Gesamtverband der Deutschen Versicherungswirtschaft e. V.

CYBER SICHER

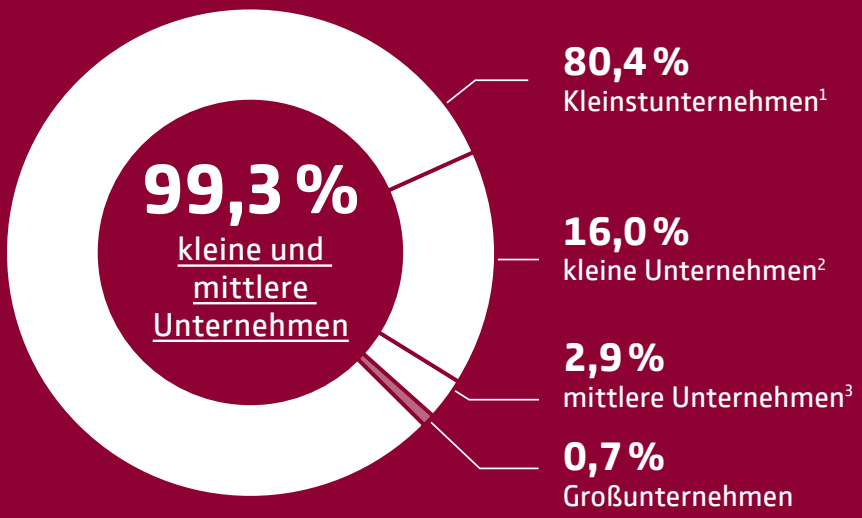
Eine Initiative der deutschen Versicherer.

Ergebnisse einer Forsa-Befragung
Frühjahr 2019

Cyberrisiken im Mittelstand

GDV
DIE DEUTSCHEN VERSICHERER

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 2016

Über die Umfrage

„Cyberrisiken im Mittelstand 2019" – Der GDV hat die Forsa Politik- und Sozialforschung GmbH mit einer repräsentativen Befragung von 300 Entscheidern in kleinen und mittleren Unternehmen beauftragt. Die Befragung wurde so angelegt, dass repräsentative Aussagen zu Kleinstunternehmen, kleinen Unternehmen und mittleren Unternehmen getroffen werden können. Die Interviews fanden zwischen dem 11. März und dem 5. April 2019 statt.

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

Ergebnisse einer Forsa-Befragung im Frühjahr 2019

Wenn nichts mehr geht

Erfolgreiche Cyberattacken können Unternehmen existenziell gefährden – denn in den meisten Fällen legen sie den kompletten Betrieb lahm. Dann beginnt der Kampf gegen die Zeit.

Wenn Gerhard Klein an den Oktober 2018 denkt, fällt ihm vor allem ein Wort ein: „Desaster." In seiner Saarbrücker Druckerei geht an diesem Herbstmorgen nichts mehr. Und das wird auch noch für einige Tage so sein. Die Computer streiken. Programme lassen sich nicht öffnen, das Mailsystem reagiert nicht, die Telefonanlage ist tot. Über eine bis dato nicht bekannte Lücke in der Firewall haben sich Cyberkriminelle Zugang verschafft und sämtliche Daten auf den lokalen Festplatten verschlüsselt.

Die Druckerei Braun und Klein stellt unter anderem Werbe- und Angebotsplakate für große Einzelhändler her, termingenaue Auslieferung ist deshalb besonders wichtig. Zu allem Überfluss ist Monatsanfang und die Lohnabrechnung fällig. Geschäftsführer Klein ist schnell klar: „Das ist ein Wettlauf gegen die Zeit." Auftrags- und Rechnungserfassung sind unmöglich. Wenn der völlige Stillstand nicht wenige Tage, sondern zwei bis drei Wochen andauert, „ist die Firma platt".

Wenig tröstlich für den Unternehmer, dass er mit seinen Sorgen nicht allein ist. Die deutsche Wirtschaft leidet flächendeckend unter Hackerangriffen. Längst sind nicht mehr nur große Konzerne im Visier der Kriminellen – auch der Mittelstand wird täglich angegriffen. Es trifft Autozulieferer und Maschinenbauer, Hotels und Restaurants, Ärzte und Apotheker, Einzelhändler,

„Die sagen: Was soll mir schon passieren, wenn meine Daten abhandenkommen?"

Arne Schönbohm, Präsident des Bundesamtes für Sicherheit in der Informationstechnik, über die fahrlässige Haltung vieler Unternehmen

Handwerker, Dienstleister. Jedes vierte mittelständische Unternehmen in Deutschland war bereits Opfer mindestens eines erfolgreichen Cyberangriffs, wie eine aktuelle Forsa-Umfrage im Auftrag des GDV zeigt.

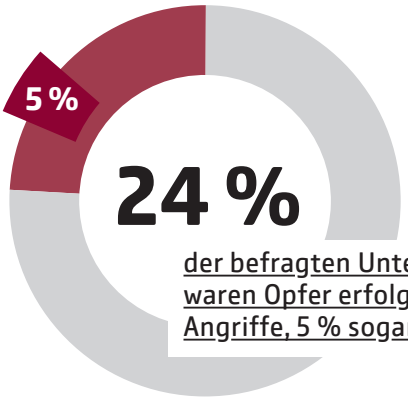
Vielen geht es dann wie der Druckerei von Gerhard Klein. Plötzlich geht nichts mehr, kommt der gesamte Geschäftsbetrieb zum Erliegen. In der Forsa-Umfrage berichten mehr als die Hälfte der betroffenen Unternehmen (59 Prozent) über Betriebsausfälle. Sie sind zusammen mit den Ausgaben für die Wiederherstellung der Daten und IT-Systeme die häufigsten Folgen einer Cyberattacke – und stellen für die Opfer das größte unternehmerische Risiko eines erfolgreichen Angriffs dar.

Als beispielsweise im IT-System des Münchner Maschinenbauers Krauss Maffei im November 2018 ein Trojaner aktiv wird, ist auch die Produktion betroffen. Und selbst zwei Wochen später sind noch nicht alle Systeme wieder auf 100 Prozent. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) beobachtet steigende Fallzahlen bei deutschen Unternehmen. Besonders breit angelegte Spam-Kampagnen wie Emotet seien auf dem Vormarsch. Mit deren Hilfe gelinge es Kriminellen in Firmennetzwerke einzudringen und diese nach vielversprechenden Zielen zu durchsuchen. „Wir erleben derzeit die massenhafte Verbreitung von raffinierten Angriffsmethoden durch die Organisierte Kriminalität, die bis vor einigen Monaten nachrichtendienstlichen Akteuren vorbehalten waren“, sagt Behördenchef Arne Schönbohm.

Keine besonders beruhigenden Aussichten – zumal sich Kriminellen bei fortschreitender Digitalisierung eher mehr als weniger Angriffspunkte in Unternehmen bieten. In Hotels ist es das Buchungssystem, im Handel die Kasse, bei Ärzten und Apotheken sind es die Rechner mit den Patientendaten, in der Industrie die vernetzten Produktionssysteme. Funktioniert die IT nicht mehr, liegen die meisten Betriebe schnell komplett lahm. In der Forsa-Umfrage des GDV sind ganze elf Prozent der Unternehmen der Ansicht, dass sie auch ohne IT-Systeme problemlos weiterarbeiten könnten, zwei Drittel wären deutlich eingeschränkt. Doch obwohl die Abhängigkeit so groß ist, gehen viele Firmen mit der Gefahr noch eher hemdsärmlig um. Auch BSI-Chef Schönbohm beobachtet eine fahrlässige Haltung von Unternehmen. „Die sagen: Was soll mir schon passieren, wenn meine Daten abhandenkommen?“. Gerade bei kleinen und mittelständischen Unternehmen ist das Bewusstsein für Cybersicherheit eher gering ausgeprägt. Vor allem die Gefahr für das eigene Unternehmen sehen viele nicht, wie die Forsa-Studie für den GDV zeigt. Während beinahe drei Viertel (72 Prozent) der Mittelständler ein hohes Risiko von →

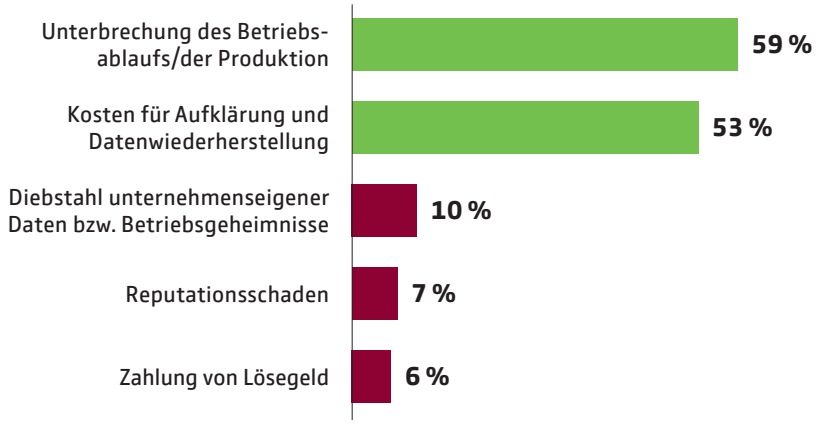
Jedes vierte Unternehmen bereits betroffen

Wurde Ihr Unternehmen durch Cyberangriffe geschädigt?



Die Schäden

Welche Schäden sind im Unternehmen durch den Cyberangriff entstanden?



→ Cyberkriminalität erkennen, bestätigt lediglich ein Drittel (34 Prozent) diese Gefahr auch für den eigenen Betrieb.

Die Folgen dieser Sorglosigkeit kennt Michael Wiesner genau. Als White-Hat-Hacker prüft er die IT-Sicherheit von Firmen. Und staunt nicht schlecht, als er im Auftrag des GDV 25 Arztpraxen untersucht: In 22 der Praxen werden sehr einfache oder gleich gar keine Passwörter verwendet. „Das beliebteste Passwort in einer Praxis ist ‚Praxis', der beliebteste Benutzername ist auch ‚Praxis', gefolgt von ‚Behandlung' oder dem Namen des Arztes", berichtet Wiesner. Auch bei seinen Aufträgen im produzierenden Gewerbe findet er immer wieder große Sicherheitslücken: „Was in der Industrie früher analog gesteuert wurde, wird heute über das Internet gemacht. Aber viel zu oft geht bei den Themen Industrie 4.0 und Internet of Things Funktion und Machbarkeit vor Sicherheit", so Wiesner.

Mit ihrer laxen Einstellung zur IT-Sicherheit sind Firmen vor allem eines: einfache und lohnenswerte Ziele. BSI-Chef Schönbohm setzt darauf, dass sich mit der fortschreitenden Digitalisierung nach und nach ein anderes Verständnis für die Cybersicherheit entwickelt. Noch sind es aber vor allem externe Faktoren, die Unternehmen dazu bringen, sich abzusichern. So wie die europäische Datenschutzgrundverordnung (DSGVO), die seit Mai 2018 scharfgeschaltet ist. Sie verlangt von Betrieben, egal welcher Größe, eine umfassende Datensicherheit. Wer sich nicht an die Spielregeln hält – zum Beispiel indem er Kunden und Datenschutzbehörden nicht mitteilt, wenn es ein Datenleck gibt – muss mit empfindlichen Strafen rechnen. Bei schweren Verstößen, etwa der Nutzung persönlicher Daten ohne ausreichende Einwilligung der Betroffenen, drohen Geldstrafen bis maximal 20 Millionen Euro.

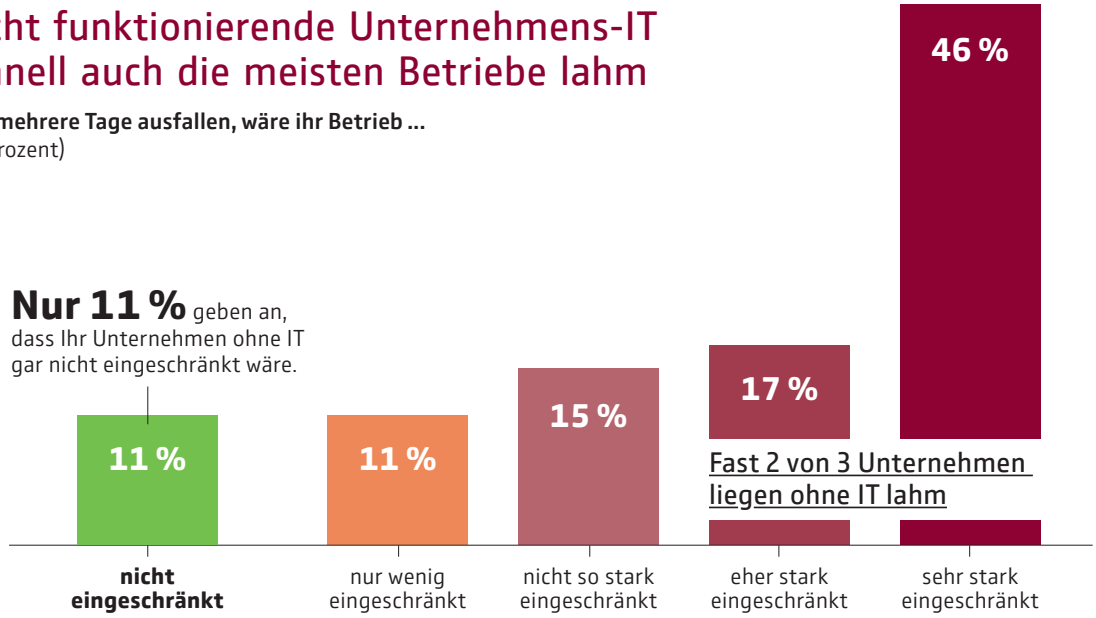
„Das beliebteste Passwort in einer Praxis ist ‚Praxis', der beliebteste Benutzername ist auch ‚Praxis', gefolgt von ‚Behandlung' oder dem Namen des Arztes."

Michael Wiesner, White-Hat-Hacker

Spätestens Beispiele wie das der Chatplattform mit dem sympathischen Namen Knuddels dürften seither so manchen Unternehmer aufgerüttelt haben: Hier knacken Hacker im vergangenen Jahr die Server des sozialen Netzwerks. Die E-Mail-Adressen und Passwörter von mehr als 300.000 Knuddels-Nutzern tauchen kurz darauf im Netz auf. Zum Reputationsschaden, den ein solches Datenleck ohne Zweifel verursacht, kommt von den Datenschützern ein Bußgeldbescheid über 20.000 Euro hinzu, der den Betreibern noch vor dem Jahreswechsel auf den Schreibtisch flattert. Um nicht in dieselbe Situation zu geraten, haben viele Unternehmen die →

Eine nicht funktionierende Unternehmens-IT legt schnell auch die meisten Betriebe lahm

Würde die IT mehrere Tage ausfallen, wäre ihr Betrieb …
(Angaben in Prozent)



So begrenzen Sie die Folgen eines erfolgreichen Cyberangriffs

Die regelmäßige und richtige Sicherung Ihrer Daten (siehe Seite 14) ist die Basis jeder effektiven Krisenreaktion nach einem Cyberangriff. Sie allein reicht aber bei weitem nicht aus. Wie in jeder Krisensituation gilt auch hier: Handeln Sie schnell, aber bewahren Sie trotzdem einen kühlen Kopf. Das gelingt am besten, wenn Sie und Ihr Unternehmen gut vorbereitet sind.

1. Machen Sie einen Notfallplan
Panikreaktionen und überstürzte Handlungen führen zu Fehlern. Arbeiten Sie mit den IT-Verantwortlichen oder Ihrem IT-Dienstleister daher Notfallpläne für verschiedene Angriffs-Szenarien aus. Legen Sie fest wer, wann und wie reagiert und werden Sie dabei so konkret wie möglich: Sollten Sie die betroffenen IT-Systeme ausschalten? Oder besser laufen lassen und vom Netzwerk trennen? Ist Ihr Dienstleister im Ernstfall auch nachts und am Wochenende einsatzbereit? Unter welcher Nummer ist er dann erreichbar? Wo liegen die Datensicherungen und wann können diese sicher wieder auf die Systeme aufgespielt werden? Wer informiert betroffene Kunden, Vertragspartner und Behörden? Bis wann und in welcher Form? Denken Sie außerdem darüber nach, was in Ihrem Betrieb ohne IT noch möglich ist und implementieren Sie Alternativen, mit denen Sie Ihren Geschäftsbetrieb auch bei einem IT-Ausfall so gut und so lange wie möglich aufrecht erhalten können.

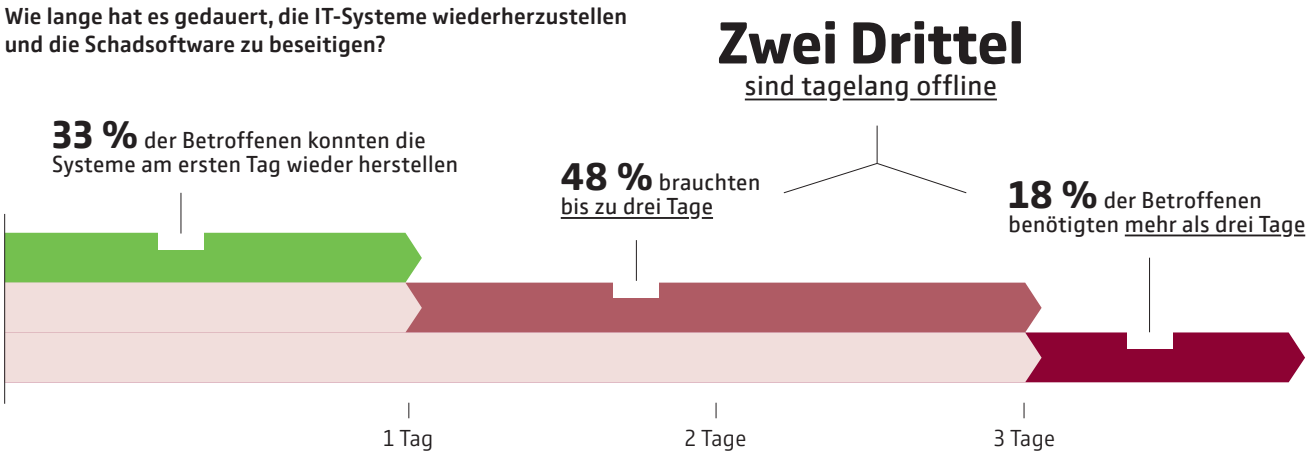
2. Halten Sie alles schriftlich fest
Reden Sie nicht nur, sondern arbeiten Sie Ihre Notfallpläne, die Verantwortlichkeiten und alle wichtigen Kontaktdaten schriftlich aus – und drucken Sie den Plan dann auch wirklich aus! Die digitale Fassung nützt Ihnen nach einem Cyberangriff herzlich wenig. Wenn Sie mit einem IT-Dienstleister zusammenarbeiten, lassen Sie sich dessen Leistungen und Reaktionszeiten vertraglich zusichern.

3. Üben, üben, üben
Machen Sie den Notfallplan allen Mitarbeitern bekannt und stellen Sie sicher, dass jeder seine Rolle und Aufgabe verstanden hat und der Plan auch wirklich funktioniert. Das finden Sie am besten heraus, indem Sie den Notfall regelmäßig simulieren. So können Sie Ihr Notfallkonzept weiter optimieren, gleichzeitig sensibilisieren Sie Ihre Mitarbeiter für die Gefahren aus dem Cyberspace.

4. Schalten Sie die Polizei ein und erstatten Sie Strafanzeige
In vielen Bundesländern haben Polizei und Justiz spezialisierte Cybercrime-Dienststellen geschaffen. Sie helfen Ihnen, Beweise zu sichern, kennen im Zweifel ähnliche Fälle und können Ihnen konkrete Empfehlungen geben. Darüber hinaus lässt sich das Geschäftsmodell der Cyberkriminellen langfristig nur dann wirksam bekämpfen, wenn möglichst viele Täter ermittelt und bestraft werden.

Die IT-Systeme wieder zum Laufen zu bringen, kann dauern …

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



→ DSGVO-Vorschriften für ein umfassendes Sicherheitsupdate genutzt. Nach den Daten der Forsa-Umfrage rüstete jedes zweite Unternehmen (50 Prozent) anlässlich der EU-Verordnung auch die eigene IT-Sicherheit auf.

Auch in der Druckerei von Gerhard Klein war das Risiko alles andere als unbekannt: „Wir haben sehr genau gewusst, welche Gefahren existieren, und hatten Maßnahmen ergriffen, um einen Angriff zu verhindern." Insofern hat Klein sich und seinen Mitarbeitern auch nichts vorzuwerfen. „Bei uns hat keiner einen Fehler gemacht, sondern wir sind von Verbrechern attackiert worden."

Wie in den meisten Fällen hatten es die Kriminellen beim Angriff auf Kleins Druckerei auf schnelles Geld abgesehen: Von außen hinzugerufene IT-Forensiker entdecken in den Tiefen des Systems einen Erpresserbrief. Die Forderung der Kriminellen scheint zunächst überschaubar: rund 4500 Euro in Bitcoin. Nachdem er die Erpresser um 1000 Euro heruntergehandelt hat, entschließt sich Klein zu zahlen. Nicht ohne einen Beweis zu verlangen, dass diese die Verschlüsselung wirklich aufheben können. Und tatsächlich: Das Mailsystem mit dem gesamten Archiv bekommen sie wieder ans Laufen. Mehr aber auch nicht – für die Entschlüsselung weiterer Daten fordern die Erpresser nun ein Vielfaches an Lösegeld.

Klein bricht den Kontakt ab. In mühevoller Handarbeit setzen Mitarbeiter und externe IT-Spezialisten die Systeme in den nächsten Tagen und Wochen wieder auf. Rund 70.000 Euro habe die Attacke das Unternehmen allein finanziell gekostet, resümiert Klein. Keine untypische Schadensbilanz. Bei einem Maschinenbauer mit einem Jahresumsatz von 40 Millionen Euro schlägt bereits eine Woche Betriebsunterbrechung – etwa durch einen Verschlüsselungs-Trojaner – mit rund 45.000 Euro zu Buche. Hinzu kommen Kosten für IT-Forensiker und Datenwiederherstellung. „Das ist eine umfangreiche Arbeit, für die man bis zu 20.000 Euro veranschlagen kann", weiß Gert Baumeister, Vorsitzender der Projektgruppe Cyberversicherung im GDV. Sind dann noch personenbezogene Daten wie etwa die Lohnabrechnung betroffen, drohen auch Ansprüche nach der DSGVO. Da kann es kaum verwundern, dass die Schäden durch Cyberkriminalität für die deutsche Wirtschaft bei mehr als 20 Milliarden Euro jährlich liegen. Das schätzen jedenfalls das Bundesamt für Verfassungsschutz und Bitkom in einer gemeinsamen Studie.

70.000 Euro
kostete Gerhard Klein die Attacke auf seine Druckerei

Angesichts solcher Zahlen und des durchaus vorhandenen Bewusstseins für die Gefahren durch Cyberattacken mutet es paradox an, dass gut die Hälfte (57 Prozent) der kleinen und mittelständischen Betriebe annimmt, ihr eigenes Unternehmen sei für Kriminelle nicht interessant. „Kleine Firmen denken immer, sie sind kein Ziel für Hackerangriffe", weiß auch Unternehmer Klein. „Das ist falsch." Er führt den Widerspruch darauf zurück, dass das Thema Cyberkriminalität für viele Firmenchefs noch immer zu abstrakt sei. „Warum sollten Freaks, die in Nordkorea, Rumänien oder Russland sitzen, meine Firma angreifen?!"

„Kleine Firmen denken immer, sie sind kein Ziel für Hackerangriffe. Das ist falsch."

Gerhard Klein, Unternehmer

Tun sie aber. Und damit es auch dem Letzten klar wird, gibt es für Klein nur einen Weg: Der Weckruf muss aus der Wirtschaft selbst kommen. Klein und seine Kollegen gehen in die Offensive. Die Geschichte vom Cyberangriff landet auf dem Firmenblog und in den Nachrichten. Der Schaden durch den erfolgreichen Cyberangriff soll kein Tabu sein. „Unternehmen sollten klar kommunizieren, wenn sie angegriffen werden", appelliert er. Eine solche Strategie – würde sie denn von vielen gewählt – würde Cyberkriminellen auf Dauer das Leben schwermachen.

Ein halbes Jahr nach der Attacke weiß Klein: Seine Strategie war richtig. Kunden seien nicht davongelaufen und auch von anderen Unternehmen habe es viel positives Feedback gegeben. „Wir haben uns erholt – gedanklich, finanziell – und schauen positiv nach vorne. Wir wissen aber auch: Der nächste Angriff kommt bestimmt." ←

Was eine Cyberattacke kosten kann – und eine Cyberversicherung deckt (🏷)

Musterszenario Diebstahl sensibler Daten:

Hacker attackieren die IT-Systeme einer Arztpraxis. Sie kopieren die Patientendaten und versprechen, gegen die Zahlung von Lösegeld auf eine Veröffentlichung der Daten zu verzichten.

Angriff

Die Arztpraxis erhält per Mail einen Erpresserbrief. Die Kriminellen behaupten, im Besitz aller Patientendaten zu sein. Als Beleg senden sie kompromittierende Daten über fünf Patienten, die tatsächlich in der betroffenen Praxis in Behandlung waren. Sie drohen damit, die Daten zu veröffentlichen, wenn der Arzt nicht bereit ist, ein hohes Lösegeld zu zahlen.

Informationen an Patienten und Behörden

Nach Rücksprache mit Polizei und Staatsanwaltschaft zahlt der Arzt kein Lösegeld. Er muss aber die Datenschutzbehörden und seine Patienten über den Verlust der sensiblen Daten informieren. Um sicher zu gehen, dass er seinen Pflichten in vollem Umfang nachkommt, holt er sich Hilfe bei einem Rechtsanwalt. Die Patienten sind nach der Information verunsichert und haben intensiven Gesprächsbedarf.

- *Informationskosten: 4.000 Euro*
- *Anwaltskosten: 2.000 Euro*

Security-Initiative

IT-Spezialisten suchen und schließen die Schwachstelle, die den Tätern Zugriff zu den Daten erlaubte. Die Systeme werden desinfiziert und gehärtet.

- *Kosten für IT-Forensik: 5.000 Euro*

Betriebsunterbrechung

Bis die Schwachstellen geschlossen und weitere Datendiebstähle verhindert sind, bleibt die Arztpraxis geschlossen. Auch die Abrechnung mit den Krankenkassen ist unmöglich.

- *Kosten für 2 Tage Betriebsunterbrechung: 5.000 Euro*

Datenmissbrauch

Die Hacker veröffentlichen die Gesundheitsdaten einiger Patienten. Die Betroffenen beauftragen Spezialisten mit der Löschung der unrechtmäßig veröffentlichten Daten und verlangen vom Arzt Schadenersatz.

- *Schadensersatz: 20.000 Euro nach Art. 82 DSGVO*

Vertrauenskrise

Nachdem die lokale Presse über den Datendiebstahl berichtet, wenden sich zahlreiche Patienten von der Praxis ab, der Patientenstamm schrumpft deutlich.

- *Krisenkommunikation: 1.000 Euro*

Der Umsatzrückgang ist nicht gedeckt

Aufarbeitung

Die Datenschutzbehörden verhängen aufgrund des Datenverlustes ein hohes Bußgeld.

Das Bußgeld ist nicht gedeckt

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: 20.000 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

Schwachstelle Mensch: Zwei Drittel der erfolgreichen Angriffe kommen per E-Mail

Das E-Mail-Postfach ist für viele Unternehmen die wichtigste digitale Schnittstelle zu Kunden und Lieferanten. Mit immer ausgefeilteren Methoden bringen Hacker ihre Opfer dazu, die elektronische Post samt Anhängen zu öffnen – und legen mit ihrer Schadsoftware nicht nur die IT-Systeme, sondern ganze Betriebe lahm.

Sie haben 10.000 Euro gewonnen! Klicken Sie hier!“ – Über derartige E-Mails werden die meisten nur müde lächeln. Falls sie es durch den Spam-Filter schaffen, werden sie ungelesen gelöscht. Dabei wird unterschätzt: Beim E-Mail-Angriff auf Unternehmen gehen Kriminelle inzwischen deutlich professioneller vor. „Social Hacking“ nennt sich die Kunst, potentielle Opfer möglichst geschickt zu manipulieren. Kriminelle geben sich mit zuvor gesammelten Daten eines Unternehmens zum Beispiel als Abteilungsleiter oder Kunde aus – und bringen den Empfänger so dazu, Schadsoftware herunterzuladen oder Passwörter herauszugeben.

Auch einfache Reize wie Neugierde helfen den Tätern ans Ziel: So wurde die renommierte amerikanische IT-Sicherheitsfirma RSA Security gehackt, indem eine infizierte Excel-Datei mit dem Namen „Stellenbesetzungsplan“ an die Mitarbeiter verschickt wurde. Für eine von ihnen klang der Inhalt derartig verlockend, dass sie die Mail sogar extra aus ihrem Spam-Ordner hervorholte und öffnete.

„Technische Hilfsmittel können den gesunden Menschenverstand und eine gewisse Skepsis nicht ersetzen.“

Peter Graß, Cyberversicherungsexperte im GDV

Für die Cyberkriminellen lohnen sich die gezielten Attacken auf die Schwachstelle Mensch: 70 Prozent aller erfolgreichen Angriffe treffen über das E-Mail-Postfach der Unternehmen ins Ziel. Nur bei rund einem Viertel der Attacken verschafften sich Hacker gezielt Zugriff auf die IT-Systeme, andere Angriffswege wie beispielsweise DDoS-Attacken spielen kaum eine Rolle.

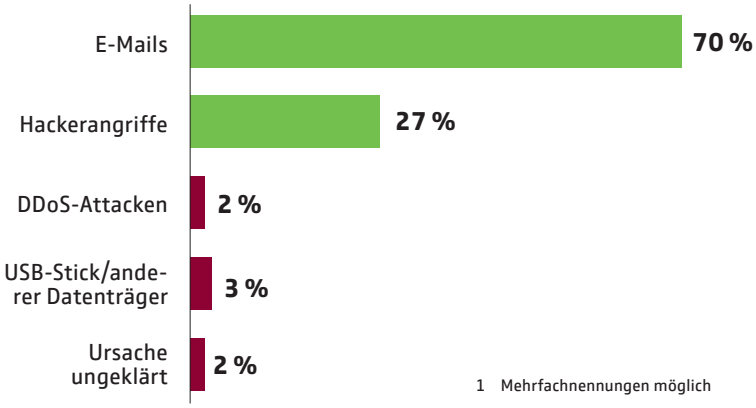
Die hohe Zahl erfolgreicher Attacken per Mail ist eine gute und eine schlechte Nachricht zugleich. Die

schlechte: In vielen Firmen gehen Chefs wie Mitarbeiter noch viel zu fahrlässig mit eingehenden E-Mails um und verlassen sich einzig und allein auf Firewall und Virenscanner. Doch die erkennen nicht jede Schadsoftware. „Die technischen Hilfsmittel können den gesunden Menschenverstand und eine gewisse Skepsis nicht ersetzen", sagt GDV-Cyberversicherungsexperte Peter Graß.

Er empfiehlt regelmäßige Schulungen und verbindliche Vorsichtsmaßnahmen für den Umgang mit E-Mails (siehe Kasten). Dann – und das ist die gute Nachricht – könnten viele Angriffe per Mail rechtzeitig erkannt und das Öffnen gefährlicher Software verhindert werden.

Die Einfallstore

Erfolgreiche Cyberangriffe erfolgten durch … [1]



1 Mehrfachnennungen möglich

So schützen Sie Ihr Unternehmen vor schädlichen E-Mails

Nur ein einziger falscher Klick auf einen verseuchten Mail-Anhang oder einen Link kann Ihre Unternehmens-IT lahmlegen. Wenn Sie Ihre Mitarbeiter regelmäßig für die Gefahren sensibilisieren und einige grundlegende Regeln für den Umgang mit E-Mails aufstellen, können Sie sich vor vielen Angriffen schützen.

1. Arbeiten Sie mit hohen Sicherheitseinstellungen
Nutzen Sie die Sicherheitseinstellungen Ihres Betriebssystems und Ihrer Software zu Ihrem Schutz. Im Office-Paket sollten zum Beispiel Makros dauerhaft deaktiviert sein und nur bei Bedarf und im Einzelfall aktiviert werden können – denn auch über diese kleinen Unterprogramme in Word-Dokumenten oder Excel-Listen kann sich Schadsoftware verbreiten.

2. Halten Sie Virenscanner und Firewall immer auf dem neuesten Stand
Die meisten schädlichen E-Mails können Sie mit einem Virenscanner und einer Firewall automatisch herausfiltern lassen. Wirksam geschützt sind Sie aber nur, wenn Sie die Sicherheits-Updates auch schnell installieren.

3. Öffnen Sie E-Mails nicht automatisch
Firewall und Virenscanner erkennen nicht alle schädlichen Mails. Öffnen Sie also nicht gedankenlos jede Mail in Ihrem Posteingang. Erster Schritt: Stellen Sie in Ihrem E-Mail-Programm die „Autovorschau" aus. So verhindern Sie, dass sich schädliche Mails automatisch öffnen und Viren oder Würmer sofort aktiv werden.

4. Vor dem Öffnen: Prüfen Sie Absender und Betreff
Cyberkriminelle verstecken sich gern hinter seriös wirkenden Absenderadressen. Ist Ihnen der Absender der Mail bekannt? Und wenn ja: Ist der Absender wirklich echt? Achten Sie auf kleine Fehler in der Schreibweise oder ungewöhnliche Domain-Angaben hinter dem @. In betrügerischen E-Mails ist auch der Betreff oft nur unpräzise formuliert, z. B. „Ihre Rechnung".

5. Öffnen Sie Links und Anhänge nur von wirklich vertrauenswürdigen Mails
Wollen Banken, Behörden oder Geschäftspartner sensible Daten wissen? Verweist eine kryptische Mail auf weitere Informationen im Anhang? Dann sollten Sie stutzig werden und auf keinen Fall auf die Mail antworten, Links folgen oder Anhänge öffnen. In Zweifelsfällen fragen Sie beim Absender nach – aber nicht per Mail, sondern am Telefon! Auch eine Google-Suche nach den ersten Sätzen der verdächtigen Mail kann sinnvoll sein – weil Sie so auch Warnungen vor der Betrugsmasche finden.

6. Löschen Sie lieber eine Mail zu viel als eine zu wenig
Erscheint Ihnen eine Mail als nicht glaubwürdig, löschen Sie die Mail aus Ihrem Postfach – und leeren Sie danach auch den Papierkorb Ihres Mailprogramms.

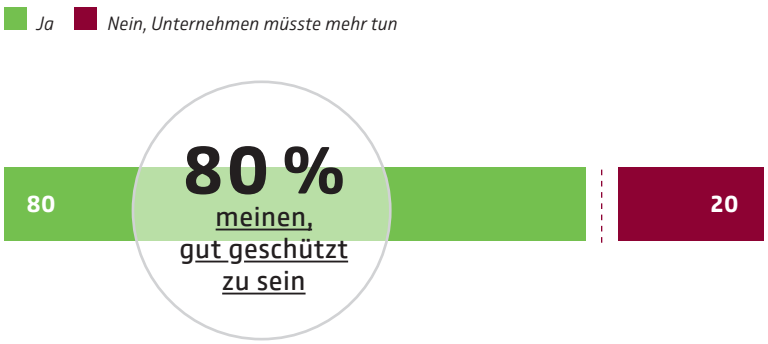
Achtung! Dringender Sicherheitshinweis

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 vier Tipps beherzigen.

1. Unterschätzen Sie die Gefahr nicht!

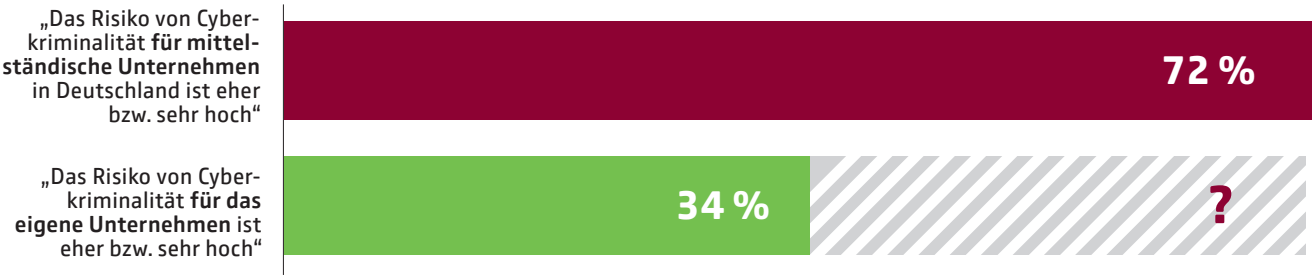
(Zu) hohes Vertrauen in den eigenen Schutz

Ist das eigene Unternehmen ausreichend gegen Cyberkriminalität geschützt?



In weiten Teilen des deutschen Mittelstandes regiert das Prinzip Hoffnung. Auch wenn eine deutliche Mehrheit das Cyberrisiko für mittelständische Unternehmen als hoch und damit durchaus realistisch einschätzt, blenden viele die Gefahr für das eigene Unternehmen aus. Sie sagen: Mein Unternehmen ist zu klein. Meine Daten sind nicht interessant. Mein Schutz reicht bestimmt aus. Richtig ist aber: Für Hacker gibt es kein zu klein. Die Daten müssen nicht interessant, sondern für Sie wertvoll sein. Und nein: Virenscanner und Firewall sind noch lange kein Rundumschutz, sondern nur ein Anfang.

„Das Risiko gibt es – aber mein Unternehmen betrifft es nicht“



2. Verwenden Sie starke Passwörter!

Ist Ihr Passwort auch 12345? Qwertz? Passwort? Der Name Ihrer Tochter? Das ist nicht gut, denn Passwörter sollen in erster Linie 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.

Sicherheit durch Zwang

Werden Mindestanforderungen an Passwörter technisch erzwungen?

26 % lassen einfache Passwörter zu

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. Ein einfaches Beispiel, das Sie bitte nicht direkt verwenden: Um „Pa$$W0rt" zu knacken, braucht ein herkömmlicher PC nach Auskunft der Webseite checkdeinpasswort.de gerade mal sechs Stunden, für „Pa$$W0rt-Hallo123" mehrere Milliarden Jahre.

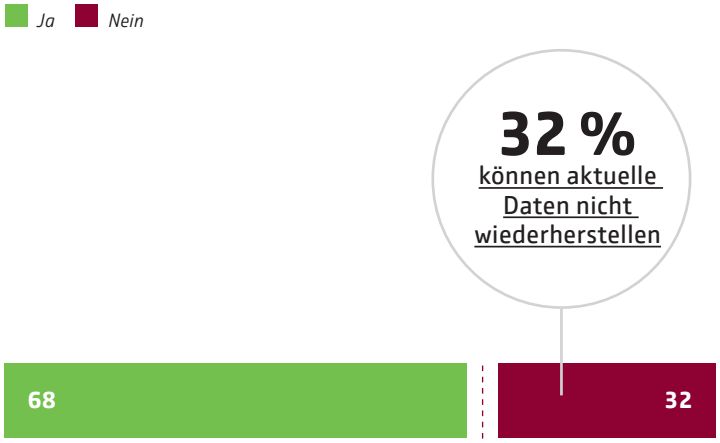
2. Verwenden Sie einen Passwort-Manager
Sie und Ihre Mitarbeiter können und wollen sich die vielen langen und komplizierten Passwörter nicht merken? Dann fangen Sie auf keinen Fall an, immer das gleiche oder nur ein leicht abgewandeltes Passwort einzugeben. Das macht es Hackern zu einfach. Die bessere Alternative sind Passwort-Manager. Sie generieren und verwalten starke (=lange) Passwörter, die Sie sich nicht merken müssen; das übernimmt der Manager. Da die Anbieter ihre Daten in aller Regel verschlüsseln, sind die Passwörter auch gegen Hackerangriffe geschützt. Sie brauchen für alle Passwörter hingegen nur noch das „Master-Kennwort" – das natürlich wiederum sehr sicher sein sollte.

3. Nutzen Sie die Zwei-Faktor-Authentifizierung
Auch wenn es etwas komplizierter ist, sollten Sie ernsthaft eine Zwei-Faktor-Authentifizierung in Betracht ziehen. Das Verfahren kennen Sie von Ihrer Bank: Am Geldautomaten brauchen Sie ihre Giro-Karte (1. Faktor) und die PIN (2. Faktor), auch eine Überweisung beim Online-Banking funktioniert in aller Regel nur mit PIN und TAN. Den Zugang zu Ihren Systemen können Sie genauso schützen – 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.

3. Sichern Sie Ihre Daten richtig!

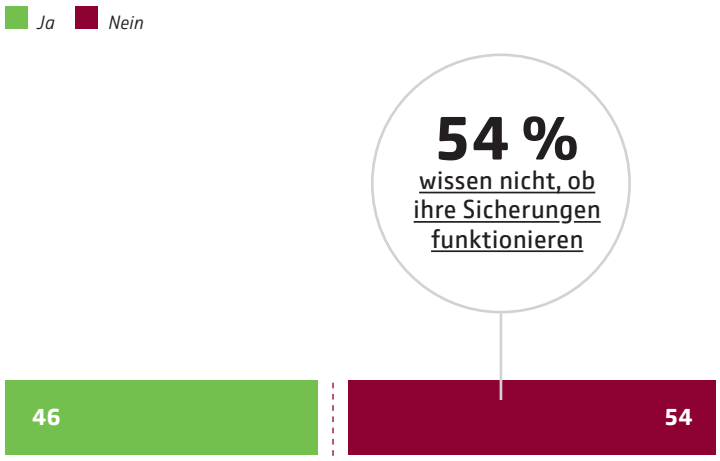
Je öfter, desto besser

Erstellen Sie mindestens wöchentlich eine Sicherungskopie Ihrer Daten?



Wie sicher ist das Backup?

Wird das Wiederherstellen der Daten aus der Sicherungskopie regelmäßig getestet??



Datensicherungen sind Ihre letzte Rückversicherung für den Fall gelöschter oder manipulierter Daten. Das Backup kann Sie auch dann vor dem Verlust Ihrer Daten schützen, wenn Sie keinen physischen 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 und leider noch zu oft ignoriert: Stellen Sie durch regelmäßige Testläufe sicher, dass Ihr Backup auch wirklich funktioniert. Im Fall von verlorenen oder manipulierten Daten zählt oft jede Minute – das ist der schlechteste Zeitpunkt um festzustellen, dass Ihre Sicherungskopie fehlerhaft ist.

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.

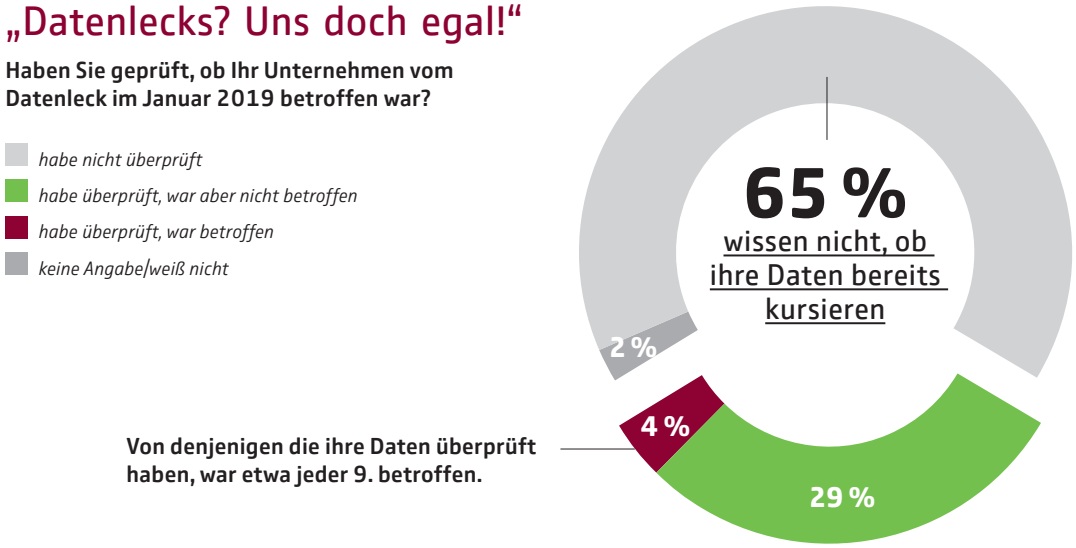
4. Reagieren Sie auf neue Sicherheitslücken!

Mitte Januar 2019 landeten mit der Collection#1 und später mit den Collection #2-#5 mehrere Milliarden von E-Mail-Adressen und Passwörtern im Netz. Für Kriminelle können diese Daten Gold wert sein, denn viele nutzen immer dieselben Zugangsdaten für die Anmeldung bei verschiedenen Diensten oder Portalen. Werden sie bekannt, können Angreifer leicht gleich mehrere Accounts kapern oder sogar die ganze Identität ihrer Opfer übernehmen.

Werden solche Datenlecks bekannt, ist also eine schnelle Reaktion gefragt: Die Passwörter sollten umgehend geändert werden. Und zwar nicht nur auf der betroffenen Seite, sondern bei allen Zugängen, die mit demselben oder einem ähnlichen Passwort geschützt sind. Zwei Drittel der befragten Unternehmen lässt diese Gefahr aber völlig kalt – sie haben sich nicht mal die Mühe gemacht, ihre Daten zu überprüfen. Dabei lohnte sich der Aufwand in vielen Fällen: Jedes neunte Unternehmen fand heraus, dass seine Zugangsdaten betroffen waren.

„Datenlecks? Uns doch egal!“

Haben Sie geprüft, ob Ihr Unternehmen vom Datenleck im Januar 2019 betroffen war?



Sind Sie betroffen? Hier finden Sie es heraus.

Der Service „Have I Been Pwned?“ (Pwned wird gesprochen wie „poned“) hat über 6 Milliarden Datensätze aus mehr als 300 Datenlecks gesammelt. Wenn Sie überprüfen wollen, ob auch Ihre Mail-Adresse darunter ist, geben Sie diese einfach in der entsprechenden Suchmaske ein, das Ergebnis wird sofort angezeigt.
→ https://haveibeenpwned.com/

Das Hasso-Plattner-Institut bietet den „HPI Identity Leak Checker“ an. Sie können anhand Ihrer E-Mail-Adresse prüfen, ob die Adresse in Verbindung mit anderen persönlichen Daten wie Geburtsdatum oder Adresse im Internet offengelegt wurde und missbraucht werden könnte. Anders als bei „Have I been Pwned?“ erhalten Sie das Ergebnis per Mail. → https://sec.hpi.de/ilc/

Wie gut ist Ihre IT-Sicherheit?

Absolute Sicherheit im Netz gibt es nicht. Doch Widerstand 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).

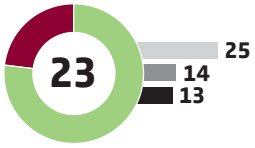
Der **Cyber-Sicherheits-check des GDV** unter www.gdv.de/cybercheck stellt Ihnen die wichtigsten Fragen rund um Ihre IT-Sicherheit. So finden Sie schnell heraus, wie sicher Ihre Systeme sind, wo Sie Schwachstellen haben und wie Sie diese schließen können. Ob Sie die zehn grundlegenden Anforderungen erfüllen, können Sie gleich hier beantworten. Wie gut Sie dabei abgeschnitten haben und ob es andere besser machen, können Sie auf Seite 18 herausfinden.

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

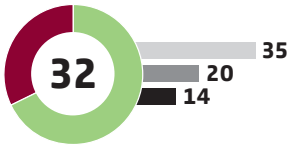
Kleinstunternehmen *Mittlere Unternehmen* *Große Unternehmen*

Selbsttest

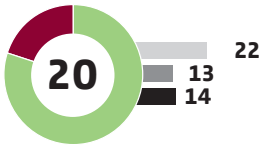
1. **Sicherheitsupdates automatisch und zeitnah einspielen und alle Systeme auf dem aktuellen Stand halten**
   Die meiste Software erhält regelmäßig Updates. Sie dienen oft dazu, bekannt gewordene Sicherheitslücken zu schließen. Das Installieren der Updates schützt die Systeme vor Angreifern.



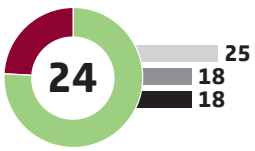
2. **Mindestens einmal wöchentlich Sicherungskopien machen**
   Daten und digitale Systeme können gezielt angegriffen, versehentlich gelöscht oder durch Hardware zerstört werden. Deshalb ist es dringend nötig, die vorhandenen Daten regelmäßig zu sichern. Grundsätzlich gilt: Je öfter Sie Ihre Daten sichern,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

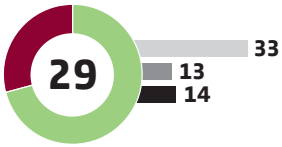


4. **Alle Systeme, die über das Internet erreichbar oder im mobilen Einsatz sind, zusätzlich schützen**
   Mobile Geräte können leicht verloren gehen oder gestohlen werden. Sind die darauf gespeicherten Daten nicht verschlüsselt, können sie vollständig ausgelesen werden – selbst wenn sie mit einem Passwort 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.

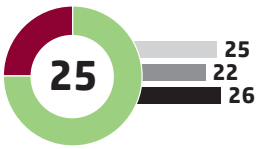


6. Alle Systeme mit einem Schutz gegen Schadsoftware ausstatten und diesen automatisch aktualisieren lassen

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.

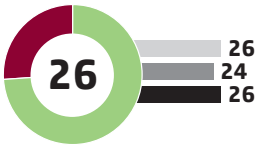
7. Sicherungskopien physisch vom gesicherten System trennen

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.



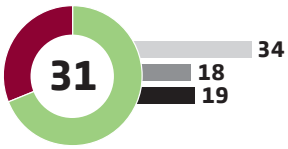
8. Mindestanforderungen für Passwörter (z.B. Länge, Sonderzeichen) verlangen und technisch erzwingen

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



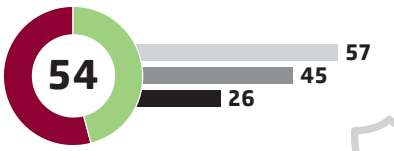
9. Jeden Nutzer mit eigener Zugangskennung und individuellem Passwort ausstatten

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 16/17 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 so gering wie möglich.

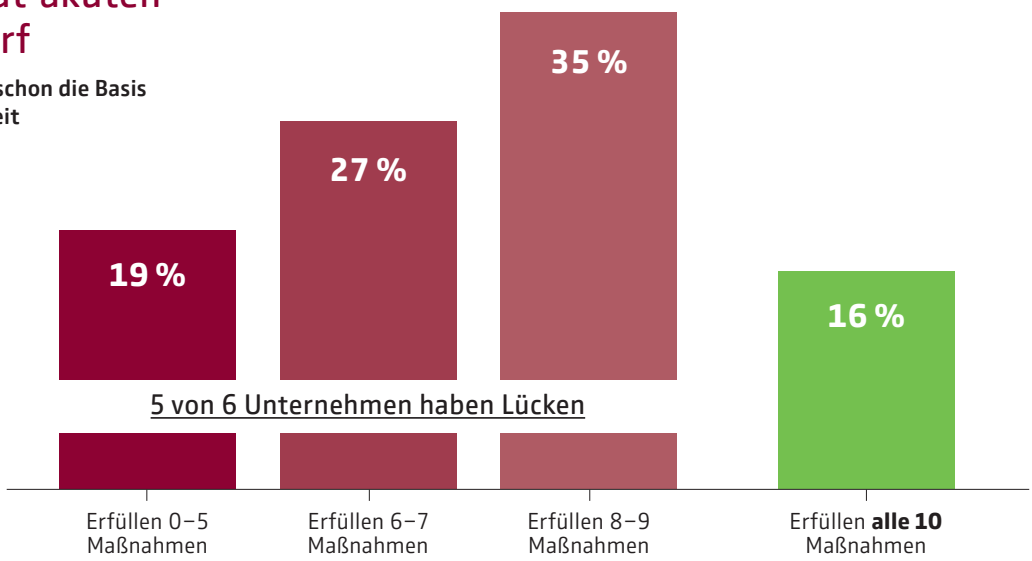
8–9
Das Niveau Ihrer IT-Sicherheit ist überdurchschnittlich, aber leider noch nicht perfekt – beachten Sie unsere Hinweise und schließen sie die noch vorhandenen Sicherheitslücken.

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.:
Christoph Hardt

Redaktion:
Lucas Fömpe, Simon Frost, Christian Siemens

Bildnachweis:
S. 1: shutterstock/TippaPatt
S. 4: shutterstock/Anucha Cheechang
S. 10: shutterstock/Monkey Business Images
S. 12: shutterstock/13_Phunkod

CYBER@SICHER

Eine Initiative der deutschen Versicherer.

GDV
DIE DEUTSCHEN VERSICHERER

Wilhelmstraße 43 / 43 G
10117 Berlin
Tel. +49 30 2020-5000
Fax +49 30 2020-6000
E-Mail: berlin@gdv.de

51, rue Montoyer
B-1000 Brüssel
Tel. +32 2 28247-30
Fax +32 2 28247-39
E-Mail: bruessel@gdv.de

www.gdv.de
www.DieVERSiCHERER.de
facebook.com/DieVERSiCHERER.de
Twitter: @gdv_de
www.youtube.com/user/GDVBerlin