Gesamtverband der Deutschen Versicherungswirtschaft e. V.

CYBER SICHER

Eine Initiative der deutschen Versicherer.

Ergebnisse einer Forsa-Befragung
Frühjahr 2018

Cyberrisiken im Mittelstand

GDV
DIE DEUTSCHEN VERSICHERER

Cyberrisiken und der deutsche Mittelstand

30 % berichten von wirtschaftlichen **Schäden** durch Cyberattacken → Seite 3

59 % der erfolgreichen Cyberangriffe erfolgten per **E-Mail** → Seite 4/5

43 % der betroffenen Unternehmen mussten den **Betrieb** zeitweise **stilllegen** → Seite 4/5

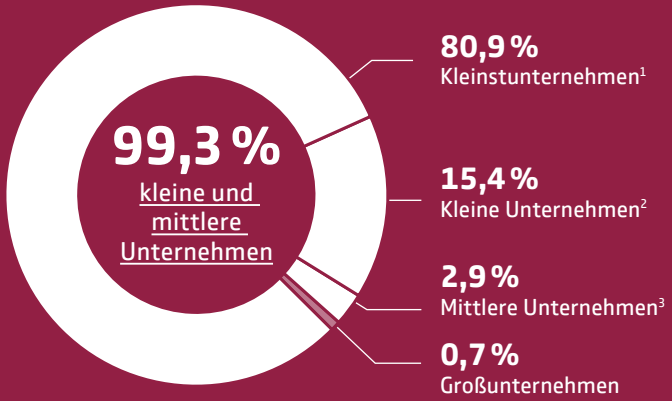
Interesse an Cyberversicherungen haben fast nur Unternehmen, die schon Opfer von Cyberattacken waren → Seite 6/7

67 % halten das **Cyberrisiko** für das eigene Unternehmen für eher oder sehr **gering** → Seite 6/7

73 % meinen, ihr Unternehmen sei **ausreichend** gegen Cyberrisiken **geschützt** → Seite 6/7

Je kleiner das Unternehmen, desto häufiger sind **Attacken erfolgreich** → Seite 8/9

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 2015

Fast jeder dritte Mittelständler war bereits Opfer von Cyberangriffen

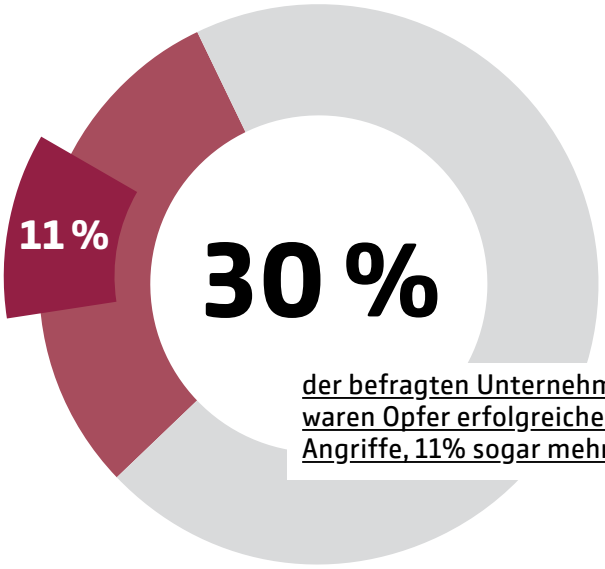
Die Gefahr von Cyberattacken ist im deutschen Mittelstand längst Alltag, doch die Abwehrbemühungen der Unternehmen halten mit der wachsenden Gefahr nicht Schritt. Das zeigt die aktuelle Forsa-Umfrage zu „Cyberrisiken im Mittelstand“ im Auftrag des Gesamtverbandes der Deutschen Versicherungswirtschaft.

Mehr als 99 Prozent der deutschen Unternehmen zählen zum Mittelstand - und die Bedrohung dieser kleinen und mittleren Unternehmen durch Cyberangriffe wächst: 30 Prozent haben durch Attacken von Cyberkriminellen bereits wirtschaftliche Schäden erlitten. Jeder zehnte Mittelständler (11 Prozent) ist sogar schon mehrfach Opfer geworden. Zudem hat das Problem in der jüngsten Zeit offenbar nochmals deutlich zugenommen: Rund drei Viertel der berichteten Angriffe haben sich den Angaben der Befragten zufolge innerhalb der vergangenen zwei Jahre ereignet, bei vier von zehn Betroffenen stand der Betrieb nach einem Angriff zeitweise still (siehe Seite 4).

Die aktuelle Umfrage zeigt aber auch: Obwohl vielen mittelständischen Unternehmern das allgemeine Risiko bewusst ist, wird die Gefahr für das eigene Unternehmen weiterhin unterschätzt. Zu oft setzen Unternehmer bei der Prävention auf das „Prinzip Hoffnung“ (siehe Seite 6/7), zu viele Kleinst- und Kleinunternehmer geben sich der trügerischen Hoffnung hin, dass ihr eigenes Unternehmen zu klein sei, um ins Visier von Cyberkriminellen zu geraten. Ein gefährlicher Irrglaube – der dazu führt, dass ausgerechnet die kleinsten Unternehmen die meisten erfolgreichen Cyberangriffe beklagen (siehe Seite 8/9).

Drei von zehn Unternehmen bereits betroffen

Wurde Ihr Unternehmen durch Cyber-Angriffe geschädigt?



Über die Umfrage „Cyberrisiken im Mittelstand 2018“

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 5. März und dem 6. April 2018 statt.

Größtes Einfallstor für Cyberattacken sind E-Mails

Das E-Mail-Postfach ist für viele Unternehmen die wichtigste digitale Schnittstelle zu Kunden und Lieferanten. Cyberkriminelle nutzen aus, dass die elektronische Post samt Anhängen zu oft gedankenlos geöffnet wird – und legen mit ihrer Schadsoftware nicht nur die IT-Systeme, sondern ganze Betriebe lahm.

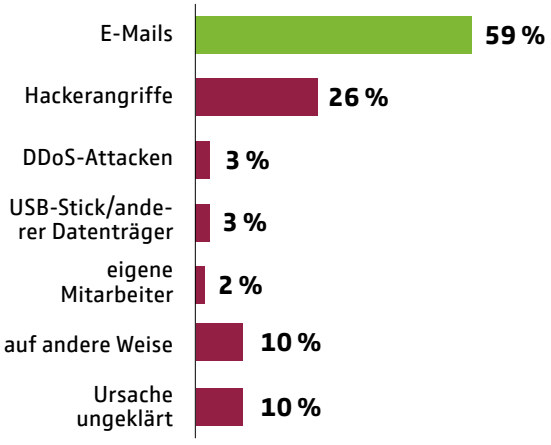
Hintertüren in Spezial-Software nutzen? Passwörter ausspähen? Tastaturanschläge mitschneiden? Müssen Cyberkriminelle nicht. Bei vielen kleinen und mittelständischen Unternehmen reicht es vollkommen aus, ganz einfach Schadsoftware per Mail zu verschicken. Fast 60 Prozent aller erfolgreichen Angriffe trafen über das E-Mail-Postfach der Unternehmen ins Ziel. Nur bei 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 rechts). Dann – und das ist die gute Nachricht – könnten die meisten Angriffe per Mail relativ leicht rechtzeitig erkannt und das Öffnen gefährlicher Software verhindert werden.

Hat schädliche Software erst einmal die Unternehmens-IT befallen, wird man sie ohne die Hilfe externer Experten kaum wieder los. Fast 60 Prozent aller Attacken führten dementsprechend zu Kosten für die Aufklärung des Angriffs und für die Wiederherstellung der Daten. Je länger das dauert und je abhängiger der Betrieb von einer funktionierenden IT ist, desto wahrscheinlicher ist es auch, dass der Betrieb nach einer Cyberattacke länger stillsteht – 43 Prozent der befragten Opfer von Cyberattacken berichten von entsprechenden Kosten. Und: Zukünftig dürften die Folgekosten eines Cyberangriffs durch das neue europäische Datenschutzrecht (siehe Seite 10) weiter steigen.

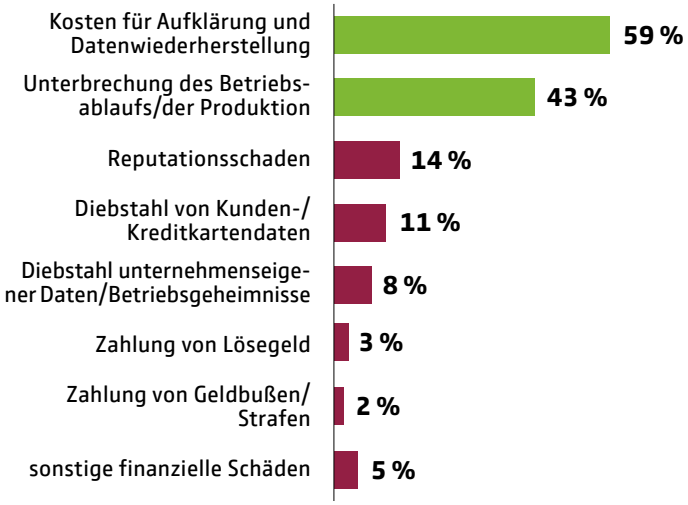
Die Einfallstore

Erfolgreiche Cyberangriffe erfolgten durch … [1]



Die Schäden

Die Attacken führten zu wirtschaftlichen Schäden 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 Betriebssystem 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.

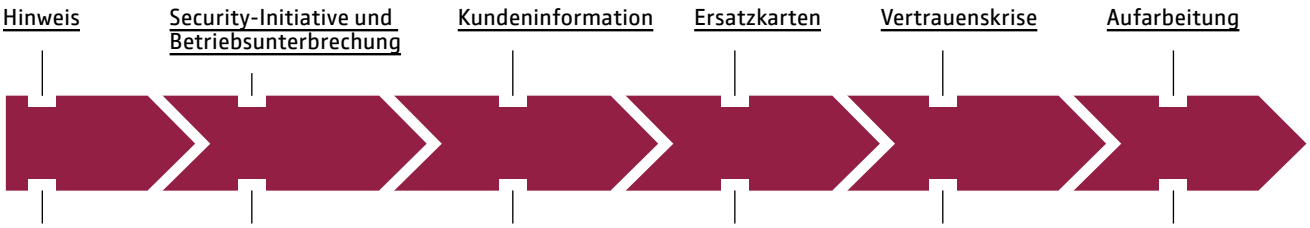
4. Vor dem Öffnen: Prüfen Sie Absender und Betreff
Cyberkriminelle verstecken sich gern hinter seriös wirkenden Absenderadressen. Ist Ihnen der Absender der Mail bekannt? Und wenn ja: Ist der Absender wirklich echt? Achten Sie auf kleine Fehler in der Schreibweise oder ungewöhnliche Domain-Angaben hinter 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.

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

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



Kreditkartenunternehmen weist Shop-Betreiber auf möglichen Datendiebstahl hin.

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

✓ *Kosten für IT-Forensik: 40.000 Euro*

Der Online-Shop bleibt währenddessen geschlossen.

✓ *Kosten für Betriebsunterbrechung: 50.000 Euro*

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

✓ *Informationskosten: 80.000 Euro*

Alle potenziell betroffenen Kunden erhalten neue Kreditkarten.

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

✓ *Krisenkommunikation: 30.000 Euro*

Der Umsatzrückgang ist nicht gedeckt

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

✓ *Vertragsstrafen: 50.000 Euro*

Prinzip Hoffnung

Im deutschen Mittelstand regiert das Prinzip Hoffnung – zumindest was die Einschätzung von Cyberattacken angeht. Zwar wird von einer deutlichen Mehrheit der Befragten das Cyberrisiko für mittelständische Unternehmen durchaus hoch und damit realistisch eingeschätzt. Dass sie selbst einmal Opfer von Cyberkriminalität sein könnten, blenden viele jedoch aus.

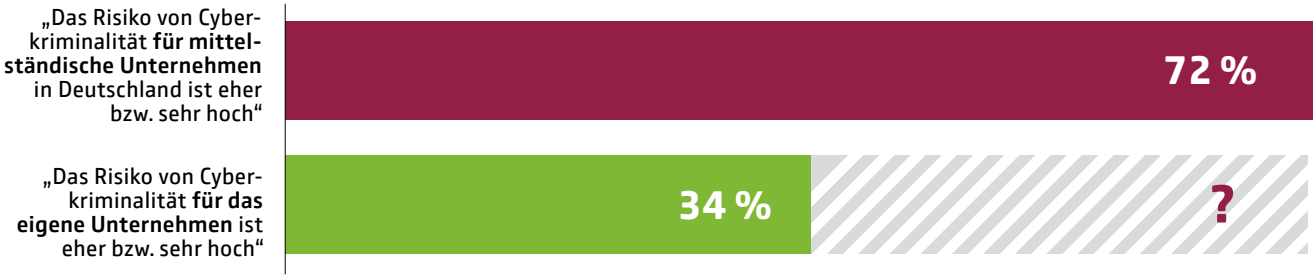
Den meisten Unternehmern sind die möglichen Folgen eines Cyberangriffs durchaus bewusst: Zwei Drittel der Befragten bestätigen eine sehr hohe Abhängigkeit von der eigenen IT und gehen bei einem mehrtägigen IT-Ausfall von starken Einschränkungen für ihr Geschäft aus. Doch diese düstere Aussicht kann den Optimismus in den Unternehmen nicht erschüttern. Das Vertrauen in die bestehenden Schutzmaßnahmen ist hoch. Fast drei Viertel halten sie für vollkommen ausreichend, jeder zweite Unternehmer will seine IT-Sicherheit in naher Zukunft auch nicht weiter ausbauen. Dabei zeigt sich, dass es durchaus Potenzial zur Verbesserung gäbe – viele Unternehmen müssten den Zugang zu ihren Geräten ebenso wie ihre sensiblen Daten besser schützen.

Ebenso noch gering ausgeprägt ist in den meisten Unternehmen das Interesse an einer Cyberversicherung – zumindest dort, wo Cyberkriminelle bislang noch nicht zugeschlagen haben. Nur wer bereits eine erfolgreiche Attacke erlebt hat, denkt in aller Regel anders – fast die Hälfte der Betroffenen denkt ernsthaft über eine Cyberpolice nach oder hat die Versicherung bereits abgeschlossen. Dabei müssten IT-Sicherheit und Versicherungsschutz in allen Unternehmen Hand in Hand gehen, mahnt Peter Graß, Cyberversicherungs-Experte des GDV: „Wenn Sie am Rhein wohnen, sollten Sie sowohl in Hochwasserschutz investieren als auch Ihr Haus gegen eine Überschwemmung versichern. Dasselbe gilt auch für Cyberattacken."

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 Back-up 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 Back-up nicht mit Ihrem Hauptsystem verbunden ist – weder über Kabel noch über das WLAN.
Was noch? Testen Sie regelmäßig, ob sich die Daten Ihrer Back-ups im Ernstfall auch wirklich wiederherstellen lassen.

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

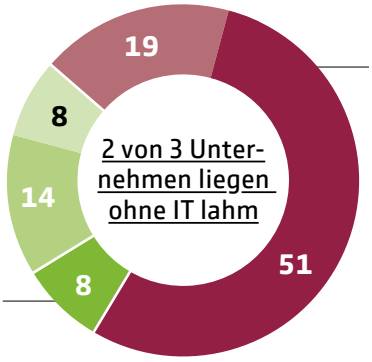


Eine nicht funktionierende Unternehmens-IT legt schnell auch die meisten Betriebe lahm

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

- *nicht eingeschränkt*
- *nur wenig eingeschränkt*
- *nicht so stark eingeschränkt*
- *eher stark eingeschränkt*
- *sehr stark eingeschränkt*

Nur 8 % geben an, dass Ihr Unternehmen ohne IT gar nicht eingeschränkt wäre.

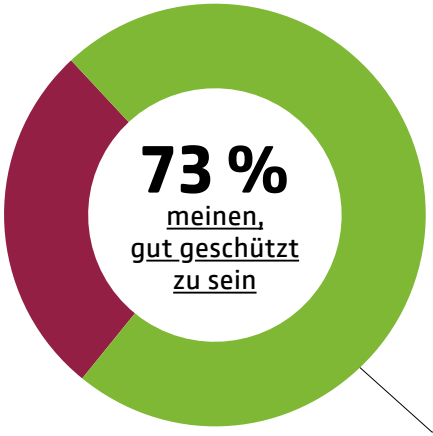


70 % wären ohne funktionierende Unternehmens-IT eher oder sehr stark eingeschränkt.

Das hohe Vertrauen in den eigenen Schutz …

Ist das eigene Unternehmen ausreichend gegen Cyberkrimninalität geschützt?

- *Ja*
- *Nein, Unternehmen müsste mehr tun*

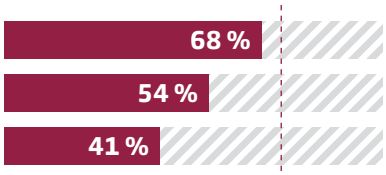


… hält einem genaueren Blick oft nicht stand:

Aktuelle Virenscanner und Firewalls haben fast alle …

- 97 % nutzen Virenscanner und Firewalls
- 94 % installieren Sicherheitsupdates automatisch
- 84 % erstellen systematisch Backups

… aber nur:

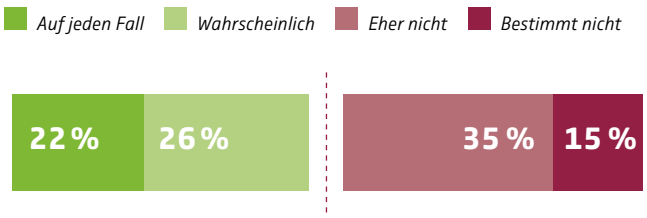


- 68 % vergeben für jeden Mitarbeiter einen eigenen, passwortgeschützten Zugang
- 54 % verschlüsseln sensible Daten
- 41 % verbieten die Nutzung privater Geräte* in der Unternehmens-IT

* z. B. Smartphones oder USB-Sticks

Trügerische Sicherheit führt zu geringer Investitionsbereitschaft in IT-Sicherheit

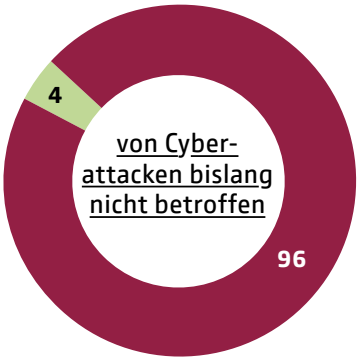
Wollen Sie in den kommenden zwei Jahren in weitere Schutzmaßnahmen gegen Cyberkriminalität investieren?
An 100 % fehlende Angaben: „weiß nicht".

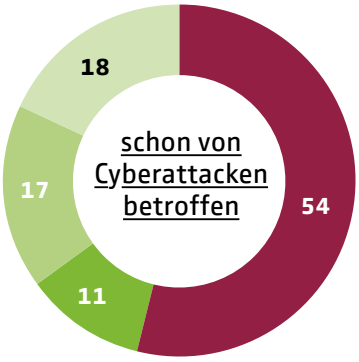


Aus Schaden klüger?

Hat Ihr Unternehmen eine Cyberversicherung abgeschlossen oder interessiert sich für einen Abschluss?
Angaben in Prozent.

- *Nicht bekannt / Nicht interessant*
- *Interessant*
- *Abschluss geplant*
- *Versicherung abgeschlossen*





Fehleinschätzung mit Folgen

Cyberkriminellen kommt es auf die Größe ihrer Opfer in aller Regel nicht an. Trotzdem gibt es einen Zusammenhang zwischen der Unternehmensgröße und der Gefahr erfolgreicher Cyberattacken.

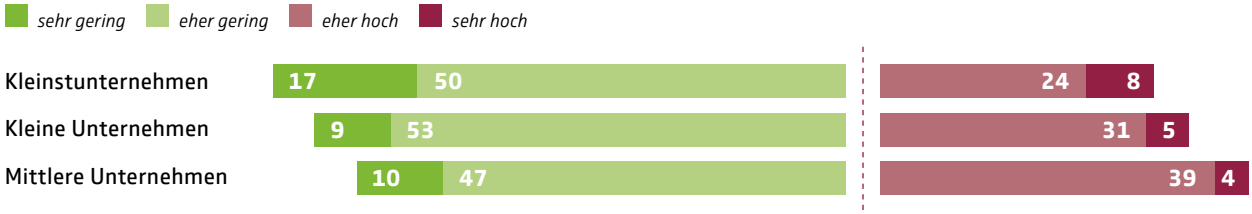
Das Ergebnis überrascht: Gerade die kleinsten Unternehmen berichten überdurchschnittlich oft von erfolgreichen Cyberattacken und werden auch häufiger nicht nur einmal, sondern mehrmals Opfer von Cyberkriminellen. Haben die Gangster es also vor allem auf die Kleinsten abgesehen? Eher nicht. Die Ergebnisse der Forsa-Umfrage legen einen anderen Schluss nahe. Zu viele halten ihr Unternehmen schlicht für zu klein oder ihre Daten für nicht interessant genug, um angegriffen zu werden. Doch wer so denkt, hat noch nicht wirklich verstanden, wie Cyberkriminelle vorgehen. Für massenhaft versuchte und ungezielte Attacken spielen Umsatz- oder Mitarbeiterzahlen genauso wenig eine Rolle wie die Brisanz der gespeicherten Daten. Alle Unternehmen, die in irgendeiner Form am Netz hängen, werden angegriffen. Und auch die vermeintlich langweiligsten Daten haben ihren Wert – mindestens für diejenigen, deren Daten nach einer Ransomware-Attacke plötzlich gesperrt sind.

Auf die Fehleinschätzung des Risikos folgen bei vielen kleinen Unternehmen Fehlentscheidungen bei der Prävention. Wer seinen Schutz an der gefühlten statt an der tatsächlichen Gefahr ausrichtet,

Je kleiner das Unternehmen, …

… desto geringer wird das eigene Risiko eingeschätzt:

Das Risiko von Cyberkriminalität für das eigene Unternehmen ist …
(Angaben in Prozent; an 100 % fehlende Angaben: „weiß nicht“)



71 % der Kleinst- und 48 % der Kleinunternehmen, die nur ein geringes Cyberrisiko sehen, **halten ihr Unternehmen für zu klein**, um in den Fokus von Cyberkriminellen zu geraten.

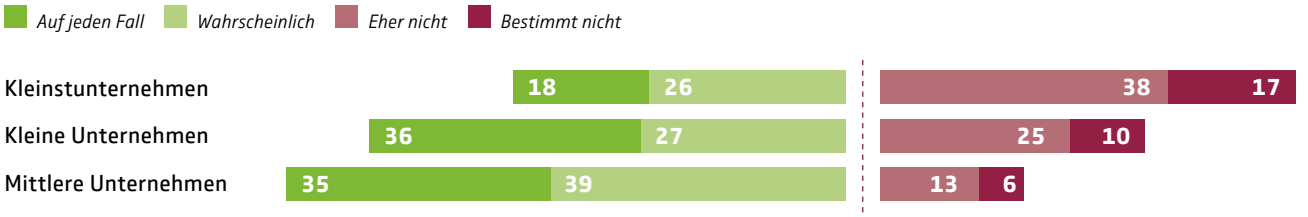
… desto besser wird der eigene Schutz eingeschätzt:

Ist das eigene Unternehmen ausreichend gegen Cyberkrimninalität geschützt?

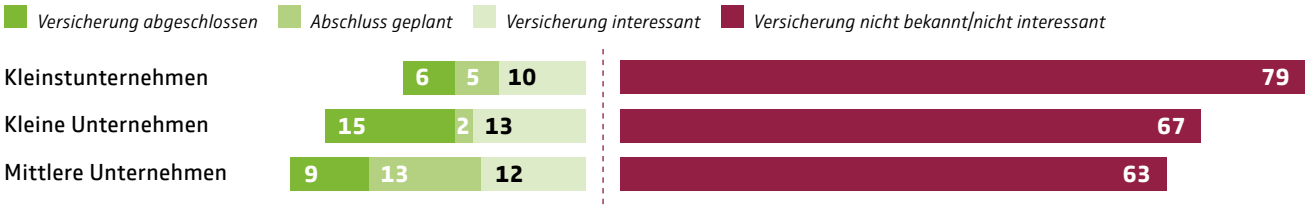
wähnt sich schon mit Virenscanner und Firewall ausreichend geschützt. Zu oft sind kleine Unternehmer von ihren Sicherheitsmaßnahmen überzeugt, zu gering ist ihre Bereitschaft, in Cybersicherheit zu investieren. Als Ergebnis ihrer digitalen Sorglosigkeit sind sie für Cyberkriminelle ein leichtes Ziel. Häufiger getroffen von den Cyberattacken werden viele Kleinstunternehmen ganz einfach deshalb, weil sie den Angreifern den geringsten Widerstand entgegensetzen.

… desto geringer ist die Investitionsbereitschaft in IT-Sicherheit und Versicherungsschutz:

Wollen Sie in den kommenden zwei Jahren in weitere Schutzmaßnahmen gegen Cyberkriminalität investieren?
Angaben in Prozent; an 100 % fehlende Angaben: „weiß nicht".

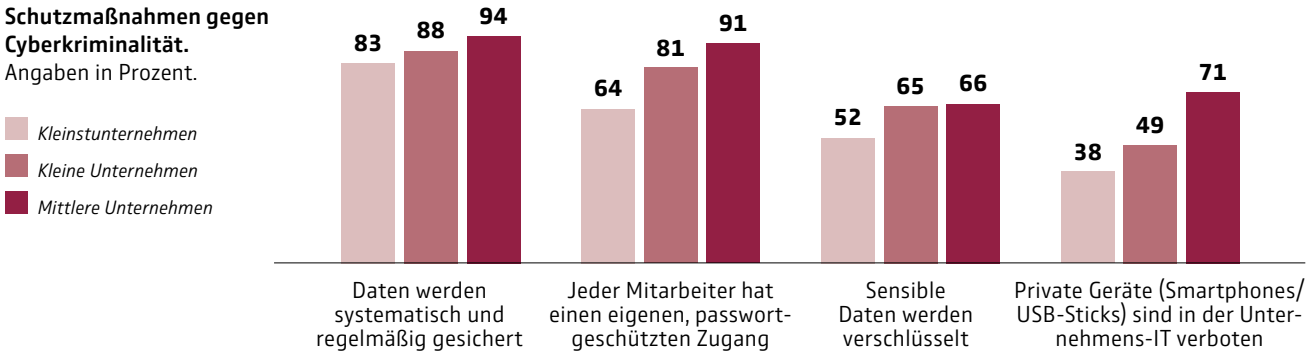


Abschluss einer Cyberversicherung?
Angaben in Prozent; an 100 % fehlende Angaben: „weiß nicht".

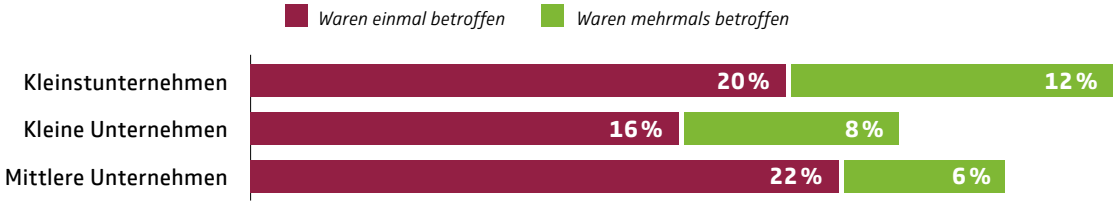


… desto schlechter ist der tatsächliche Schutz vor IT-Risiken:

Schutzmaßnahmen gegen Cyberkriminalität.
Angaben in Prozent.



… desto anfälliger sind Unternehmen auch für mehrfache Cyberangriffe:



Jeder zweite Mittelständler nicht auf neues Datenschutzrecht vorbereitet

Ab dem 25. Mai 2018 gelten mit der EU-Datenschutzgrundverordnung (DSGVO) für alle Unternehmen mit Niederlassung in der EU neue Datenschutzregeln. In der Praxis dürften fast alle Betriebe davon betroffen sein, doch viele deutsche Mittelständler sind noch völlig planlos.

Die Mehrheit der kleinen und mittleren Unternehmen nimmt den Datenschutz noch immer auf die leichte Schulter: 36 Prozent der kleinen und mittleren Unternehmen (KMU) haben von den neuen Datenschutzregeln noch nicht einmal etwas gehört. Ein Fünftel weiß zwar davon, hat sich aber noch nicht darauf vorbereitet. Nur jeweils 22 Prozent der KMU haben sich auf die Scharfschaltung der EU-Datenschutzgrundverordnung vorbereitet oder wollen noch Änderungen umsetzen.

Als Gründe für die ausgebliebene Vorbereitung nennen die KMU vor allem mangelndes Wissen, zu wenig Zeit und geringe Relevanz des Datenschutzes. Je kleiner die Betriebe, desto weniger sind die Unternehmen vorbereitet: So ist 38 Prozent der Kleinstunternehmen nicht bekannt, dass sich das Datenschutzrecht ändert. Von den mittleren Unternehmen haben hingegen lediglich 13 Prozent nichts von der EU-DSGVO gehört.

Die wichtigsten Neuerungen der EU-DSGVO

→ Für Unternehmen gelten künftig umfangreichere Informationspflichten. Zum Beispiel müssen die meisten Unternehmen für die Aufsichtsbehörden ein Verzeichnis anlegen, in dem sie Ihre Verarbeitungstätigkeiten dokumentieren.

→ Völlig neu ist die sogenannte Datenschutzfolgeabschätzung, die vor allem auf Unternehmen zukommt, die besonders viele oder sensible Daten verarbeiten.

→ Künftig gelten neue Grenzen, ab der Unternehmen einen Datenschutzbeauftragten stellen müssen.

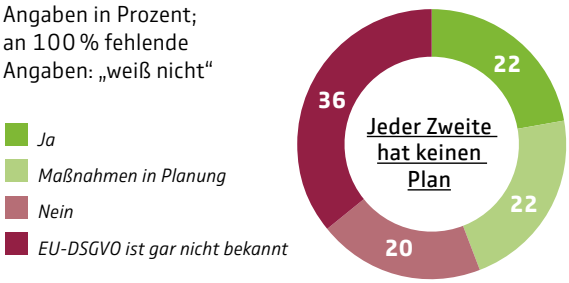
→ Die Meldepflichten für den Fall, dass personenbezogene Informationen in unbefugte Hände geraten, werden mit der EU-DSGVO verschärft.

→ Die Unternehmen müssen auch technisch aufrüsten. Im Zweifel sollten Betriebe künftig mehr als nötig in ihre IT-Sicherheit investieren, um im Ernstfall von den Aufsichtsbehörden nicht für Versäumnisse belangt werden zu können.

→ Die Missachtung der Datenschutzvorschriften wird künftig härter sanktioniert. So drohen Geldstrafen in Höhe von bis zu vier Prozent des Jahresumsatzes oder bis maximal 20 Mio. Euro.

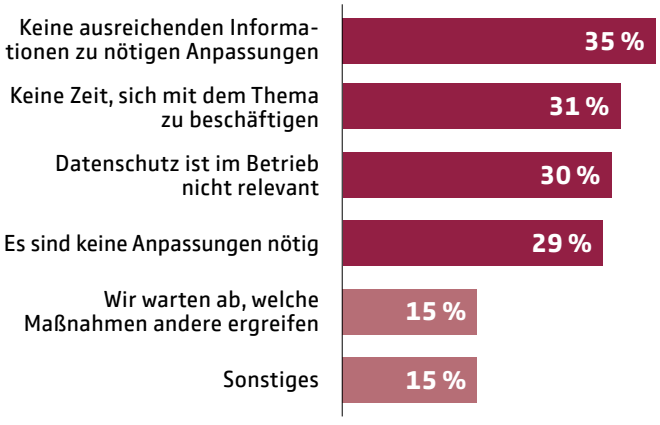
Überwiegend planlos

Haben Sie bereits Vorbereitungen zum neuen EU-Datenschutzrecht getroffen?
Angaben in Prozent; an 100 % fehlende Angaben: „weiß nicht“



Keine Ahnung, keine Zeit, keine Relevanz

Warum haben Sie bislang keine Vorbereitungen für die neue EU-DSGVO getroffen?[1]



1 Mehrfachnennungen möglich

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:
Henning Engelage
Hardy Herlt
Christian Siemens

Bildnachweis:
S. 1: iStock Photos / matejmo

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