Mein Geld
ANLEGERMAGAZIN

01 | 2019
JANUAR | FEBRUAR | MÄRZ
25. JAHRGANG

VERSICHERUNG

Cyberrisiken

Die hässliche Seite der schönen digitalen Welt

DEFINITION CYBER-KRIMINALITÄT (BMI):

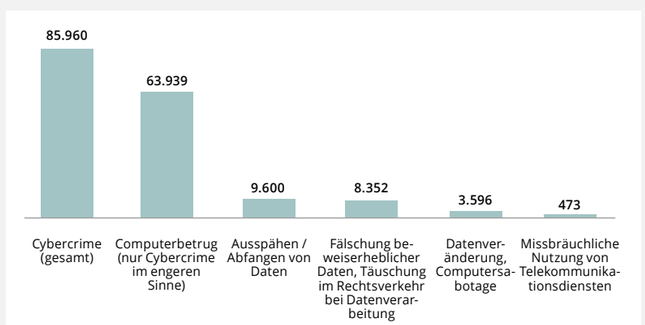
„Straftaten, bei denen die Täter moderne Informationstechnik nutzen, werden zunächst ganz allgemein als Cyberkriminalität (engl. cybercrime) bezeichnet. Cyberkriminalität ist zum Beispiel ein Betrugsversuch, der das potentielle Opfer via E-Mail statt per Post erreicht."

„Im engeren Sinne umfasst der Begriff jedoch Straftaten, die auf Computersysteme und Netzwerke selbst zielen. Dabei kann es sich auch um Cyberspionage oder Cyberterrorismus handeln."

Trojaner, Hacking, Cyberattacken, Ransomware, Botnetze – sowohl die Namen als auch die Arten der möglichen Bedrohungen sind erschreckend vielfältig. Im aktuellen Bundeslagebericht des Bundeskriminalamtes werden 85.960 Fälle von Cybercrime im engeren Sinne genannt, 251.617 erfasste Straftaten stehen zu Buche, bei denen das Internet als Tatmittel genutzt wurde. Von den gemeldeten Straftaten von Cybercrime konnten immerhin 40,3 Prozent aufgeklärt werden. Die Zahl der Phishing-Betrugsfälle im Online-Banking konnte seit 2014 dank stetiger Verbesserung der Sicherheiten im Online-Banking von 7.000 auf 1.425 in 2017 reduziert werden. Am Beispiel Online-Banking kann man erkennen, dass das Zusammenspiel von hohen Sicherheitsstandards und Sensibilisierung der Nutzer das Risiko, Cyber-Opfer zu werden, deutlich verringert. Dennoch bescheinigen Studienergebnisse des Digitalverbandes Bitkom sowie des amerikanischen IT-Sicherheitsunternehmens Norton by Symantec deutschen Internetnutzern eine hohe Betroffenheit. So soll bereits jeder zweite Deutsche Opfer von Cyberkriminalität geworden sein, in jedem zweiten Fall sei ein finanzieller Schaden entstanden – Gesamtschaden 2,2 Milliarden Euro.

Das Bundeskriminalamt kann diese Zahlen zwar nicht evaluieren, geht aber von einer enormen Dunkelziffer aus. Es werde nur ein sehr kleiner Teil der Straftaten zur Anzeige gebracht, häufig aus Unwissenheit, Scham oder Misstrauen in den Erfolg einer Strafverfolgung. Mit dem Diebstahl von Daten und Identitäten, dem Einsatz von Schadsoftware, Phishing, Kreditkartenbetrug und digitaler Erpressung können Verbrecher sowohl Privatpersonen als auch Unternehmen beträchtlichen monetären Schaden zufügen.

FÄLLE FÜR CYBERCRIME IM ENGEREN SINNE (2017)



CYBERGEFAHREN IM PRIVATEN UMFELD

Eine Arbeitswelt ohne Computer, ohne Smartphone, ohne Zugriff auf Dokumente, geteilte Inhalte und Vernetzung der Systeme ist nicht mehr wegzudenken. Auch in privaten Haushalten steuern zunehmend Router nicht nur den Musikgenuss, sondern bieten über das Internet auch Zugriff auf Fotos, private Inhalte und Zugriff auf die Smart Home-Steuerung von unterwegs. Die komfortable digitale Welt hat aber auch hässliche Seiten.

Fühlen Sie sich von Alexa kontrolliert? Was macht die Webcam, die Sie bei Ihrer Arbeit am Laptop beobachtet, eigentlich? Die Vielzahl unserer internetfähigen Geräte wie Tablets, Smartphones, Smartwatches, WiFi-Router, Spielekonsolen, Smart Home und Unterhaltungselektronik bietet für Schadprogramm- und Virenhersteller geradezu paradiesische Zustände an „Einbruchsmöglichkeiten". Algorithmen und Analysen von Nutzerverhalten nehmen Einfluss auf unsere Aktionen im Netz. Zudem öffnen die potentiellen Opfer die „Tür" zu Ihren Sicherheitssystemen selbst, zum Beispiel über Onlinekauf-Fallen und kostenlose Downloadangebote.

Die weltweite Vernetzung ermöglicht nicht nur die sekundenschnelle Videotelefonie mit Freunden über tausende Kilometer – sie ermöglicht auch die sekundenschnelle Verbreitung von persönlichkeitsverletzenden Inhalten im Internet. Gespeicherte Kontakte, Profile und vermeintlich private Chatinhalte werden zur Ware und beflügeln nicht nur den Einfallsreichtum von Kriminellen, sondern bieten auch viel Raum für Mobbing – jeder Dritte aller Zwölf- bis 19-Jährigen hat schon Erfahrungen mit Cybermobbing gemacht.

CYBERGEFAHREN IM GEWERBLICHEN UMFELD

Cyberattacken können auch kleine, mittelständische und große Unternehmen betreffen, die Gefahren und deren Folgen sind aber weit umfangreicher als bei Privatpersonen. Gemäß einer Bitkomstudie wurde mehr als jedes zweite Unternehmen in Deutschland bereits digital attackiert. Schlagworte wie Botnetze, Hackerangriffe, digitale Wirtschaftsspionage, Sabotage, Datendiebstahl, Spam- und Phishing-Mails, Onlinebanking – um nur einige der Gefahren aus der schönen vernetzten Welt zu nennen – sind vielen aus den Medien bekannt. Entsteht durch Hacking ein Datenleck und gelangen sensible Kundendaten an die Öffentlichkeit, kann es unangenehme Folgen für ein Unternehmen haben, zudem wirft es in der öffentlichen Wahrnehmung ein schlechtes Licht auf das Unternehmen.

Der Diebstahl und Missbrauch von sensiblen elektronischen Dokumenten sowie Umsatzeinbußen durch Plagiate können die Folge sein. Dramatisch wird es für ein Unternehmen, wenn als Folge einer Cyberattacke die Handlungsfähigkeit gefährdet und sogar unterbrochen wird – die finanziellen Folgen sind mitunter erheblich. Das Risiko ist nicht auf einzelne Person begrenzt sondern viele Mitarbeiter. Ob fünf, 500 oder 5.000 Mitarbeiter, alle müssen über Cyberrisiken aufgeklärt werden, denn oft ist Malware kaum von einer richtigen Mail zu unterscheiden. Ein unachtsamer Klick in einer vermeintlich seriösen E-Mail und ein verheerender Virus oder Trojaner verteilt sich im Firmen-Netzwerk. Zudem können durch Phishing die Bankdaten des Unternehmens und die geschäftlichen Kreditkarten- oder Bankdaten aller Kunden gestolen werden, mit einem DDoS-Angriff können die IT-Systeme mutwillig überlastet werden und, wie aktuell in den Medien, können quasi alle Daten durch einen Hacker-Angriff gestohlen werden.

Der GDV-Cyber-Versicherungsexperte Peter Graß empfiehlt regelmäßige Schulungen und verbindliche Vorsichtsmaßnahmen für den Umgang mit E-Mails. Dann könnten die meisten Angriffe per Mail relativ leicht rechtzeitig erkannt und das Öffnen gefährlicher Software verhindert werden.

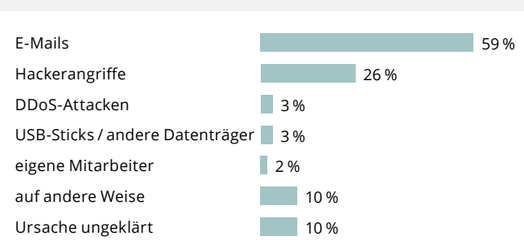
Es wird zu Schulungen der Mitarbeiter geraten, um die Sensibilität im Umgang mit Kundendaten zu schärfen. Jeder sollte, sowohl im privaten als auch betrieblichen Umgang mit dem Netz, vorsichtig sein, um rechtszeitig „Einfallstore" zu erkennen. Aktuelle und umfangreiche Sicherungssysteme sowie Virenschutzprogramme sind Pflicht – für den privaten sowie gewerblichen Bereich – einen 100-prozentigen Schutz können sie aber nicht leisten. Es wird Zeit, den Cyber-Bereich als Risiko zu erkennen und sich rechtszeitig gegen die finanziellen Folgen zu versichern.

ÜBERSICHT ÜBER DIE AKTUELLEN CYBER-SCHUTZ-POLICEN FÜR PRIVATPERSONEN

UNTERNEHMEN	TARIF	SCORING
Allianz Versicherungs-AG	Internetschutz*	★★½
AXA Versicherung AG	Internetschutz*	★★★
BavariaDirekt	Cyber-Versicherung SorglosOnline	★★★½
BGV-Versicherung AG	Onlineschutz	★★★½
INTER Allgemeine AG	INTER CyberGuard EXKLUSIV	★★★★★½
INTER Allgemeine AG	INTER CyberGuard PREMIUM	★★★★★½
INTER Allgemeine AG	INTER CyberGuard BASIS	★★★★½
Janitos Versicherung AG	OnlineSchutz*	★★★
R+V Allgemeine Versicherung AG	R+V-PrivatPolice Comfort*	★★★
VGH Versicherungen	CyberSchutz	★★★★½

Quelle: ascore Das Scoring |Stand 21.01.2019 * Abschluss nur in Kombination mit Hausrat-Tarifen möglich

DIE EINFALLSTORE – ERFOLGREICHE CYBER-ANGRIFFE ERFOLGTEN DURCH ...



1 | Mehrfachnennung möglich

GOTHAER

Risiko Hackerangriffe und Datenklau

Cyber-Policen langsam im Aufwind

Die deutsche Wirtschaft boomt. Aber mit der wachsenden Zahl an Aufträgen und der zunehmenden Digitalisierung steigt die Gefahr für die Unternehmen, Opfer von Cyber-Kriminalität zu werden. So sehen 40 Prozent der kleinen und mittelständischen Unternehmen (KMU) in Deutschland Cyber-Risiken wie einen Hackerangriff oder Datenklau als eine der bedrohlichsten Gefahren für ihren Betrieb an. Im Vorjahr waren es mit 32 Prozent noch deutlich weniger. 37 Prozent halten es für wahrscheinlich, dass ihr Unternehmen von einem solchen Risiko konkret betroffen sein könnte (2017 34 Prozent, 2015 30 Prozent).

Bereits jedes fünfte Unternehmen (19 Prozent) war bereits Opfer eines Hackerangriffs, Trojaners oder Datendiebstahls. Dennoch gibt es bei entsprechenden Vorsichtsmaßnahmen weiterhin eklatante Lücken. Jedes fünfte KMU verzichtet noch immer auf die Installation von Virenschutzprogrammen, jedes vierte hat keine Firewall. Fast ein Drittel der kleinen und mittelständischen Unternehmen führen keine regelmäßigen Backups durch. Das zeigt die KMU-Studie 2018 der Gothaer Versicherung, im Rahmen derer im Januar 2018 rund 1.000 Betriebe befragt wurden. Bereits zum fünften Mal hat die Gothaer die Risiken und den Versicherungsschutz von KMU detailliert untersucht.

Einen Versicherungsschutz für Cyberrisiken haben laut der Studie aktuell aber nur 13 Prozent der Unternehmen, 2015 waren es mit sieben Prozent noch weniger. Damit zeigt sich ein Trend zum Abschluss einer Cyber-Police – auch wenn noch auf zu niedrigem Niveau. Die Studien zeigen, dass das Risikobewusstsein und die Angst vor Cyber-Angriffen bei den KMUs seit Jahren steigen. Das Risiko, selbst von einem Hackerangriff, Datendiebstahl oder Virenbefall betroffen zu sein, haben die Unternehmen zwar erkannt.

Dennoch wird die Absicherung durch eine Cyber-Police immer noch zu selten genutzt. Die Gothaer spürt aber nach jedem öffentlichkeitswirksamen Hackerangriff eine deutlich steigende Nachfrage nach Cyber-Policen.

ANGEBOT CYBER-POLICEN

Daher gibt es bei der Gothaer gleich zwei Angebote für Cyber-Policen. Ein standardisiertes Produkt für Gewerbekunden mit einem Umsatz bis zu zehn Millionen Euro sowie ein individuell konfektionierbares Industrieprodukt für größere Unternehmen. Während viele Industriekunden in erster Linie die Kosten einer Betriebsunterbrechung versichern möchten, stehen dabei für Gewerbekunden schnelle Hilfen und IT-Services im Vordergrund, die den durch die Cyber-Attacke verursachten Schaden schnell wieder beheben.

Ein besonderes Highlight beider Produktvarianten besteht in den weitreichenden Assistance-Leistungen, die rund um die Uhr eingefordert werden können. Dabei geht es zunächst um eine 24-Stunden-Hotline sowie um die Wiederherstellung von Daten und Programmen: Denn gerade bei der Versicherung von Eigenschäden ist schnelle Hilfe wichtig. Deswegen trägt die Gothaer die Kosten der Hilfsmaßnahmen der ersten 48 Stunden immer – auch dann, wenn sich später herausstellt, dass kein Hackerangriff gegeben war. Die Gothaer hält diese Hilfe für wichtig, weil es manchen IT-Verantwortlichen ohnehin schwerfällt, eigene Unzulänglichkeiten in der IT einzuräumen – und sie dadurch vielleicht eher zu spät reagieren würden. Versicherer und Vermittler benötigen an dieser Stelle viel Sensibilität, geht es doch einerseits um Transparenz, Klarheit und Offenheit, andererseits um die Wahrung von Betriebsgeheimnissen. Weil die Gothaer das weiß, möchte sie ihre Kunden mit der 48-Stunden-Hilfe unabhängig von der Kostenfrage ermutigen, schnell zu reagieren.

Was bietet die Gothaer Cyber-Versicherung im Schadensfall?

Bei Drittschäden bietet Ihnen die Gothaer Cyber-Versicherung folgende Leistungen:

- *Haftpflichtversicherungsschutz durch Prüfung der Haftpflichtfrage, Abwehr unberechtigter Schadenersatzansprüche und Freistellung des Versicherten von berechtigten Schadenersatzansprüchen*
- *Versicherungsschutz bei behördlichen Verfahren*
- *Einstweiligen Rechtsschutz, Kosten der Abwehr von Unterlassungs- und Widerrufsklagen*
- *Ausgegliederte Datenverarbeitung, welche eine Freistellungsverpflichtung des Versicherten gegenüber dem beauftragten Unternehmen zur Folge hat.*
- *Versicherungsschutz bei der Verletzung von Persönlichkeits-, Urheber-, Marken- und Wettbewerbsrechten*
- *Umstandsmeldungen bis ein Jahr nach Beendigung des Versicherungsvertrages*

Bei Eigenschäden übernimmt die Gothaer Cyber-Versicherung:

- *Kosten für sicherheitstechnische Dienstleistungen*
- *Kosten im Zusammenhang mit Benachrichtigungspflichten*
- *Kosten für Kommunikations- und PR-Maßnahmen*
- *Kosten für Kreditüberwachungsdienstleistungen*
- *Kosten der Wiederherstellung von Daten und Programmen*
- *Kosten für Krisenmanager*

Optionale Deckungserweiterung bei der Cyber-Versicherung:

- *Betriebsunterbrechung*
- *Vertragsstrafen im Zusammenhang mit der Verletzung von Payment Card Industry-Datensicherheitsstandards*
- *Erweiterte Eigenschäden bei Schadensverursachung durch Mitarbeiter, bei Cyber-Diebstahl, Bedienfehlern oder auch Sachschäden am Computersystem*
- *Unter- und Überspannung, elektromagnetische Störung*
- *Bring your own device (BYOD)*

Die Gothaer Cyber-Versicherung für Gewerbekunden wurden dabei ebenfalls bewertet und erreichten eine Bewertung mit FF+ und damit einen hervorragenden Platz unter den fünf besten Cyber-Versicherungen im Markt.

Die bekannte Ratingagentur Franke und Bornberg veröffentlichte nunmehr das erste Rating für gewerbliche Cyber-Policen im deutschen Markt. Das Cyber-Rating von Franke und Bornberg bietet damit eine Entscheidungshilfe für Vermittler und gewerbliche Kunden. Untersucht wurden 35 Cyber-Tarife und Bausteinlösungen für KMU von 28 Anbietern. Die Leistungsunterschiede waren groß und es gab nur fünf Top Tarife. Herangezogen wurden 115 Ratingkriterien in 21 Bereichen. Franke und Bornberg analysierte für das Rating vor allem Merkmale, die für die Mehrheit der KMU relevant sind und typischerweise in bisherigen Haftpflicht- und Sachversicherungen nicht gedeckt sind. Die mögliche Höchstnote (FFF+) erreichte keine der angebotenen Cyber-Produkte.

UNTERSTÜTZUNG DURCH SPEZIALISIERTE DIENSTLEISTER

Den Kunden stehen hierfür spezialisierte Dienstleister zur Verfügung, die im Schadenfall umgehend unterstützen. Dies gilt insbesondere auch für die Krisen- und Public Relations-Beratung, die Rechtsberatung und für Datenüberwachungsdienstleistungen.

SIGNAL IDUNA

Der digitale Schutzschild von SIGNAL IDUNA – Schutz gegen Cyber-Angriffe

Das Konzept für kleine und mittelständische Unternehmen der SIGNAL IDUNA Gruppe zur Abwehr von Cyber-Angriffen ist mehr als nur eine Versicherung. Es bietet umfassenden Schutz für Betriebe. Was das genau heißt, zeigen wir Ihnen einfach und übersichtlich

DAS KONZEPT

Bei der SIGNAL IDUNA geht man einen Schritt weiter und steht den Kunden nicht erst im Schadenfall zur Seite. Das Konzept dahinter ist ein digitaler Schutzschild, der aus drei Verteidigungslinien besteht.

Die erste Verteidigungslinie stellt die funktionierenden Sicherheitsmaßnahmen dar, die jedes Unternehmen bereits getroffen haben sollte. Dazu gehören beispielsweise zentrale Admin-Rechte, eine Firewall, ein Virenschutz, eine Update-Politik und regelmäßige Datensicherung.

DER CLUB

Die zweite Verteidigungslinie bildet der Perseus Cyber Security Club. Das Ziel des Clubs ist die Vorbeugung von Cyber-Attacken, durch beispielsweise Online-Schulungen für die Mitarbeiter und automatisierte Sicherheitstests. Eine 24-Stunden-Hotline verspricht erste Hilfe, wenn das Unternehmen Auffälligkeiten in seiner IT feststellt. Die Spezialisten helfen direkt am Telefon, um Schäden zu beseitigen, zu vermeiden oder zu mindern.

- ✓ Mit dem Perseus Cyber Security Club stärken Unternehmen das größte Cyber-Risiko: den Menschen
- ✓ Der Cyber-Führerschein sorgt für nachhaltiges Bewusstsein bei den Mitarbeitern
- ✓ Einfache und hilfreiche Tools bieten dauerhaften Schutz für Unternehmen
- ✓ Erste Hilfe bei Cyber-Vorfällen mit der persönlichen Hotline – der direkte Draht zu den Experten

DIE VERSICHERUNG

Zu guter Letzt greift mit der umfassenden CyberPolice der SIGNAL IDUNA die dritte Verteidigungslinie im Schadenfall. Sollte es also trotz ausreichend technischer Grundausstattung, geschulter und vorsichtiger Mitarbeiter dennoch zum Schadenfall kommen, springt die CyberPolice der SIGNAL IDUNA ein. Sie bietet einen optimalen Schutz vor den finanziellen Folgen einer Cyber-Attacke. Darüber hinaus sind natürlich auch die Eigenschäden (zum Beispiel die Wiederherstellung von Daten und Programmen), Drittschäden und die daraus entstehenden Kosten (wie beispielsweise Forensiker, PR und Rechtsanwaltskosten) versichert.

- Mit der CyberPolice sind Unternehmen vor Vermögensschäden geschützt, die durch Verletzungen der Informationssicherheit entstehen
- Das heißt konkret, der Versicherungsschutz greift:
  - wenn notwendige Informationen nicht mehr abrufbar oder verfügbar sind (zum Beispiel durch Ransomware)
  - sensible Informationen verfälscht worden sind
  - Informationen in falsche Hände gelangen

FAZIT

Denn eines ist klar: Die Cyber-Kriminalität ist immer auch ein Wettrüsten zwischen Unternehmen und Kriminellen. Daher ist es gut zu wissen, dass man mit dem digitalen Schutzschild bestens dagegen gerüstet ist. Wer sich für den digitalen Schutzschild der SIGNAL IDUNA entscheidet, kann im Schadenfall unter anderem auf folgende Leistungen zurückgreifen:

- Schadensfeststellung durch einen EDV-Spezialisten (zum Beispiel Forensiker)
- Erstattung der Benachrichtigungskosten (zum Beispiel Kunden bei Datenleck)
- Erstattung der Kosten für PR-Berater bei Reputationsschäden
- Aufwendungen vor Eintritt des Versicherungsfalls
- Erstattung von Eigenschäden wie beispielsweise Wiederherstellungskosten (Daten, Programme, Netzwerke) oder Betriebsunterbrechungsschäden (sofern mitversichert)
- Erstattung von Drittschäden wie Vermögensschäden aus Malware oder Ansprüchen aufgrund von Datenverlust

INTER VERSICHERUNGSGRUPPE

Cybercrime – welcher Schutz ist möglich?

Jan Roß, Leiter Maklervertrieb der INTER Versicherungsgruppe über eine der Gefahren im digitalen Zeitalter: Cybercrime.

JAN ROSS – Leiter Maklervertrieb der INTER Versicherungsgruppe

Das digitale Zeitalter hat seine Schattenseiten. Schreckensmeldungen aller Art sorgen für Verunsicherung bei den Usern. Phishing, DOS-Attacken, Ransomware, Drive-by-Downloads und andere Gefahren halten Nutzer, Provider und Sicherheitsanbieter zunehmend in Atem.

Die digitale Welt ist im Wandel. Internet und Konnektivität sind das Maß aller Dinge, von der Smart Watch bis zum Smart Home, vom Banking über Shopping bis zum sozialen Leben. Die Cyberkriminalität hat dabei mühelos Schritt gehalten. Allein in Deutschland gab es 2017 rund 23 Millionen Opfer von Cybercrime.[1] Im selben Jahr kosteten die Eskapaden der Cybergangster ihre Opfer etwa 2,2 Milliarden Euro[2] – so viel wie das Minus der deutschen Rentenkassen im Jahr 2016.

DIE ANGST SURFT MIT

Der größte Angstfaktor deutscher User ist die Möglichkeit des Datenklaus[3]. Online erbeutete Informationen können bares Geld wert sein, selbst wenn es sich nicht um Kontonummern, PINs und TANs handelt. Fast die Hälfte der Deutschen (48 Prozent) fürchtet Phishing im Netz, wenn es um die Verarbeitung der eigenen Daten geht. Gehört so etwas inzwischen zu den allgemeinen Lebensrisiken, deren Folgen zu akzeptieren sind?

Nein. Dafür sind die Schäden, die Cyberkriminalität anrichtet, zu hoch. Für 2017 nannte das BKA[4] einen Gesamtschaden von mehr als 55 Milliarden Euro. Allerdings ist es für den normalen Nutzer nicht offensichtlich, wie er sich schützen kann. Es gibt so viele Tipps und Tricks, dass er nur schwerlich hinterherkommt. Die Lösung: Mehr Transparenz und Übersichtlichkeit. Umso wichtiger wird das, weil sich das Internet zunehmend mit der Lebensrealität vermischt. Je mehr Funktionen im Leben eines Menschen von einem elektronischen Netz ausgeführt werden, umso gravierender sind die Folgen eines Angriffs. Dabei ist es egal, ob der eigene Laptop, Computer oder gar das „smarte" Zuhause Ziel der Cyberattacke ist.

Nebst Phishing-Software, die Passwörter und andere sensible Daten auslesen kann, sorgen auch Botnets und Würmer für Unruhe im Netz. Was schon für den privaten Nutzer problematisch ist, kann für Behörden, Regierungsapparate und Parteien eine echte Krise bedeuten.

BESSER VORBEUGEN ALS AUFRÄUMEN

Sobald sich ein User mit dem Internet verbindet, kann er zum Ziel einer Cyberattacke werden. Komplett ausschließen lassen sich diese Angriffe nicht, doch gibt es Mittel und Wege, sich so gut es geht davor zu schützen. Der Rechtsweg bleibt dabei ineffektiv, da der Schuldige nicht immer ermittelt werden kann – etwa bei der Ansteckung per E-Mail.

Eine gute Vorsorge ist der effektivste Weg. Es kommt darauf an, die richtige Lösung für das jeweilige Problem zu finden. Firewall & Co. sind heute Standard, brauchen jedoch regelmäßige Updates, um zu funktionieren. Leider pflegt nur ein gutes Drittel der Verbraucher seine Sicherheitssoftware ausreichend.[5] Weniger als 50 Prozent der User informieren sich im Internet über Anbieter und Produkte. Immerhin achtet knapp die Hälfte der Verbraucher gezielt auf eine sichere Datenübertragung. Ein Fünftel macht regelmäßige Backups.[6]

TROCKEN BLEIBEN, AUCH WENN DAS KIND IN DEN BRUNNEN GEFALLEN IST

Neben Firewalls, VPN und dergleichen gibt es eine weitere Option, die mit einem Minimum an Eigeninitiative funktioniert: eine Versicherung. Entscheidend hierbei sind die Fragestellungen, was genau versichert werden kann, wann die Versicherung greift und wie sich etwaige Schäden regulieren lassen.

Wichtig ist zunächst: je umfassender der Schutz, desto sinnvoller die Versicherung. Der User braucht ein Produkt, mit dem sich das gesamte Schadensspektrum abdecken lässt. Das beinhaltet die Absicherung aller PCs und Laptops, mobiler Geräte wie Tablets und Smartphones sowie der Komponenten des Smart Homes.

Im besten Fall sorgt die Versicherung dafür, dass der Nutzer vor den durch einen Cyberangriff entstandenen Schäden ausreichend geschützt ist. Auch die juristische Erstberatung, die bei Fragen der Persönlichkeits- und Urheberrechte wertvoll wird, sowie eine psychologische Unterstützung im Fall von Cybermobbing können zur Absicherung gehören. Doch was, wenn Nutzer nicht direkt zu Schaden kommen, sondern als Mittel zum Zweck digitaler Gangster instrumentalisiert werden? Wenn diese das private Netzwerk über schlecht gesicherte Geräte kapern? Die eigenen Smart Home-Geräte werden plötzlich zum Teil eines Botnets, mit dem die Hacker Schäden bei Dritten verursachen. Daraus können für den ahnungslosen Nutzer ohne eigene Schuld Haftpflichtschäden entstehen. Auch das ist bei der Wahl des Versicherungsschutzes zu bedenken.

Cyberkriminalität ist vielseitig. Darum ist eine echte Rundum-Versicherung die beste Option, um sicherzustellen, dass der User vor sämtlichen Gefahren geschützt ist. Aufgepasst: Es ist trotzdem wichtig, als Nutzer von vornherein nur ein Minimum an Bedrohungen zuzulassen. In jeden Fall aber trägt eine Versicherung dazu bei, das (Online-) Leben sorgloser zu machen.

1| & 2| Quelle: Norton Cyber Security Insights Report 2017 (Norton by Symantec)
3| Quelle: Sopra Steria Consulting, E-Government: Angst vor Datenklau https://www.soprasteria.de/newsroom/news/e-government-angst-vor-datenklau-ist-das-gr%C3%B6%C3%9Fte-hindernis
4| Quelle: Sophos Pressemitteilung: Melissas Autos ist verurteilt https://www.sophos.com/de-de/press-office/press-releases/2002/05/pr_20020502smith.aspx
5| & 6| Quelle: Bundesamt für Sicherheit in der Informationstechnik / Programm Polizeiliche Kriminalprävention der Länder und des Bundes

ERGO

Moderner Cyberschutz – ein Muss auch für Klein-Unternehmer und Freiberufler

Angriffe auf die IT-Systeme von Unternehmen sind in den vergangenen Jahren explosionsartig angestiegen. Datenverlust und Cyber-Bedrohungen/-Erpressungen sind nur einige der möglichen Szenarien. Dabei trifft es längst nicht mehr nur große Unternehmen. Auch kleine und mittelständische Unternehmen sowie Freiberufler werden immer häufiger Opfer einer Cyberattacke. Meistens mit großen finanziellen Folgen.

Die Hacker scheinen den aktuellsten Schutzprogrammen immer einen Klick voraus zu sein. Eines ist klar: Es gibt keinen 100-prozentigen Schutz für IT-Systeme. Damit mögliche Attacken nicht die Existenz Ihres Unternehmens gefährden, benötigen Sie eine gute Absicherung und im Schadensfall einen umfassenden und jederzeit verlässlichen Service.

Das leisten die ERGO Cyber-Versicherungen:

Passgenauer Schutz: Mit der ERGO Cyber-Versicherung Kompakt sichern wir Ihre Eigenschäden ab und bieten Ihnen umfassende Serviceleistungen. Wenn Sie zusätzlich die Ansprüche Dritter sowie Ertragsausfall absichern möchten, wählen Sie einfach die ERGO Cyber-Versicherung. Die Cyber-Versicherung Kompakt ist für alle Unternehmen mit einem Umsatz bis eine Million Euro erhältlich und unsere Cyber-Versicherung für alle Umsatzgrößen.

Umfangreiche Serviceleistungen und Alleinstellungsmerkmale: Im Schadensfall übernehmen wir die erforderlichen Kosten für IT-Dienstleistungen, insbesondere Forensikleistungen sowie umfassende Rechtsdienstleistungen. Im Falle eines Reputationsschadens übernehmen wir auch die Kosten für einen externen Berater und PR-Maßnahmen. Die ERGO Cyber-Versicherungen decken darüber hinaus auch Sach- und Personenschäden ab. Ein starkes Alleinstellungsmerkmal unserer Versicherungen im Markt.

Klartextbedingungen: Wir möchten, dass Sie unser Produkt verstehen. Unsere Klartextbedingungen sind besonders kundenfreundlich geschrieben, damit Sie auf wenigen Seiten erfahren, was versichert ist und was nicht.

Detaillierte Informationen zu den Produkten und den neuen ERGO Cyber-Online-Rechner finden Sie unter https://www.ergo.de.

ERGO Cyber Online-Rechner

Klein-Unternehmer und Freiberufler benötigen einen Cyber-Versicherungsschutz, den sie einfach und schnell abschließen können. Die ERGO bietet jetzt als einer der ersten deutschen Versicherer online über den Cyber-Online-Rechner die beiden Produktvarianten „Cyber-Versicherung Kompakt" und „Cyber-Versicherung" sowie das Cyber-Spezialkonzept für Kammerberufe (Rechtsanwälte, Steuerberater, Wirtschaftsprüfer und Notare) an. Eine Zielgruppe, die intensiv personenbezogene Daten nutzt und daher einem höheren Risiko ausgesetzt ist. Der Online-Rechner bietet kostenfrei weitere kundenorientierte Features: eine Cyber-Checkliste, die die Cyber-Risiken der Kunden aufzeigt und bei der Reduzierung dieser Risiken helfen kann. Zudem enthält er Erläuterungen und Details zu Cyber-Risiken anhand von Schadensbeispielen sowie einen umfassenden Erklärfilm.