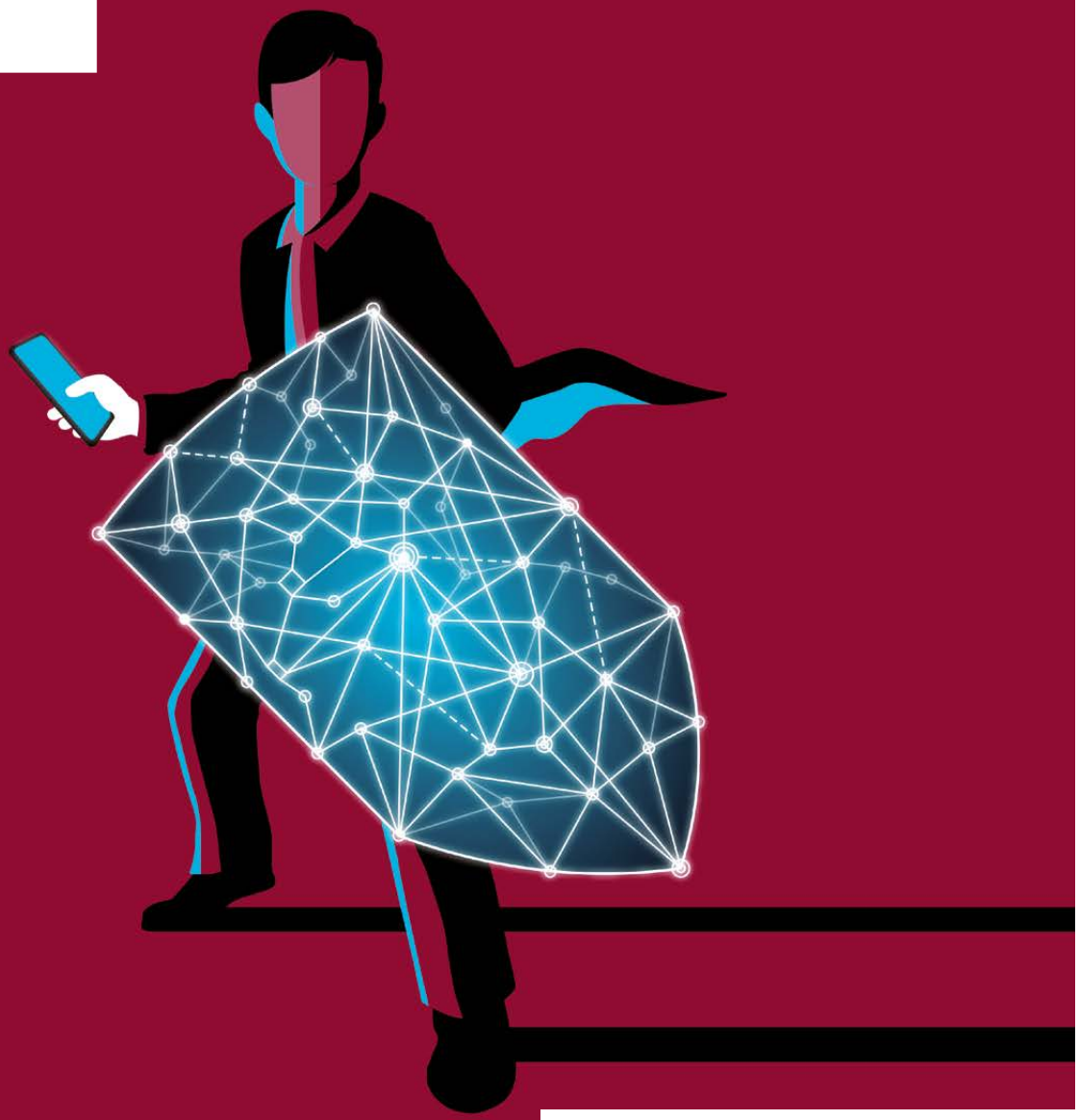
Gesamtverband der Deutschen Versicherungswirtschaft e. V.

CYBER SICHER

Eine Initiative der deutschen Versicherer.

VdS Quick-Check Cyber Security

Lagebericht Cyberschutz 2019



VdS

GDV DIE DEUTSCHEN VERSICHERER

Inhalt

Über den VdS Quick-Check Cyber Security

Der kostenlose Quick-Check Cyber Security der VdS Schadenverhütung GmbH richtet sich speziell an kleine und mittelständische Unternehmen. Das Online-Tool leitet durch 39 Fragen aus vier verschiedenen Handlungsfeldern der Informationssicherheit: Organisation, Technik, Prävention und Management. In der Bilanz erhalten die teilnehmenden Unternehmen den Status Quo ihres Schutzniveaus, einen Überblick über die besonderen Schwachstellen und Empfehlungen, wie sie etwaige Sicherheitslücken schließen können.

Hier geht es zum Online-Tool: **www.vds-quick-check.de**

Cyber-Sicherheit ist die Voraussetzung für eine erfolgreiche Digitalisierung

Täglich beobachtet das Bundesamt für Sicherheit in der Informationstechnik neue Cyber-Angriffe auf deutsche Institutionen. Diese betreffen – entgegen der häufigen vorzufindenden Annahme – jedoch nicht nur Großkonzerne: Kleine und mittlere Unternehmen geraten ebenso häufig in das Visier der Täter. Schließlich zeichnet sich die Unternehmenslandschaft in Deutschland durch einen starken Mittelstand und die große Anzahl an Hidden Champions aus, die zwar nur selten im Fokus der Öffentlichkeit stehen, gleichzeitig jedoch immenses Know-how vorhalten, das für Angreifer interessant ist. Insbesondere vor Bedrohungsszenarien mit Verschlüsselungs-Software (Ransomware) musste das BSI in den vergangenen Monaten immer wieder warnen. Infektionen mit dem von der Schadsoftware Emotet nachgeladenen Verschlüsselungstrojaner Ryuk etwa legten zuletzt zahlreiche Unternehmen lahm. Bestenfalls waren die Betroffenen auf derartige Notfälle vorbereitet, in einigen Fällen kam es jedoch zu existenzbedrohenden Datenverlusten, die mitunter zur Insolvenz führten.

Vor diesem Hintergrund beobachten wir die Initiative des VdS, mit dem Quick-Check Cyber Security das Cyber-Sicherheitsniveau in deutschen KMU zu untersuchen, seit mehreren Jahren mit großem Interesse – schließlich erhalten Teilnehmende wertvolle Anhaltspunkte dafür, wie der eigene Umsetzungsstand einzuordnen ist.

Bereits jetzt kann anhand der Ergebnisse festgehalten werden, dass immer mehr Unternehmen aus den Cyber-Bedrohungen der vergangenen Jahre lernen – etwa am Anteil derer, die Anweisungen für den Ernstfall definiert haben. Seit 2016 ist in diesem Bereich eine Steigerung um nahezu 20% zu erkennen – auch wenn der aktuelle Prozentsatz von 57% immer noch viel zu gering ist. Gerade hier sieht das BSI eine der Kernkompetenzen zum Schutz vor Cyber-Angriffen: Wer weiß, was bei einem Angriff zu tun ist, kann im Ernstfall routiniert auf das Geschehen einwirken. In der Praxis hat sich bereits der BSI-Standard 100-4 bewährt, der demnächst in einer überarbeiteten Fassung erscheinen wird. Generell finden Anwender hilfreiche Handlungsempfehlungen zur Erhöhung des Cyber-Sicherheitsniveaus im BSI IT-Grundschutz. Dass diese Reihe und KMU in keinem Widerspruch stehen, zeigen auch die zahlreichen neuen IT-Grundschutzprofile, die das BSI gemeinsam mit verschiedenen Branchenverbänden entwickelt hat. Hier finden zum Beispiel Handwerksbetriebe und Reedereien Blaupausen für die Umsetzung von Cyber-Sicherheitsmaßnahmen. Weitere Profile sind bereits in Arbeit – Interessierte können sich gerne beteiligen. Mit Angeboten wie diesen nimmt das BSI als nationale Cyber-Sicherheitsbehörde eine Vorreiterrolle bei der Gestaltung von Cyber-Sicherheit in der deutschen Wirtschaft und in der Gesellschaft im Allgemeinen ein. Diese beschränkt sich nicht nur auf präventive Sicherheitskonzepte, sondern beinhaltet auch Maßnahmen zur Detektion von und Reaktion auf Cyber-Angriffe. Unternehmen möchte ich in diesem Zusammenhang eine Registrierung bei der Allianz für Cyber-Sicherheit nahelegen. Neben dem Austausch mit anderen Unternehmen zu konkreten Themen der Cyber-Sicherheit stellen wir den Mitgliedern eine Vielzahl an Informationen, Handlungsempfehlungen und Warnmeldungen zur Verfügung, mit denen Sie das Schutzniveau des Unternehmens verbessern können.

Die rasante Digitalisierung in allen Lebensbereichen ist sowohl Chance als auch Herausforderung. Neben den zahlreichen neuen Möglichkeiten darf das Bedrohungspotenzial durch Cyber-Angriffe nicht außer Acht gelassen werden. Denn nur hinreichend geschützte Unternehmen werden sich in Zukunft gegenüber immer raffinierteren Angriffsmethoden aus dem Cyber-Raum behaupten können. Cyber-Sicherheit wird somit zum Enabler für die Unternehmen und zum Schlüssel für den Wohlstand in Deutschland.

Ich möchte Sie daher dazu ermuntern, den Maßnahmenkatalog Ihrer Institution beim Lesen dieser Broschüre kritisch zu hinterfragen. Sicherlich finden auch Sie noch Anhaltspunkte, um das Schutzniveau weiter zu optimieren. Gleichzeitig danke ich VdS und GDV, die mit dem Quick-Check wertvolle Arbeit leisten, um KMU auf die Herausforderungen der Cyber-Sicherheit aufmerksam zu machen.

Arne Schönbohm
Präsident, Bundesamt für Sicherheit in der Informationstechnik

Für Hacker gibt es kein zu klein

Schnelle Prozesse, neue Dienstleistungen, mehr Flexibilität – das ist die helle Seite der Digitalisierung. Doch es gibt auch die dunkle Seite. Massive Datendiebstähle, geleakte Passwörter und lahmgelegte IT-Systeme beunruhigen Wirtschaft, Politik und Gesellschaft. Immer klarer wird: Wir werden die Chancen und Möglichkeiten der Digitalisierung nur dann nachhaltig nutzen können, wenn wir auch ihre Risiken ernst nehmen und eindämmen.

Die erste Voraussetzung für einen besseren Schutz ist also, die Gefahr nicht zu unterschätzen. In großen Unternehmen und im globalen Maßstab ist man hier schon sehr weit. Viele Mittelständler glauben hingegen, sie seien zu klein, zu unwichtig oder zu uninteressant, um das Interesse der Cyberkriminellen zu wecken. Das ist eine fatale Fehleinschätzung, denn für Hacker gibt es kein zu klein. Die Ergebnisse des VdS Quick Checks zeigen: Allmählich setzt sich diese Erkenntnis auch bei kleinen und mittleren Unternehmen durch. Ein Anfang ist also gemacht – jetzt gilt es, die IT-Sicherheit und die Risikokultur auf allen Ebenen weiter zu stärken.

Die deutsche Versicherungswirtschaft engagiert sich intensiv beim Kampf gegen und Schutz vor Cyberkriminalität. Versicherer sorgen für Prävention, indem sie die Prozesse zur Cybersicherheit ihrer Kunden abfragen, auf Sicherheitslücken hinweisen und – falls notwendig – vor dem Abschluss einer Versicherung technische und organisatorische Änderungen bei der Cybersicherheit der Unternehmen einfordern. So tragen wir dazu bei, den Standort Deutschland und jeden hier tätigen kleinen und mittelständischen Unternehmer zu stärken.

Dr. Wolfgang Weiler
Präsident des GDV

Im Mittelstand herrscht Handlungsbedarf

Seit nunmehr fünf Jahren führen wir die VdS Quick-Checks für kleine und mittelständische Unternehmen (KMU) durch. Mit den Daten von über 5.000 teilnehmenden Firmen hat sich unsere Auswertung als eine der größten Untersuchungen über das Niveau der IT-Sicherheit in Deutschland etabliert.

Durch die Differenzierung der vier Handlungsfelder Organisation, Technik, Prävention und Management ergibt sich ein valides Bild, in welchen Bereichen deutsche Unternehmen gut aufgestellt sind und in welchen Feldern am meisten Handlungsbedarf besteht.

Die diesjährigen Auswertungen zeigen nach einer langen Phase des Stillhaltens einen deutlich positiven Trend. Das Problembewusstsein für IT-Sicherheit in mittelständischen Unternehmen schärft sich zunehmend. Immer mehr Mittelständler arbeiten aktiv daran, den Widerstandsgrad ihrer IT-Landschaften systematisch zu erhöhen.

Dennoch: Trotz dieser spürbaren Bemühungen und Verbesserungen ist der Cyber-Schutz in vielen Teilbereichen noch immer nicht auf einem angemessen hohen Niveau. So sind präventive Maßnahmen für den Ernstfall bei mehr als der Hälfte der Unternehmen noch immer nicht vorhanden. Auch beim Thema Cloud Computing und IT-Outsourcing haben 60 Prozent keine angemessenen Maßnahmen formuliert.

Um das insgesamt noch zu schwache Schutzniveau weiter zu verbessern, werden wir unseren Anspruch, den Mittelstand beim Thema Cyber-Security mit bedarfsgerechten Angeboten zu unterstützen, weiterhin tatkräftig vorantreiben.

Dr. Robert Reinermann
Geschäftsführer des VdS

Luft nach oben

Die gute Nachricht vorweg: Mit der IT-Sicherheit im deutschen Mittelstand geht es aufwärts. Wie die aktuellen Ergebnisse des VdS Quick-Checks Cyber Security zeigen, haben sich die kleinen und mittleren Unternehmen gleich auf mehreren zentralen Feldern verbessert. Immer mehr Firmen benennen konkrete Verantwortliche für die IT-Sicherheit, implementieren Zugangs- und Datenschutzkonzepte, regeln den Umgang mit mobilen Geräten und Datenträgern, regulieren die private Nutzung der Unternehmens-IT und sensibilisieren ihre Mitarbeiter für die Gefahren aus dem Netz. Auch die Datensicherung hat sich weiter professionalisiert: Regelmäßige Backups gehören fast überall zum Alltag, und mittlerweile werden die Sicherungskopien zumeist auch sicher aufbewahrt und regelmäßig getestet. Das ist wichtig, denn der Notfall ist der schlechteste Zeitpunkt um festzustellen, dass eine Datensicherung fehlerhaft ist.

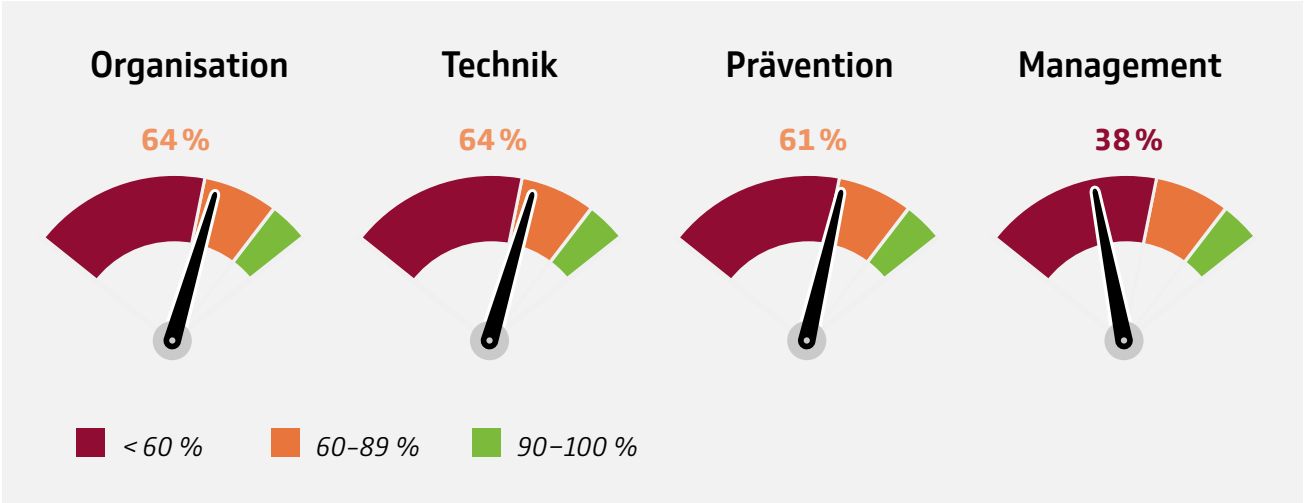
Dennoch: Es bleibt viel zu tun. Fast die Hälfte der Unternehmen gibt an, dass die IT-Sicherheit bei ihnen keineswegs Chefsache sei.

Informationssicherheit muss Chefsache sein

Viele Unternehmen, die ihre Verantwortung für ihre Daten und IT-Systeme an Dritte oder in die Cloud outsourcen, haben ihren Dienstleistern überhaupt keine konkreten Sicherheitsanforderungen auferlegt. Bei einem Drittel der Teilnehmer ist immer noch nicht klar geregelt, wer für die Sicherheit der Unternehmensdaten eigentlich verantwortlich ist. Die Folgen: Niemand hat einen genauen Überblick, wer wo wann welche Daten speichert und wie diese geschützt sind. Es gibt keine regelmäßigen Risiko-Analysen. Fehlende Notfallpläne lassen für den Ernstfall chaotische Zustände und unnötig lange Ausfallzeiten der IT-Systeme erwarten.

Im Ergebnis ist der Mittelstand trotz aller Verbesserungen noch in keinem einzigen der vier Handlungsfelder des VdS Quick-Checks im grünen Bereich. Erst wenn dieses Ziel erreicht ist, kann und wird es den kleinen und mittleren Unternehmen in Deutschland gelingen, den hochprofessionellen und gut organisierten Cyberkriminellen wirksam und dauerhaft Paroli zu bieten.

Die Ergebnisse im Überblick



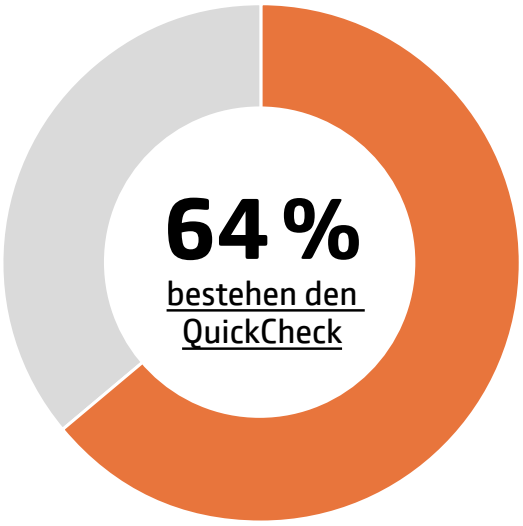
Organisation

In einem idealen Unternehmen gilt:

- → IT-Sicherheit ist Chefsache.
- → Die Verantwortlichkeiten sind klar definiert.
- → Die geltenden Regeln sind schriftlich fixiert.
- → Alle Mitarbeiter und Dienstleister wissen zu jedem Zeitpunkt, wie sie mit der IT und den Daten des Unternehmens umgehen müssen.
- → Zugang zu den IT-Systemen bekommt nur, wer ihn wirklich braucht und nur im jeweils erforderlichen Umfang.

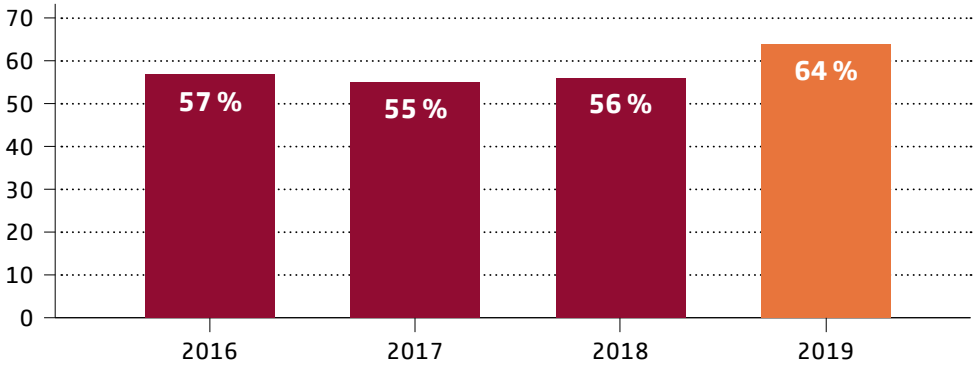
Ergebnis

Trotz Verbesserung zum Vorjahr besteht im Teilbereich „Organisation“ weiterhin Nachholbedarf. Eine schriftliche Verpflichtung des Top-Managements für die Gesamtverantwortung der Informationssicherheit liegt nur bei rund der Hälfte der Unternehmen vor. Deutlich verbessert hat sich die Sensibilisierung und Verpflichtung der Mitarbeiter zu Fragen der IT-Sicherheit. Auch das Management der Zugänge haben viele der teilnehmenden Unternehmen gut im Griff.



90–100 % 60–89 % < 60 %

Tendenz



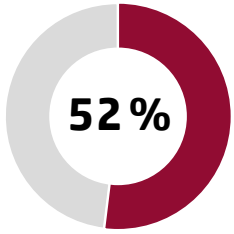
Tendenz: positiv

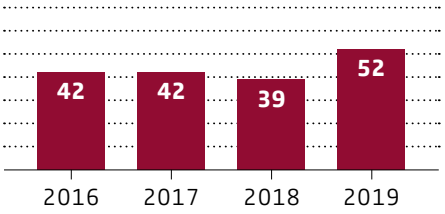
In der Realität zeigen sich in vielen Unternehmen diese Probleme:

→ Keine Chefsache, keine klaren Verantwortlichkeiten

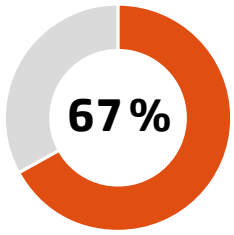
Damit IT-Sicherheit im Unternehmen gelebt und fest im Alltag verankert wird, braucht es ein deutliches Bekenntnis der obersten Führungsebene und klare Verantwortlichkeiten. Ziele und Regeln sollten schriftlich fixiert sein, Verantwortliche ihre Aufgaben genau kennen. Wie der VdS Quick-Check zeigt, fehlen diese wichtigen Grundlagen noch viel zu häufig. Deutlich wird aber auch: Einige Unternehmen haben im vergangenen Jahr diese Lücken geschlossen. Sie dürften sich künftig auch in anderen Bereichen verbessern. Für den Rest gilt: Sie nehmen die Gefahren noch nicht ernst genug.

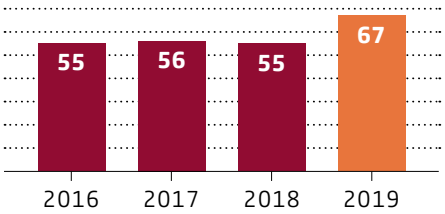
Unser Topmanagement hat sich schriftlich verpflichtet, die Gesamtverantwortung für die Informationssicherheit wahrzunehmen.





Wir haben klare Verantwortlichkeiten für unsere Informationssicherheit definiert.

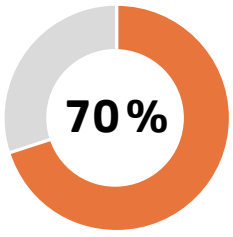


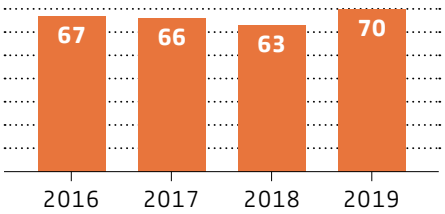


→ Keine Verbindlichkeit

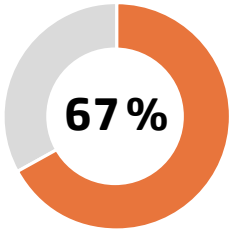
Wo werden welche Daten gespeichert? Wer darf wann auf sie zugreifen? Können Passwörter an Kollegen weitergegeben werden? Dürfen Mitarbeiter das Internet in der Firma auch privat nutzen oder berufliche Dinge am PC zuhause erledigen? In einem Drittel der Unternehmen lautet die Antwort auf diese Fragen: „weiß nicht". Sie haben all das nie geklärt. Im Ergebnis macht im Unternehmen jeder, was er für richtig hält – mit den entsprechenden Risiken.

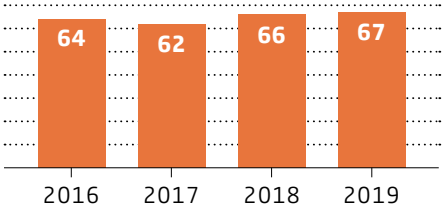
Wir haben eine Richtlinie für unsere Mitarbeiter, in der definiert ist, wie mit der IT und den Daten des Unternehmens umgegangen werden muss.





Die private Nutzung unserer Unternehmens-IT ist in einer Richtlinie geregelt.

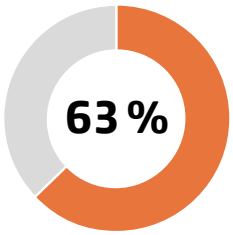


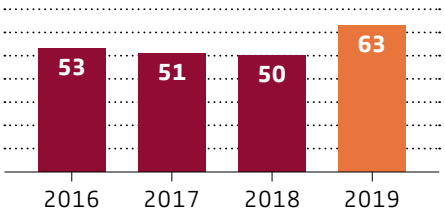


→ Kein Wissenstransfer

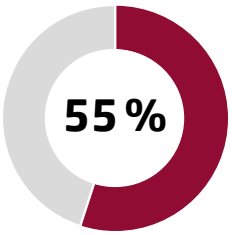
Der Umgang mit Daten und Informationen unterliegt einem ständigen technischen und rechtlichen Wandel. Nur wenn das Wissen über aktuelle Gefährdungen, geänderte Regeln und das korrekte Verhalten in Notfällen bei allen Mitarbeitern auf dem neuesten Stand ist, können sie richtig handeln. Diese Erkenntnis setzt sich im deutschen Mittelstand leider nur langsam durch: Die Ergebnisse haben sich im Vergleich zu 2018 zwar deutlich verbessert, bleiben aber nach wie vor auf einem zu niedrigen Niveau.

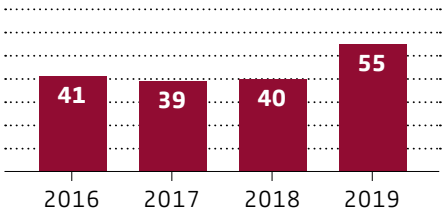
Alle internen und externen Mitarbeiter kennen die betreffenden Regelungen zur Informationssicherheit.





Alle internen und externen Mitarbeiter werden regelmäßig über unsere Maßnahmen zur Informationssicherheit informiert.

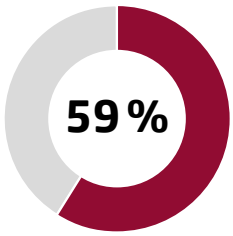


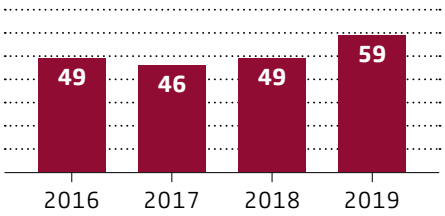


→ Bestehende Zugänge werden kaum überprüft

Grundsätzlich gilt in den meisten Unternehmen: Einen Zugang erhält nur, wer ihn wirklich braucht. Auch mit Administratoren-Rechten gehen nur noch wenige Unternehmen fahrlässig um. Doch ein großer Schwachpunkt bleibt: Sind Zugänge und Berechtigungen erst einmal vergeben, bleiben sie häufig auf unbestimmte Zeit bestehen. Auf Dauer entsteht dadurch Wildwuchs. Besser ist es, alle Administratoren-Zugänge in regelmäßigen Abständen zu prüfen und die nicht mehr benötigten konsequent abzuschalten.

Administrative Zugänge werden von uns regelmäßig nach einem festgelegten Turnnus auf deren Notwendigkeit überprüft.





Informations-sicherheit, die zu Ihrem Unter-nehmen passt.

Mit den VdS-Paket-lösungen

Für die sofortige Verbesserung von Informationssicherheit und Datenschutz sorgen die neuen Cyber-Paketlösungen von VdS. Verschiedene Module bilden die Bausteine für Ihre Cyber-Sicherheit und werden zu den vier Paketen ‚Bronze', ‚Silber', ‚Gold' und ‚Platin' zusammengesetzt.

Die Angebotsbausteine reichen von der Ist-Analyse über Direkt-Maßnahmen bis hin zur zertifizierten Cyber-Sicherheit nach VdS 10000.

Der Vorteil: VdS behält die finanziellen und personellen Ressourcen von kleinen und mittelständischen Unternehmen im Blick. Alle Module aus einer Hand beanspruchen weniger administrativen Aufwand auf Ihrer Seite und ermöglichen eine attraktive Preisgestaltung.

Weitere Informationen unter:

vds.de/cyber

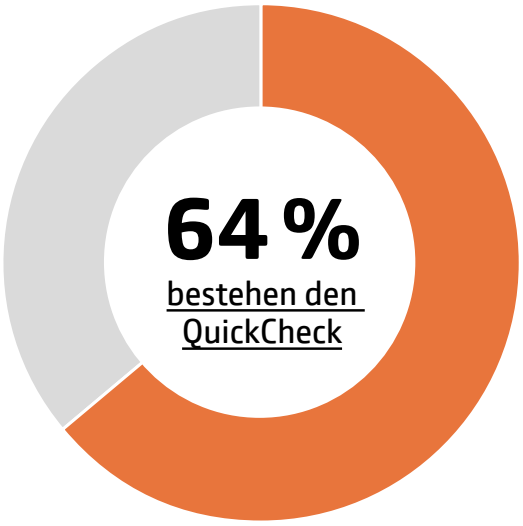
Technik

In einem idealen Unternehmen gilt:

- → Alle Mitarbeiter kennen die Risiken mobiler Geräte und mobiler Datenträger. Hier werden nur ausgewählte Daten gespeichert, die zudem besonders geschützt werden.
- → Der Zugang zum Internet wird eigens abgesichert; von außen kann nur verschlüsselt auf das Netzwerk zugegriffen werden.
- → Ausnahmslos alle IT-Systeme sind bekannt und abgesichert, besonders kritische Systeme werden regelmäßig analysiert.

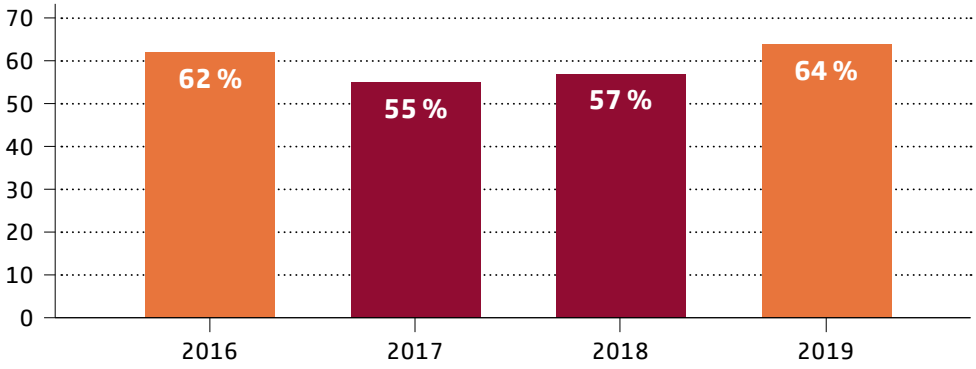
Ergebnis

Der Reifegrad der IT-Sicherheit hat sich im Teilbereich „Technik“ deutlich verbessert. Die Netzwerke und IT-Systeme sind bei den teilnehmenden Unternehmen grundsätzlich gut abgesichert – auch wenn regelmäßige Risikoanalysen noch immer vernachlässigt werden. Handlungsbedarf besteht bei vielen Unternehmen außerdem bei der Festlegung von verbindlichen Regeln für den (privaten) Umgang mit mobilen Geräten und für die Datenspeicherung auf mobilen Datenträgern, wie z. B. USB-Sticks.



90–100 % 60–89 % < 60 %

Tendenz



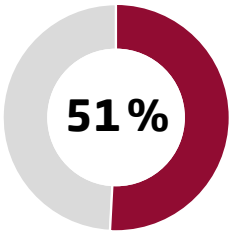
Tendenz: positiv

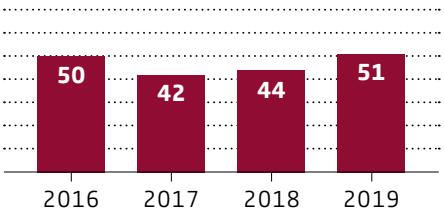
In der Realität zeigen sich in vielen Unternehmen diese Probleme:

→ Keine klaren Regeln für den Umgang mit mobilen Daten und Datenträgern

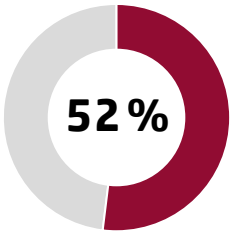
Smartphones, Laptops und USB-Sticks sind schwerer zu schützen als Server oder Netzwerkknoten. Auch wenn eine Mehrheit der Unternehmen zumindest für einen eigenen Schutz der Daten auf mobilen Geräten sorgt, bleiben Sicherheitslücken. Denn nur die Hälfte der Unternehmen hat verbindlich festgelegt, was ihre Mitarbeiter mit den mobilen Geräten treiben dürfen – und vor allem, was sie nicht tun dürfen. Cyberkriminelle setzen also am besten dort an, wo es für sie am einfachsten ist: bei einem sorglosen Mitarbeiter mit einem Smartphone.

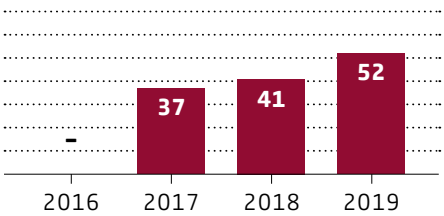
Wir haben eine Richtlinie, in der der Umgang mit mobilen Geräten festgelegt ist.





Wir haben festgelegt, welche Informationen des Unternehmens auf mobilen Datenträgern gespeichert werden dürfen.

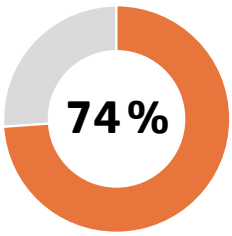


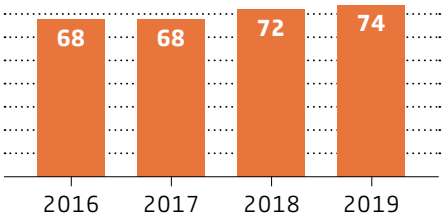


→ Kein aktueller Überblick aller IT-Systeme, keine Analyse kritischer Systeme

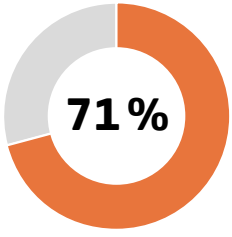
Sie glauben, die IT-Abteilung oder der IT-Dienstleister würde selbstverständlich alle Geräte im Unternehmen kennen? Das stimmt – wenn Sie Glück haben! In einem Viertel der Unternehmen sind eben nicht alle Geräte bekannt – da nutzt der eine die Firmen-Applikation auf seinem privaten Smartphone, der andere kauft schnell eine externe Festplatte oder installiert gleich einen eigenen Server. Ein umfassendes Schutzkonzept für die eigene IT-Infrastruktur ist unter solchen Umständen unmöglich.

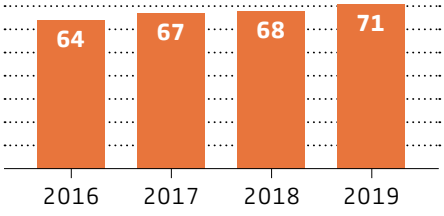
Wir haben eine Aufstellung aller IT-Systeme unseres Unternehmens, die wir laufend aktualisieren.





Wir haben ein Schutzkonzept, wie unsere IT-Systeme abgesichert werden.





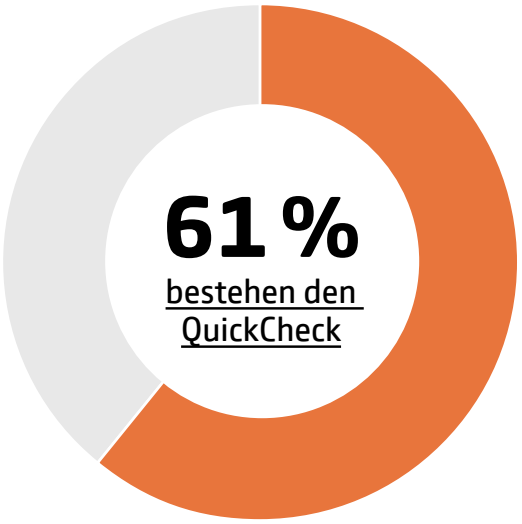
Prävention

In einem idealen Unternehmen gilt:

- Es gibt eine Datensicherung, die sicher aufbewahrt und regelmäßig getestet wird.
- Server und Netzwerkverteiler sind gegen Brände, Stromausfälle, Blitzschläge und mechanische Schäden geschützt.
- Der IT-Notfall ist klar definiert und es gibt einen Notfallplan, mit dem die wichtigsten Systeme schnell wieder in Betrieb gehen können.

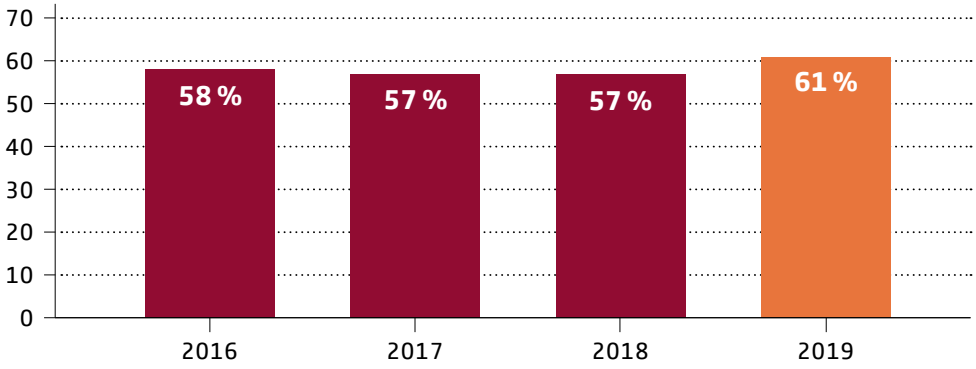
Ergebnis

Wie in den Vorjahren fällt beim Thema „Prävention“ eine Ungleichverteilung der Ergebnisse auf. So sind Fragestellungen zur Datensicherung sowie der physikalischen Sicherung der IT-Systeme, z. B. vor Brand oder unbefugtem Zutritt, zufriedenstellend abgedeckt. Die Prävention für Ausfälle oder Sicherheitsvorfälle ist hingegen unterdurchschnittlich: Rund 60 % der teilnehmenden Unternehmen sind für diese Ernstfälle nicht ausreichend gewappnet.



90–100 % 60–89 % < 60 %

Tendenz



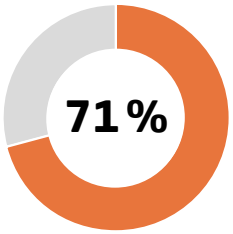
Tendenz: leicht positiv

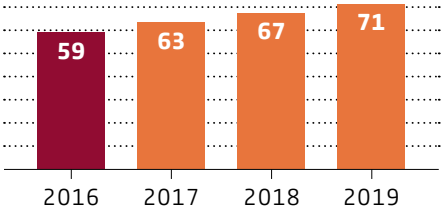
In der Realität zeigen sich in vielen Unternehmen diese Probleme:

→ Auf die Datensicherung ist im Ernstfall kein Verlass, weil sie nicht getestet wird

Datensicherungen sind die letzte Rückversicherung für den Fall gelöschter oder manipulierter Daten. Unternehmen sind gut beraten, die Datensicherungen nicht nur regelmäßig anzufertigen, sondern auch zu prüfen, ob die Daten so tatsächlich wiederhergestellt werden können. Der Notfall ist der schlechteste Zeitpunkt um festzustellen, dass eine Sicherungskopie fehlerhaft ist.

Wir stellen durch regelmäßige Tests nach einem festgelegten Turnus sicher, dass unsere Datensicherung funktioniert.

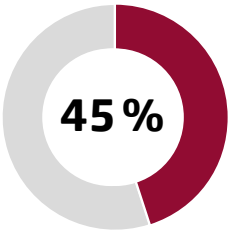


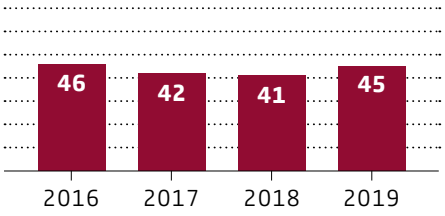


→ Im Notfall wird nicht planvoll gehandelt, sondern auf die Schnelle improvisiert

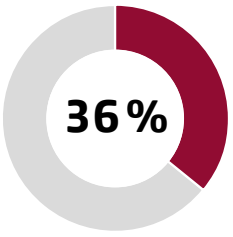
Wer sich auf Schwierigkeiten nicht vorbereitet, wird von ihnen schnell überrollt. Niemand hat einen Plan, Chaos bricht aus. Dann macht ein Kollege hektisch irgendwas, ein anderer macht gar nichts mehr, der Dritte macht das Gegenteil des ersten. Das zieht den Notfall unnötig in die Länge und vergrößert die negativen Folgen. Gute Vorbereitung und klare Handlungsanweisungen können Probleme hingegen auf ein Minimum beschränken. Doch dieser Aufgabe gestellt hat sich bislang nicht einmal jedes zweite Unternehmen.

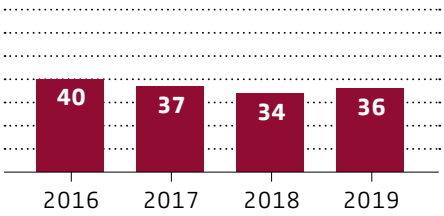
Wir besitzen für unsere kritischen Systeme Wiederanlaufpläne.





Wir besitzen einen Übersichtsplan, aus dem hervorgeht, in welcher Reihenfolge kritische Systeme wieder in Betrieb genommen werden müssen.





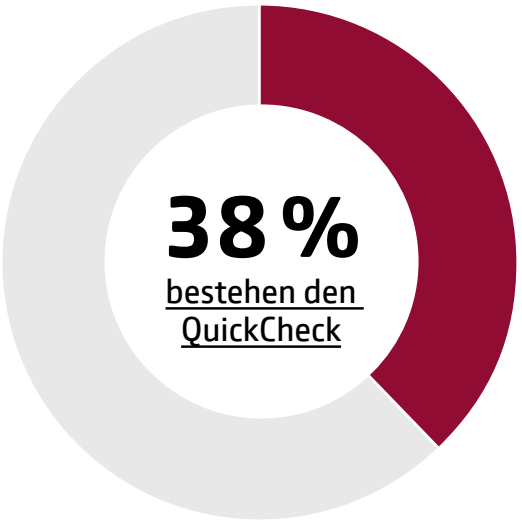
Management

In einem idealen Unternehmen gilt:

→ Das Unternehmen definiert die Sicherheitsanforderungen und verpflichtet seine externen IT-Dienstleister oder Cloud-Anbieter zur Einhaltung.

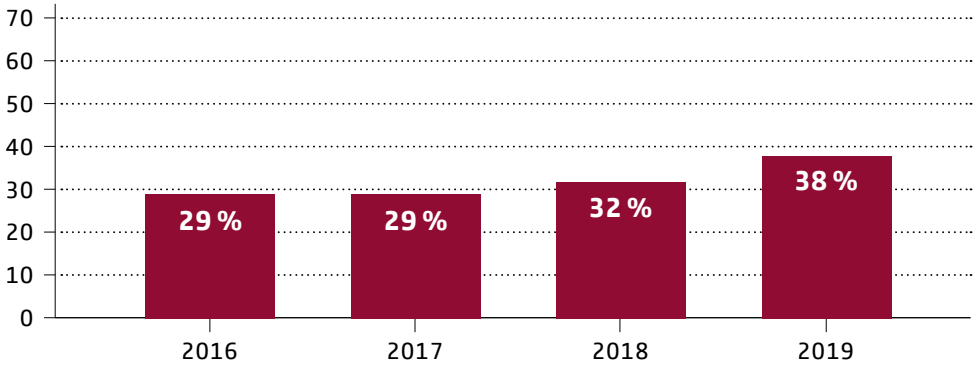
Ergebnis

Das Gesamtergebnis im Bereich „Management“ deutet auf einen großen Handlungsbedarf hin. Der Reifegrad der teilnehmenden Unternehmen ist mit Blick auf die Merkmale „IT-Outsourcing und Cloud-Computing“ weiterhin nicht zufriedenstellend. Bei über 60% fehlen sowohl die Definition der Sicherheitsanforderungen für das IT-Outsourcing und Cloud Computing als auch die rechtliche Absicherung bei entsprechenden Dienstleistern.



90–100 % 60–89 % < 60 %

Tendenz



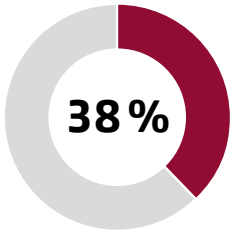
Tendenz: positiv

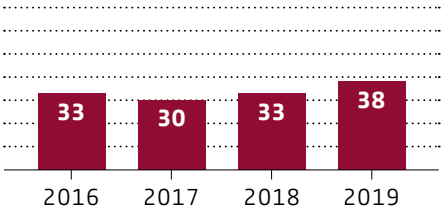
In der Realität zeigt sich in vielen Unternehmen dieses Problem:

→ Sicherheit spielt beim Outsourcen von IT und der Nutzung von Clouds so gut wie keine Rolle

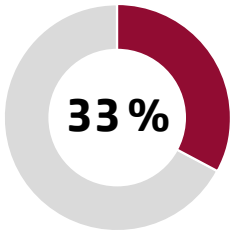
Wer seine IT outsourct oder seine Daten in der Cloud speichert, muss seinen Vertragspartnern vertrauen. Er sollte das aber nicht so blind tun wie rund zwei Drittel der Unternehmen im VdS Quick-Check. Sie lagern offenbar nicht nur den Betrieb und ihre Daten aus, sondern gleich jeden Gedanken an die IT-Sicherheit.

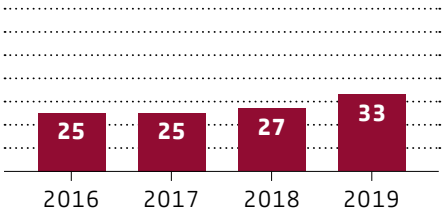
Für jedes IT-Outsourcing Vorhaben haben wir notwendige Anforderungen an die Sicherheit definiert



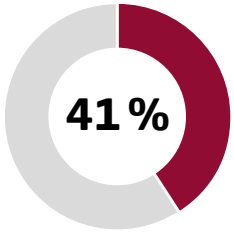


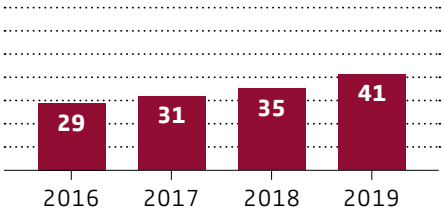
Für jede Nutzung von Cloud Computing haben wir notwendige Anforderungen an die Sicherheit definiert.





Wir haben mit jedem unserer Dienstleister für IT-Outsourcing bzw. Cloud Computing einen Vertrag geschlossen, der unsere definierten Anforderungen enthält und zu deren Erfüllung verpflichtet.





VdS Quick-Check 2019: Alle Ergebnisse

Organisation (64 %)

Organisation der Informationssicherheit		Ja	Nein	trifft nicht zu
56 %	Unser Topmanagement hat sich schriftlich verpflichtet, die Gesamtverantwortung für die Informationssicherheit wahrzunehmen.	52%	33%	15%
	Wir haben klare Verantwortlichkeiten für unsere Informationssicherheit definiert.	67%	28%	5%
	Wir haben das Prinzip der Funktionstrennung umgesetzt, d.h. Ausführung und Kontrolle der Aufgaben zur Gewährleistung der Informationssicherheit sind voneinander getrennt.	50%	36%	14%

Richtlinien		Ja	Nein	trifft nicht zu
64 %	Wir haben eine Richtlinie für unsere Mitarbeiter, in der definiert ist, wie mit der IT und den Daten des Unternehmens umgegangen werden muss.	70%	26%	4%
	Wir haben klare Verantwortlichkeiten für unsere Informationssicherheit definiert.	67%	28%	5%
	Wir haben eine Richtlinie für unsere IT-Dienstleister, in der definiert ist, wie mit der IT und den Daten des Unternehmens umgegangen werden muss.	54%	35%	11%

Personal		Ja	Nein	trifft nicht zu
61 %	Alle internen und externen Mitarbeiter kennen die betreffenden Regelungen zur Informationssicherheit.	63%	33%	4%
	Alle internen und externen Mitarbeiter haben eine schriftliche Vertraulichkeitserklärung abgegeben.	64%	31%	5%
	Alle internen und externen Mitarbeiter werden regelmäßig über unsere Maßnahmen zur Informationssicherheit informiert.	55%	40%	5%

Zugänge		Ja	Nein	trifft nicht zu
77 %	Zugänge für unsere IT-Infrastruktur werden konsequent nur gewährt, wenn sie für die Aufgabenerfüllung notwendig sind.	85%	13%	2%
	Administrative Zugänge sind ausschließlich unseren Administratoren vorbehalten.	89%	9%	2%
	Administrative Zugänge werden von uns regelmäßig nach einem festgelegten Turnus auf deren Notwendigkeit überprüft.	59%	33%	8%

Technik (64 %)

Mobile Geräte		Ja	Nein	trifft nicht zu
61 %	Wir haben eine Richtlinie, in der der Umgang mit mobilen Geräten festgelegt ist.	51%	38%	11%
	Die Daten auf unseren mobilen Geräten sind vor unberechtigtem Zugriff geschützt.	67%	22%	11%
	Im Fall eines Verlust oder Diebstahles eines mobilen Gerätes wissen unsere Nutzer was zu tun ist.	65%	24%	10%

Mobile Datenträger		Ja	Nein	trifft nicht zu
65 %	Wir haben festgelegt, welche Informationen des Unternehmens auf mobilen Datenträgern, wie z.B. USB-Sticks, CD-ROMs, DVD-ROMs, Speicherkarten oder mobilen Festplatten gespeichert werden dürfen.	52%	41%	7%
	Unsere Nutzer werden über die spezifischen Risiken mobiler Datenträger (z. B. Gefahren durch Verlust oder Diebstahl oder durch das Einschleppen von Schad-software) informiert und sensibilisert.	69%	26%	5%
	Unseren Nutzern wird untersagt, mobile Datenträger an unberechtigte Dritte weiterzugeben oder zu verleihen.	74%	21%	5%

Netzwerke		Ja	Nein	trifft nicht zu
70 %	Wir haben den Zugriff auf das Internet durch Schutzmaßnahmen abgesichert.	89%	9%	2%
	Der Zugriff auf unsere interne IT-Infrastruktur über öffentliche oder drahtlose Netze erfolgt ausschließlich verschlüsselt.	86%	9%	5%
	Wir führen für besonders kritische IT-Netzwerke regelmäßig Risikoanalysen nach einem festgelegten Turnus durch.	35%	46%	19%

IT-Systeme		Ja	Nein	trifft nicht zu
60 %	Wir haben eine Aufstellung aller IT-Systeme unseres Unternehmens, die wir laufend aktualisieren.	74%	22%	4%
	Wir haben ein Schutzkonzept, wie unsere IT-Systeme abgesichert werden.	71%	25%	4%
	Wir führen für besonders kritische IT-Systeme regelmäßig Risikoanalysen nach einem festgelegten Turnus durch.	35%	48%	17%

Prävention (61 %)

Sicherheitsvorfälle		Ja	Nein	trifft nicht zu
43 %	Wir haben den Begriff „IT-Sicherheitsvorfall“ für unser Unternehmen verbindlich definiert.	34%	60%	6%
	Wir haben eine Richtlinie, in welcher der Umgang mit Sicherheitsvorfällen festgelegt ist.	39%	55%	6%
	Im Fall eines Sicherheitsvorfalls wissen unsere Nutzer was zu tun ist.	57%	39%	4%

Umgebung		Ja	Nein	trifft nicht zu
77 %	Wir haben unsere wichtigen IT-Systeme, wie z.B. Server und Netzwerkverteiler, vor unberechtigtem physischem Zugriff gesichert.	86%	12%	3%
	Wir haben unsere wichtigen IT-Systeme, wie z.B. Server und Netzwerkverteiler, vor Brandschäden gesichert.	62%	34%	4%
	Wir haben unsere wichtigen IT-Systeme, wie z.B. Server und Netzwerkverteiler, mit einer unterbrechungsfreien Stromversorgung vor Stromausfällen und Überspannung gesichert.	82%	14%	3%

Datensicherung		Ja	Nein	trifft nicht zu
84 %	Wir schützen uns vor dem Verlust der wichtigsten Unternehmensdaten durch eine Datensicherung.	95%	3%	1%
	Wir stellen durch regelmäßige Tests nach einem festgelegten Turnus sicher, dass unsere Datensicherung funktioniert.	71%	27%	3%
	Unsere Datensicherungsmedien werden örtlich getrennt von den gesicherten Systemen aufbewahrt, so dass bei einem Brand oder Wasserschaden nicht beide Datenquellen betroffen sind.	86%	12%	2%

Ausfälle		Ja	Nein	trifft nicht zu
40 %	Wir besitzen für unsere kritischen Systeme Wiederanlaufpläne.	45%	38%	17%
	Wir besitzen einen Übersichtsplan, aus dem hervorgeht, in welcher Reihenfolge kritische Systeme wieder in Betrieb genommen werden müssen.	36%	42%	22%
	Unsere Wiederanlaufpläne und unser Übersichtsplan werden so aufbewahrt, dass sie auch bei einem Notfall schnell verfügbar sind.	39%	38%	23%

Management (38 %)

IT-Outsourcing und Cloud Computing		Ja	Nein	trifft nicht zu
38 %	Für jedes IT-Outsourcing Vorhaben haben wir notwendige Anforderungen an die Sicherheit definiert.	38%	27%	35%
	Für jede Nutzung von Cloud Computing haben wir notwendige Anforderungen an die Sicherheit definiert.	33%	23%	44%
	Wir haben mit jedem unserer Dienstleister für IT-Outsourcing bzw. Cloud Computing einen Vertrag geschlossen, der unsere definierten Anforderungen enthält und zu deren Erfüllung verpflichtet.	41%	23%	35%

Über die Initiative CyberSicher

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.

Impressum

Herausgeber
Gesamtverband der Deutschen Versicherungswirtschaft e. V.
Wilhelmstraße 43 / 43 G, 10117 Berlin
Postfach 08 02 64, 10002 Berlin
Tel. +49 30 2020–5000, Fax +49 30 2020–6000
www.gdv.de, berlin@gdv.de

V.i.S.d.P.
Christoph Hardt

Redaktion
Christian Siemens
Svenja Urban

Bildnachweis
Illustrationen: Malte Knaack

GDV
DIE DEUTSCHEN VERSICHERER

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

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

VdS

VdS Schadenverhütung GmbH
Amsterdamer Str. 172
50735 Köln
Tel.: +49 (0)221-7766-0
Fax: +49 (0)221-7766-341
E-Mail: info@vds.de
www.vds.de

Ein Unternehmen des Gesamtverbandes der Deutschen Versicherungswirtschaft e.V. (GDV)