auf Weiß“ in der E-Mail hat: Zahlungsüberweisung für die geordnete Ware bitte künftig auf ein anderes Geschäftskonto. „Sehr einfach und gewinnbringend für die Täter. Darauf fallen sehr viele Unternehmen rein“, so Rüdiger Kirsch, Vorsitzender der AG Vertrauensschadenversicherung im GDV. Oder ein Hacker fischt eine Mail heraus und verändert die IBAN. *Payment Diversion* wird dieses Betrugsszenario genannt, bei dem die Vertrauensschadenversicherer bereits mehrere Fälle mit einem Volumen von über zwei Millionen Euro verzeichneten. „Gerade wenn es um die Umleitung von Zahlungsströmen geht“, sind aber auch viele kleine Firmen und Handwerksunternehmen betroffen, so Kirsch, der bei Euler Hermes den Bereich Schaden bei der Vertrauensschadenversicherung (VSV) verantwortet. Und bei einer Bilanzsumme von einer Million Euro tun Summen von 20000 oder 50000 Euro dann genauso weh wie

NEU

Praktiker-Seminare: Messen & Prüfen

Wir empfehlen – die bundesweiten Praktiker-Seminare unserer namhaften Partner MEBEDO Akademie, WEKA Akademie und PRO-EL zu den Themen:

- Prüfung von elektrischen Arbeitsmitteln, Maschinen, Anlagen und Betriebsmitteln
- Prüfen der Elektrosicherheit für Fortgeschrittene
- Prüfung von Potenzialausgleich und Erdung in elektrotechnischen Anlagen
- Netzmessung und Stromversorgung
- Prüfen von E-Ladesäulen als elektrische Anlage



Jetzt anmelden!





www.elektropraktiker.de/praktiker-seminare

SCHNABL BEGEISTERT MIT NEUEN IDEEN. BIS ZU 60% MEHR KAPAZITÄT!



NEU!

Der neue SH 80.
Auch in der Variante SH 40 lieferbar.



Der neue KB 26.
Auch in der Variante KB 13 lieferbar.

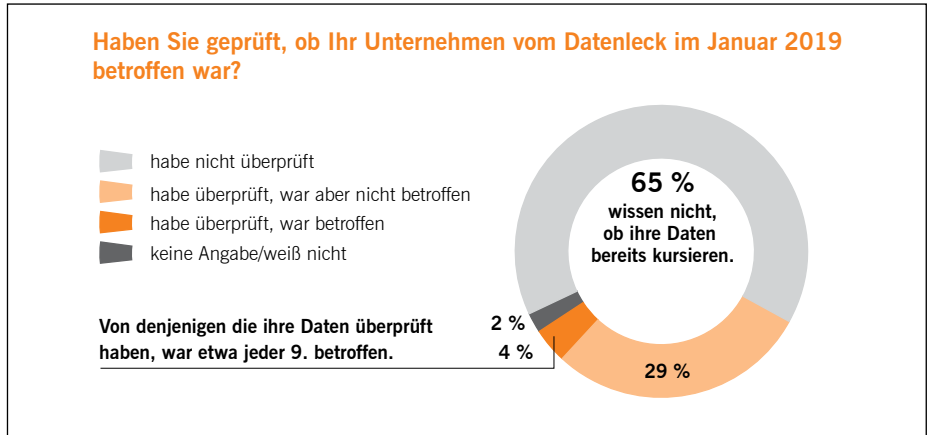
Besuchen Sie uns auf der Light+Building, Frankfurt am Main, 8.–13. März 2020, Halle 12.1 • Stand E31

Wir schaffen Mehrwert und machen das Leben von Monteuren einfacher – mit den optimierten Schnabl-Produkten für die Mehrfachverlegung von bis zu 80 Mantelleitungen.

einem Großunternehmen ein Millionenschaden. Nur landen nach seinen Worten viele dieser Betrugsfälle oft nicht bei der Kriminalpolizei und werden nicht systematisch erfasst.

Big Brother und Fake President

Spektakulärer und aufwendiger für die Täter ist das Betrugsszenario *Fake President*. Dabei hackt sich der Kriminelle beispielsweise ins Intranet ein, bewegt sich dort zwei Wochen, schaut, wer mit wem wie kommuniziert: „Duzt man sich beispielsweise? Spricht man Englisch? Das pickt er heraus und weiß am Ende, wer im Unternehmen für Zahlungsanweisungen zuständig ist“, schildert Kirsch das typische Vorgehen. Der Buchhalter wird dann – auch mit Lob für seine Zuverlässigkeit und Appellen an seine Diskretion – teils auch telefonisch unter Druck gesetzt, um erhebliche Summen zu überweisen: z. B. für die „streng geheime“ angebliche Übernahme einer Firma. Beim Betrugsszenario *Fake Identity Fraud* schlüpft der Hacker in die Person eines Vertragspartners und ordert beispielsweise



Quelle: GDV

6 „Datenlecks? Uns doch egal!“

bei einem kleinen Produzenten Ware in hoher Stückzahl mit kurzer Lieferfrist und an eine Adresse, die nur kurz existiert und dann leergeräumt ist. Neuester Trend, auf den Kirsch verweist: Fake-IT – mit zunächst demselben Szenario wie bei Fake President. Nur, meldet sich zwischendurch der angebliche IT-Chef und warnt die Buchhalterin: Wir haben eine Fake-President-Attacke. Die Kripo ist informiert. Machen Sie weiter wie gehabt.

Vertrauen ist gut, Police im Fall der Fälle besser

Das alles sind nach Kirschs Worten Fälle, wo eine Vertrauensschadenversicherung betroffenen Unternehmen Schadensersatz leistet, das heißt all das, was auch strafrechtlich verfolgt wird und zu einem Vermögensschaden führt. Für Vermögensverluste dieser Art bietet sich insofern – nicht zuletzt als Ergänzung zur

Grundlagen Beleuchtungstechnik

NEU



Neues Grundlagenwerk Beleuchtungstechnik

Die 5. Auflage dieses Standardwerkes für die Beleuchtungstechnik entstand wieder unter der bewährten Herausgeberschaft der Lichttechnischen Gesellschaft e. V. (LiTG), unter deren Dach sich ein kompetentes Autorenteam aus Lichtlehrenden und Praktikern vereint hat.

Neben den wissenschaftlich-technischen Grundlagen werden LED-Leuchten und -Leuchtmittel, Berechnungen und Berechnungsprogramme sowie Lichtsteuerungen behandelt. Während alle Kapitel sorgfältig überarbeitet wurden, ist das hochaktuelle Kapitel Lichtsteuerungen neu hinzugekommen.

5. Auflage: März 2020, 59,00 €, 576 Seiten, ca. 466 Bilder, 104 Tabellen, Hardcover
Bestell-Nr. 3-341-016343-0
Hrsg: Deutsche Lichttechnische Gesellschaft e.V., LiTG und namhafte Autoren

Jetzt bestellen!

ep ELEKTRO PRAKTIKER

www.elektropraktiker.de/buecher
oder Bestellschein hinten im Heft

Cyberpolice – die Vertrauensschadenversicherung an (s. Kasten S. 236). Die Zielrichtung beim Cyberschutz ist bekanntlich eine andere: Vereinfacht gesagt geht es dort um Folgeschäden eines Hackerangriffs, bei der Vertrauensschadenversicherung dagegen sozusagen um Betrug „pur“ durch Mitarbeiter, aber auch gänzlich „betriebsfremde“ Internetkriminelle, die analog oder digital direkt Waren oder Geld aus dem Betrieb „abziehen“. Es gibt aber auch Cyberpolicen und Firmenversicherungspakete, die einen solchen Leistungsbaustein enthalten. Wie weit der Schutz dort reicht, wäre im Vergleich und abhängig vom eigenen Bedarf wiederum mit Maklerhilfe genau zu prüfen.

Ist Ihr Betrieb von Datenlecks betroffen?

Wissen Sie, ob Ihre Daten bereits im Internet kursieren (Bild 6)? Das Hasso-Plattner-Institut bietet den „HPI Identity Leak Checker“ an. Anhand Ihrer E-Mail-Adresse können Sie prüfen, ob die Adresse in Verbindung mit

anderen persönlichen Daten wie Geburtsdatum oder Adresse im Internet offengelegt wurde und missbraucht werden könnte. Insgesamt haben bereits mehr als 14 Millionen Nutzer mithilfe des Identity Leak Checkers die Sicherheit ihrer Daten in den letzten fünf Jahren überprüfen lassen. In mehr als drei Millionen Fällen mussten Betroffene darüber informiert werden, dass ihre E-Mail-Adresse in Verbindung mit anderen persönlichen Daten im Internet offen zugänglich war. Prüfung unter: <https://sec.hpi.de/ilc/>

Polizei einschalten

In vielen Bundesländern haben Polizei und Justiz spezialisierte Cybercrime-Dienststellen geschaffen. Sie helfen, Beweise zu sichern, kennen im Zweifel ähnliche Fälle und können konkrete Empfehlungen geben. Speziell für Wirtschaftsunternehmen gibt es bei der Polizei „Zentrale Ansprechstellen Cybercrime“ (ZAC) – mit Website, E-Mail etc. geordnet nach Ländern online abrufbar unter (Kurzlink): <https://bit.ly/2SEEONz>

Nützliche Links für kleine und mittlere Unternehmen (KMU)

! <https://www.vds-quick-check.de/quick-check-fuer-cyber-security/>

kostenloser Quick-Check der VdS Schadenverhütung zur IT-Sicherheit in Unternehmen

! <https://www.sicher-im-netz.de/>

DsiN-Sicherheitscheck greift aktuelle Herausforderungen von Industrie 4.0 bis zur EU-Datenschutz-Grundverordnung auf und geht auf Versicherbarkeit von Cyber Risiken ein. Dahinter steht die vom BSI unterstützte Initiative Deutschland sicher im Netz e.V. Dort kann man bereits jetzt unter info@cyberfibel.de die Cyberfibel kostenlos vorbestellen, die ab Frühjahr 2020 verfügbar sein soll und zusammen mit dem BSI erarbeitet wurde. Weitere Informationen zum Projekt in Kürze auf www.cyberfibel.de.

! www.bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik

! www.allianz-fuer-cybersicherheit.de/ kostenlose aktuelle Infos zur IT-Sicherheitslage, Tipps für konkrete Maßnahmen zur Erhöhung der Informationssicherheit im Unternehmen

! <https://siwecos.de/>

steht für „Sichere Webseiten und Content Management Systeme“ und hilft kleinen und mittleren Unternehmen (KMU), Sicherheitslücken auf ihren Webseiten zu erkennen und zu beheben (dahinter steht u. a. der eco-Verband der Internetwirtschaft, siehe auch:

! <https://www.it-sicherheit-in-der-wirtschaft.de/>

eine Initiative des Bundesministeriums für Wirtschaft und Energie zur Verbesserung der IT-Sicherheit von KMU.

! www.gdv.de/downloads/versicherungsbedingungen

Allgemeine Versicherungsbedingungen (Musterbedingungen) + unverbindlicher Risiko-Fragebogen zur Cybersicherheit von KMU (s. dort unter Schaden- und Unfallversicherungen)

! www.gdv.de/cybercheck

der Cyber-Sicherheitscheck des GDV stellt Ihnen die wichtigsten Fragen rund um die IT-Sicherheit Ihres Unternehmens

230V über IP

Ausführungen für 230V:

- 1xNO (16A), 1xIN
- 4xNO, 4xC0 (6A)
- 1xNO, 1xC0



W&T Web-IO®

Ehrliche E/A-Geräte zum Überwachen & Schalten für Hausautomation, IoT & Industrie 4.0.



Infos & Test unter:

wut.de/web-io

