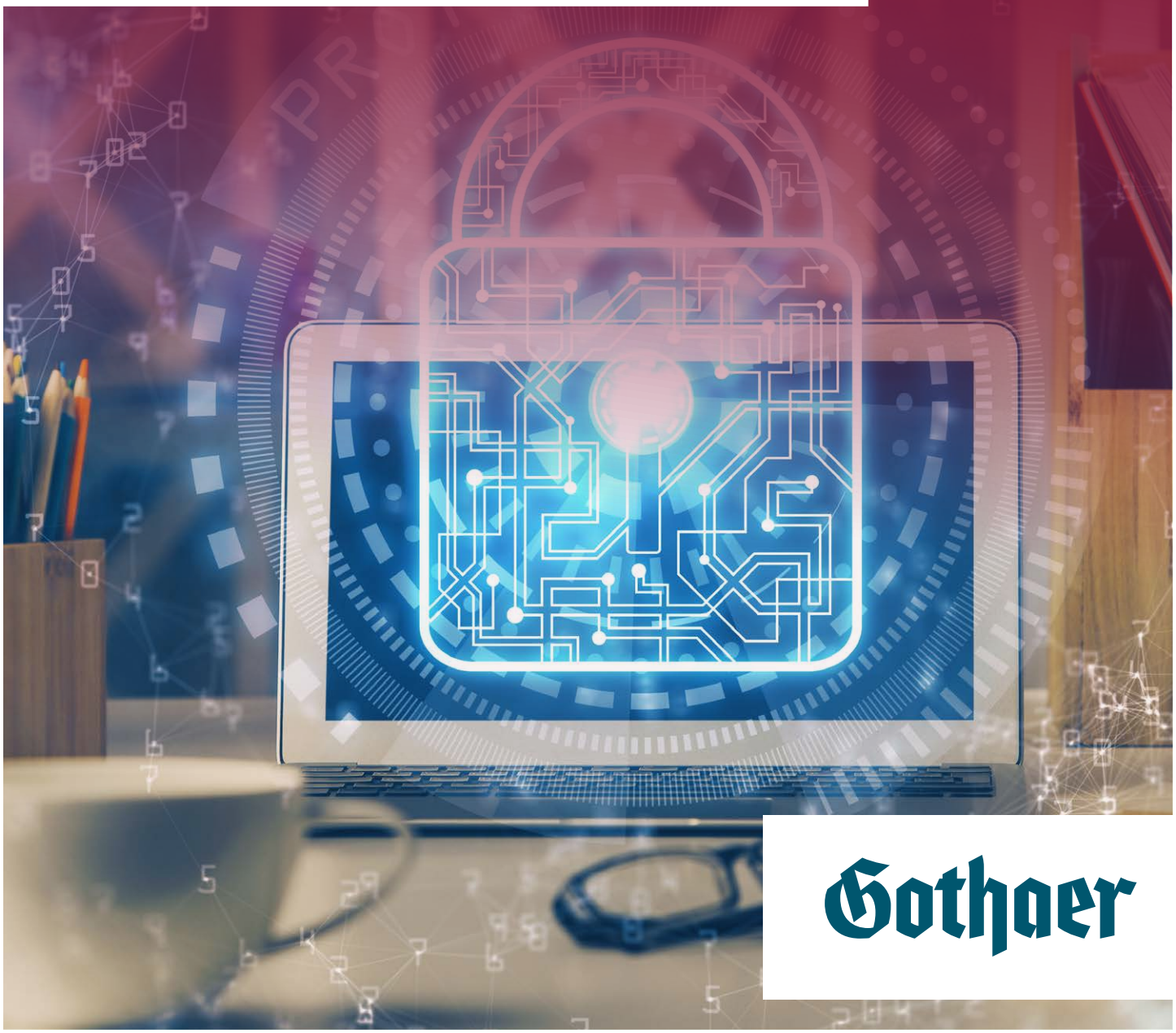
Gesamtverband der Deutschen Versicherungswirtschaft e. V.

CYBER SICHER

Eine Initiative der deutschen Versicherer.

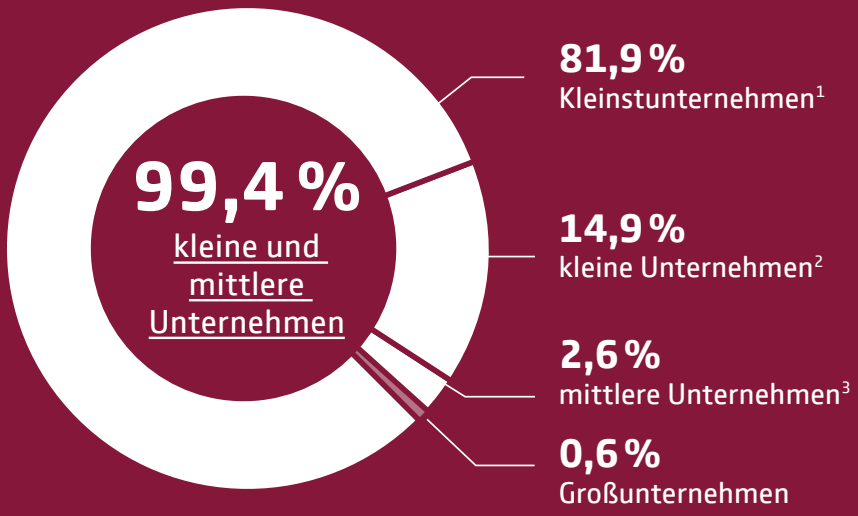
Report

Cyberrisiken im Mittelstand 2021



Gothaer

Der Mittelstand – Rückgrat der deutschen Wirtschaft



1 bis 9 Mitarbeiter/bis 2 Mio. Euro Jahresumsatz
2 10 bis 49 Mitarbeiter/2 bis 10 Mio. Euro Jahresumsatz
3 50 bis 249 Mitarbeiter/10 bis 50 Mio. Euro Jahresumsatz

Quelle: Destatis, Werte für 2019

Über die Initiative

Mit der Initiative CyberSicher sensibilisieren die Versicherer für die Gefahren aus dem Cyberspace und zeigen, wie sich kleine und mittlere Unternehmen schützen können.

CYBER@SICHER

Eine Initiative der Deutschen Versicherer.

Cyberrisiken im Mittelstand 2021



1 Die verdrängte Gefahr

Wenn mobiles Arbeiten zum Sicherheitsrisiko wird

Das Homeoffice wird für Millionen Beschäftigte über die Pandemie hinaus Teil der neuen Arbeitswelt bleiben. Doch weite Teile des Mittelstands sind nach wie vor nicht ausreichend gegen die Risiken des mobilen Arbeits gewappnet. → **Seite 04**



2 Die Sicherheitslücken

Wenn die Cloud brennt …

Auch Stromausfälle, Stürme und Brände können die IT-Sicherheit gefährden und zu Datenverlusten führen. Denn letztendlich ist auch die Cloud ein physischer Ort. → **Seite 12**



Die Schwachen zuerst

Pandemien und Cyberattacken ähneln sich: Beide verursachen große Schäden durch exponentielles Wachstum. Was wir vom Kampf gegen Corona für die IT-Sicherheit lernen können.
Eine Kolumne von Linus Neumann. → **Seite 16**



3 Der Schutz

Achtung: Dringender Sicherheitshinweis!

Diese drei Tipps sollte jedes Unternehmen beherzigen. → **Seite 18**



Selbsttest: Wie gut ist Ihre IT-Sicherheit?

Finden Sie heraus, wo Ihre Schwachstellen sind und wie Sie diese schließen können. → **Seite 20**



Wenn mobiles Arbeiten zum Sicherheitsrisiko wird

Die Corona-Pandemie hat Millionen Beschäftigte zum mobilen Arbeiten gebracht und die Arbeitswelt wohl unwiderruflich revolutioniert: Das Homeoffice wird auch nach der Pandemie weiterhin völlig selbstverständlich zum Arbeitsalltag vieler Unternehmen gehören. Doch Studien und Erfahrungen der Versicherer zeigen: Weite Teile des deutschen Mittelstands sind noch immer nicht ausreichend gegen die Risiken des mobilen Arbeitens gewappnet. Zeit für ein Sicherheitsupdate.



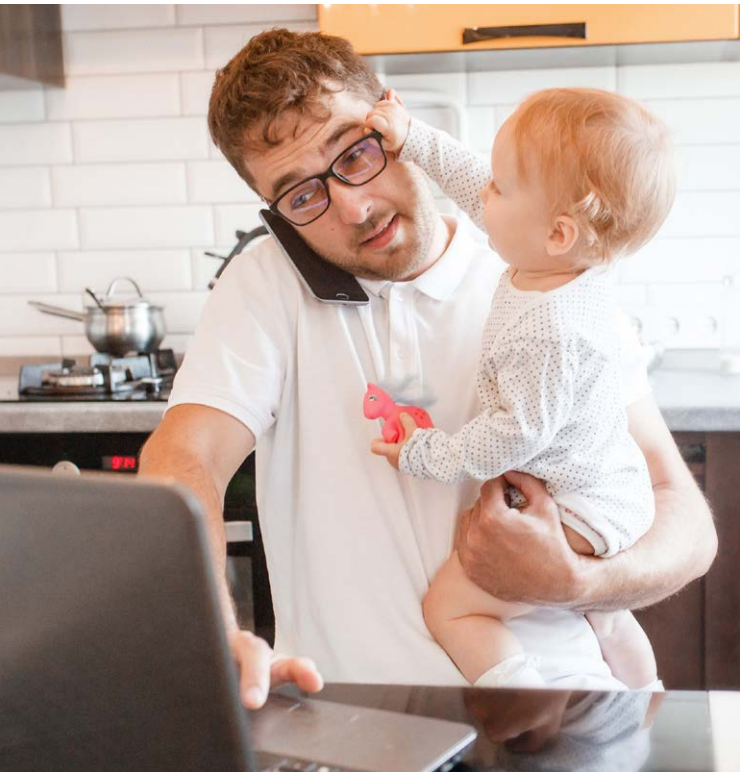
Neue Arbeitswelt – neue Risiken. Wie bei jedem tiefgreifenden und dauerhaften Wandel müssten auch die neuen Abläufe und Prozesse des mobilen Arbeitens auf ihre Sicherheit geprüft und entsprechend angepasst werden. Doch genau das passiert nur in einer kleinen Minderheit der Unternehmen, wie eine Forsa-Umfrage im Auftrag der GDV-Initiative CyberSicher zeigt. Grund ist eine ebenso bemerkenswerte wie besorgniserregende Diskrepanz: Obwohl in jedem zweiten Unternehmen mobil gearbeitet wird und jedes vierte von verstärkten Cyberangriffen in der Pandemie berichtet, sehen viele der befragten Entscheider gar keine neuen Risiken. Gerade einmal acht Prozent meinen, dass sich in der Pandemie neue Cyber-Bedrohungen ergeben hätten – mehr als 90 Prozent glauben das nicht.

In Folge dieser mangelhaften Risikowahrnehmung werden die Gefahren – sozusagen als Folgefehler – auch nicht entschärft. Denn bei der Frage nach konkreten Maßnahmen für mehr Sicherheit findet sich wiederum nur die kleine Minderheit von weniger als zehn Prozent der Unternehmen, die ihre Regeln angepasst und in mehr IT-Sicherheit investiert haben. Für die breite Mehrheit gilt auch hier: Fehlanzeige.

Dieser Befund wäre nur dann unproblematisch, wenn die Sicherheitsvorkehrungen schon vorher perfekt gewesen wären. Doch: Sie sind es nicht, ganz im Gegenteil. Auch das zeigen die Ergebnisse von Forsa.

So arbeiten in der Hälfte der Unternehmen Beschäftigte ausschließlich oder zumindest teilweise mit ihren privaten Geräten. Auf solche privaten Geräte und ihre Sicherheit haben die Unternehmen aber keinen direkten Einfluss. Und weil diese Geräte eben nicht nur beruflich, sondern auch für private Zwecke und sogar von der ganzen Familie genutzt werden, stellen sie ein hohes und für das Unternehmen kaum einzuschätzendes Risiko dar.

Dasselbe gilt für Messenger-Dienste, die im Rahmen des mobilen Arbeitens in vielen Unternehmen Einzug gehalten haben – und so die Grenze zwischen privaten und beruflichen Anwendungen und Geräten weiter verschwimmen lassen.

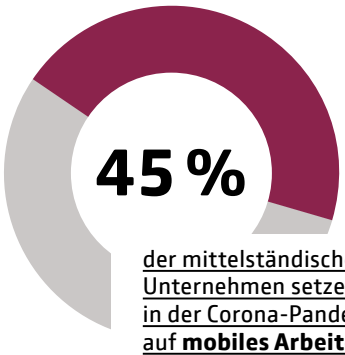




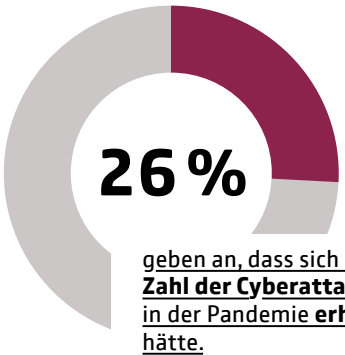
Neue Arbeitswelt – …

… gleiche Risiken?

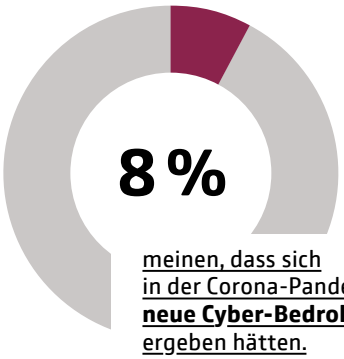
Trotz deutlich mehr mobiler Arbeit und mehr Cyberattacken erkennt nur eine Minderheit neue Risiken



der mittelständischen Unternehmen setzen in der Corona-Pandemie auf **mobiles Arbeiten**.



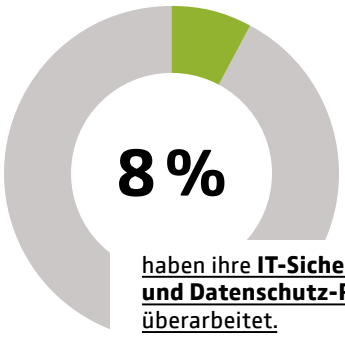
geben an, dass sich die **Zahl der Cyberattacken** in der Pandemie **erhöht** hätte.



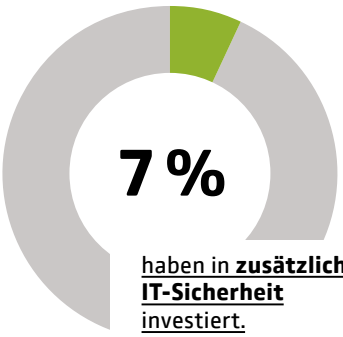
meinen, dass sich in der Corona-Pandemie **neue Cyber-Bedrohungen** ergeben hätten.

… gleiche Regeln

Nur eine Minderheit hat ihre Sicherheitsvorkehrungen den neuen Risiken angepasst



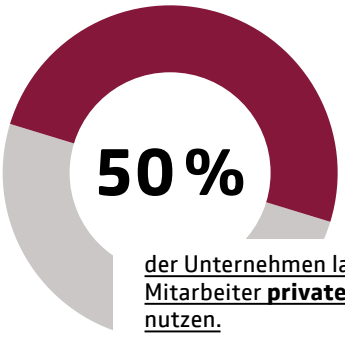
haben ihre **IT-Sicherheits- und Datenschutz-Regeln** überarbeitet.



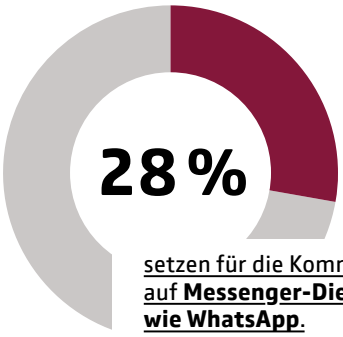
haben in **zusätzliche IT-Sicherheit** investiert.

… laxe Regeln

Durch mobiles Arbeiten sind in vielen Unternehmen leicht zu schließende Sicherheitslücken entstanden

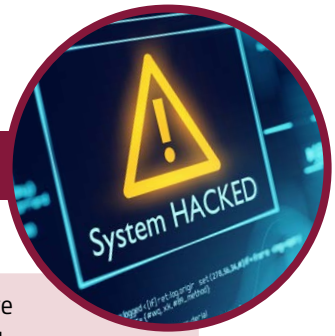


der Unternehmen lassen ihre Mitarbeiter **private Geräte** nutzen.



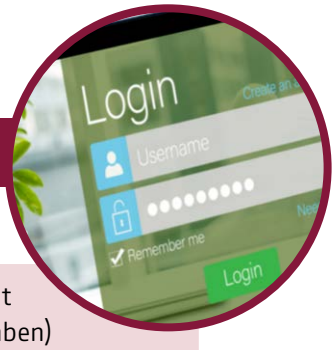
setzen für die Kommunikation auf **Messenger-Dienste wie WhatsApp**.

Quelle: Forsa-Befragung von 300 mittelständischen Unternehmen, Frühjahr 2021



Praxisbeispiel: Ransomware

Betroffenes Unternehmen	Steuerberatung
Vorgehensweise der Täter	Cyberkriminelle verschlüsseln mithilfe einer Schadsoftware sämtliche Daten und sperren alle IT-Systeme des Unternehmens.
Sicherheitslücke / Die Tat begünstigende Umstände	Alle Beschäftigte inklusive der IT-Abteilung arbeiten pandemiebedingt aus dem Home-Office. Niemand kann mehr auf das verschlüsselte Unternehmensnetzwerk zugreifen. Die IT-Abteilung muss inklusive externer IT-Krisenexperten wieder physisch ins Büro kommen, um das Unternehmensnetzwerk zunächst in einem Offline-Notbetrieb neu aufzubauen. Erst nach und nach können Zugriffe von außen wieder freigegeben werden, damit die anderen Abteilungen ihrer gewohnten Arbeit nachgehen können.
Schaden für das Unternehmen	Tagelange Betriebsunterbrechung; Kosten für IT-Forensik (Analyse zur Aufklärung des Angriffs); Wiederherstellung der IT-Systeme und Unternehmensdaten; insgesamt niedriger sechsstelliger Betrag.
Präventionsmöglichkeiten	Ausgearbeitete und stets aktuelle Notfallpläne für den Ausfall des IT-Systems; vertragliche Vereinbarung mit kompetentem IT-Dienstleister für IT-Notfälle; regelmäßige Sicherungskopien außerhalb des direkten Zugriffs.



Praxisbeispiel: Zugangsdaten

Betroffenes Unternehmen	Arztpraxis
Vorgehensweise der Täter	Cyberkriminelle infizieren den Privatrechner des Arztes mit einem Keylogger (dient zur Aufzeichung der Tastatureingaben) und gelangen so an die Zugangsdaten für den Fernzugriff auf die Praxis-IT. Über diesen Fernzugriff gelangen die Täter an vertrauliche Patientendaten.
Sicherheitslücke / Die Tat begünstigende Umstände	Das private Endgerät des Arztes ist deutlich schlechter geschützt und höheren Risiken ausgesetzt als die von der eigenen IT kontrollierten Geräte in der Praxis.
Schaden für das Unternehmen	Kosten für IT-Forensik; Anwaltskosten im Zusammenhang mit der Information der betroffenen Patienten und der zuständigen Datenschutzbehörde; insg. mittlerer fünfstelliger Betrag; zusätzlich Vertrauensverlust bei betroffenen Patienten.
Präventionsmöglichkeiten	Verzicht bzw. Verbot, private Geräte für den Zugriff auf berufliche Dokumente und Daten zu nutzen; Ausstattung aller mobil arbeitenden Beschäftigten mit sicheren Endgeräten, die wiederum nicht für private Zwecke genutzt werden dürfen.

„Wer seine Prozesse jetzt noch nicht an die neue Arbeitswelt angepasst hat, handelt fahrlässig und lädt Cyberkriminelle und Betrüger geradezu ein."

GDV-Hauptgeschäftsführer Jörg Asmussen



„Dass zu Beginn der Pandemie viele Sicherheitsroutinen gestört waren, ist noch verständlich. Aber wer seine Prozesse jetzt noch nicht an die neue Situation angepasst hat, handelt fahrlässig und lädt Cyberkriminelle und Betrüger geradezu ein", kritisiert GDV-Hauptgeschäftsführer Jörg Asmussen. Denn Cyberkriminelle nutzen die neuen Schwachstellen ganz gezielt für ihre Angriffe aus (siehe Praxisbeispiele auf Seite 08) und zeigen damit: Risiken verschwinden nicht dadurch, dass man die Augen ganz fest schließt. Wenn man sie nicht ernst nimmt, führen sie früher oder später zu ganz realen und unter Umständen sehr bitteren Schäden.

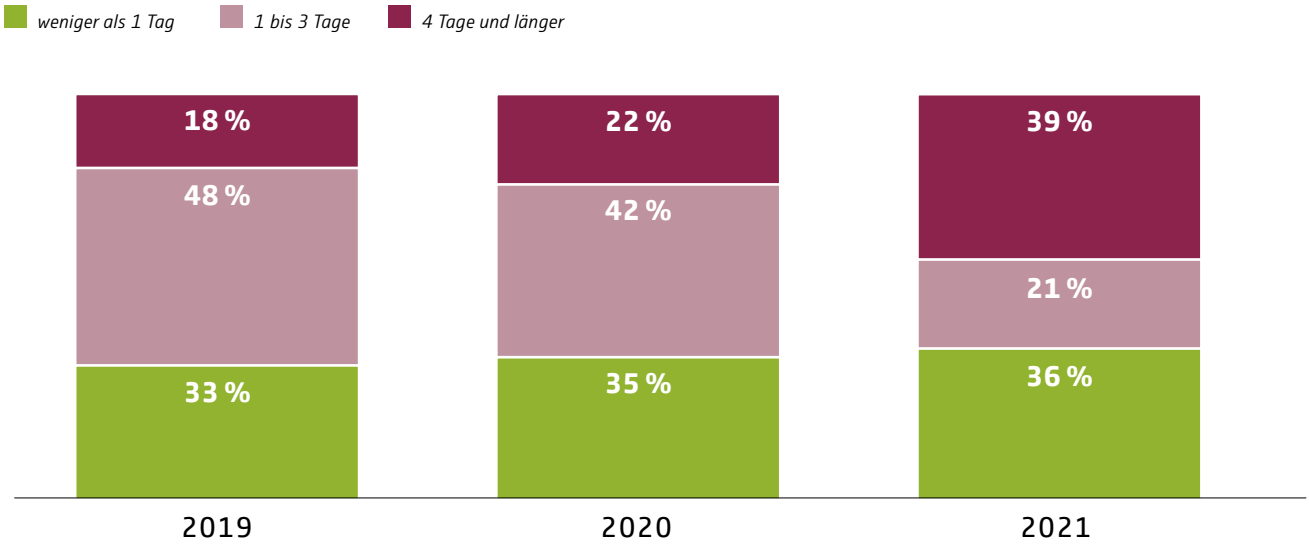
Cyberattacken legen Unternehmen länger lahm

Eine weitere Folge mangelnder Prävention zeigt sich bei den Folgen von Cyberattacken – denn sie sind deutlich gravierender geworden: So gaben in diesem Jahr 39 Prozent der betroffenen mittelständischen Unternehmen an, vier oder mehr Tage für die Wiederherstellung ihrer IT-Systeme gebraucht zu haben. In den Vorjahren hatte der Anteil noch rund 20 Prozent betragen.

Asmussen macht die fehlende Vorbereitung vieler Firmen für die Entwicklung verantwortlich: „Ein Drittel hat niemanden, der explizit für die IT-Sicherheit verantwortlich ist. Die Hälfte hat keinerlei Plan für den Umgang mit einer

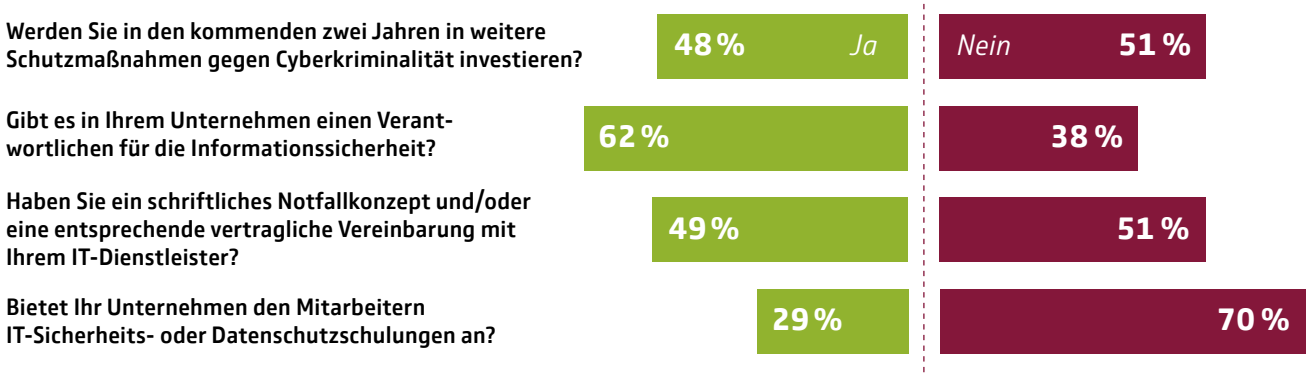
Cyberattacken legen Unternehmen länger lahm

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

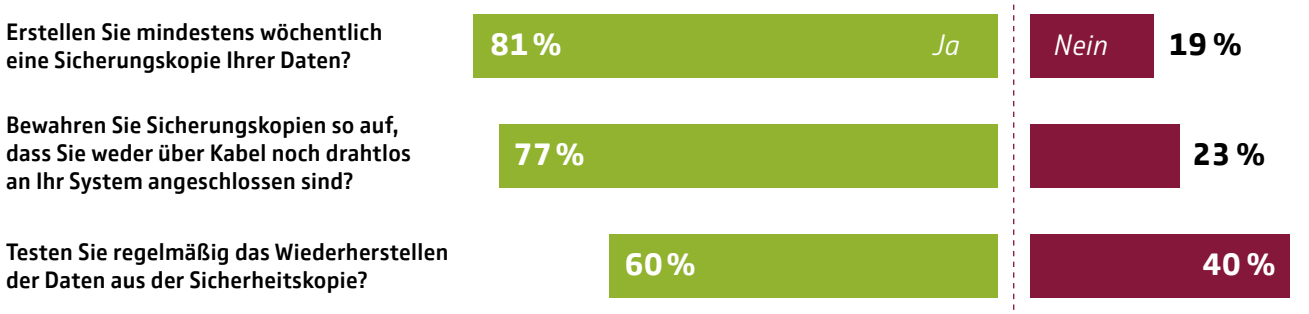


Quelle: Repräsentative Forsa-Befragung von 300 Entscheidern in kleinen und mittleren Unternehmen im April 2021

IT-Sicherheit hat in vielen Firmen keine Priorität



Lückenhafte Datensicherung



Quelle: Repräsentative Forsa-Befragung von 300 Entscheidern in kleinen und mittleren Unternehmen im April 2021

Cyberattacke. Daher reagieren diese Unternehmen auf einen Angriff zu langsam und erleiden unnötig schwere wirtschaftliche Folgen“, so Asmussen.

Ein wesentliches Problem ist der laxe Umgang mit Datensicherungen. Nach der repräsentativen Umfrage verzichtet jedes fünfte mittelständische Unternehmen auf mindestens wöchentliche Backups oder bewahrt diese nicht sicher auf. Ob die Daten aus den Sicherungskopien wirklich wiederhergestellt werden können, überprüfen nur 60 Prozent der befragten Firmen. „Sicherungskopien sind gerade bei Ransomware-Attacken das wirksamste Gegenmittel und sollten daher so aktuell und so sicher wie möglich sein“, sagt Asmussen.

Paradox: Trotz der Sicherheitslücken und obwohl 27 Prozent der Befragten bereits Opfer einer Cyberattacke waren, hält eine breite Mehrheit (70%) die Gefahr für das eigene Unternehmen für gering; 79 Prozent meinen, bereits genug für ihre IT-Sicherheit zu tun. Richtig sei aber das Gegenteil, so Asmussen: „Der Mittelstand ist gerade wegen seiner Arglosigkeit stark durch Cyberkriminalität gefährdet und müsste viel mehr für den Schutz seiner IT-Systeme tun.“

Über die Umfrage

Im Auftrag des GDV führt die Forsa Gesellschaft für Sozialforschung und statistische Analysen mbH seit 2017 jährlich eine repräsentative Befragung von 300 Entscheidern in kleinen und mittleren Unternehmen (max. 250 Mitarbeiter und max. 50 Mio. Euro Jahresumsatz) zu Cyberrisiken und IT-Sicherheit durch. Die diesjährige Befragung fand im Frühjahr 2021 statt.



Was eine Cyberattacke kosten kann – und eine Cyberversicherung deckt

Musterszenario Diebstahl Online-Shop/Kreditkartendaten:

Hacker attackieren die Datenbank eines mittelständischen Online-Shops und erbeuten die Kreditkarten-Daten von 50.000 Kunden.

Hinweis

Kreditkartenunternehmen weist Shop-Betreiber auf möglichen Datendiebstahl hin.

Security-Initiative & Betriebsunterbrechung

Nach Bestätigung des Angriffs werden die Ursachen gesucht, die Systeme desinfiziert und gehärtet.

Der Online-Shop bleibt währenddessen geschlossen.

- *Kosten für IT-Forensik: 40.000 Euro*
- *Kosten der Betriebsunterbrechung: 50.000 Euro*

Kundeninformation

Der Shop-Betreiber muss seine Kunden über den Diebstahl ihrer Daten informieren.

- *Informationskosten: 80.000 Euro*

Ersatzkarten

Alle potenziell betroffenen Kunden erhalten neue Kreditkarten.

Vertrauenskrise

Die Presse berichtet über den Diebstahl der Kreditkartendaten, der Online-Shop verzeichnet einen erheblichen Umsatzrückgang.

- *Krisenkommunikation: 30.000 Euro*

Der Umsatzrückgang ist nicht gedeckt.

Aufarbeitung

Die Strafverfolgungsbehörden ermitteln. Das Kreditkartenunternehmen nimmt den Shop-Betreiber für die Ausstellung der Ersatzkarten in Regress.

- *Vertragsstrafen: 50.000 Euro*

Musterszenario Ransomware:

Hacker attackieren mit einem Verschlüsselungs-Trojaner die IT-Systeme eines Maschinenbauers. Sie wollen die gesperrten Rechner erst wieder freigeben, wenn sie Lösegeld bekommen.

Angriff

Sämtliche Rechner und die vernetzten Produktionssysteme des Maschinenbauers sind ohne Funktion. Auf den Bildschirmen der Steuerungsrechner erscheint lediglich eine Nachricht der Erpresser.

IT-Forensik und Datenwiederherstellung

Nach Rücksprache mit Polizei und Staatsanwaltschaft zahlt das Unternehmen kein Lösegeld. IT-Spezialisten arbeiten mehrere Tage daran, den Trojaner von sämtlichen Systemen zu entfernen; anschließend müssen sie alle Daten aus den Backups wiederherstellen.

- *Kosten für IT-Forensik und Datenwiederherstellung: 40.000 Euro*

Betriebsunterbrechung

Bis die Systeme wieder laufen, kann das Unternehmen nicht produzieren. Die Mitarbeiter aus Fertigung und Verwaltung bleiben zuhause.

- *Kosten für 5 Tage Betriebsunterbrechung: 45.000 Euro*

Information von Kunden und Vertragspartnern

Die IT-Forensiker können nicht ausschließen, dass Daten nicht nur gesperrt, sondern auch entwendet wurden. In diesem Fall wären auch Betriebsgeheimnisse von Vertragspartnern betroffen, die vorsorglich informiert werden müssen.

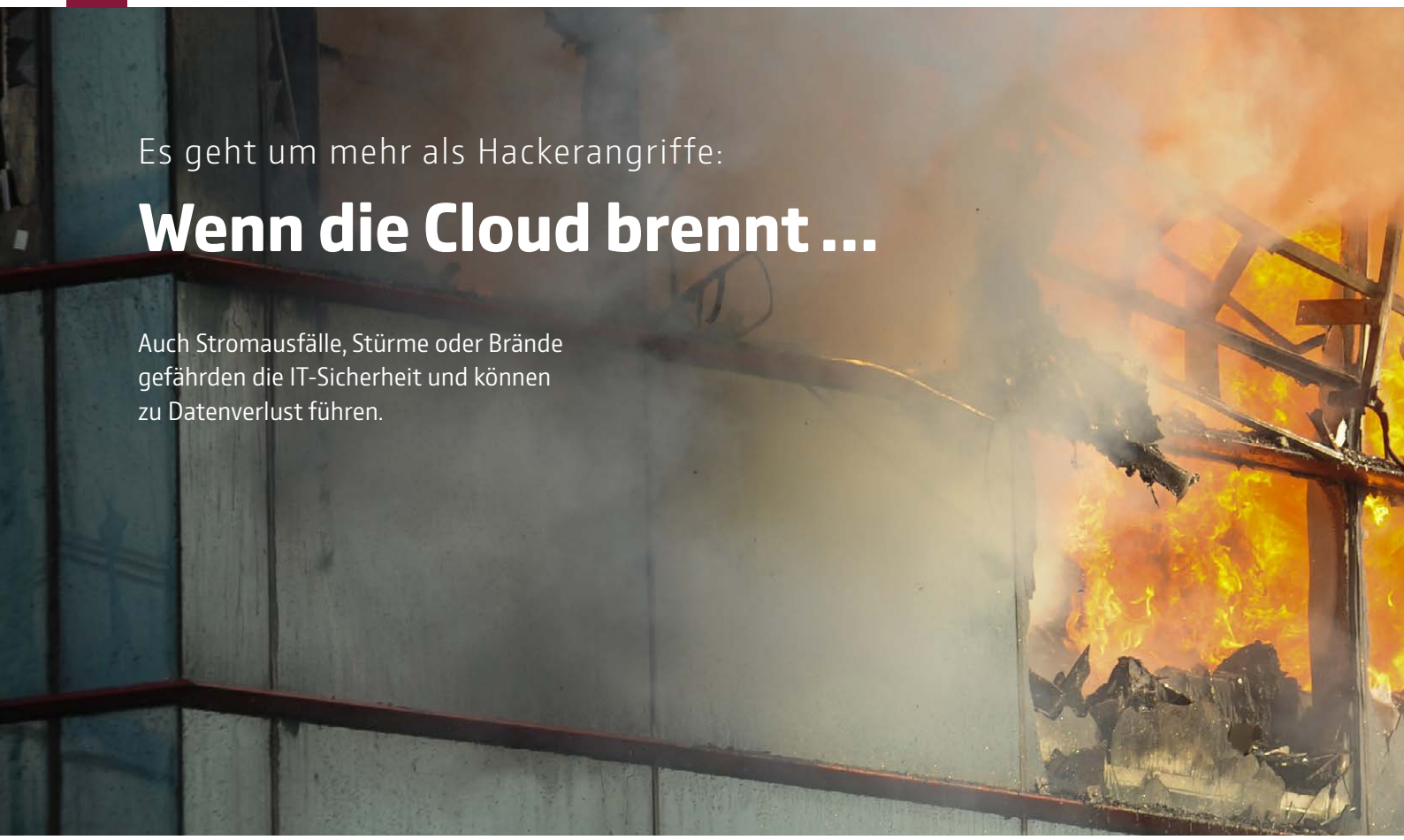
- *Informationskosten und Rechtsberatung: 20.000 Euro*

Vertrauenskrise

Der bisher tadellose Ruf des Unternehmens nimmt in wichtigen Kundenbranchen Schaden; einige Kunden wenden sich vom Unternehmen ab, der Umsatz sinkt spürbar.

- *Krisenkommunikation: 30.000 Euro*

Der Umsatzrückgang ist nicht gedeckt.



Es geht um mehr als Hackerangriffe:

Wenn die Cloud brennt …

Auch Stromausfälle, Stürme oder Brände gefährden die IT-Sicherheit und können zu Datenverlust führen.

Ein Industriegebiet bei Straßburg Anfang März: Meterhohe Flammen schlagen aus allen fünf Stockwerken eines Zweckbaus, dessen Fassade von Lüftungsgittern übersät ist. Der Nachthimmel färbt sich orange, beißender Gestank von verbranntem Plastik hängt in der Luft. Auf dem Gelände betreibt ein Cloud-Anbieter vier Rechenzentren. Eines brennt vollständig ab, ein zweites zum Teil, die beiden anderen müssen zur Sicherheit heruntergefahren werden. Mehr als 10.000 Server werden in dieser Nacht zerstört. 3,5 Millionen Websites und fast 500.000 Domains fallen stundenlang aus. Internetauftritte der französischen Regierung sind ebenso betroffen wie die namhafter Unternehmen. Schlimmer noch: Viele Daten sind unwiederbringlich verloren. Es ist eine Katastrophe, die in der digitalen Welt nicht vorgesehen ist. Die Cloud ist das Betriebssystem der Wirtschaft, Basis unzähliger Geschäftsmodelle, unverzichtbar für das Funktionieren von Fabriken und die Arbeit in Unternehmen. Vom Konzern zum Handwerksbetrieb vertrauen Firmen der Cloud ihre Daten an – weil sie als so sicher gilt. Man hortet sein Geld ja auch nicht daheim im Tresor, sondern bringt es zur Bank, von der man es selbst nach einem Überfall zurückbekommt. Sollten Daten in der Cloud nicht genauso sicher sein?

200 Kilometer

Abstand müssen zwischen zwei Rechenzentren liegen, damit die Behörden ihnen das Sicherheitsprädikat „georedundant“ verleihen: Selbst bei großen Naturkatastrophen ist der Ausfall beider Standorte unwahrscheinlich.

„Was viele ausblenden, ist die Tatsache, dass auch die Cloud letztlich ein physischer Ort ist“, sagt Thomas Pache, Head of Specialty Cyber beim Versicherungsmakler Aon in Hamburg. „Die Daten liegen nicht in einer unantastbaren virtuellen Wolke, sondern sind auf Servern gespeichert, die irgendwo auf der Welt stehen und damit realen Gefahren ausgesetzt sind.“ Sie könnten einem Brand zum Opfer fallen wie in Straßburg, durch eine Überschwemmung zerstört werden oder bei einem Stromausfall unerreichbar sein. Was nicht heißt, dass Daten in der Cloud nicht trotzdem sicher sein können. Denn für all diese Fälle gebe es Lösungen, sagt Pache. Im weitesten Sinne fallen sie unter das Stichwort Redundanz.



Feuer in der Cloud: Im März stehen zwei Rechenzentren bei Straßburg in Flammen. Millionen Websites fallen aus, viele Daten gehen unwiederbringlich verloren.

Was hat Blitzeis mit Datensicherheit zu tun? Eine Menge, wie ein Fall von 2005 zeigt

Gemeint ist das Vorhalten zusätzlicher Ressourcen für den Fall, dass die Primärressource ausfällt. Klingt kompliziert, erschließt sich aber schnell: Ein Bagger zerstört die Stromleitung ins Rechenzentrum? Kein Problem, wenn auf der anderen Seite ein zweites Kabel ins Gebäude führt oder das Notstromaggregat anspringt. Ein Feuer bricht aus? Noch bevor es die Server erreicht, legen diese automatisch Backups aller Daten auf weiteren Servern ab – die sich im besten Fall nicht im Nachbargebäude befinden. Von „Georedundanz“ spricht das Bundesamt für Sicherheit in der Informationstechnik (BSI), wenn der Backup-Rechner mindestens 200 Kilometer vom Originalserver entfernt steht. Viel Aufwand, könnte man meinen. Aus Sicht von Marc Thamm, Datensicherheitsexperte beim Spezialversicherer Hiscox, kann der aber durchaus gerechtfertigt sein. „Naturkatastrophen können große Gebiete zerstören, denken Sie an den Tsunami 2004 in Asien.“ Und auch wenn die Erdbebengefahr

Viele Mittelständler setzen auf die Cloud

Anteil der Unternehmen, die Clouddienste nutzen



Quelle: Forsa-Umfrage 2020

in Deutschland vergleichsweise gering ist, seien auch hier Unglücke denkbar, die weite Landstriche betreffen könnten. 2005 etwa knickten im Münsterland nach einem Schneesturm reihenweise Strommasten um. Es kam zum größten Blackout der deutschen Nachkriegsgeschichte. Obendrein machte Blitzeis viele Straßen unpassierbar und behinderte die Tankfahrzeuge, die dieselbetriebene Notstromaggregate versorgen sollten. „Ein zweites Rechenzentrum am anderen Ende desselben Gewerbegebiets bringt Ihnen in solchen Fällen nichts“, sagt Thamm.

„Auch die Cloud ist letztlich ein physischer Ort.“

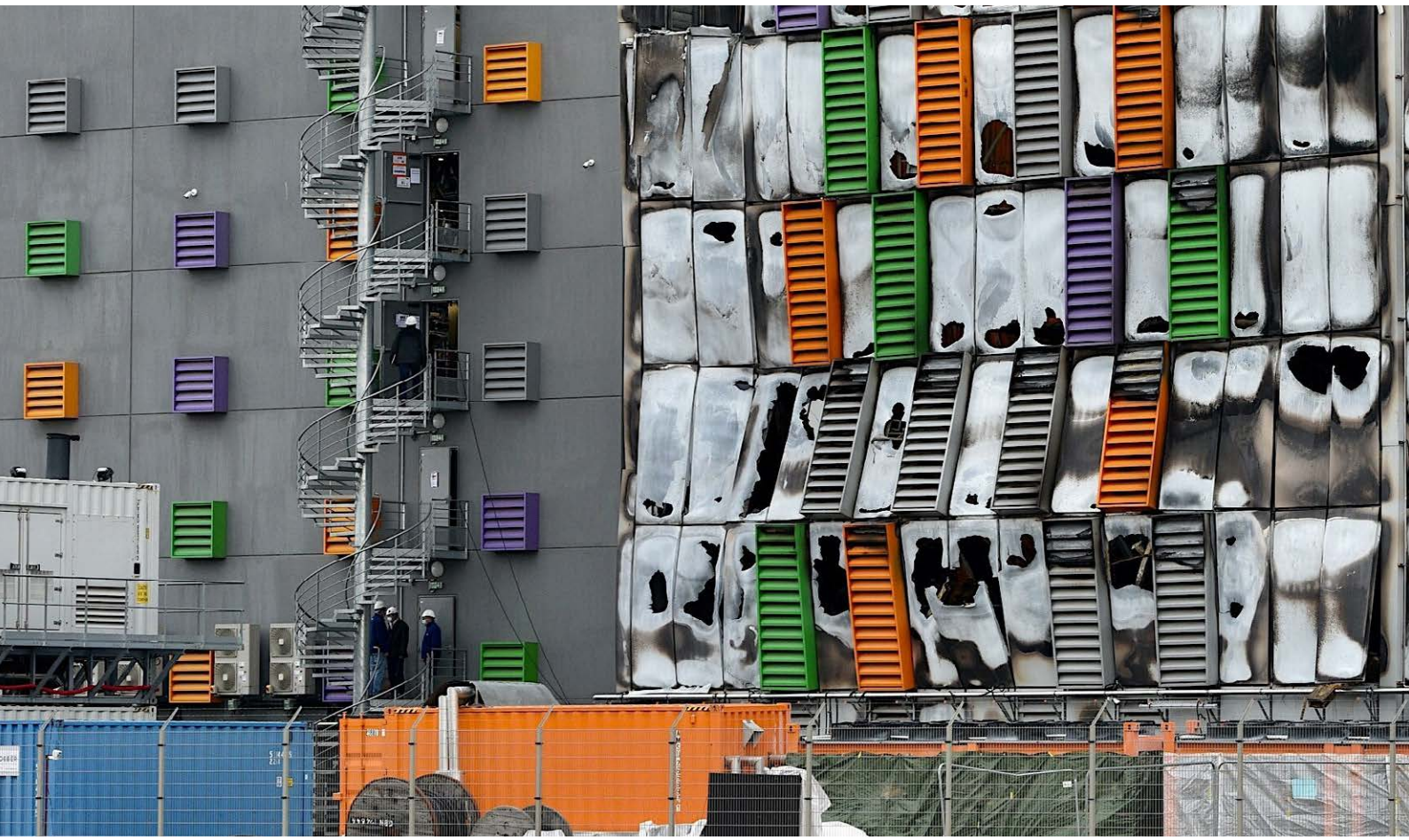
Thomas Pache,
Head of Specialty Cyber bei Aon

Nicht alle Daten besitzen den gleichen Wert. Manchmal reicht ein niedriger Schutzfaktor

Doppelt und dreifach gesicherte Infrastrukturen sind allerdings teurer. Das Problem beim Brand in Straßburg war offenbar, dass viele Kunden das günstigste Angebot des Cloud Betreibers gebucht hatten. Ob allen bewusst war, dass sie damit auf ein Backup verzichteten, ist unbekannt. In der IT-Szene kursiert eine launige Redewendung für falsche Sparsamkeit: Kein Backup, kein Mitleid. Der Spruch findet sich längst auf Tassen und T-Shirts von Systemadministratoren. Betriebswirtschaftlich könne es aber durchaus Sinn ergeben, auch günstige Angebote zu buchen, sagt Peter Pillath, wie Thamm Experte bei Hiscox. Unternehmen müssten abwägen, wie geschäftskritisch einzelne Datensätze seien und was es bedeute, wenn sie vorübergehend nicht abrufbar seien. Nicht jederzeit auf Reisekostenabrechnungen zugreifen zu können sei womöglich verschmerzbar, sodass eine niedrigere Qualitätsstufe genüge. Betriebsgeheimnisse oder sensible Kundendaten dagegen gehörten in höhere Schutzstufen, was dann sehr viel teurer sein könne.

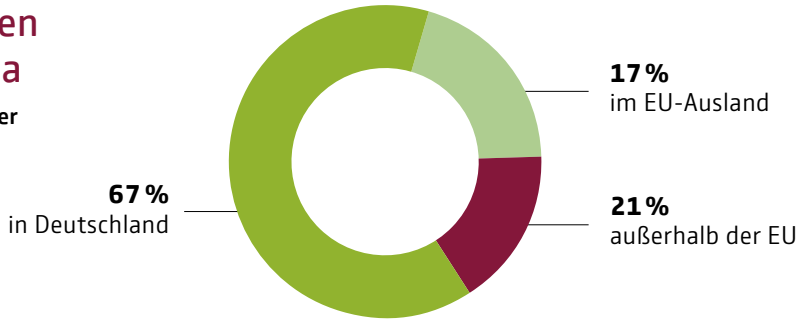
Die Assekuranz versichert sowohl die Betreiber von Rechenzentren als auch deren Kunden. Entsprechend groß ist ihr Interesse, dass die Rechenzentren Vorsorge treffen.

Markus Preissinger, Experte im Bereich Cyber Risks Continental Europe bei Munich Re, nennt beispielhaft zentrale Vorkehrungen: Der Schutz gegen technische Defekte, Naturereignisse und menschliche Einwirkung etwa sei unter anderem durch eine sachgemäße Verkabelung, die Wahl eines passenden Standorts oder Zutrittskontrollen zu gewährleisten. Nach Worten von Ulrich Rappold, Leiter



Die meisten Daten bleiben in Europa

Wo hat ihr Cloud-Dienstleister seinen Sitz?



Quelle: Forsa-Umfrage 2020

Risk Engineering bei Munich Re, helfen gegen Feuer und Löschwasserschäden passende Baumaterialien und Trennwände, die eine Ausbreitung des Feuers verhindern. Auf die Bedeutung von Sicherheitsnormen verweist Roman Bansen, Bereichsleiter IT-Infrastrukturen beim Branchenverband Bitkom. „Trotz des großen Stellenwerts von Risikovermeidung bei Design und Betrieb von Rechenzentren bleiben gewisse Restrisiken bestehen“, erklärt er. Zwar seien Vorfälle in der Größenordnung wie in Straßburg extrem selten. Das ändere aber nichts an der Notwendigkeit, stets entsprechend der Normen zu planen und zu bauen, auch wenn diese Normen nicht verpflichtend seien. „Natürlich sollten immer auch Backup-Szenarien berücksichtigt werden“, so Bansen. Das könne unter Umständen auch den Einsatz eines zweiten Rechenzentrums bedeuten. Viele Unternehmen beherzigen das offenbar bereits: „Eine Wolke ist nicht genug“, sagt Cloud Computing-Experte Peter Heidkamp von KPMG. Der Trend gehe inzwischen zur „Mehrfachwolke“.

„Eine Cloud ist nicht genug“

Peter Heidkamp, Cloud-Computing-Experte bei KPMG



Zahlreiche Kunden der zerstörten Rechenzentren hatten ein günstiges Angebot ohne Backups gebucht. IT-Administratoren haben dafür wenig Verständnis: Kein Backup, kein Mitleid.

Die Schwachen zuerst

Pandemien und Cyberattacken ähneln sich: Beide verursachen große Schäden durch exponentielles Wachstum. Was wir vom Kampf gegen Corona für die IT-Sicherheit lernen können.

Seit ihrer ersten mathematischen Beschreibung sprengen Exponentialfunktionen das Vorstellungsvermögen der Menschen. Sicherlich kennen auch Sie die Überlieferung vom indischen Kaiser Sheram, der Zeta, den Erfinder des Schachspiels großzügig entlohnen wollte. Zeta wünschte sich, für das erste Feld des Schachbrettes ein Reiskorn, zwei Körner für das zweite Feld, vier für das dritte und für jedes weitere Feld doppelt so viele Körner wie für das vorhergehende. Was wie ein bescheidener Wunsch klingt, führt nach 64 Iterationen zu vielen Milliarden Tonnen Reis, der Welt-Reis-Ernte von mehreren Hundert Jahren.

Die Exponentialfunktion und der Cyber-Angriff

Auch Hacker haben immer wieder mit Exponentialfunktionen zu tun. Sie brauchen beispielsweise zum Cracken eines Passworts von sieben Zeichen wenige Millisekunden, zum Cracken eines Passworts von zehn Zeichen - nur drei mehr – aber mehrere Monate. So kleine Unterschiede mit so großer Wirkung sind für uns Menschen schwer intuitiv zu erfassen.

Auch die Autoren und Autorinnen von Computer-Würmern geraten immer wieder an die Grenzen ihrer eigenen Vorstellungskraft. Als „Wurm“ wird eine Schadsoftware bezeichnet, die sich selbst automatisch weiterverbreitet. Dafür kommt in der Regel eine kritische Schwachstelle zum Einsatz, die automatisiert ausnutzbar ist. Ein infiziertes System beginnt also, automatisch andere Systeme zu infizieren, welche wiederum beginnen, andere Systeme zu infizieren... Zeta, der bis heute auf seine Reislieferung wartet, lässt grüßen.

Vielzitierte historische Beispiele sind der „Morris“-Wurm, dessen Autor als erster Verurteilter nach dem Computer Fraud and Abuse Act in die Geschichte einging und der Wurm ILOVEYOU, der im Mai 2000 einen Großteil des E-Mail-Verkehrs zum Erliegen brachte. Auch der Ausfall von rund einer Million Telekom-Routern Ende 2016 war Kollateralschaden der Aktivität eines Computer-Wurms.

Nicht zuletzt konnten die Softwaregewordenen Alpträume der Versicherungswirtschaft, WannaCry und NOTPETYA nur durch ihre Fähigkeit zur automatischen Weiterverbreitung immense Schäden anrichten: Auf die „Erstinfektion“ eines Rechners in einem Firmennetz folgte die automatische Ausbreitung innerhalb vieler Firmennetze – also in Bereiche, die Angreifer sonst nicht ohne weiteres zugänglich und daher gern schlechter geschützt sind.

Die SARS-CoV-2-Pandemie hat weltweit zu einem besseren Verständnis von sich selbst verbreitenden Infektionen geführt. Auch der Begriff der „Welle“ ist fester Bestandteil des Pandemie-Vokabulars, ebenso wie wir es im Bereich der IT-Sicherheit immer wieder mit Angriffswellen zu tun haben.

Ein Vergleich des Infektionsgeschehens und der Mechanismen einer Pandemie und einer Cyberattacke kann helfen, Risiken besser einzuschätzen und zu managen:

Zeitachse | Während eine Pandemie sich über Monate und Jahre erstrecken kann, spielt sich bei einem exponentiell skalierenden IT-Angriff das Geschehen binnen weniger Stunden oder Tage ab. Ressourcengrenzen werden so sehr viel schneller erreicht, Gegenmaßnahmen müssen unmittelbar eingeleitet werden. Auch Landesgrenzen spielen im Internet keine Rolle.

Lockdown | Eine Abschottung von IT-Systemen im Notfall kann sowohl Ultima Ratio als auch drakonische Schutzmaßnahme zu Beginn des Ausbruchs sein. Sie ist mit potenziell hohen Kosten verbunden und hat eine ähnlich bittere Eigenschaft wie in der Pandemie: Je schneller der Lockdown kommt, desto kürzer ist er nötig. Und keinesfalls ist er eine tragfähige Dauerlösung.

Immunisierung | Das Analogon zur Impfung in der IT ist die Beseitigung der ausgenutzten Schwachstelle. Glücklicherweise kann diese in der Regel schnell gefunden und beseitigt werden. Das Wissen zur „Impfung" kann der Menschheit schnell, kostenlos und weltweit zur Verfügung gestellt werden. Dafür bleibt jedoch nur wenig Zeit, wenn die Exponentialfunktion gnadenlos läuft.

Intensivbetten | Schon ohne einen weltweiten IT-Sicherheitsvorfall sind die „Intensiv-Stationen" der IT-Sicherheit heutzutage gut belegt. Nennenswerte Überschusskapazitäten werden auch heute schon mit einer „stressigen Woche" erschöpft. Glücklicherweise lässt sich zumindest das Wissen über die Immunisierung leicht vermitteln und in der Breite teilen. Anders sieht es potenziell mit der Intensiv-Behandlung von komplexen Großschäden aus: Komplexe IT-Systeme mit vielen Abhängigkeiten werden mitunter intensive Betreuung von Expertinnen erfordern, bis sie als vollständig „genesen" gelten können.

„Flattening the curve" | Die Pandemie-Strategie, vorhandene medizinische Ressourcen nicht zu überstrapazieren und Patientinnen erst nach und nach dem Schadenfall zuzuführen, steht nicht auf dem Programm: Der Zeitraum zwischen ersten Schadenfällen und der Verfügbarkeit einer Immunisierung durch Update wird dafür kurz sein. Es hängt von Aggressivität und Schadenspotenzial der Schadsoftware ab, wie positiv oder negativ dieser Umstand zu bewerten ist.

„Long Covid" | Spätfolgen und Langzeitschäden gehören zurzeit zu den großen Unwägbarkeiten der SARS-CoV-2-Pandemie. Bei einem katastrophalen Hacking-Schaden sind auch diese in vielfältiger Form nicht auszuschließen – übliche und korrekt behandelte Hacking-Schäden entwickeln jedoch selten einen „long tail" – das risiko steigt jedoch mit unqualifizierter oder unsauberer „Behandlung", wie sie im Fall von akuter Überlastung der Behandelnden durchaus möglich ist.

Impfgegner | Auch im Bereich der IT-Sicherheit sind esoterische Ausreden verbreitet, um auf notwendige Schutzmaßnahmen zu verzichten. Diese lassen sich derzeit schön bei den Exchange-Schwachstellen beobachten, für die Microsoft Anfang März 2021 verspätet Security-Updates bereitstellte. Eine größere Anzahl von Exchange-Servern war zu diesem Zeitpunkt schon kompromittiert. Trotzdem finden sich auch heute noch Exchange-Server, deren Betreiber sie noch nicht in den Genuss der kritischen Updates haben kommen lassen. Vermutlich feiert die halbe Hacking-Unterwelt auf diesem System inzwischen virtuelle Corona-Parties.



Risikofaktoren | Hier liegt der größte Unterschied zwischen Pandemie und IT-Sicherheit – aber auch die größte Chance: Während bei Covid-19 die Betroffenen kaum direkten Einfluss auf das Risiko eines schweren Verlaufs haben, können Menschen und Organisationen ihre Resilienz gegen Cyberangriffe mit relativ geringem Aufwand stärken. Moderate Investitionen in Backup-Konzepte machen im Schadenfall den Unterschied zwischen kurzer Störung und Ruin. Unsere größte Chance besteht daher in der Vorsorge: Auch die Cyber-Pandemie bedroht zuerst die „Alten und Schwachen".

Fazit

Ein sich exponentiell verbreitendes Großschadenereignis in Bereich der IT kann schnell katastrophale Folgen haben. Unsere größte Chance besteht in der Vorsorge und der Verringerung unserer Risiko-Faktoren: Auch die Cyber-Pandemie wird die „Alten und Schwachen" zuerst bedrohen. Glücklicherweise können wir unsere Rolle selbst bestimmen.

Linus Neumann
ist Berater für IT-Sicherheit und einer der bekanntesten Hacker Deutschlands. Regelmäßig tritt der Diplom-Psychologe als Sachverständiger für IT-Sicherheit im Deutschen Bundestag auf, mit dem Podcast „Logbuch: Netzpolitik" erreicht er wöchentlich Zehntausende.



Achtung! Dringender Sicherheitshinweis

Kaum ein Tag vergeht ohne großangelegte Cyberattacken – dabei greifen Hacker nicht immer gezielt an, sondern suchen vor allem nach leichten Opfern. Wenn Sie nicht dazugehören wollen, sollten Sie mindestens diese drei Tipps beherzigen.

1. Schützen Sie die Zugänge zu Ihren IT-Systemen!

Ihr Passwort ist 12345? Qwertz? Passwort? Der Name Ihres Mannes? Das ist nicht gut, denn Passwörter sollen nicht leicht zu merken, sondern schwer zu knacken sein. Machen Sie es Hackern also nicht zu leicht. Am besten stellen Sie Ihre Computer-Systeme so ein, dass sie zu einfache Passwörter gar nicht erst akzeptieren oder einen zweiten Faktor zur Legitimation verlangen.

Doppelt hält besser

Schützen Sie Ihre IT-Systeme mit einer Zwei-Faktor-Authentifizierung?

Ja *Nein*

Quelle: Forsa



71 % verlassen sich auf ein Passwort

Drei Tipps für sichere Passwörter

1. Denken Sie sich laaaaaaange Passwörter aus
Sonderzeichen und Großbuchstaben helfen nur bedingt weiter, ebenso das ständige Wechseln von Passwörtern. Wichtiger ist die Länge. Hacker „raten" Passwörter in der Regel nicht, sondern probieren in kurzer Zeit große Mengen möglicher Kombinationen aus. Je länger das Passwort ist, desto länger braucht auch der Computer.

2. Verwenden Sie einen Passwort-Manager
Sie und Ihre Mitarbeiter können und wollen sich die vielen langen und komplizierten Passwörter nicht merken? Dann fangen Sie auf keinen Fall an, immer das gleiche oder nur ein leicht abgewandeltes Passwort einzugeben. Das macht es Hackern zu einfach. Die bessere Alternative sind Passwort-Manager. Sie generieren und verwalten starke (=lange) Passwörter, die Sie sich nicht merken müssen; das übernimmt der Manager.

3. Nutzen Sie die Zwei-Faktor-Authentifizierung
Auch wenn es etwas komplizierter ist, sollten Sie eine Zwei-Faktor-Authentifizierung in Betracht ziehen. Dann bekommen Sie nach der Eingabe Ihres Passwortes zum Beispiel noch einen Code auf Ihr Smartphone geschickt. Alternativ bekommt jeder Mitarbeiter eine Chipkarte, mit der er sich identifizieren kann. Mit dem Passwort allein können Hacker dann nichts mehr anfangen.

2. Sichern Sie Ihre Daten richtig!

Ein Backup schützt Sie vor dem Verlust Ihrer Daten, wenn Sie keinen Zugriff mehr auf Ihre Systeme haben, etwa nach einem Brand oder einem Diebstahl. Doch dafür dürfen Sie die Kopien nicht in der Nähe der laufenden Systeme aufbewahren. Noch wichtiger: Stellen Sie durch regelmäßige Testläufe sicher, dass Ihr Backup auch wirklich funktioniert. Der Ernstfall ist der schlechteste Zeitpunkt um festzustellen, dass Ihre Sicherungskopie fehlerhaft ist.

Je öfter, desto besser

Erstellen Sie mindestens wöchentlich eine Sicherungskopie Ihrer Daten?



Quelle: Forsa

19 % können aktuelle Daten nicht wiederherstellen

So sichern Sie Ihre Daten richtig

Was? Vom Smartphone bis zum Desktop-Rechner sollten alle Geräte gesichert werden. Kritische Daten sollten besser mehrfach gesichert werden.
Wie oft? So oft und so regelmäßig wie möglich. Stellen Sie am besten mit einem automatisierten Zeitplan sicher, dass keine Lücken entstehen.
Wohin? Speichern Sie das Backup auf jeden Fall isoliert vom Hauptsystem, also auf einer externen Festplatte, einem Netzwerkspeicher oder in einer Cloud. Kritische Daten sollten auf mindestens zwei unterschiedlichen Speichermedien liegen, von denen eines außerhalb Ihres Unternehmens liegt (z. B. in der Cloud).
Wie aufbewahren? Achten Sie darauf, dass Ihr Backup nicht mit Ihrem Hauptsystem verbunden ist – weder über Kabel noch über das WLAN.
Was noch? Testen Sie regelmäßig, ob sich die Daten Ihrer Backups im Ernstfall auch wirklich wiederherstellen lassen.

3. Halten Sie Ihren Schutz immer aktuell!

Software-Anbieter veröffentlichen für ihre Produkte regelmäßig Sicherheitsupdates. Das bedeutet auch: In der bisher benutzten Version gibt es Sicherheitslücken – und die sind Cyberkriminellen auch bekannt. Schließen Sie diese Lücken sofort und spielen Sie sämtliche Updates am besten automatisch in ihre Systeme ein. Software, die keine Updates mehr erhält, hat auf Ihren Rechnern schon gar nichts mehr zu suchen – und dennoch sind in vier Prozent der Unternehmen noch Programme im Einsatz, die teilweise schon seit Jahren veraltet sind.

Updates in der Warteschleife

Werden Sicherheitsupdates automatisch und zeitnah eingespielt?



Quelle: Forsa

13 % lassen sich mit Sicherheitsupdates auch mal Zeit

Wie gut ist Ihre IT-Sicherheit?

Absolute Sicherheit im Netz gibt es nicht. Doch Widerstand gegen Cyberkriminelle ist möglich. Wer die Gefahren realistisch einschätzt und bei seiner IT-Sicherheit die folgenden Grundlagen beachtet, ist gegen viele Angriffe wirksam geschützt und kann die wirtschaftlichen Folgen eines erfolgreichen Angriffs eindämmen. Die Forsa-Umfrage des GDV zeigt aber: An vielen Stellen klaffen Lücken in der IT-Sicherheit (Angaben in Prozent).

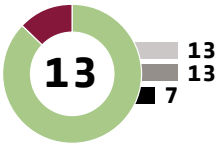
Der **Cyber-Sicherheits-check des GDV** unter www.gdv.de/cybercheck stellt Ihnen die wichtigsten Fragen rund um Ihre IT-Sicherheit. So finden Sie schnell heraus, wie sicher Ihre Systeme sind, wo Sie Schwachstellen haben und wie Sie diese schließen können. Ob Sie die zehn grundlegenden Anforderungen erfüllen, können Sie gleich hier beantworten. Wie gut Sie dabei abgeschnitten haben und ob es andere besser machen, können Sie auf Seite 22 herausfinden.

Anteil der Unternehmen, die den Schutz nicht erfüllen; nach Unternehmensgröße:

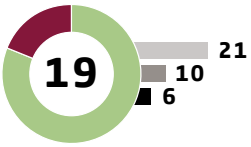
Kleinstunternehmen *Kleine Unternehmen* *Mittlere Unternehmen*

Selbsttest

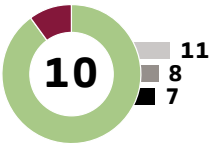
1. **Sicherheitsupdates automatisch und zeitnah einspielen und alle Systeme auf dem aktuellen Stand halten**
   Die meiste Software erhält regelmäßig Updates. Sie dienen oft dazu, bekannt gewordene Sicherheitslücken zu schließen. Das Installieren der Updates schützt die Systeme vor Angreifern.



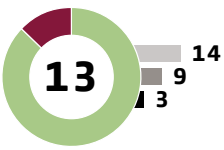
2. **Mindestens einmal wöchentlich Sicherungskopien machen**
   Daten und digitale Systeme können gezielt angegriffen, versehentlich gelöscht oder durch Hardware zerstört werden. Deshalb ist es dringend nötig, die vorhandenen Daten regelmäßig zu sichern. Grundsätzlich gilt: Je öfter Sie Ihre Daten sichern, desto besser.



3. **Administratoren-Rechte nur an Administratoren vergeben**
   Wer mit Administrator-Rechten an einem IT-System arbeitet, kann dabei verheerende Schäden anrichten. Deshalb ist es ratsam, solche Rechte nur sehr sparsam zu vergeben und nur dann zu nutzen, wenn sie für die aktuelle Aufgabe wirklich nötig sind.

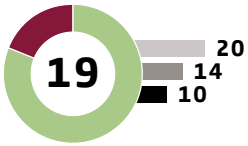


4. **Alle Systeme, die über das Internet erreichbar oder im mobilen Einsatz sind, zusätzlich schützen**
   Mobile Geräte können leicht verloren gehen oder gestohlen werden. Sind die darauf gespeicherten Daten nicht verschlüsselt, können sie vollständig ausgelesen werden – selbst wenn sie mit einem Passwort geschützt sind. Server sind über das Internet ständig erreichbar und daher für Angriffe besonders beliebte Ziele. Sie sollten am besten mit einer 2-Faktor-Authentifizierung gesichert werden.



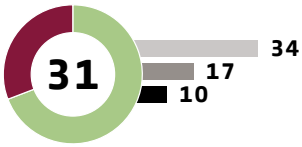
5. Manipulationen und unberechtigten Zugriff auf Sicherungskopien verhindern

Backups sind die Rückversicherung für den Fall gelöschter oder manipulierter Daten. Gesonderte Authentifizierungsstufen und ein entsprechendes Rechtemanagement sollten daher die versehentliche oder absichtliche Manipulation gesicherter Daten ausschließen.



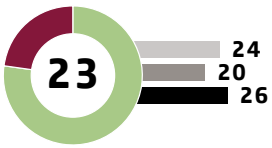
6. Alle Systeme mit einem Schutz gegen Schadsoftware ausstatten und diesen automatisch aktualisieren lassen

Viren, Trojaner oder Ransomware: Die meisten Schäden entstehen durch das unbeabsichtigte Infizieren der Systeme mit so genannter Schadsoftware. Auch wenn Virenscanner hier keinen hundertprozentigen Schutz bieten, sollte mindestens einer auf den Systemen installiert sein und regelmäßig aktualisiert werden.



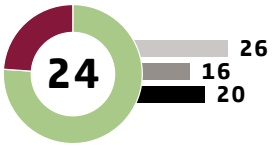
7. Sicherungskopien physisch vom gesicherten System trennen

Datensicherungen können auch dann vor dem Verlust Ihrer Daten schützen, wenn die Systeme gestohlen oder durch einen Brand zerstört wurden. Deshalb ist es ratsam, die Backups nicht in der Nähe der laufenden Systeme aufzubewahren, sondern mindestens in anderen Brandabschnitten, besser jedoch an einem ganz anderen Ort.



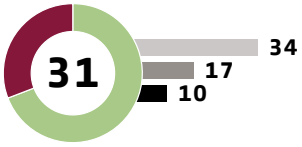
8. Mindestanforderungen für Passwörter (z. B. Länge, Sonderzeichen) verlangen und technisch erzwingen

Gerade wenn Passwörter das einzige Authentifizierungsmittel sind, sollte eine geeignete Passwortstärke technisch erzwungen werden. Andernfalls sind IT-Systeme schon durch einfachste Angriffe gefährdet.



9. Jeden Nutzer mit eigener Zugangskennung und individuellem Passwort ausstatten

Ohne benutzerindividuelle Kennungen ist es nicht möglich, den Zugang zu Systemen zu sichern. Die individuelle Authentifizierung ist auch deswegen wichtig, weil nur so später nachvollzogen werden kann, wer das System wann verwendet hat.



10. Wiederherstellen der Daten aus der Sicherungskopie regelmäßig testen

Regelmäßige Testläufe stellen sicher, dass bei der Sicherungskopie keine Datenquelle fehlt und die Wiederherstellung tatsächlich funktioniert. Der Notfall ist der schlechteste Zeitpunkt um festzustellen, dass eine Sicherungskopie fehlerhaft ist.



Ergebnis: Ich erfülle _____ von 10 Maßnahmen

So gut ist Ihre IT-Sicherheit – und so gut sind die anderen

Die Schutzmaßnahmen auf den Seiten 20/21 sind nicht der Goldstandard und auch kein Garant für volle Sicherheit, sondern nur die Basis – doch schon hier haben die meisten Unternehmen Lücken. Wie viele der zehn Schutzmaßnahmen haben Sie umgesetzt?



10
Herzlichen Glückwunsch! Durch das hohe Niveau Ihrer IT-Sicherheit halten Sie das Risiko einer erfolgreichen Cyberattacke gering.



8–9
Das Niveau Ihrer IT-Sicherheit ist leider noch nicht perfekt – beachten Sie unsere Hinweise und schließen sie die noch vorhandenen Sicherheitslücken.



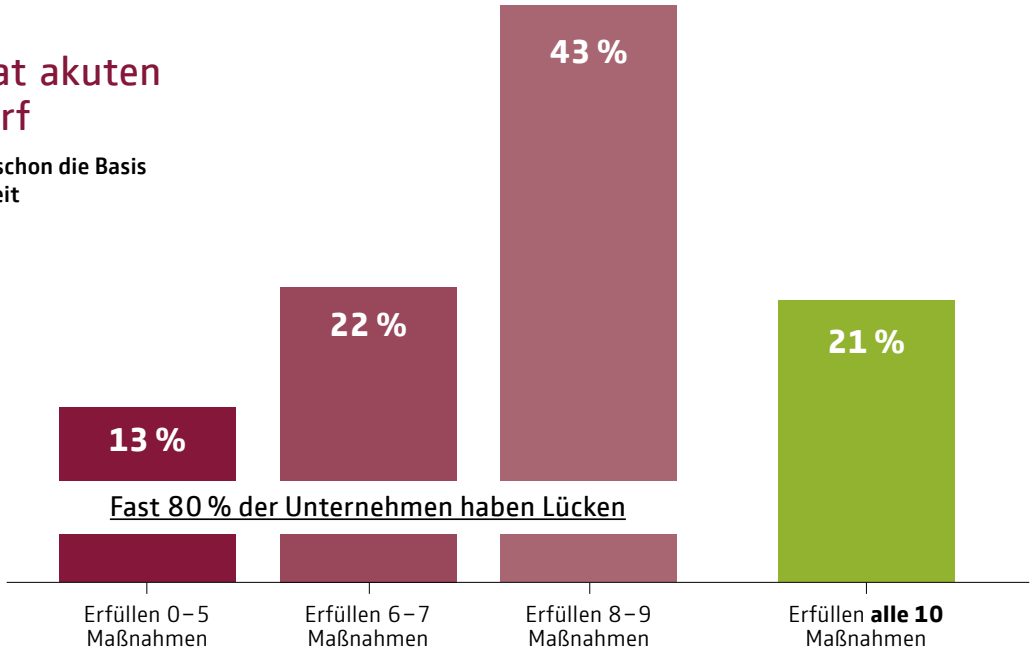
6–7
Über gute Ansätze kommt Ihre IT-Sicherheit leider nicht hinaus. Machen Sie es Cyberkriminellen nicht zu einfach und kümmern Sie sich möglichst schnell darum, Ihre Sicherheitslücken zu schließen.



0–5
Achtung, Ihre IT-Sicherheit weist deutliche Schwächen auf und kann Ihr Unternehmen zur leichten Beute für Hacker machen. Beachten Sie unsere Hinweise und holen Sie sich am besten professionelle Hilfe, um Ihren Schutz gegen Cyberrisiken schnell zu verbessern.

Die Mehrheit hat akuten Handlungsbedarf

Vielen Unternehmen fehlt schon die Basis für umfassende IT-Sicherheit



Das leistet eine Cyberversicherung



Der Gesamtverband der Deutschen Versicherungswirtschaft hat unverbindliche Musterbedingungen für eine Cyberversicherung entwickelt. Sie sind speziell auf die Bedürfnisse von kleinen und mittleren Unternehmen zugeschnitten und richten sich sowohl an Arztpraxen oder Anwaltskanzleien als auch an Handwerksbetriebe und Industriezulieferer. Die Versicherung übernimmt nicht nur die Kosten durch Datendiebstähle, Betriebsunterbrechungen und für den Schadenersatz an Dritte, sondern steht den Kunden im Ernstfall mit einem umfangreichen Service-Angebot zur Seite: Nach einem erfolgreichen Angriff schickt und bezahlt die Versicherung Experten für IT-Forensik, vermittelt spezialisierte Anwälte und Krisenkommunikatoren. So hilft sie, den Schaden für das betroffene Unternehmen so gering wie möglich zu halten.

	Schaden	Leistung
Eigenschäden	Wirtschaftliche Schäden durch Betriebsunterbrechung.	Zahlung eines Tagessatzes.
	Kosten der Datenwiederherstellung und System-Rekonstruktion.	Übernahme der Kosten.
Drittschäden	Schadenersatzforderungen von Kunden wegen Datenmissbrauch und/oder Lieferverzug.	Entschädigung und Abwehr unberechtigter Forderungen.
Service-Leistungen	IT-Forensik-Experten zur Analyse, Beweissicherung und Schadenbegrenzung.	Jeweils Vermittlung und Kostenübernahme.
	Anwälte für IT- und Datenschutzrecht zur Beratung.	
	PR-Spezialisten für Krisenkommunikation zur Eindämmung des Imageschadens.	

Impressum

Herausgeber:
Gesamtverband der Deutschen Versicherungswirtschaft e. V.
Wilhelmstraße 43 / 43 G
10117 Berlin
Tel. +49 30 2020-5000
berlin@gdv.de, www.gdv.de

V.i.S.d.P.: Jörn Paterak

Redaktion: Volker Kühn, Christian Siemens

Bildnachweis:
S. 1: shutterstock/Peshkova; S. 4/5: shutterstock/Chinnapong; S. 6 l.: shutterstock/Maria Svetlychnaja; S. 6 r.: shutterstock/TippaPatt; S. 8 o.: shutterstock/solarseven; S. 8 u.: shutterstock/vectorfusionart S. 12/13: iStock/CatEye-Perspective; S. 14/15: picture alliance/abaca/Roses Nicolas; S. 17: Urban Illustration; S. 18: shutterstock/13_Phunkod

CYBER@SICHER

Eine Initiative der deutschen Versicherer.

Gothaer

Gothaer Allgemeine Versicherung AG
Gothaer Allee 1 . 50969 Köln
Telefon 0221 303-00
Telefax 0221 308 103
www.gothaer.de

117258- 12.2021