Gesamtverband der Deutschen Versicherungswirtschaft e. V.

CYBER SICHER

Eine Initiative der deutschen Versicherer.

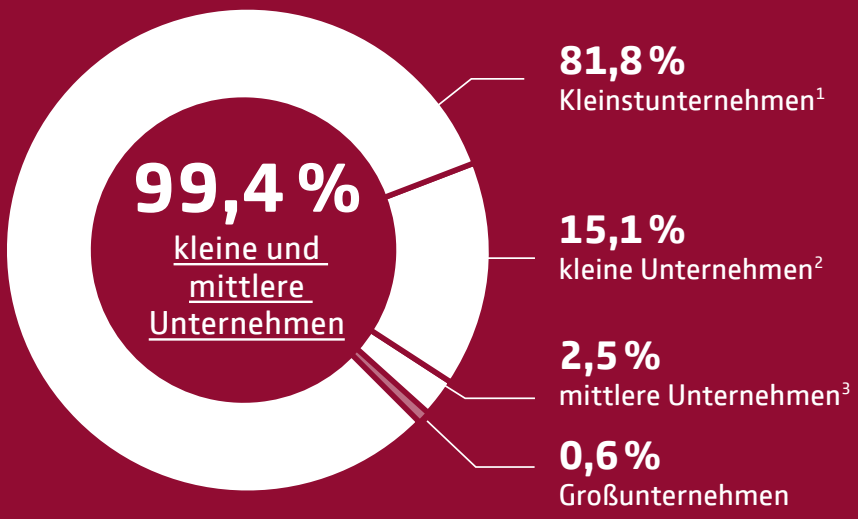
Report

Cyberrisiken im Mittelstand 2020



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 2018

Methodik

Im Auftrag der Initiative CyberSicher hat die **Forsa** Politik- und Sozialforschung GmbH 300 Entscheider in kleinen und mittleren Unternehmen befragt. Die Befragung wurde so angelegt, dass repräsentative Aussagen zu Kleinstunternehmen, kleinen Unternehmen und mittleren Unternehmen getroffen werden können. Die Interviews fanden zwischen dem 27. März und dem 23. April 2020 statt.
Darüber hinaus hat die PPI AG mit ihrem Analyse-Tool **cysmo** die Sicherheit der IT-Systeme von 1.019 mittelständischen Unternehmen passiv getestet und dabei alle öffentlich einsehbaren Informationen aus Sicht eines potentiellen Angreifers erfasst und bewertet.
Die Tests fanden im Juni 2020 statt.
Die Grafiken in diesem Report sind entsprechend gekennzeichnet.

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 2020



1 Die verdrängte Gefahr

Das Prinzip Hoffnung regiert

Obwohl die meisten Unternehmen eine Cyberattacke hart treffen würde, hat IT-Sicherheit vielerorts keine Priorität. → **Seite 04**



2 Die Sicherheitslücken

Neugier und Komfort schlagen die Datensparsamkeit

Viele Unternehmen legen mehr Wert darauf, Daten zu sammeln als Daten zu schützen. → **Seite 08**



Gefährliche Post

E-Mails sind für Cyberkriminelle die ideale Angriffswaffe. Und die erfolgversprechendste. → **Seite 12**

Wie eine erfolgreiche Attacke Unternehmen verändert

Wer nicht mehr zum Opfer werden will, stärkt die Strukturen und sensibilisiert seine Mitarbeiter. → **Seite 15**



Ab in die Cloud?

Wer seine Daten in der Cloud speichert, sollte die Chancen und Risiken kennen. → **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**



Das Prinzip Hoffnung regiert

Den meisten kleinen und mittelständischen Unternehmen in Deutschland ist bewusst, wie sehr ihre Arbeit mittlerweile von funktionierenden Computersystemen abhängig ist. Sie wissen auch, dass Cyberkriminalität eine Gefahr darstellt. Doch das Risiko, selbst einmal Opfer eines Cyberangriffs zu werden, verdrängen viele – es trifft ja immer nur die anderen.

Betriebsunterbrechungen sind eine der häufigsten und in der Regel die teuersten Folgen von Cyberattacken – und können Unternehmen quer über alle Branchen ins Mark treffen. In der Produktion stehen die Bänder still, Händler können weder liefern noch Zahlungen abwickeln, Ärzte haben keinen Zugriff auf Patientendaten, Hoteliers keinen Überblick über Gäste und die noch freien Zimmer. Dieser Zustand ist in den wenigsten Fällen innerhalb kurzer Zeit behoben: Wie aus der diesjährigen Forsa-Umfrage zur Cybersicherheit des deutschen Mittelstandes hervorgeht, braucht die Hälfte der Betroffenen bis zu drei Tage, bis alle Systeme wieder laufen, bei 22 Prozent dauerte es sogar noch länger.

Das stellt die meisten vor große Probleme: Sechs von zehn kleinen und mittelständischen Unternehmen müssten ihre Arbeit in dieser Zeit einstellen oder zumindest stark einschränken. Je größer die Unternehmen, desto größer ist auch die Abhängigkeit von funktionierenden IT-Systemen: Unter den Firmen mit 50 oder mehr Mitarbeitern wären 87 Prozent bei einem mehrtägigen Ausfall der IT voraussichtlich lahmgelegt.

Wie sehr sie mittlerweile vom Funktionieren der Technik abhängig sind, haben die Unternehmen in Deutschland also längst verinnerlicht, und auch das Risikobewusstsein ist durchaus vorhanden – immerhin 69 Prozent erkennen ein hohes Risiko durch Cyberkriminalität für die mittelständische Wirtschaft. →

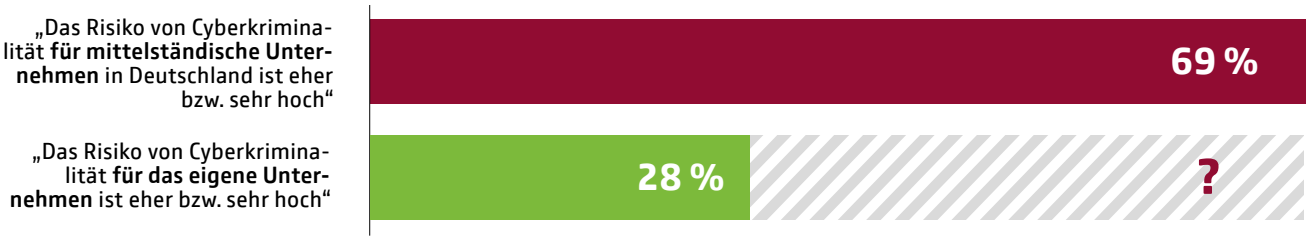
→ Dennoch bleibt das Risiko für die meisten abstrakt. Denn erstaunlicherweise bewerten die gleichen Befragten die Gefahr für sich selbst ganz anders: Hier sehen auf einmal nicht mehr 69 Prozent ein hohes Risiko, sondern nur noch 28 Prozent. Anders ausgedrückt: 41 Prozent meinen, es gibt ein hohes Risiko für andere, aber nicht für sie.

Wie erklärt sich diese Lücke? Die Antwort auf diese Frage ist nicht wirklich schmeichelhaft, denn sie lässt wohl am ehesten auf gut funktionierende Verdrängungsprozesse schließen. So meinen 70 Prozent, dass ihre Daten für Hacker nicht interessant wären, 60 Prozent halten ihr Unternehmen für zu klein, um in den Fokus von Cyberkriminellen zu gelangen. 58 Prozent machen geltend, dass sie bisher schließlich noch nie Opfer einer erfolgreichen Cyberattacke waren – und ganze 81 Prozent halten ihr Unternehmen für umfassend geschützt. „Die ganzen Irrglauben rund um Cyberkriminalität halten sich seit Jahren hartnäckig und führen zu nichts anderem, als dass die Angreifer leichtes Spiel haben", ärgert sich GDV-Cyberexperte Peter Graß. Dabei sollten gerade die sogenannten Ransomware-Angriffe in den vergangenen Jahren klar gemacht haben, dass es jeden treffen kann; gerade weil Hacker nicht das eine große und gut geschützte Ziel ins Visier nehmen, solange es viel leichter ist, massenhaft Kleinbeiträge zu erpressen.

Wo das eigene Risiko verdrängt oder gar nicht erst erkannt wird, liegt häufig auch die IT-Sicherheit im Argen

Denn eines wissen die Cyberkriminellen mit Sicherheit: Wo das Risiko verdrängt oder gar nicht erst erkannt wird, liegt in der Regel auch die IT-Sicherheit im Argen. Auch das zeigt die Umfrage. So wollen gerade einmal etwas mehr als die Hälfte der befragten Unternehmen in den kommenden zwei Jahren in die Sicherheit ihrer Systeme investieren – obwohl die Investition von Zeit und Geld in vielen Fällen angebracht wäre. Vielerorts fehlt es schon an den notwendigen Strukturen: in 44 Prozent der Unternehmen ist niemand explizit für die IT-Sicherheit verantwortlich, 48 Prozent bereiten sich auf eine Cyberattacke auch nicht vor. Geradezu folgerichtig werden auch die Mitarbeiter (siehe dazu „Gefährliche Post", S. 12) nicht für die Gefahren sensibilisiert: Nicht mal in einem Drittel der befragten Unternehmen gibt es entsprechende Schulungen. Wozu auch, wenn es das eigene Unternehmen ja sowieso nicht trifft? ←

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

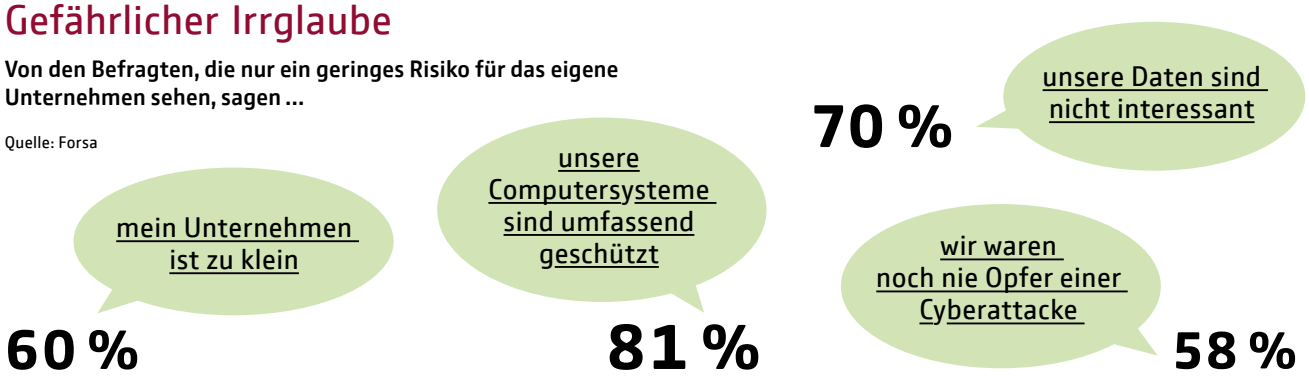


Quelle: Forsa

Gefährlicher Irrglaube

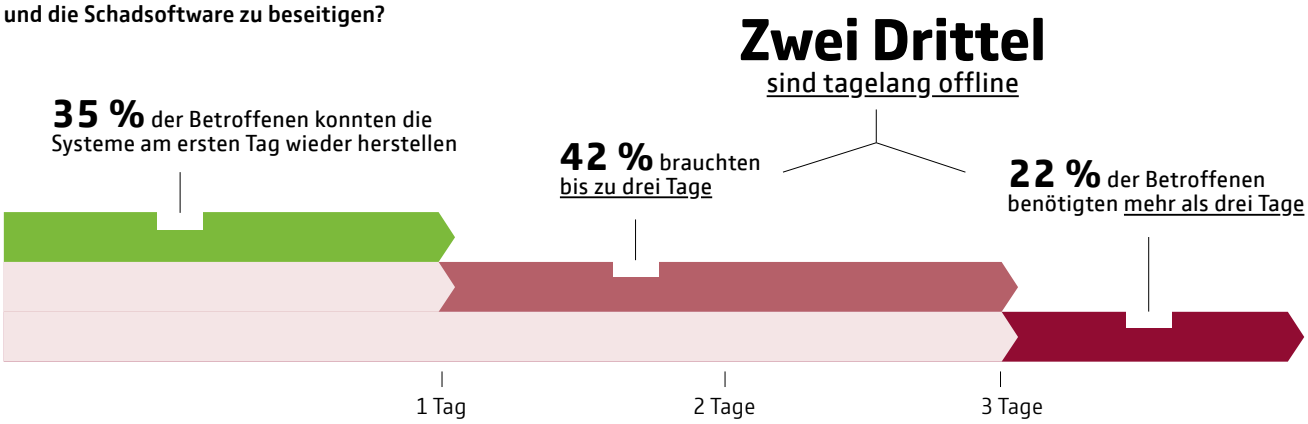
Von den Befragten, die nur ein geringes Risiko für das eigene Unternehmen sehen, sagen …

Quelle: Forsa



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

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

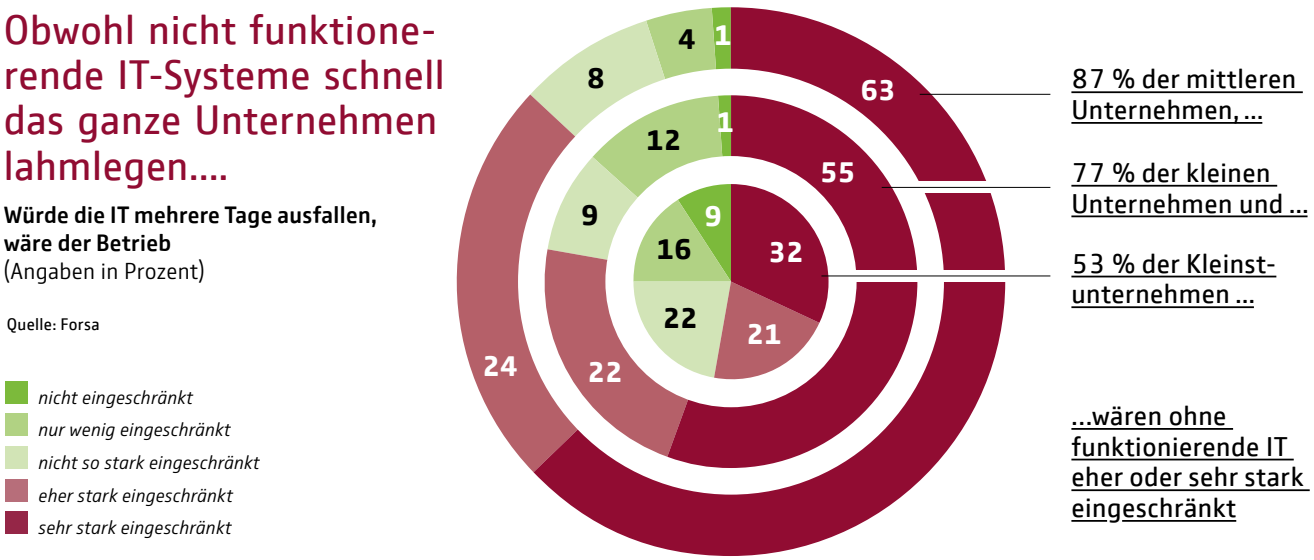


Quelle: Forsa

Obwohl nicht funktionierende IT-Systeme schnell das ganze Unternehmen lahmlegen….

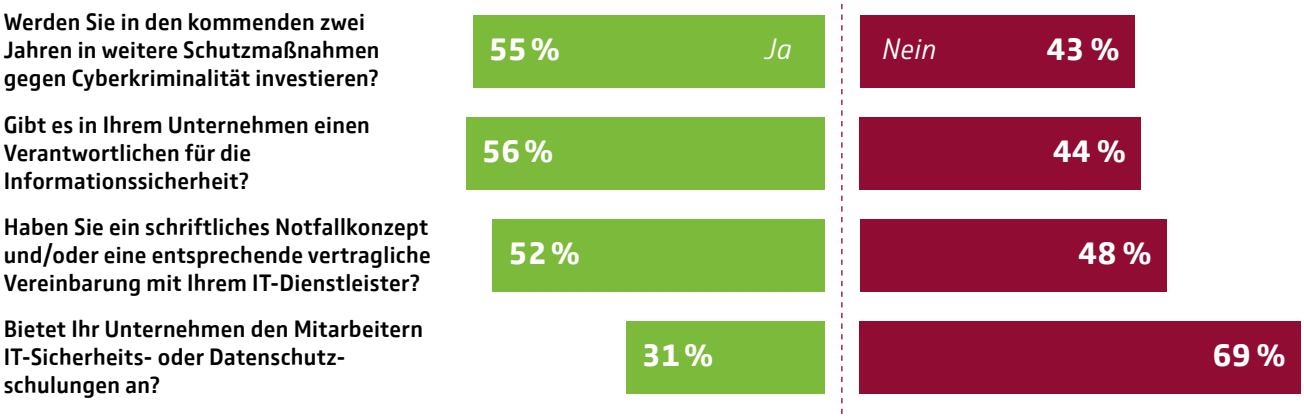
Würde die IT mehrere Tage ausfallen, wäre der Betrieb
(Angaben in Prozent)

Quelle: Forsa



… hat IT-Sicherheit vielerorts keine Priorität

Quelle: Forsa



Neugier und Komfort schlagen die Datensparsamkeit



Eine Analyse von Webseiten und Mailservern zeigt, dass zahlreiche mittelständische Unternehmen mehr Wert darauf legen, Daten zu sammeln als Daten zu schützen. Viele handeln blauäugig.

Die meisten Besuche auf deutschen Unternehmenswebseiten werden gleich von mehreren global agierenden Großkonzernen der digitalen Welt registriert. Wie die vom GDV beauftragte Untersuchung der IT-Systeme von 1.019 kleinen und mittelständischen Unternehmen mit dem Analyse-Tool cysmo zeigt, sind auf rund 70 Prozent der Webseiten fremde Inhalte eingebunden. Denn die sind kostenlos und bequem – Kunden können sich im unternehmenseigenen Youtube-Kanal informieren, finden dank Google Maps schnell und einfach ihren Weg und können mit nur einem Klick der Firma auf Twitter folgen. Dass die Besucher dafür mit der Preisgabe ihrer Daten bezahlen und diese nicht nur innerhalb Europas, sondern weltweit zirkulieren, nehmen die Unternehmen billigend in Kauf.

Wer IP-Adressen nicht anonymisiert speichert, verstößt im Zweifel gegen die DSGVO

Viele Unternehmen haben aber auch selbst ein großes Interesse zu erfahren, wer sich wann, wie oft und wo genau auf ihren Webseiten tummelt. Um das herauszufinden, setzt jedes vierte Unternehmen sogenannte Tracker ein. So können sie feststellen, von welchen Seiten ihre Besucher kommen, wie lange sie auf der Webseite bleiben und was sie sich wie lange ansehen. Tracker schreiben aber nicht nur Aktivitäten auf einer Webseite mit, sondern können Nutzer durch das ganze Internet verfolgen.

Besonders problematisch: Mindestens fünf Prozent der untersuchten Unternehmen haben ihren Tracker so eingestellt, dass die IP-Adressen der Benutzer nicht anonymisiert werden. Das kann zulässig sein, muss aber in der Datenschutzerklärung klar und korrekt benannt sein. Die Realität sieht in den meisten Fällen anders aus. Die Erfahrung zeigt: Die meisten dieser Tracker wurden vor Inkrafttreten der →

»Viele Firmen setzen auch einfache Empfehlungen nicht um«



Mit dem Analyse-Tool cysmo findet der IT-Berater Jonas Schwade auch ohne Penetrationstests Schutzlücken in IT-Systemen.

Herr Schwade, Sie haben für den GDV die IT-Systeme von 1.019 mittelständischen Unternehmen mit dem Analyse-Tool cysmo überprüft – welches Ergebnis hat Sie am meisten überrascht?
Jonas Schwade: Tatsächlich sind wir bei den Analysen immer wieder über die teilweise nicht mehr zeitgemäße Verwendung von Verschlüsselungen im Mailverkehr überrascht. Obwohl es vom Bundesamt für Sicherheit in der Informationstechnik (BSI) klare Empfehlungen gibt, welche Verschlüsselungen aktuell sind und welche veraltet, so sehen wir doch leider noch sehr viele Unternehmen, die diesen Empfehlungen nicht nachkommen.

Können Unternehmen denn noch mit allen Geschäftspartnern und Kunden kommunizieren, wenn sie ausschließlich auf die neuesten Verschlüsselungsstandards setzen?
Schwade: Das Problem liegt nicht in einer mangelnden Verwendung der sicheren Verschlüsselungen, hier haben nahezu alle Unternehmen auch die empfohlenen Versionen im Einsatz. Das Problem ist, dass die veralteten Versionen weiterhin zusätzlich verwendet werden, obwohl sie das nicht müssten.

Und welches Risiko besteht, wenn ich unsichere Verschlüsselungen nutze?
Schwade: Unterstütze ich weiterhin auch die unsicheren Verschlüsselungen, mache ich mich potentiell angreifbar. Ein Angreifer könnte mich nun mit einer sogenannten Downgrade-Attacke dazu zwingen eine unsichere Verschlüsselungsversion zu akzeptieren. Dann könnte er sich in einem zweiten Schritt zwischen den Mailverkehr setzen und Mails abfangen oder mitlesen. Mit einer solchen Man-in-the-middle-Attacke sind die eigentlich verschlüsselt versendeten Mails nicht mehr vertraulich und der Mailverkehr wird manipulierbar.

Müssen Sie für Ihre Analyse die IT-Systeme tatsächlich hacken und wenn ja: Dürfen Sie das überhaupt ohne das Wissen der Unternehmen?
Schwade: cysmo arbeitet zu 100 % passiv. Anders als bei einem Penetrationstest wird die zu analysierende Infrastruktur nicht angegriffen, sondern es werden Daten aus frei verfügbaren, offenen Quellen gesammelt und aufbereitet, im Fachjargon heißt das Open Source Intelligence (OSINT). Auf Basis dieser Daten wird eine Außensicht auf das Unternehmen erstellt und bewertet. Durch den reinen Einsatz von OSINT-Methoden bedarf es keiner Zustimmung des zu bewertenden Unternehmens und es besteht für das Unternehmen dadurch auch keine Gefahr.

Zu Ihrer Untersuchung gehört auch eine Recherche im Darknet. Ist das wie die Suche nach einer Nadel im Heuhaufen oder gibt es auch im Darknet Suchmaschinen wie Google?
Schwade:Tatsächlich ist das Aufspüren von Daten im Darknet deutlich schwieriger als im herkömmlichen Internet. Suchmaschinen existieren, decken aber nur einen Bruchteil der dortigen Daten ab. Auch erschweren fehlende Standards eine automatische Suche und Bewertung. cysmo prüft mit Hilfe eines Dienstleisters, ob E-Mail-Adressen oder andere technische Details des zu bewertenden Unternehmens im Darknet auftauchen. Ein besonderes Augenmerk wird hierbei auf die Datensicherheit gelegt. Alle Daten werden ausschließlich anonymisiert übertragen, damit zu keinem Zeitpunkt personenbezogene oder sensible Informationen aus dem Darknet verarbeitet werden.

Wie können Unternehmen verhindern, dass ihre Daten ins Darknet gelangen?
Schwade: Wir beobachten, dass unternehmensspezifische Daten primär über Datenlecks bei Drittanbietern ins Darknet gelangen und nicht direkt aus dem Unternehmensnetz entwendet werden. Da die Sicherheit der IT-Infrastruktur anderer Anbieter meist nicht in der Hand des Unternehmens liegt, hilft hier vor allem der Grundsatz der Datensparsamkeit. Mitarbeiter sollten dazu angehalten werden, umsichtig bei der Weitergabe von Daten wie E-Mail-Adressen und Telefonnummern zu sein. Im Idealfall wird die private Nutzung der geschäftlichen E-Mail-Adresse, zum Beispiel für Social Media, durch den Arbeitgeber eingeschränkt.

„Wer weiterhin alte Mail-Verschlüsselungen einsetzt, riskiert Opfer sogenannter Man-in-the-Middle-Attacken zu werden – völlig ohne Not."

Jonas Schwade, PPI AG

→ EU-Datenschutzgrundverordnung (DSGVO) installiert und dann nicht mehr angepasst – in der Regel fehlt in solchen Fällen auch eine korrekte Datenschutzerklärung. Wird ein solcher Verstoß gegen die DSGVO festgestellt, können empfindliche Strafen drohen.

Handlungsbedarf bei der Verschlüsselung von Mails

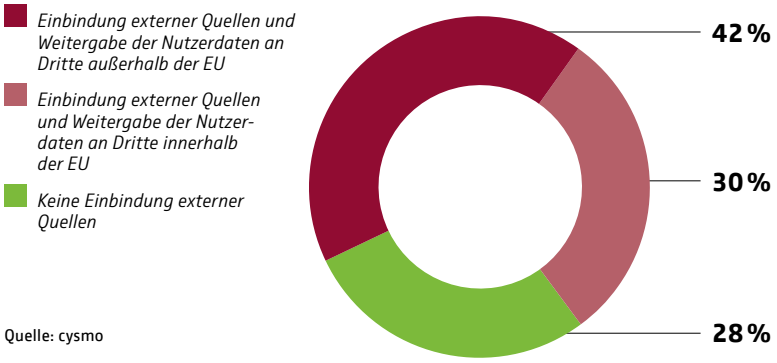
Ebenfalls nicht auf dem neuesten Stand sind bei den meisten untersuchten Unternehmen die unterstützten Verschlüsselungsstandards im Mailverkehr. Rund 25 Prozent der Mail-Server sind so eingestellt, dass sie noch Verschlüsselungen unterstützen, die schon seit mehreren Jahren veraltet und damit unsicher sind. Die neuesten Verschlüsselungstechnologien und damit einen sehr guten Schutz haben nur 13 der mehr als 1.000 getesteten Unternehmen, die breite Masse hinkt der Entwicklung hinterher. Dabei besteht akuter Handlungsbedarf: Die Verschlüsselungsstandards TLS 1.0 und TLS 1.1 liegen schon seit Sommer 2018 unter dem vom Bundesamt für Sicherheit in der Infomationstechnik (BSI) geforderten Mindeststandard für ein angemessenes IT-Sicherheitsniveau. Die Auswertungen zeigen jedoch, dass auch zwei Jahre später die meisten der untersuchten Unternehmen hierauf noch nicht reagiert haben. ←

Handlungsbedarf bei der Mail-Verschlüsselung



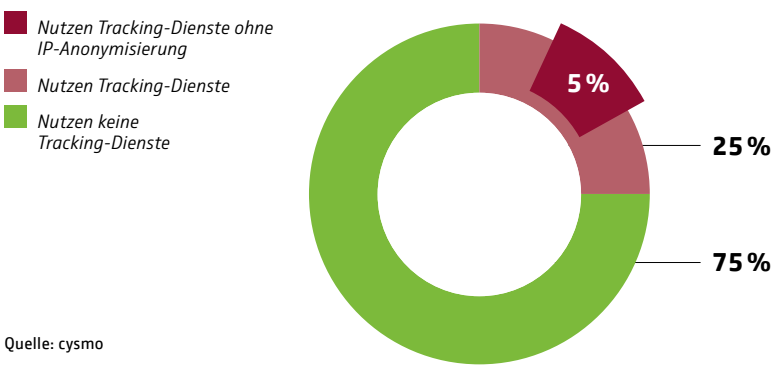
Quelle: cysmo

Viele Nutzerdaten gehen an Dritte



Quelle: cysmo

Hohes Interesse am Verhalten der Nutzer



Quelle: cysmo

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.



Gefährliche Post

Das E-Mail-Postfach ist für viele Unternehmen die wichtigste digitale Schnittstelle zu Kunden und Lieferanten. Für Hacker ist dies der ideale Angriffspunkt: Sie bringen mit immer raffinierteren Methoden ihre Opfer dazu, Spam E-Mails zu öffnen – und legen mit ihrer Schadsoftware nicht nur die IT-Systeme, sondern ganze Betriebe lahm. Doch die Gefahr geht über den Spam-Ordner hinaus: Bei der privaten Nutzung dienstlicher Accounts können Mail-Adressen und Passwörter ins Darknet geraten und werden Hackern somit auf dem Silbertablett präsentiert.

Früher war Spam leicht zu erkennen: unseriöse Absender, vermeintliche Gewinn-Überraschungen oder kuriose Satzstellungen. Diese Zeiten sind vorbei. Und falls solche E-Mails es durch den Spam-Filter schaffen, liegt es an den Empfängern, diese als unseriös einzustufen und in den Papierkorb zu verschieben. Hacker finden jedoch immer wieder ausgefeilte Methoden, Menschen so zu manipulieren, dass sie die Fälschungen nicht erkennen und eben doch Schadsoftware herunterladen oder Passwörter herausgeben. Mit zuvor gesammelten Daten eines Unternehmens können sie ihren Angriff als seriöse E-Mail ausgeben und nutzen so die menschliche Neugierde aus. Social Hacking nennt sich diese geschickte Manipulation.

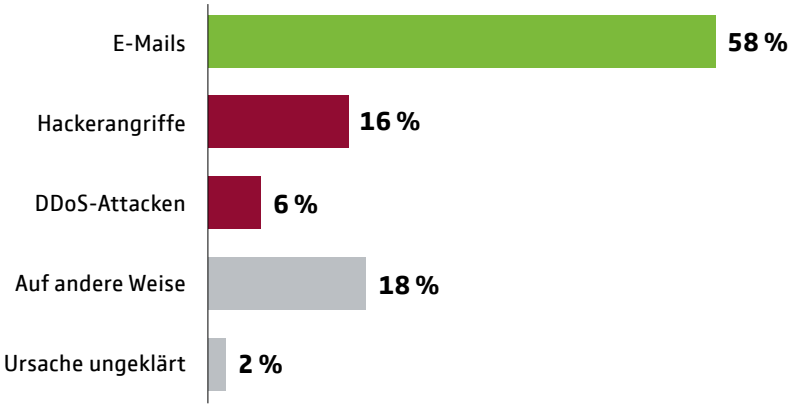
„Berufliches und Privates sollte man trennen. Das gilt auch für Mail-Accounts und Passwörter."

Peter Graß,
GDV-Cyberversicherungsexperte

In einer YouGov-Umfrage im Auftrag des GDV gab jeder achte Mitarbeiter an, schon mal Spam-Mails geöffnet zu haben. Ein Grund dafür sind offenbar schlechte Spam-Filter: Fast die Hälfte der Befragten (47 %) findet mindestens einmal pro Woche Spam-Mails in ihrem Postfach. Wenn sich viele nur auf Firewall und Virenscanner verlassen, ist es somit keine Überraschung, dass fast 60 Prozent aller erfolgreichen Hacker-Angriffe genau hier ansetzen. „Die technischen Hilfsmittel können den

Die Einfallstore

Erfolgreiche Cyberangriffe erfolgten durch … [1]



Quelle: Forsa

1 Mehrfachnennungen möglich

gesunden Menschenverstand und eine gewisse Skepsis nicht ersetzen, Unternehmen müssen ihre Mitarbeiter daher besser auf die Gefahren aus dem Netz vorbereiten", sagt Peter Graß, Cyberversicherungsexperte des GDV. „Cyberangriffe sind selten ausgefeilte Angriffe durch Netzwerklücken, viel öfter entstehen Schäden durch Menschen, die unbedacht eine infizierte E-Mail öffnen." Deswegen ist es umso wichtiger, Mitarbeiterinnen und Mitarbeiter entsprechend zu schulen und Richtlinien zur Nutzung von E-Mails festzulegen. →

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 E-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 E-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 E-Mails
Wollen Banken, Behörden oder Geschäftspartner sensible Daten wissen? Verweist eine kryptische E-Mail auf weitere Informationen im Anhang? Dann sollten Sie stutzig werden und auf keinen Fall auf die E-Mail antworten, Links folgen oder Anhänge öffnen. In Zweifelsfällen fragen Sie beim Absender nach – aber nicht per E-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.

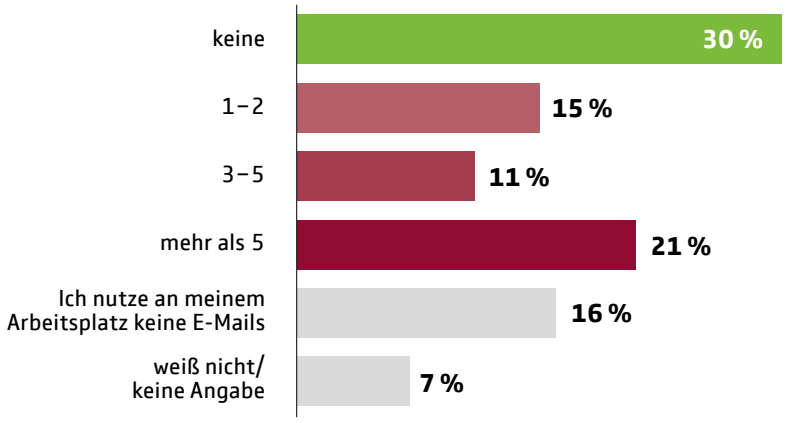
6. Löschen Sie lieber eine E-Mail zu viel als eine zu wenig
Erscheint Ihnen eine E-Mail als nicht glaubwürdig, löschen Sie die E-Mail aus Ihrem Postfach – und leeren Sie danach auch den Papierkorb Ihres Mailprogramms.

→ Vor allem in Bezug auf die private Nutzung des dienstlichen Mail-Accounts sollte es verbindliche Regelungen geben, denn viele sind sich der Gefahr bei privater Nutzung offenbar nicht bewusst: Bei der Prüfung von 1.019 mittelständischen Unternehmen mit dem Analyse-Tool cysmo konnten von 543 Firmen (53 %) Daten im Darknet gefunden werden, darunter ungefähr 6.500 Mail-Adressen mit den dazugehörigen Passwörtern.

Doch wie kommen die dienstlichen E-Mail Adressen der Mitarbeiter ins Darknet? In 64 % der Unternehmen gibt es keine verbindlichen Regelungen zur Nutzung des dienstlichen Mail-Accounts für private Zwecke. Die Studie zeigt, dass Mitarbeiter ihre dienstlichen Mail-Adressen daher vielfach eben nicht nur dienstlich, sondern auch privat benutzen – und das nicht nur für Einkäufe in Online-Shops oder soziale Netzwerke wie Facebook. So manch einer scheut nicht davor, sich mit seiner Dienstadresse auch in Dating-Portalen wie Badoo, Dating.de oder Fling zu registrieren. Andere melden sich sogar gleich bei Portalen für „Erwachsenenunterhaltung“ an. Zu den gefundenen Rückzugsorten gehören hier zum Beispiel Brazzers oder Youporn. Durch diese fragwürdige private Nutzung der dienstlichen Mail-Adresse schleusen die Mitarbeiter möglicherweise sogar Daten ins Darknet, die von Hackern zur Erpressung genutzt werden können. „Private und berufliche Mail-Accounts und die entsprechenden Aktivitäten sollten immer strikt voneinander getrennt werden – dazu gehört auch, nicht ein und dasselbe Passwort für beide Accounts zu benutzen“, warnt Graß. ←

Durchlässige Spamfilter

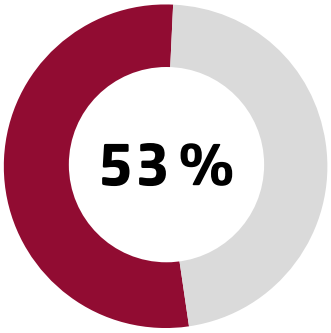
Wie viele Spam-Mails landen in einer durchschnittlichen Arbeitswoche in ihrem dienstlichen Mail-Postfach?



Quelle: Online-Umfrage der YouGov Deutschland GmbH im Auftrag des GDV unter 2.038 Arbeitnehmern ab 18 Jahren, Befragungszeitraum: 28.06. bis 04.07.2019.

Daten im Darknet

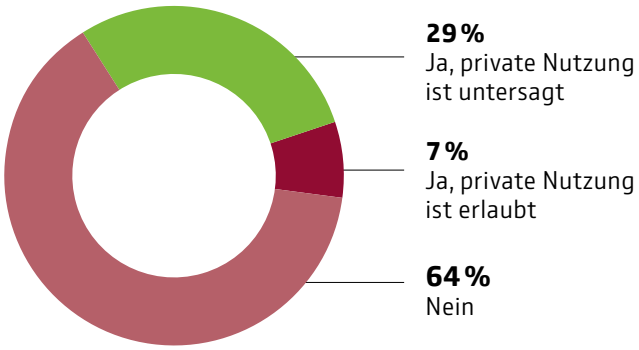
Von mehr als jedem zweiten Unternehmen waren Daten im Darknet zu finden, in den meisten Fällen E-Mail-/ Passwort-Kombinationen



Quelle: cysmo

Dienst ist Dienst?

Gibt es eine Regelung zur privaten Nutzung dienstlicher Mail-Accounts?



Quelle: Forsa

Wie eine erfolgreiche Cyberattacke Unternehmen verändert

Ein Cyberangriff und seine Folgen sind für viele Verantwortliche der endgültige Weckruf: Wer nicht wieder und wieder Opfer sein will, muss etwas ändern – und tut das dann auch.

Schritt 1: Eine neue Wahrnehmung

Chaos, Hilflosigkeit, hohe Kosten, Reputationsverlust – wer einmal eine Cyberattacke erlebt hat, will nie wieder in eine solche Situation kommen. Wie gravierend die Folgen eines Angriffs sein können, wird vielen Verantwortlichen erst durch die eigene Erfahrung bewusst. Bevor sie selbst betroffen sind, geht nur eine Minderheit von einem sehr hohen Risiko durch Cyberkriminalität aus. Nach einem erfolgreichen Angriff halten hingegen mehr als ein Drittel die Gefahr für sehr groß – und haben damit eine deutlich realistischere Einschätzung.

Schritt 2: Ein neues Handeln

Auf die Einsicht folgen in den meisten Unternehmen dann auch Taten – und die Bereitschaft, für die IT-Sicherheit Geld in die Hand zu nehmen und Strukturen zu stärken: Um künftige Angriffe besser abzuwehren und die Folgen eines erneuten Angriffs einzudämmen, benennen Firmen konkret verantwortliche Personen für die IT-Sicherheit. Die sorgen dafür, dass im Ernstfall nicht mehr plan- und kopflos, sondern schnell und konsequent reagiert wird; dafür entstehen Notfallkonzepte und entsprechende Verträge mit IT-Dienstleistern. Zum anderen werden die Mitarbeiter sensibilisiert und regelmäßig geschult – schließlich kommen Kriminelle häufig über die Schwachstelle Mensch (siehe S. 12) ans Ziel. Im gleichen Zug verbannen viele Firmen alle privaten Geräte aus der Unternehmens-IT. Eine gute Entscheidung, denn wie sicher diese Geräte sind, kann das Unternehmen weder wissen noch wirklich beeinflussen.

Schritt 3: Ein neues (Un-) Sicherheitsgefühl

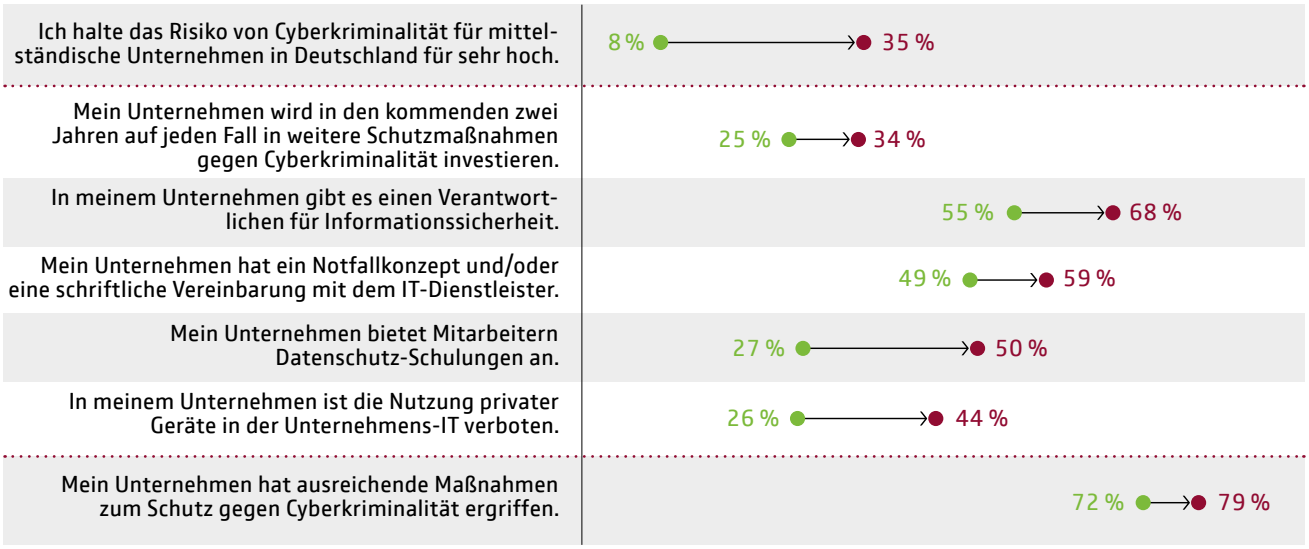
Am Ende sind die Betroffenen für einen erneuten Angriff besser gewappnet als beim ersten Mal – und wissen das auch. Völlig sicher, dass die Bemühungen ausreichen, können aber auch sie nicht sein.

Lernen durch Schmerzen

Diese Konsequenzen ziehen Opfer nach einer erfolgreichen Cyberattacke

Unternehmen ohne Schäden durch Cyberangriffe *Unternehmen mit Schäden durch Cyberangriffe*

Quelle: Forsa





Ab in die Cloud?

Unternehmen beeinflussen selbst, wie gut sie sich gegen Cyberattacken schützen. Speichern sie ihre Daten in einer Cloud, fällt ein Teil dieser Kontrolle weg. Das birgt sowohl Risiken als auch Chancen.

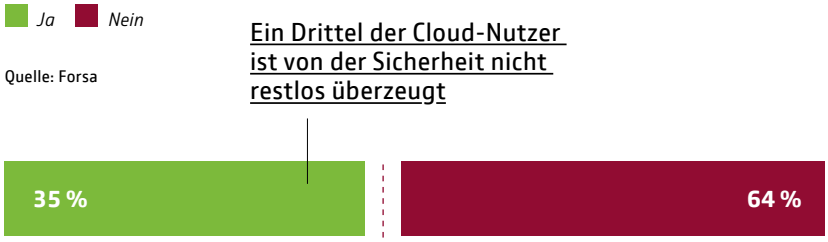
Cloud Computing wächst: Schon heute nutzt fast jeder dritte Mittelständler die Infrastruktur übers Netz, wie aus der Forsa-Umfrage im Auftrag des GDV hervorgeht. Je größer das Unternehmen, desto verbreiteter ist der Einsatz einer Cloud. Doch wer dem Trend folgen und seine Daten in eine Cloud auslagern will, sollte grundsätzliche Risiken, Chancen und Ziele der Technologie erwägen. Je nach Unternehmen können diese unterschiedlich aussehen. Für alle steht jedoch fest: Die wichtigsten Anforderungen an Cloud Services sind Datenschutz, Transparenz und Integrationsfähigkeit.

Laut Bundesamt für Sicherheit in der Informationstechnik beschreibt Cloud Computing die Nutzung von IT-Diensten wie Software, Speicher oder Rechenleistungen über Datennetze. Bislang nutzen die meisten Unternehmen aufgrund von Sicherheitsbedenken ein organisationsinternes Intranet (Private Cloud Computing). Wenn Mittelständler ihre Daten in eine Public Cloud auslagern, setzen sie fast ausschließlich auf deutsche und europäische Anbieter, nur ein Fünftel vertraut seine Daten außereuropäischen Dienstleistern an. Darauf reagieren inzwischen auch US-Cloud-Anbieter: Sie garantieren europäischen Kunden, ihre Daten nur auf Servern zu speichern, die in der EU stehen und deren Anforderungen an den Datenschutz erfüllen.

Ein großer Nachteil von Cloud-Services ist die Abhängigkeit vom jeweiligen Provider: Wichtige Daten liegen beim Anbieter und werden nicht immer standardisiert gespeichert. Sollen die Daten zum Beispiel im Fall eines Ausstiegs aus der Cloud bewegt werden, kann dies

Mancher Cloudnutzer bleibt skeptisch

Haben Sie schon einmal darüber nachgedacht, aus Sicherheitsgründen auf Clouddienste zu verzichten?



ein langwieriger und teurer Prozess sein. Mit zunehmender Datenmenge steigt somit auch die Abhängigkeit.

Andererseits haben die meisten Provider genügend Ressourcen, um Inhalte vervielfältigt an mehreren Orten zu speichern. Dies bietet zusätzliche Sicherheit im Fall eines Datenverlusts. Für ein hohes Schutzniveau sorgen auch die IT-Spezialisten, die dem Provider im Problemfall zur Verfügung stehen und die sich viele mittelständische Unternehmen selbst nicht leisten können.

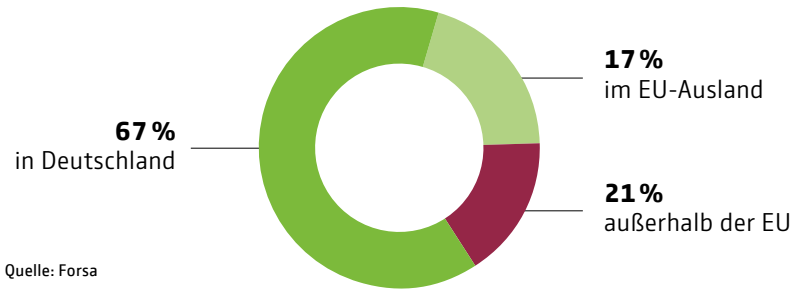
Nichtdestotrotz bergen Cloud-Dienste auch Sicherheitsrisiken, die das größte Hemmnis bei einer Entscheidung für eine Ausgliederung darstellen. Selbst ein Drittel der aktuellen Cloud-Nutzer in mittelständischen Unternehmen (35 %) hat schon einmal darüber nachgedacht, aus Sicherheitsgründen auf Cloud-Dienste zu verzichten. Ganz unberechtigt sind die Sorgen sicher nicht: Für Cloud-Nutzer kann die Kontrolle über die rechtliche Handhabung der Daten erschwert werden, wenn der Provider keine transparente Sicherheitsarchitektur hat. Außerdem müssen Cloud-Nutzer bestimmte technische Voraussetzungen erfüllen, nur dann sind eine ausreichende Übertragungsgeschwindigkeit, Transaktionssicherheit und Datenschutz garantiert. Insgesamt bedeutet dies für viele auslagernde Unternehmen einen zusätzlichen Aufwand für Steuerung und Qualitätskontrolle der Dienstleister und IT-Systeme.

Dennoch bietet Cloud Computing wirtschaftliche Vorteile: IT-Prozesse werden weniger komplex und Kosten für die Anschaffung eigener Hard- und Software bleiben erspart. Hinzu kommen umfangreichere Funktionen, die durch Cloud Computing ohne größeren Ressourcen-Aufwand zur Verfügung stehen. Dies erhöht die Skalierbarkeit und verringert somit das Investitionsrisiko. Insgesamt kann die Nutzung von Cloud-Diensten einen großen Beitrag zur Digitalisierung in Unternehmen leisten.

Letztlich kommt es jedoch immer auf die individuellen Voraussetzungen im Unternehmen und die betroffenen Daten an, ob und in welcher Form Cloud Computing sinnvoll sein kann. Überlegungen hierzu sollten in die IT-Strategie des jeweiligen Unternehmens aufgenommen und einer Risiko-Analyse unterzogen werden. Angesichts der aktuellen Entwicklungen im Cloud-Bereich stellt sich für die meisten allerdings inzwischen nicht mehr die Frage, ob sie Cloud Computing nutzen sollen, sondern wie.

Die meisten Daten bleiben in Europa

Wo hat ihr Cloud-Dienstleister seinen Sitz?



Quelle: Forsa

Begriffsbestimmung: Private und Public Cloud Computing

Private Cloud Computing beschränkt sich auf eine bestimmte Nutzergruppe, die ihre Daten über ein Intranet oder ein VPN (Virtual Private Network) hochladen, austauschen und nutzen. Der Vorteil: Die Daten sind leicht verfügbar und die jeweiligen Nutzer behalten die volle Kontrolle über Daten und Dienste, was deren Sicherheit erhöht.

Beim **Public Cloud Computing** betreibt der Anbieter seine Dienste für alle Kunden auf der gleichen Infrastruktur, die über das öffentliche Internet zugänglich ist. Dies spart Kosten; zudem stehen den Nutzern durch den Cloud-Anbieter immer die neuesten Software-Versionen zur Verfügung. Datenschutzexperten empfehlen hier, Anbietern aus dem EU-Raum Vorzug zu geben.



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?



Quelle: Forsa

69 % 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

24 % können aktuelle Daten nicht wiederherstellen

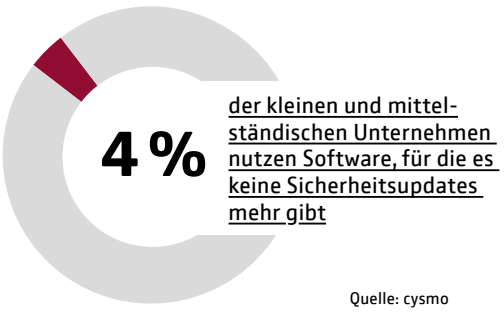
So sichern Sie Ihre Daten richtig

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.

Tickende Zeitbomben



4 % der kleinen und mittelständischen Unternehmen nutzen Software, für die es keine Sicherheitsupdates mehr gibt

Quelle: cysmo

Updates in der Warteschleife

Werden Sicherheitsupdates automatisch und zeitnah eingespielt?



Quelle: Forsa

12 % 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).

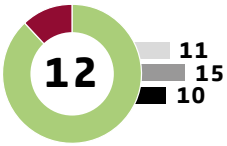
Der **Cyber-Sicherheits-check des GDV** unter www.gdv.de/cybercheck stellt Ihnen die wichtigsten Fragen rund um Ihre IT-Sicherheit. So finden Sie schnell heraus, wie sicher Ihre Systeme sind, wo Sie Schwachstellen haben und wie Sie diese schließen können. Ob Sie die zehn grundlegenden Anforderungen erfüllen,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

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

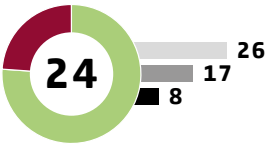
Kleinstunternehmen *Kleine Unternehmen* *Mittlere Unternehmen*

Selbsttest

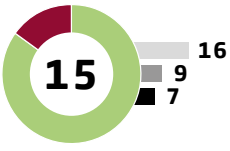
1. **Sicherheitsupdates automatisch und zeitnah einspielen und alle Systeme auf dem aktuellen Stand halten**
   Die meiste Software erhält regelmäßig Updates. Sie dienen oft dazu, bekannt gewordene Sicherheitslücken zu schließen. Das Installieren der Updates schützt die Systeme vor Angreifern.



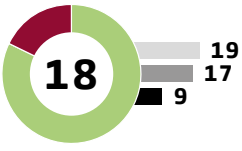
2. **Mindestens einmal wöchentlich Sicherungskopien machen**
   Daten und digitale Systeme können gezielt angegriffen, versehentlich gelöscht oder durch Hardware zerstört werden. Deshalb ist es dringend nötig, die vorhandenen Daten regelmäßig zu sichern. Grundsätzlich gilt: Je öfter Sie Ihre Daten sichern,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

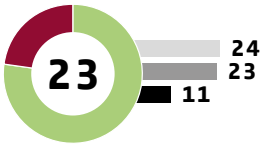


4. **Alle Systeme, die über das Internet erreichbar oder im mobilen Einsatz sind, zusätzlich schützen**
   Mobile Geräte können leicht verloren gehen oder gestohlen werden. Sind die darauf gespeicherten Daten nicht verschlüsselt, können sie vollständig ausgelesen werden – selbst wenn sie mit einem Passwort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



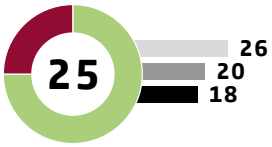
7. Sicherungskopien physisch vom gesicherten System trennen

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.



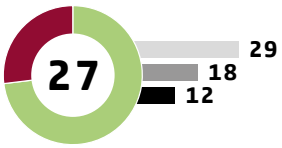
8. Mindestanforderungen für Passwörter (z.B. Länge, Sonderzeichen) verlangen und technisch erzwingen

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



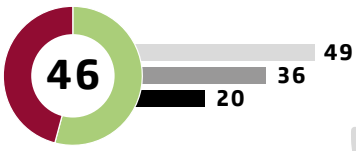
9. Jeden Nutzer mit eigener Zugangskennung und individuellem Passwort ausstatten

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.



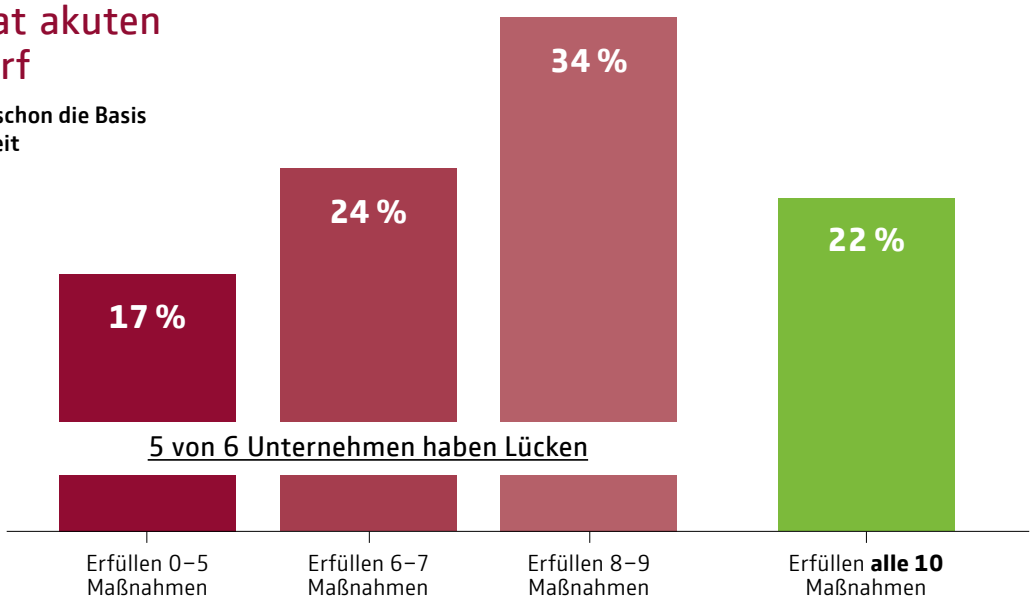
6–7
Über gute Ansätze kommt Ihre IT-Sicherheit leider nicht hinaus. Machen Sie es Cyberkriminellen nicht zu einfach und kümmern Sie sich möglichst schnell darum, Ihre Sicherheitslücken zu schließen.



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.:
Christoph Hardt

Redaktion:
Melina Maier, Christian Siemens

Bildnachweis:
S. 1: shutterstock/Rawpixel.com; S. 4/5: gettyimages/Tinpixels; S. 8: shutterstock/sdecoret; S. 12: shutterstock/fizkes; S. 16: shutterstock/chanchai howharn; S. 18: 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