BUNDESDRUCKEREI

STUDIE

AUSGABE
2017

# Digitalisierung und IT-Sicherheit in deutschen Unternehmen

**Eine repräsentative Untersuchung, erstellt von der Bundesdruckerei GmbH in Zusammenarbeit mit KANTAR EMNID**

Sichere Organisation

# Inhalt

## Vorwort

Was in der hochtourigen IT-Branche zum zweiten Mal geschieht, wird oft bereits unter „Tradition" verbucht. Als traditionsreiches IT-Unternehmen haben wir daher zum zweiten Mal die deutschen Unternehmen empirisch fundiert (und segmentiert nach Größe und Branche) befragen lassen, wie sie es halten: mit der Digitalisierung, der Sicherheit – und der Sicherheit bei der Digitalisierung. Nächstes Jahr geht die Umfrage folgerichtig in die dritte Runde.

Schließlich bleibt uns das Thema erhalten. Die Digitalisierung der Wirtschaft geht in großen Schritten voran. Damit wächst die Bedeutung der IT-Sicherheit, betriebswirtschaftlich wie gesellschaftlich. Hard- und Software können noch so praktisch sein – ohne ein Mindestmaß an Sicherheit gibt es kein Vertrauen in eine IT-Lösung. Und ohne ein Mindestmaß an Vertrauen gibt es keine breite Nutzung und damit weniger Effizienzgewinne und Wachstum. Digitalisierung und IT-Sicherheit müssen und können gemeinsam und koordiniert angegangen werden.

Da wir bei aller Tradition am Puls der Zeit sind, haben wir den Fragenkatalog aktualisiert. Ein eigener Schwerpunkt sind nun Cloud-Technologien: Wie viele Unternehmen nutzen sie, welche Kriterien sollten Anbieter erfüllen und aus welchen Gründen lehnen weiterhin viele Verantwortliche für IT-Sicherheit die Cloud ab?

Als Gesamtfazit lässt sich feststellen: Die Ergebnisse haben sich im Vergleich zum Vorjahr in der Regel leicht verbessert, wenn auch häufig von niedrigem Niveau ausgehend.

Fühlten sich beispielsweise 2016 laut Umfrage 29 Prozent der Unternehmen gut gerüstet für die digitale Transformation, so sind es nun 32 Prozent. In immerhin jedem sechsten Unternehmen werden notwendige IT-Sicherheitsmaßnahmen aus Kostengründen nur begrenzt umgesetzt. IT-Sicherheit wird eben weiterhin zu häufig als Kostenfaktor gesehen – und nicht als der Wettbewerbsfaktor, zu dem sie immer mehr wird.

Sollten Sie nach der Lektüre dieser Studie noch Fragen haben, sprechen Sie uns gerne an. Wir freuen uns auf den Austausch mit Ihnen.

Mit freundlichen Grüßen

**Ulrich Hamann**
Vorsitzender der Geschäftsführung der Bundesdruckerei GmbH

## Studiendesign

**Mit diesem Bericht legt Kantar EMNID, Bielefeld, im Auftrag der Bundesdruckerei die Ergebnisse einer bundesweiten Befragung vor. Die Studie untersucht Kenntnisse und Bewertungen zu Themen der Informationssicherheit in Unternehmen aus Sicht von Entscheidern für IT-Sicherheit in deutschen Unternehmen. Für die Datenerhebung und Auswertung ist EMNID verantwortlich.**

Um sicherzustellen, dass die verschiedenen Unternehmensgrößen und Branchen für die Auswertung in ausreichender Zahl in der Stichprobe vertreten sind, wurde die Stichprobe nach diesen Merkmalen geschichtet. Durch eine anschließende Gewichtung der Stichprobe hinsichtlich Unternehmensgröße und Branche entspricht die der Auswertung zugrunde liegende Stichprobe in ihrer Zusammensetzung der Struktur der Grundgesamtheit. Damit sind die Untersuchungsergebnisse repräsentativ und können im Rahmen der statistischen Fehlertoleranzen auf die Grundgesamtheit der Unternehmen ab 20 Mitarbeitern in der Bundesrepublik Deutschland verallgemeinert werden.

Da die dargestellten Anteilswerte auf ganze Zahlen gerundet sind, kann es vorkommen, dass sie sich nicht zu 100 Prozent aufsummieren. Bei Fragen mit mehreren Antwortoptionen können die aufaddierten Nennungen 100 Prozent überschreiten.

Alle Befragungen, die auf Stichproben beruhen, weisen eine statistische Unsicherheit auf. Bei der vorliegenden Erhebung beträgt diese sogenannte statistische Fehlertoleranz ±2 (bei einem Anteilswert von 5 Prozent) bis ±4 Prozentpunkte (Anteilswert von 50 Prozent). Wo methodisch angebracht, werden die Befragungsergebnisse mit denen einer im März und April 2016 für die Bundesdruckerei durchgeführten früheren Erhebung verglichen, um Trendentwicklungen zu erfassen. Damals wurden nach derselben Methode 556 Unternehmen mit mindestens 20 Mitarbeitern befragt.

## Zusammensetzung der Stichprobe

**Befragungsgebiet**
Bundesrepublik Deutschland

**Stichprobe**
500 Interviews

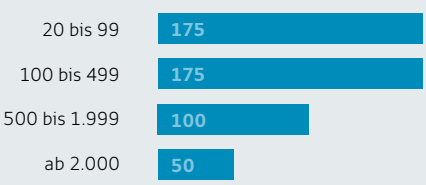
**Zielgruppe**
Hauptverantwortliche Entscheider für IT- Sicherheit

**Methode**
Telefonische Interviews (CATI ad hoc)

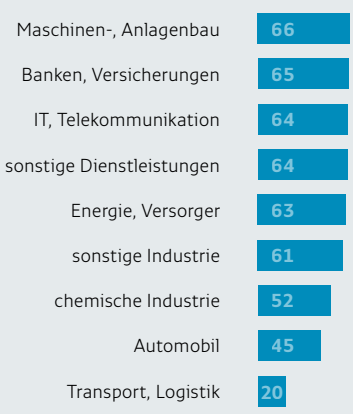
**Grundgesamtheit**
Unternehmen ab 20 Mitarbeitern

**Erhebungszeitraum**
06. Februar bis 22. März 2017

### Fallzahlen nach Mitarbeiterzahl




### Fallzahlen nach Branchen



## Management Summary

# Digitalisierung und IT-Sicherheit in deutschen Unternehmen

## 32 Prozent

der Unternehmen fühlen sich gut gerüstet für die digitale Transformation. 2016 waren es 29 Prozent.

## 74 Prozent

der Unternehmen sehen IT-Sicherheit als Basis für eine erfolgreiche Digitalisierung.

## 31 Prozent

der Unternehmen nehmen das Thema IT-Sicherheit mehr als Wettbewerbsfaktor statt als Kostenfaktor wahr.

## 16 Prozent

der Unternehmen befürchten Umsatzeinbußen durch die Verzögerung der Digitalisierung aufgrund von IT-Sicherheitsbedenken, fünf Prozentpunkte weniger als im Vorjahr.

## 17 Prozent

der Unternehmen nutzen bereits externe Cloud-Services, weitere neun Prozent planen dies konkret. Wichtigstes Kriterium für die Wahl des Cloud-Anbieters ist die Gewährleistung der Datensicherheit. Häufigstes Argument gegen eine Cloud-Nutzung: Unternehmen wollen die Hoheit über die IT behalten.

## 43 Prozent

der Unternehmen erkennen Verbesserungsbedarf bei technischen IT-Sicherheitsmaßnahmen, 39 Prozent bei organisatorischen und 32 Prozent bei personellen IT-Sicherheitsmaßnahmen.

## 46 Prozent

der Unternehmen schulen ihre Mitarbeiter regelmäßig zu IT-Sicherheit. Im vergangenen Jahr waren es 55 Prozent.

## 57 Prozent

der Unternehmen fühlen sich zumindest ab und zu von den gesetzlichen Regeln zu IT-Sicherheit und Datenschutz überfordert, sechs Prozentpunkte weniger als im Vorjahr.

## 56 Prozent

der Unternehmen gehen für dieses Jahr von steigenden Investitionen in ihre IT-Sicherheit aus, 2016 lag die Quote bei 60 Prozent.

# 1 Bedeutung der IT-Sicherheit in den Unternehmen

## 1.1 Verhältnis von IT-Sicherheit und Digitalisierung

**Die zunehmende Verzahnung der Unternehmensprozesse mit moderner Informations- und Kommunikationstechnik, die Vernetzung von Systemen sowie die wachsende Verfügbarkeit digitaler Technologien machen eine immer stärkere Digitalisierung von Unternehmensprozessen erforderlich. Das ist eine große Herausforderung für die Informationssicherheit. Je stärker Unternehmensprozesse digitalisiert und vernetzt werden, desto größer die Angriffsfläche für Cyberangriffe.**

Fast drei Viertel der Unternehmen in Deutschland sind sich dieser Sicherheitsrisiken durch eine fortscheitende Digitalisierung durchaus bewusst und sehen daher IT-Sicherheit als Basis für eine erfolgreiche Digitalisierung. Vor allem die im Bereich Industrie 4.0 besonders aktive Automobilindustrie und die Banken- und Versicherungsbranche, in der es schon lange hohe sicherheitstechnische Vorgaben gibt, sind dieser Meinung (jeweils über 90 Prozent).

Allerdings haben bisher nur knapp zwei von fünf Unternehmen ihre Produktionsprozesse bereits digitalisiert. Lediglich in den Großunternehmen mit mindestens 2.000 Mitarbeitern hat die digitale Transformation schon mehrheitlich stattgefunden (58 Prozent). Vor allem bei Banken und Versicherungen sowie bei Unternehmen der ITK-Branche ist die Digitalisierung schon weit fortgeschritten (55 Prozent bzw. 53 Prozent).

Dabei sehen die meisten IT-Entscheider den Herausforderungen der Digitalisierung eher mit Sorge entgegen: Insgesamt hat der entsprechende Anteilswert seit dem Frühjahr 2016 zwar leicht zugenommen (2016: 29 Prozent), ). Jedoch sieht weiterhin nicht einmal jeder Dritte (32 Prozent) sein eigenes Unternehmen schon gut gerüstet für die digitale Transformation.

Für drei Viertel ist IT-Sicherheit die Grundbedingung für eine erfolgreiche Digitalisierung.


**Frage:** Wie würden Sie das Verhältnis von IT-Sicherheit und Digitalisierung in Ihrem Unternehmen beschreiben?

**Dargestellt:** Summe der Nennungsanteile „trifft voll und ganz zu" sowie „trifft eher zu" in Prozent

Auffällig ist dabei, dass sich – abgesehen von der Automobilbranche (36 Prozent) – vor allem die IT-Entscheider von Industrieunternehmen im Hinblick auf die Herausforderungen der Digitalisierung schlecht aufgestellt fühlen (Maschinen- und Anlagenbau, chemische und sonstige Industrie). Das hat unterschiedliche Gründe: Ein wesentlicher ist sicherlich die bisher noch mangelnde Anerkennung des Themas IT-Sicherheit als wichtiger Wettbewerbsfaktor: In nur drei von zehn Unternehmen wird IT-Sicherheit unternehmenspolitisch als Wettbewerbsvorteil im Konkurrenzumfeld und nicht nur als Kostenfaktor wahrgenommen. Entsprechend werden in jedem sechsten Unternehmen IT-Sicherheitsmaßnahmen aus Kostengründen nur begrenzt umgesetzt.

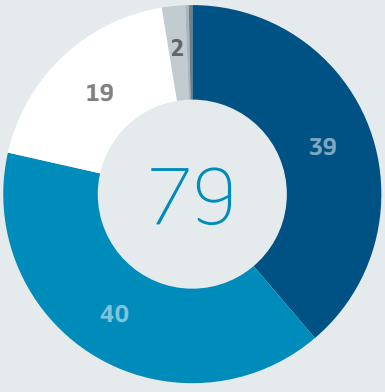
Zum anderen kann die Digitalisierung auch selbst als problematisch angesehen werden, etwa aufgrund von Sicherheitsbedenken oder weil Digitalisierung das eigene Geschäftsmodell bedroht. Trotz leichter Fortschritte (2016: 21 Prozent; 2017: 16 Prozent) wird in ebenfalls jedem sechsten Unternehmen aus Angst vor IT-Sicherheitsvorfällen die Digitalisierung nicht ausreichend vorangetrieben – mit der Folge erheblicher Umsatzeinbußen. Sehr selten wird Digitalisierung schließlich per se als Bedrohung für das eigene Geschäftsmodell angesehen; gilt vor allem für die Finanzbranche (12 Prozent), in der etwa das Filialgeschäft von Banken zunehmend unter Konkurrenzdruck durch online-basierte Fintech-Unternehmen gerät.

## 1.2 Stellenwert der IT-Sicherheit im Unternehmen

**Auch angesichts der von den Unternehmen wahrgenommenen Herausforderungen der Digitalisierung wird dem Thema IT-Sicherheit in der deutschen Wirtschaft aktuell große Bedeutung beigemessen.**

Vier von fünf Unternehmen geben an, dass IT-Sicherheit einen hohen oder sogar sehr hohen Stellenwert in ihrem Unternehmen habe, quer über alle Unternehmensgrößen hinweg. Besonders wichtig wird IT-Sicherheit im Banken- und Versicherungswesen sowie in Unternehmen der Informationstechnologie und Telekommunikation genommen: In jeweils über 90 Prozent der Unternehmen dieser Branchen besitzt die IT-Sicherheit einen hohen oder sehr hohen Stellenwert.

### Für acht von zehn Entscheider hat IT-Sicherheit hohe Priorität.




**Ringinneres:** „sehr hoher" bzw. „hoher Stellenwert"

**Frage:** Welchen Stellenwert hat das Thema IT-Sicherheit in Ihrem Unternehmen?

Angaben in Prozent

## 1.3 Entwicklung der Investitionen in IT-Sicherheit

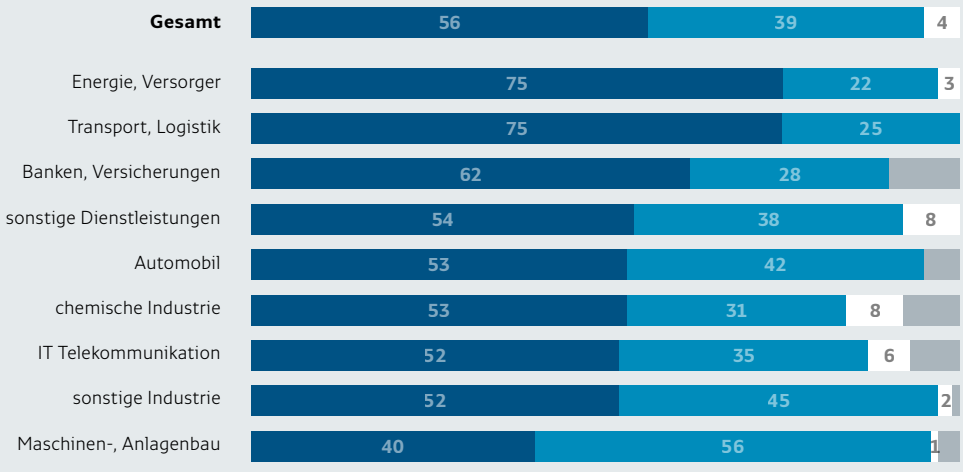
**Die Mehrheit der Unternehmen in Deutschland (56 Prozent) beabsichtigt, dieses Jahr mehr in ihre IT-Sicherheit zu investieren als im Vorjahr. Jedes fünfte erwartet sogar eine starke Zunahme, dies vor allem in größeren Unternehmen.**

So planen 35 Prozent der Unternehmen mit 2.000 oder mehr Mitarbeitern, die Investitionen in IT-Sicherheit im laufenden Jahr stark auszubauen. Bei Unternehmen mit weniger als 100 Mitarbeiter sind dies nur 18 Prozent.

Damit spiegelt sich die hohe Bedeutung der IT-Sicherheit in den Unternehmen auch in deren Budgetplanungen wider. Von einem unveränderten IT-Sicherheits-Budget gehen zwei von fünf Unternehmen aus. Mit einem Rückgang der Investitionen rechnet hingegen kaum ein Unternehmen. Im Trendvergleich mit der Vorjahresumfrage zeigt sich, dass die Investitionsabsichten der Unternehmen für 2017 etwa auf dem gleichen Niveau bleiben (2016: 60 Prozent Zunahme; 2017: 56 Prozent Zunahme).

Vor allem Energie- und Versorgungsunternehmen sowie die Transport- und Logistikbranche gehen von Investitionszuwächsen in diesem Jahr aus (jeweils 75 Prozent). Auch in fast allen anderen Branchen werden die Unternehmensbudgets für IT-Sicherheit in diesem Jahr mehrheitlich aufgestockt. Lediglich die Maschinen- und Anlagenbauer gehen mehrheitlich unveränderten Investitionen aus (56 Prozent). Nur 40 Prozent von ihnen wollen mehr investieren als im Vorjahr.

### Investitionen in IT-Sicherheit steigen.




**Frage:** Wie werden sich die Investitionen Ihres Unternehmens in die IT-Sicherheit im Jahr 2017 im Vergleich zu 2016 voraussichtlich entwickeln?

Angaben in Prozent

# 2 Verantwortung für IT-Sicherheit im Unternehmen

## 2.1 Verantwortung für IT-Sicherheit

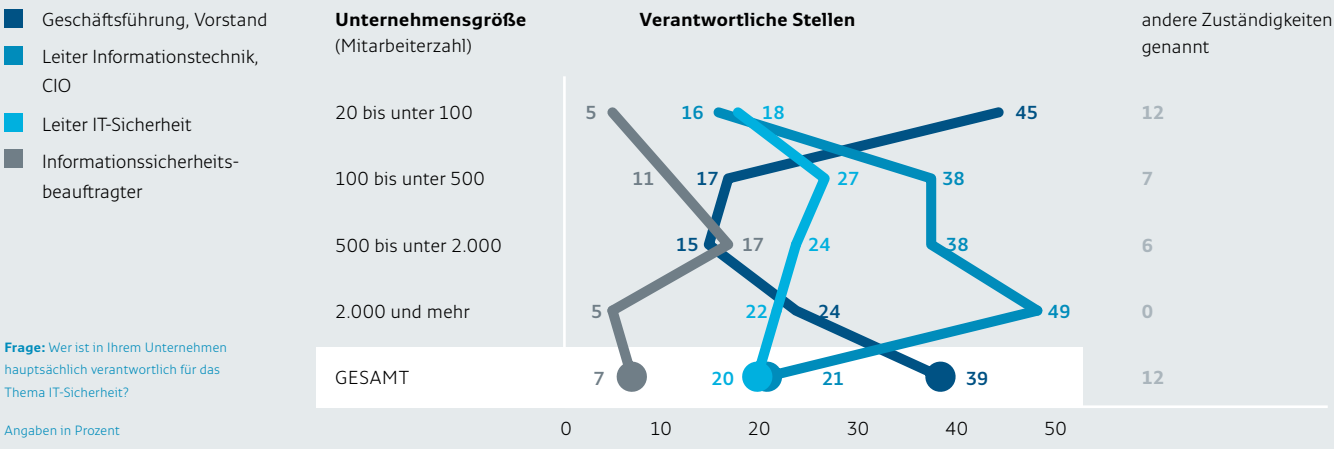
**Welche Person im Unternehmen für die IT-Sicherheit hauptsächlich verantwortlich ist, hängt vor allem von der Größe des jeweiligen Unternehmens ab.**

Während in kleinen Unternehmen am häufigsten die Geschäftsführung bzw. der Vorstand selbst die Verantwortung dafür tragen, können größere Unternehmen es sich leisten, für diese Aufgabe spezielles Personal einzusetzen, etwa IT-Leiter bzw. CIOs, Leiter der IT-Sicherheit oder Informationssicherheitsbeauftragte.

So ist in 45 Prozent der Unternehmen mit weniger als 100 Beschäftigten die Geschäftsführung hauptverantwortlich. Je größer das Unternehmen, desto eher ist allerdings der Chief Information Officer (CIO) bzw. der IT-Leiter für dieses Thema zuständig. In fast jedem zweiten großen Unternehmen mit mindestens 2.000 Mitarbeitern gehört die IT-Sicherheit zum Verantwortungsbereich des CIO.

In etwa jedem vierten Unternehmen gibt es stattdessen eine spezielle Position für Aufgaben der IT-Sicherheit, sei es als Leiter der IT-Sicherheit (20 Prozent) oder als Informationssicherheitsbeauftragter (7 Prozent). Letzterer wird vergleichsweise oft (25 Prozent) von Unternehmen im Banken- und Versicherungswesen als die für IT-Sicherheit hauptverantwortliche Person genannt. Nur in 2 Prozent der Unternehmen gibt es überhaupt keine zuständige Abteilung für dieses wichtige Thema.

Je größer das Unternehmen, desto eher ist das Thema IT-Sicherheit beim IT-Leiter bzw. CIO angesiedelt.




**Frage:** Wer ist in Ihrem Unternehmen hauptsächlich verantwortlich für das Thema IT-Sicherheit?

Angaben in Prozent

## 2.2 Zuständigkeiten für die IT-Sicherheitsstrategie

**Eine wesentliche Bedingung für eine hohe Informationssicherheit in Unternehmen ist die Wahrnehmung dieses Themas in den Chefetagen. In den allermeisten Unternehmen sind die Entscheidungen zur IT-Sicherheitsstrategie denn auch Chefsache.**

In fast vier von fünf Unternehmen in Deutschland fällt die Geschäftsführung die strategischen Entscheidungen im Hinblick auf die IT-Sicherheit.

Mit zunehmender Größe der Unternehmen wird immer häufiger auch eine eigene IT-Abteilung an sicherheitsstrategischen Entscheidungen beteiligt (43 Prozent).

Auch externe Dienstleister im Bereich der IT-Sicherheit werden häufig einbezogen, wenn es um die Sicherheitsstrategie im IT-Bereich geht: zwei von fünf Unternehmen tun dies. Allerdings überlassen nur die wenigsten Unternehmen (4 Prozent) Dritten völlig die Entscheidung über die Entwicklung der IT-Sicherheit des eigenen Unternehmens, ohne selbst in irgendeiner Form daran beteiligt zu sein.

Die Umsetzung der jeweiligen Sicherheitsstrategie obliegt zumeist den eigenen IT-Abteilungen (54 Prozent). Fast ebenso häufig (53 Prozent) werden externe Anbieter mit der Umsetzung der beschlossenen IT-Sicherheitsmaßnahmen beauftragt.

### Die Geschäftsführung bezieht häufig Dritte in strategische Entscheidungen zum Thema IT-Sicherheit ein.


**Frage:** Wer entscheidet in Ihrem Unternehmen über die IT-Sicherheitsstrategie? Und wer setzt in Ihrem Unternehmen die IT-Sicherheitsstrategie um?

**Basis:** Frage nach der Entscheidung: Alle Unternehmen // Frage nach der Umsetzung: Unternehmen mit interner Entscheidung zur IT-Sicherheitsstrategie

Angaben in Prozent

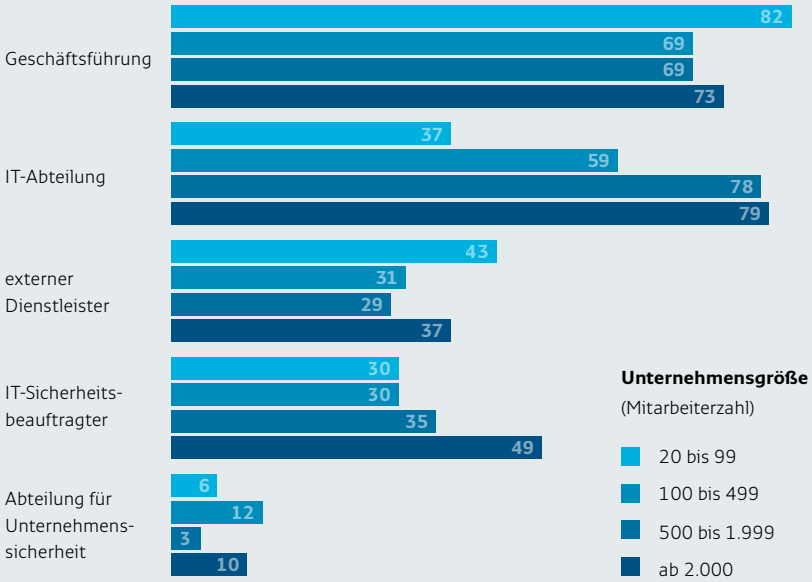
## Entscheidungen über IT-Sicherheitsstrategie

**Während bei den kleinen Unternehmen mit weniger als 100 Mitarbeitern oft die Geschäftsführung allein über IT-Sicherheitsstrategie entscheidet, wächst der Kreis der Entscheidungsbeteiligten mit der Unternehmensgröße.**

Vor allem ist dies darauf zurückzuführen, dass auf IT-Sicherheit spezialisierte Abteilungen oder Führungspositionen oft erst ab einer gewissen Unternehmensgröße eingerichtet werden. So ist in etwa vier von fünf größeren Unternehmen ab 500 Mitarbeitern eine IT-Abteilung vorhanden, die in sicherheitsstrategischen Fragen mitentscheidet. Hingegen verfügen nur zwei von fünf kleinen Unternehmen mit unter 100 Mitarbeitern über eine eigene IT-Abteilung mit Mitspracherecht bei der IT-Sicherheitsstrategie. Ähnliches gilt für die IT-Sicherheitsbeauftragten, die in fast jedem zweiten Großunternehmen die Sicherheitsstrategie mitbestimmen. Bei kleineren Unternehmen mit weniger als 500 Mitarbeitern ist dies nicht einmal in jedem dritten Betrieb der Fall.

Kleinere Unternehmen lassen sich dagegen verhältnismäßig häufig (43 Prozent) durch externe Dienstleister bei der IT-Sicherheit strategisch beraten. Weil in kleineren Unternehmen nur selten Spezialisten für IT-Sicherheit verfügbar sind, erscheint hier eine verstärkte Einbeziehung externer Sicherheitsexperten nachvollziehbar. Allerdings kompensieren die kleinen Unternehmen fehlendes betriebseigenes Know-how nur selten ausreichend durch externe Berater und Dienstleister: So entscheidet in fast jedem dritten kleinen Unternehmen mit weniger als 100 Beschäftigten die Geschäftsführung allein (!) über die IT-Sicherheitsstrategie (30 Prozent), also ohne Beratung durch interne oder externe Spezialisten. Dies geschieht in größeren Unternehmen ab 100 Beschäftigten kaum (12 Prozent), in sehr großen Unternehmen praktisch überhaupt nicht.

## IT-Sicherheitsstrategie: Je größer ein Unternehmen, umso mehr Entscheider.




**Frage:** Wer entscheidet in Ihrem Unternehmen über die IT-Sicherheitsstrategie?

Angaben in Prozent

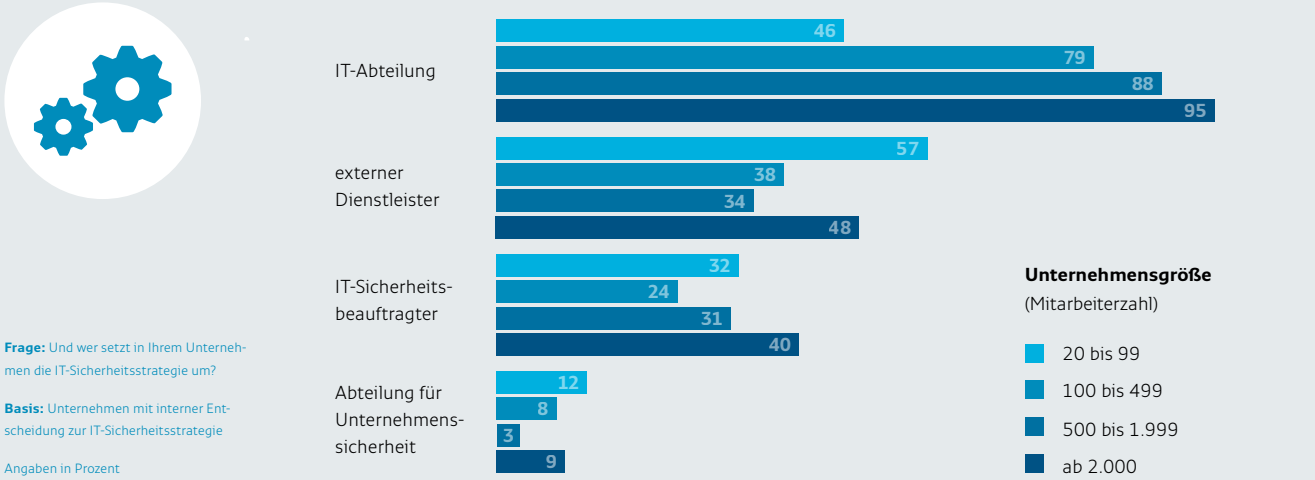
## Umsetzung der IT-Sicherheitsstrategie

Bei der Umsetzung der IT-Sicherheitsstrategie ergibt sich ein ähnliches Bild wie bei der Strategieentwicklung: Während die meisten kleineren Unternehmen häufig mangels interner personeller Ressourcen eher auf externe Anbieter setzen (unter 100 Mitarbeiter: 57 Prozent), ist mit zunehmender Unternehmensgröße vor allem die eigene IT-Abteilung für die Umsetzung der Sicherheitsstrategie verantwortlich.

Insgesamt sind bei größeren Unternehmen deutlich mehr Akteure an der Gewährleistung von IT-Sicherheit im Unternehmen beteiligt als bei kleineren Unternehmen.

Jedoch spielen externe Dienstleister auch bei sehr großen Unternehmen mit 2.000 oder mehr Mitarbeitern eine bedeutende Rolle. Fast jedes zweite Großunternehmen beauftragt externe Anbieter von IT-Sicherheitsdienstleistungen mit der Umsetzung der eigenen Sicherheitsstrategie.

## Umsetzung der IT-Sicherheitsstrategie: Sehr kleine und sehr große Unternehmen setzen besonders häufig auf Externe.




**Frage:** Und wer setzt in Ihrem Unternehmen die IT-Sicherheitsstrategie um?

**Basis:** Unternehmen mit interner Entscheidung zur IT-Sicherheitsstrategie

Angaben in Prozent

# 3 Umsetzung von IT-Sicherheitsmaßnahmen

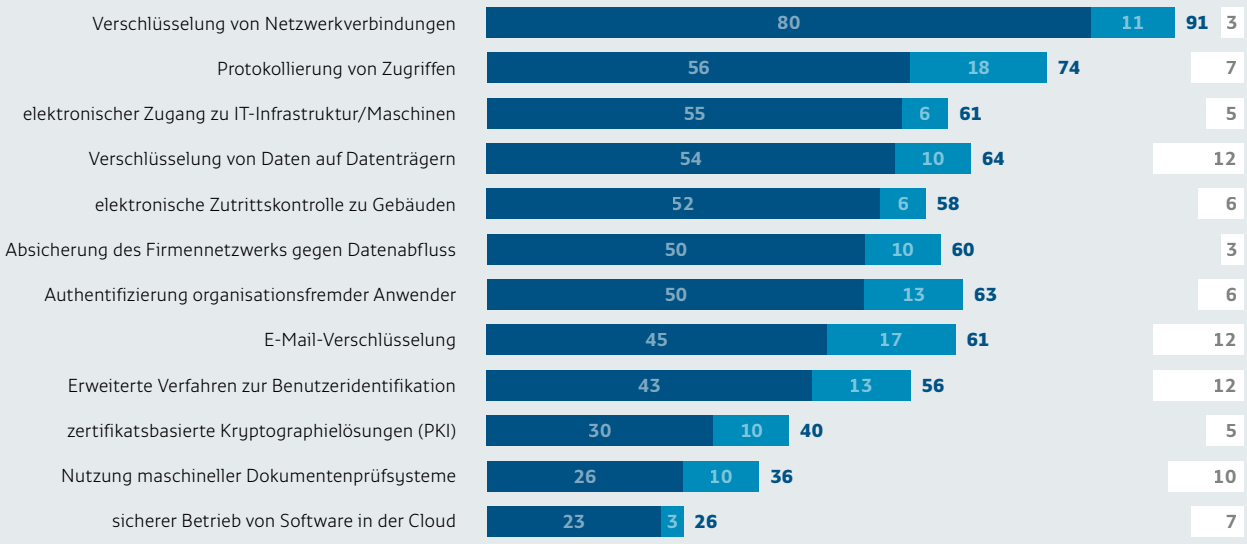
**IT-Sicherheitsmaßnahmen lassen sich grob und technische, organisatorische und personelle einteilen. Im Folgenden soll dargestellt werden, in welchem Maße die Unternehmen in Deutschland solche Maßnahmen bereits umgesetzt haben oder dies planen.**

## 3.1 Technische IT-Sicherheitsmaßnahmen

**Während essenzielle technische Maßnahmen der IT-Sicherheit wie die Verschlüsselung des eigenen Netzwerks in Unternehmen weit verbreitet sind, werden darüber hinausgehende Sicherheitsmaßnahmen wie eine sicherere Benutzerauthentifizierung oder zertifikatsbasierte PKI-Lösungen nur von wenigen Unternehmen in Deutschland eingesetzt.**

So nutzen die allermeisten Unternehmen in der einen oder anderen Form verschlüsselte Netzwerkverbindungen, um eine sichere standortunabhängige Kommunikation mit ihren Mitarbeitern zu gewährleisten: vier von fünf Unternehmen tun dies bereits, von den größeren Unternehmen mit mindestens 500 Mitarbeitern verwenden fast alle eine Netzwerkverschlüsselung. Weitere 11 Prozent planen eine Verschlüsselung ihres Firmennetzwerks. Für lediglich 5 Prozent der Unternehmen in Deutschland ist dies aktuell kein Thema.

### Verschlüsselung des Firmennetzwerks ist am weitesten verbreitet.




**Frage:** Welche der folgenden technischen IT-Sicherheitsmaßnahmen hat Ihr Unternehmen bereits umgesetzt bzw. plant Ihr Unternehmen in Zukunft umzusetzen, um sich gegen IT-Sicherheitsvorfälle zu schützen?

Angaben in Prozent

Deutlich seltener werden Netzwerkzugriffe auch protokolliert (56 Prozent). Allerdings ist hier der Anteil der Nutzungsplaner sehr hoch: 18 Prozent planen eine Protokollierung von Zugriffen.

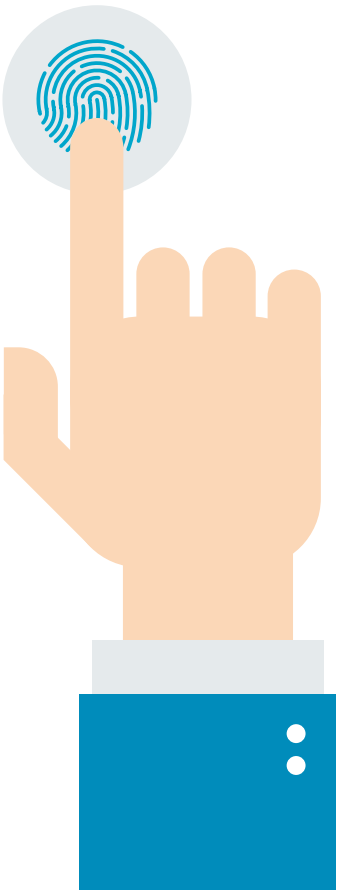
Während die große Mehrheit der Unternehmen ihre virtuelle Infrastruktur etwa mittels verschlüsselter Netzwerkverbindungen schützt, ist ihre physische Infrastruktur oft deutlich schlechter gesichert: So schützt jeweils nur etwas mehr als die Hälfte der befragten Unternehmen ihre Datenträger durch eine Verschlüsselung vor unbefugtem Zugriff (54 Prozent) oder verhindert durch elektronische Kontrollen den Zugang von Fremden zu ihren IT-Anlagen, Maschinen oder Gebäuden (55 Prozent bzw. 52 Prozent).

Neben der Verhinderung von Fremdzugriffen auf die eigene IT-Infrastruktur ist für Unternehmen der Datenabfluss von innen besonders problematisch, da hier der Zugriff durch autorisiertes Personal erfolgt. Nur jedes zweite Unternehmen verfügt über geeignete Lösungen für dieses Problem.

Erweiterte Authentifizierungsverfahren, die etwa über die Eingabe statischer Passwörter zur Benutzeridentifikation hinausgehen, setzen weniger als die Hälfte der Unternehmen in Deutschland ein (43 Prozent). Für organisationsfremde Nutzer werden häufiger sichere Identifikationsverfahren angewendet, allerdings auch nur in jedem zweiten Unternehmen (50 Prozent).

Auch E-Mail-Verschlüsselung gehört keineswegs zum Standard in deutschen Unternehmen: Nur 45 Prozent schützen ihre E-Mail-Kommunikation über ein Verschlüsselungssystem.

Noch seltener werden zertifikatsbasierte Kryptographielösungen über eine – eigene oder fremde – Public-Key-Infrastruktur genutzt: Nur drei von zehn nutzen solche PKI-Lösungen, die herkömmlichen Verschlüsselungs- und Authentifizierungsverfahren überlegen sind.



Während die oben genannten IT-Sicherheitsmaßnahmen praktisch für jedes Unternehmen relevant sind, sind andere nur in bestimmten Unternehmen anwendbar: Maschinelle Dokumentenprüfsysteme etwa sind nur in solchen Unternehmen empfehlenswert, in denen in größerem Umfang Dokumente geprüft werden müssen, etwa im Bank- und Versicherungswesen. 37 Prozent der Unternehmen in dieser Branche verwenden solche Systeme, beispielsweise zur Überprüfung der Echtheit von Identitätsdokumenten bei der Kontoeröffnung oder Vertragsabschlüssen mit Kunden. Unter den Unternehmen in Deutschland insgesamt kommen nur in etwa jedem vierten maschinelle Dokumentenprüfsysteme zur Anwendung.

Ähnliches gilt für IT-Sicherheitsmaßnahmen für Software, die in einer Cloud betrieben wird: Da bisher nur eine Minderheit der Unternehmen externe Cloud-Angebote nutzt (siehe Abschnitt 7.1), wenden – bezogen auf die gesamte deutsche Wirtschaft – nur wenige Unternehmen (23 Prozent) entsprechende Sicherheitsmaßnahmen an. Jene Unternehmen, die bereits Cloud-Angebote nutzen, haben jedoch zu 74 Prozent spezielle Maßnahmen zum sicheren Betrieb von Software in der Cloud umgesetzt.

Insgesamt zeigt sich: Kleine Unternehmen mit weniger als 100 Beschäftigten sind bei der Umsetzung der meisten technischen IT-Sicherheitsmaßnahmen deutlich schlechter aufgestellt als größere Unternehmen.

Vergleicht man die aktuelle Umsetzung der einzelnen IT-Sicherheitsmaßnahmen in den Unternehmen mit deren Umsetzung im Vorjahr, so zeigt sich bei einigen der genannten Maßnahmen eine leichte Zunahme, beispielsweise bei der Protokollierung von Zugriffen (von 48 auf 56 Prozent), bei der Absicherung des Firmennetzwerks gegen Datenabfluss von innen (von 46 auf 50 Prozent) oder bei Verfahren zur sicheren Authentifizierung organisationsfremder Anwender (von 44 auf 50 Prozent). In diesen Bereichen hat sich der Schutz der Unternehmen vor IT-Sicherheitsvorfällen seit dem Vorjahr also etwas verbessert. Bei einigen relevanten Maßnahmen (Netzwerkverschlüsselung, Datenträgerverschlüsselung, E-Mail-Verschlüsselung, erweiterte Benutzeridentifikationsverfahren und zertifikatsbasierte Kryptographielösungen) haben sich jedoch die Nutzeranteile gegenüber 2016 nicht wesentlich erhöht.

## 3.2 Organisatorische IT-Sicherheitsmaßnahmen

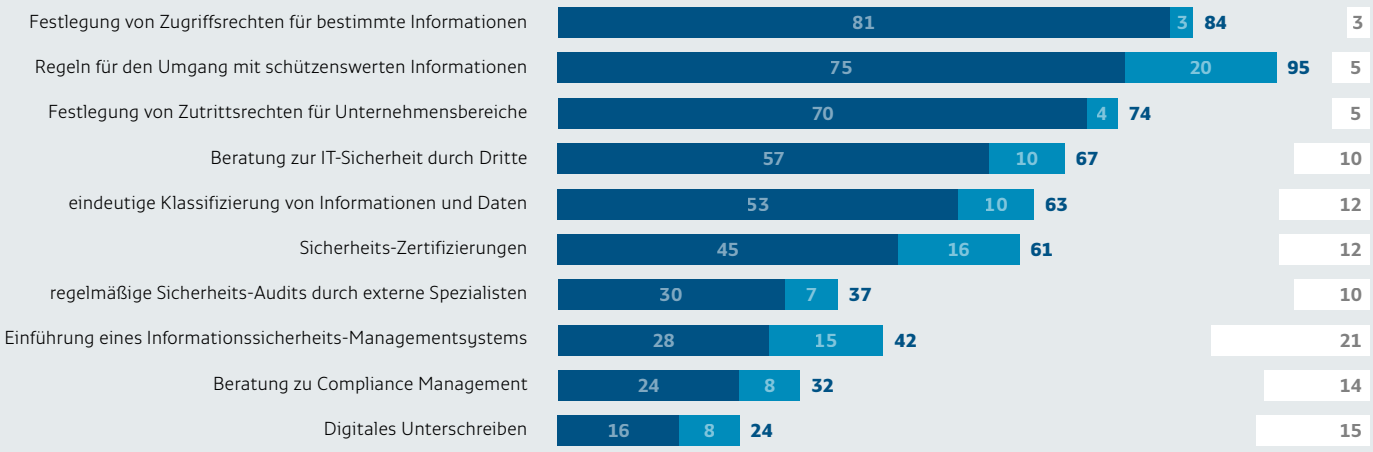
**Während es in den meisten Unternehmen grundlegende organisatorische Maßnahmen zum Schutz vor IT-Sicherheitsvorfällen gibt, verzichtet die große Mehrheit auf aufwändigere Maßnahmen für eine umfassende und dauerhafte Gewährleistung von Informationssicherheit wie etwa regelmäßige Sicherheits-Audits oder die Einrichtung eines Informationssicherheits-Managementsystems (ISMS).**

In vier von fünf deutschen Unternehmen sind die Zugriffsrechte für bestimmte Informationen klar festgelegt. Fast ebenso häufig gibt es klare Regeln für den Umgang mit schützenswerten Informationen (75 Prozent). Zudem sieht jedes fünfte Unternehmen bei diesem wichtigen Thema Nachholbedarf und plant daher, solche Regeln für alle Mitarbeiter verbindlich festzulegen. Eine eindeutige Klassifizierung von Informationen und Daten, die die Schutzklasse von Daten und Dokumenten festlegt und damit schützenswerte Informationen zu identifizieren hilft, wird allerdings nur in jedem zweiten Unternehmen (53 Prozent) vorgenommen.

Über zwei Drittel der Unternehmen regeln den Zugang zu bestimmten Unternehmensbereichen wie z. B. Serverräumen mittels Festlegung von Zutrittsrechten.

Zwar lässt sich die Mehrheit der Unternehmen beim Thema IT-Sicherheit von externen Spezialisten beraten (57 Prozent), regelmäßige von Experten durchgeführte Sicherheits-Audits nehmen aber nur die wenigsten in Anspruch (30 Prozent), ebenso wie externe Beratung zum Compliance Management (24 Prozent).

### Die meisten Unternehmen verzichten auf aufwändigere organisatorische IT-Sicherheitsmaßnahmen.




**Frage:** Welche der folgenden organisatorischen bzw. prozesstechnischen Sicherheitsmaßnahmen hat Ihr Unternehmen bereits umgesetzt bzw. plant Ihr Unternehmen in Zukunft umzusetzen, um sich gegen IT-Sicherheitsvorfälle zu schützen?

Angaben in Prozent

Auch externe IT-Sicherheits-Zertifizierungen – etwa nach der internationalen Norm ISO 27001 oder dem BSI-Grundschutz-Standard – nimmt nicht einmal jedes zweite Unternehmen (45 Prozent) in Anspruch.

Noch seltener ist die Etablierung eines Managementsystems für Informationssicherheit (ISMS): Weniger als drei von zehn Unternehmen haben bisher ein solches standardisiertes System für die umfassende und dauerhafte Gewährleistung von IT-Sicherheit eingeführt.

Digitale Signaturen sind schließlich von allen genannten Sicherheitsmaßnahmen noch am wenigsten verbreitet: Nur in jedem sechsten Unternehmen existieren die Voraussetzungen für das digitale Unterschreiben.

Wie schon die technischen Sicherheitsmaßnahmen werden auch organisatorisch-prozesstechnische Maßnahmen in größeren Unternehmen deutlich häufiger umgesetzt als in kleineren Unternehmen. So nimmt jeweils eine deutliche Mehrheit der großen Unternehmen mit mindestens 2.000 Mitarbeitern Informationsklassifizierungen vor oder nimmt Sicherheitszertifizierungen in Anspruch (75 Prozent bzw. 68 Prozent). Und immerhin jedes zweite Großunternehmen lässt regelmäßig Sicherheits-Audits durchführen, verfügt über ein ISMS oder lässt sich zum Thema Compliance beraten. Demgegenüber schützt sich nur eine Minderheit der kleinen Unternehmen durch solche Maßnahmen vor IT-Sicherheitsrisiken.

Anders als bei den technischen IT-Sicherheitsmaßnahmen gibt es bei den organisatorischen Maßnahmen gegenüber der Vergleichsbefragung von 2016 leider keine signifikanten Verbesserungen.

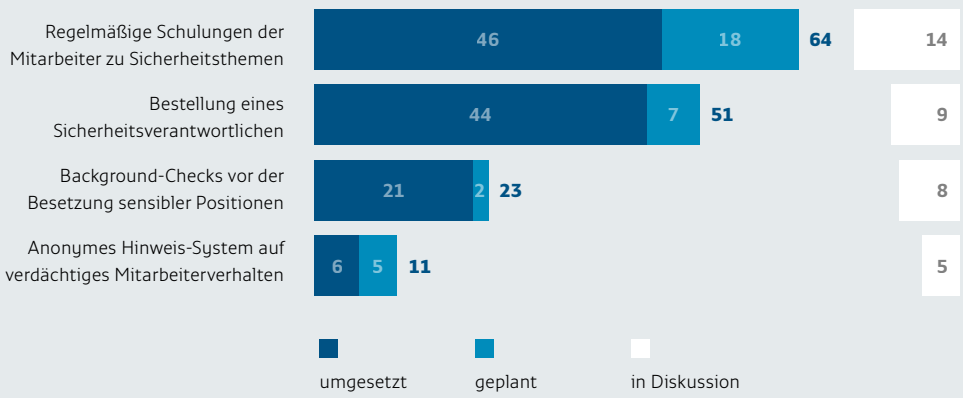
## 3.3 Personelle IT-Sicherheitsmaßnahmen

**Damit technische und organisatorische Maßnahmen von Unternehmen zur Verhinderung von Cyberangriffen nicht ins Leere laufen, muss das gesamte Personal auf die verschiedenen Aspekte der Informationssicherheit sensibilisiert sein.**

Schlecht geschulte Mitarbeiter, die sorglos E-Mail-Anhänge öffnen oder fremde USB-Sticks an ihren Firmen-Laptop anschließen, sind ein ernstes Sicherheitsrisiko für jedes Unternehmen. Umso beunruhigender ist der Befund, dass nicht einmal die Hälfte der befragten Unternehmen (46 Prozent) regelmäßige Schulungen ihrer Mitarbeiter zu Themen der IT-Sicherheit durchführt. Lediglich Banken, Versicherungen sowie ITK-Unternehmen schulen hierzu regelmäßig (89 Prozent bzw. 80 Prozent). Allerdings planen zumindest viele Unternehmen regelmäßige Schulungen, fast jedes fünfte Unternehmen (18 Prozent) sieht hier offenbar einen Nachholbedarf.

Einen IT-Sicherheitsverantwortlichen (44 Prozent), der die Unternehmensleitung zu Fragen der IT-Sicherheit berät, zudem beispielsweise auch die Mitarbeiter über Sicherheitsrisiken aufklärt, gibt es vor allem in größeren Unternehmen: Drei Viertel der Unternehmen mit mindestens 2.000 Mitarbeitern haben einen Sicherheitsverantwortlichen bestellt, während nur zwei von fünf kleinen Unternehmen mit weniger als 100 Mitarbeitern eine solche Position besetzen. Background-Checks von Bewerbern für sensible Positionen lässt nur jedes fünfte Unternehmen in Deutschland durchführen; vor allem Banken und Versicherungen sowie Transport- und Logistik- Unternehmen versuchen auf diese Weise, Risiken zu minimieren (46 bzw. 48 Prozent). Whistle-Blowing-Tools, also anonyme Hinweissysteme, die verdächtiges Mitarbeiterverhalten aufdecken sollen, haben nur die wenigsten Unternehmen etabliert (6 Prozent). Bei Großunternehmen sind sie allerdings deutlich stärker verbreitet (24 Prozent). Im Branchenvergleich zeigt sich vor allem der Finanzsektor als Vorreiter: Von den Banken und Versicherungen hat sogar eine Mehrheit (54 Prozent) bereits ein solches System eingeführt.

### Nur jedes zweite Unternehmen schult seine Mitarbeiter regelmäßig zu IT-Sicherheit.




**Frage:** Welche der folgenden personellen Sicherheitsmaßnahmen hat Ihr Unternehmen bereits umgesetzt bzw. plant Ihr Unternehmen in Zukunft umzusetzen, um sich gegen IT-Sicherheitsvorfälle zu schützen?

Angaben in Prozent

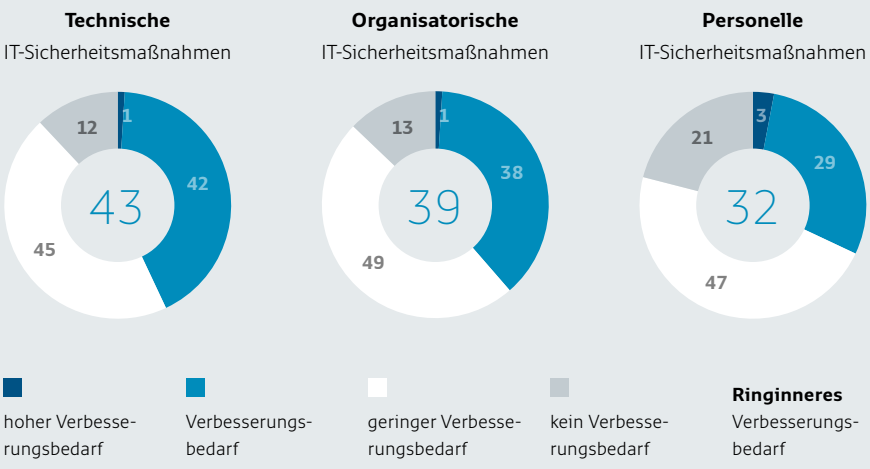
## 3.4 Verbesserungsbedarf bei Sicherheitsmaßnahmen

**Um festzustellen, wie stark ihr derzeitiges Engagement in Sachen IT-Sicherheit aus eigener Sicht von dem Erreichbaren abweicht, wurden die Unternehmen auch gefragt, ob und in welchem Maße sie im eigenen Unternehmen Verbesserungsbedarf in den drei verschiedenen Maßnahmenbereichen sehen.**

Dabei sieht sich die Mehrheit der Unternehmen – unabhängig vom tatsächlichen Stand – insgesamt zwar gut aufgestellt und sieht entsprechend keinen oder nur geringen Verbesserungsbedarf. Je nach Maßnahmenbereich sind aber immerhin drei bis vier von zehn Unternehmen der Meinung, dass die bisher im eigenen Unternehmen umgesetzten IT-Sicherheitsmaßnahmen noch verbessert werden müssen. Wie erwartet, werden vor allem die technischen Maßnahmen zum Schutz vor IT-Sicherheitsvorfällen als noch nicht ausreichend angesehen: 43 Prozent der Unternehmen sehen hier Verbesserungsbedarf. Etwas niedriger ist dieser Anteil bei den organisatorischen bzw. prozesstechnischen Sicherheitsmaßnahmen (39 Prozent). Am vergleichsweise geringsten ist der subjektive Verbesserungsbedarf jedoch bei den verfügbaren personellen Maßnahmen (32 Prozent).

Auffällig ist: Die größeren Unternehmen, die viele der angesprochenen Maßnahmen bereits vergleichsweise häufig anwenden, sehen in allen Bereichen mehr Handlungsbedarf als kleine Unternehmen. So sehen zwei Drittel der Großunternehmen Verbesserungsbedarf bei den eigenen organisatorischen IT-Sicherheitsmaßnahmen. Bei Unternehmen mit weniger als 100 Mitarbeitern ist es nur ein Drittel. Dies kann zweierlei Gründe haben: Zum einen erreichen kleinere Unternehmen bei der IT-Sicherheit häufiger personelle und finanzielle Grenzen. Zweitens sind größere Unternehmen häufiger Ziel von Cyberattacken, entsprechend steigen Risikowahrnehmung und Handlungsdruck. Im Branchenvergleich sind es vor allem Energie- und Versorgungsunternehmen sowie Maschinen- und Anlagenbauer, die in ihren Unternehmen Verbesserungsbedarf bei Maßnahmen der IT-Sicherheit sehen.

### Maßnahmen zur IT-Sicherheit: Verbesserungsbedarf in mindestens jedem dritten Unternehmen.




**Frage:** Inwiefern sehen Sie in Ihrem Unternehmen Verbesserungsbedarf bei den technischen, organisatorischen/prozessualen und personellen IT-Sicherheitsmaßnahmen?

Angaben in Prozent

# 4 IT-Sicherheitsmaßnahmen-Index

## 4.1 Berechnung des IT-Sicherheitsmaßnahmen-Index

**Die bisher im Detail dargestellten möglichen Einzelmaßnahmen zur Verbesserung der IT-Sicherheit im Unternehmen sollen im Folgenden in einer Zusammenschau betrachtet werden. Dazu wurden die einzelnen IT-Sicherheitsmaßnahmen zu einem Gesamtindex zusammengefasst, in den sämtliche im jeweiligen Unternehmen umgesetzten und geplanten Maßnahmen eingehen.**

Der sich ergebende Index-Wert beschreibt dann das Maß, in dem sich das jeweilige Unternehmen durch betriebseigene Maßnahmen vor IT-Sicherheitsrisiken schützt: Während ein Indexwert von 0 bedeutet, dass das betreffende Unternehmen gar keine der genannten Sicherheitsmaßnahmen anwendet, besagt ein Indexwert von 100, dass alle erhobenen Sicherheitsmaßnahmen angewendet werden.

In den so gebildeten Gesamtindex gehen alle 26 genannten IT-Sicherheitsmaßnahmen ein: zwölf technische, zehn organisatorische und vier personelle, wobei die technischen Maßnahmen mit einem Gewicht von 50 Prozent in den Index eingehen, die organisatorischen und personellen jeweils mit einem Gewicht von 25 Prozent.

### IT-Sicherheitsmaßnahmen-Index: Konstruktion

Gewichtung der Einzelkomponenten

**IT-Sicherheitsmaßnahmen-Index** (0 bis 100 Punkte)

**Technische**
IT-Sicherheitsmaßnahmen

**Umgesetzte und geplante Maßnahmen, z. B. in den Bereichen:**

- Verschlüsselung von Online-Kommunikation, Netzwerkverbindungen sowie Datenträgern
- Elektronische Authentifizierungsverfahren
- Absicherung gegen unerwünschten Datenabfluss
- Sicherung von Cloud Anwendungen

**Organisatorische**
IT-Sicherheitsmaßnahmen

**Umgesetzte und geplante Maßnahmen, z. B. in den Bereichen:**

- Zugriffsrechtemanagement für Informationen und Räumlichkeiten
- Klassifizierung sensibler Informationen, Umgangsregeln
- Sicherheits-Zertifizierungen
- (Externe) Beratung zu IT-Sicherheit und Compliance Management

**Personelle**
IT-Sicherheitsmaßnahmen

**Umgesetzte und geplante Maßnahmen, z. B. in den Bereichen:**

- Regelmäßige Mitarbeiterschulungen zu Sicherheitsthemen
- Bestellung eines Sicherheitsverantwortlichen
- Background-Checks vor der Besetzung sensibler Positionen
- Whistle-Blowing-Tools

## 4.2 Der IT-Sicherheitsmaßnahmen-Index nach Unternehmensgröße und Branche

**Mit einem durchschnittlichen Indexwert von 56,4 ist das IT-Schutzniveau der Unternehmen in Deutschland nur mittelmäßig. Das Sicherheitsniveau verbessert sich mit zunehmender Unternehmensgröße.**

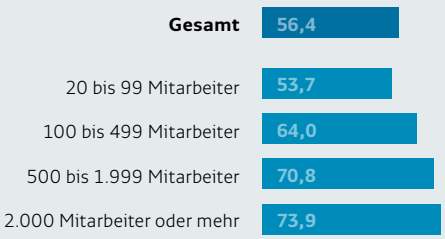
Während kleine Unternehmen mit weniger als 100 Mitarbeitern auf einen leicht unterdurchschnittlichen Indexwert von 53,7 kommen, liegt er bei den Großunternehmen um 20 Punkte höher (73,9). Das Gesamtpaket an angewandten oder geplanten IT-Sicherheitsmaßnahmen ist also umso umfangreicher, je größer das Unternehmen ist: Höhere IT-Budgets und eine bessere Personalausstattung im IT-Bereich erlauben größeren Unternehmen die Umsetzung längerer Maßnahmenkataloge als kleineren Unternehmen.

Da die allermeisten Unternehmen in Deutschland jedoch kleine Unternehmen mit weniger als 100 Beschäftigten sind, sind gerade jene Unternehmen, die das Gros der deutschen Wirtschaft ausmachen, sicherheitstechnisch besonders verwundbar.

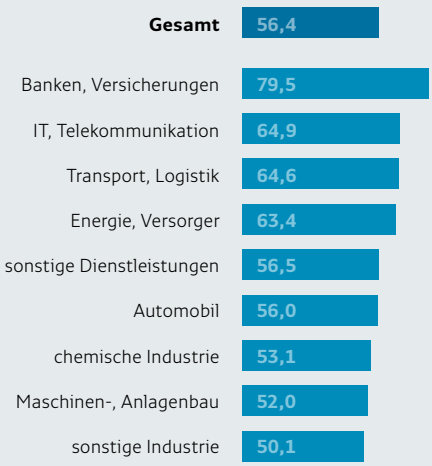
Vergleicht man die Indexwerte der einzelnen Branchen der deutschen Wirtschaft, so zeigt sich ein deutlicher Vorsprung des Finanzsektors bei der Umsetzung von IT-Sicherheitsmaßnahmen: Banken und Versicherungen liegen fast 15 Prozentpunkte vor dem Zweitplatzierten, den IT- und Telekommunikations-Unternehmen (79,5 vs. 64,9). Am schlechtesten schneiden dagegen die Maschinen- und Anlagenbauer sowie die sonstigen Industrieunternehmen ab, die jeweils auf nur etwas mehr als 50 Indexpunkte kommen (52,0 bzw. 50,1).

### Finanzsektor und Großunternehmen legen besonders großen Wert auf IT-Sicherheit.

**Indexergebnis nach Unternehmensgröße**




**Indexergebnis nach Branchen**




**Dargestellt:** Index-Durchschnittswerte auf einer Skala von 0 bis 100

## 5 Gesetzliche Regelungen zur IT-Sicherheit als Herausforderung

**Triebkraft von Investitionen der Unternehmen in die IT-Sicherheit sind oft Vorgaben des Gesetzgebers. Diese sind für die Unternehmen jedoch häufig nur schwer zu überblicken und umzusetzen.**

So fühlt sich auch die Mehrheit der IT-Entscheider in deutschen Unternehmen (57 Prozent) zumindest ab und zu von den gesetzlichen Regelungen rund um IT-Sicherheit und Datenschutz überfordert, jeder zehnte sogar sehr häufig. 32 Prozent der Befragten sind nach eigenen Angaben nur selten überfordert, nur 8 Prozent nie.

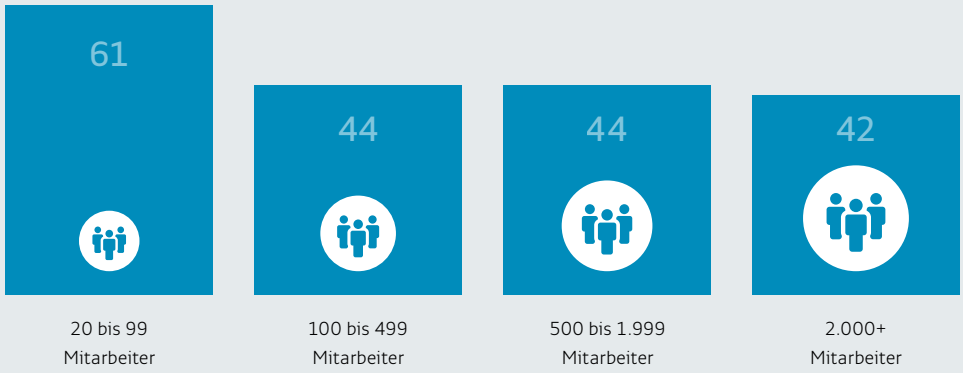
Vor allem kleinere Unternehmen haben Schwierigkeiten mit den gesetzlichen Anforderungen: Während sich jeweils knapp die Hälfte der mittleren und größeren Unternehmen mit der Umsetzung der verschiedenen Regelungen schwer tut, sind es bei Unternehmen mit weniger als 100 Beschäftigten 61 Prozent.

Unternehmen aus dem Finanzsektor und der Transport- und Logistik-Branche fühlen sich besonders häufig überfordert (73 Prozent bzw. 74 Prozent), Automobilunternehmen sowie Maschinen- und Anlagenbauer dagegen am seltensten (46 Prozent bzw. 44 Prozent).

### Mehrheit der Kleinunternehmen fühlt sich überfordert von gesetzlichen Regeln zu Datenschutz und IT-Sicherheit.

**Frage:** Fühlen Sie sich von den gesetzlichen Regeln rund um IT-Sicherheit und Datenschutz überfordert?

**Dargestellt:** Summe der Nennungsanteile „sehr häufig" und „ab und zu überfordert" in Prozent




## 6 Kooperation mit Anbietern von IT-Sicherheitslösungen

**Wie bereits im Abschnitt 2.2 festgestellt wurde, beauftragen Unternehmen oft externe Anbieter mit der Umsetzung von IT-Sicherheitsmaßnahmen. Viele Unternehmen lassen sich zusätzlich auch bei Entscheidungen zur eigenen IT-Sicherheitsstrategie von externen Spezialisten beraten.**

Wie gestaltet sich aber die Zusammenarbeit mit diesen Anbietern? Arbeiten die Unternehmen lieber mit einem einzigen Anbieter (alles aus einer Hand) zusammen oder werden die Aufträge über eine Vielzahl von Anbietern (Best Practice) gestreut? Diese Fragen sollen im folgenden Kapitel beantwortet werden.

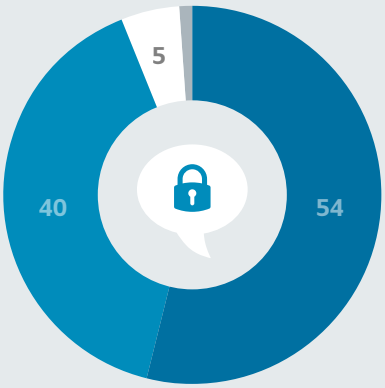
Die meisten Unternehmen in Deutschland (54 Prozent) bevorzugen externe IT-Sicherheitslösungen und entsprechende Beratung aus einer Hand; sie kooperieren dabei mit nur einem einzigen externen Anbieter. Zwei von fünf Unternehmen beziehen IT-Sicherheitslösungen von sehr wenigen Anbietern. Die wenigsten beauftragen viele verschiedene Anbieter mit Einzellösungen.

Allerdings gilt: Je größer das Unternehmen, desto eher werden mehrere verschiedene Anbieter beauftragt. Nur 6 Prozent der Unternehmen mit mehr als 2.000 Beschäftigten beziehen Sicherheitslösungen und Beratungsleistungen von nur einem einzigen Anbieter. Dies dürfte bei den vielen IT-Sicherheitsmaßnahmen, die größere Unternehmen etabliert haben, auch nur selten möglich sein.

Bemerkenswert ist: Der Anteil der Unternehmen, die mit nur einem Anbieter zusammenarbeiten, nimmt mit steigender Zahl der bereits umgesetzten oder geplanten IT-Sicherheitsmaßnahmen ab. So kooperieren immerhin zwei Drittel der Unternehmen mit einem Indexwert von unter 50 Punkten mit nur einem Anbieter. Bei Unternehmen mit einem Index von mindestens 75 Punkten sind es 40 Prozent.

**Frage:** Welche Strategie verfolgen Sie bei der Zusammenarbeit mit Anbietern von IT-Sicherheitslösungen?

Angaben in Prozent




Mehrheit bezieht IT-Lösungen und Beratungsleistungen von nur einem einzigen Anbieter.

- Inanspruchnahme eines Anbieters
- Inanspruchnahme sehr weniger Anbieter
- Inanspruchnahme vieler Anbieter
- Weiß nicht / Keine Angabe

# 7 Cloud-Angebote: Nutzung und Gründe für die Nichtnutzung

**Durch die Nutzung von Cloud-Angeboten externer Anbieter können Unternehmen Kosten und Personal für den Aufbau eigener IT-Infrastruktur und/oder Software einsparen. Gleichzeitig versprechen Cloud-Angebote Flexibilität: Durch die Skalierbarkeit der Dienste können Nutzungsspitzen ausgeglichen werden. Zudem können Mitarbeiter von allen Standorten und mobil auf die IT zugreifen.**

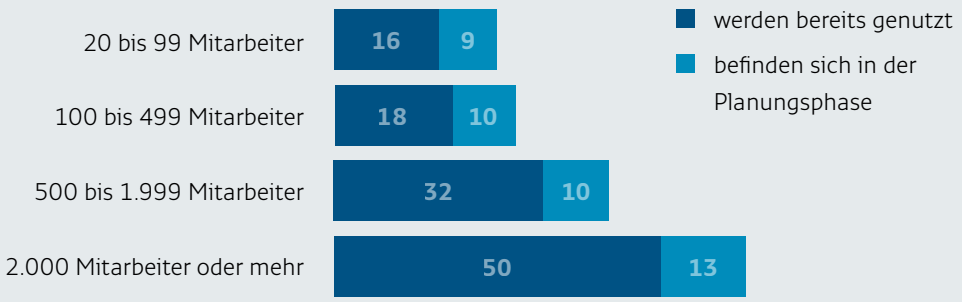
Die Nutzung von Cloud-Services kann für Unternehmen allerdings auch Nachteile haben. Im Folgenden soll untersucht werden, in welchem Maße Unternehmen in Deutschland von Cloud-Angeboten Gebrauch machen, welche Kriterien bei der Auswahl eines Cloud-Anbieters entscheidend sind und welche Argumente gegen die Nutzung von Cloud-Angeboten sprechen.

## 7.1 Nutzung von Cloud-Angeboten

**Jedes sechste deutsche Unternehmen (17 Prozent) nimmt bereits externe Cloud-Services in Anspruch. Zusätzliche neun Prozent planen eine Nutzung. Für die meisten Unternehmen (71 Prozent) ist die Nutzung von Cloud-Angeboten bisher jedoch kein Thema.**

Vor allem größere Unternehmen nutzen solche Angebote: Von den mittleren Unternehmen mit 500 bis unter 2.000 Mitarbeitern nimmt jedes dritte (32 Prozent) externe Cloud-Services in Anspruch, bei den großen Unternehmen mit mindestens 2.000 Mitarbeitern ist es sogar jedes zweite.

Vor allem größere Unternehmen nutzen Cloud-Angebote.




**Frage:** Wie steht Ihr Unternehmen zu Cloud-Angeboten?

Angaben in Prozent

## 7.2 Kriterien für die Wahl des Cloud-Anbieters

**Das mit Abstand wichtigste Kriterium für die Wahl eines Cloud-Anbieters ist Datensicherheit. Da die in der Cloud befindlichen Daten auf den Servern des jeweiligen Anbieters und nicht im betriebseigenen Rechenzentrum liegen, muss der Nutzer sich darauf verlassen können, dass die Daten dort sicher sind. So ist das Kriterium Datensicherheit für fast zwei Drittel der Unternehmen, die Cloud-Angebote nutzen oder dies planen, eines der drei wichtigsten Auswahlkriterien.**

Cloud-Anbieter haben ihren Sitz oft im Ausland, etwa den USA, und betreiben auch ihre Server dort, sodass auch die Datenschutzbestimmungen des jeweiligen Landes gelten. Deshalb legen viele Unternehmen Wert darauf, dass der Cloud-Anbieter ihrer Wahl seinen Sitz in Deutschland hat (42 Prozent) oder sich zumindest die Cloud-Server in Deutschland befinden (33 Prozent), damit etwa das Datenschutzniveau den deutschen Vorschriften entsprechen muss. So gehört auch der Datenschutz allgemein für fast drei von zehn Unternehmen zu den drei Hauptkriterien bei der Anbieterauswahl.

Die Möglichkeit, mit dem Cloud-Anbieter zusammenzuarbeiten, hält ebenfalls jedes dritte Unternehmen (32 Prozent) für wichtig. Der Preis wird zwar nur selten als wichtigstes Kriterium genannt (4 Prozent), vergleichsweise häufig aber als zweit- oder drittwichtigstes (32 Prozent). Kriterien wie Einfachheit der Nutzung (23 Prozent) oder Skalierbarkeit (15 Prozent) sind weniger zentrale Aspekte. Für größere Unternehmen ist Skalierbarkeit jedoch wichtiger, um etwa kurzfristig auftretende Nutzungsspitzen, z. B. im Weihnachtsgeschäft, kompensieren zu können.

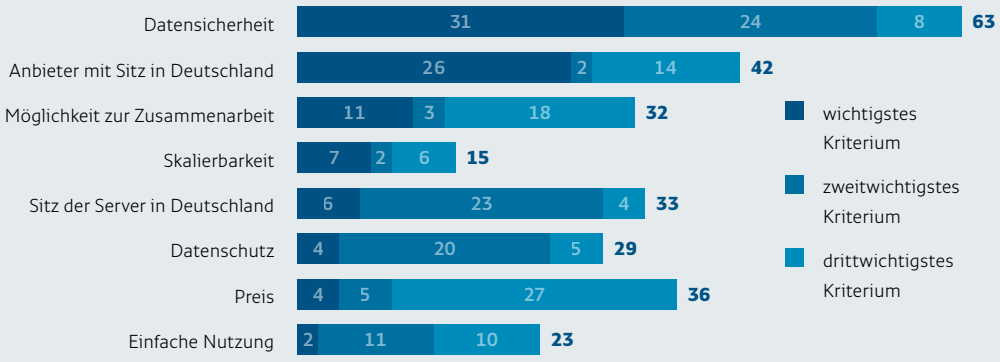
Insgesamt zeigt sich, dass die Anforderungsprofile an potenzielle Cloud-Anbieter stark abhängig sind von der Unternehmensgröße: Während kleine Unternehmen vor allem auf Datensicherheit (70 Prozent) und einen deutschen Unternehmenssitz der Anbieter (48 Prozent) achten, ist den großen Unternehmen neben der Datensicherheit und dem Sitz der Server in Deutschland (jeweils 41 Prozent) auch der Preis sehr wichtig (47 Prozent).

**Frage:** Was war bzw. wäre ausschlaggebend bei der Auswahl von Cloud-Anbietern?

**Basis:** Unternehmen, die Cloud-Angebote nutzen oder dies planen

Angaben in Prozent

### Datensicherheit ist wichtigstes Kriterium für Auswahl des Cloud-Anbieters.



## 7.3 Argumente gegen die Nutzung von Cloud-Angeboten

**Das häufigste Argument gegen die Nutzung von Cloud-Angeboten ist das Argument der mangelnden eigenen Kontrolle über die IT. 81 Prozent der Unternehmen, die bisher keine Cloud-Angebote nutzen und dies auch nicht planen, begründen ihre Entscheidung damit, dass sie selbst die Hoheit über die IT haben wollen.**

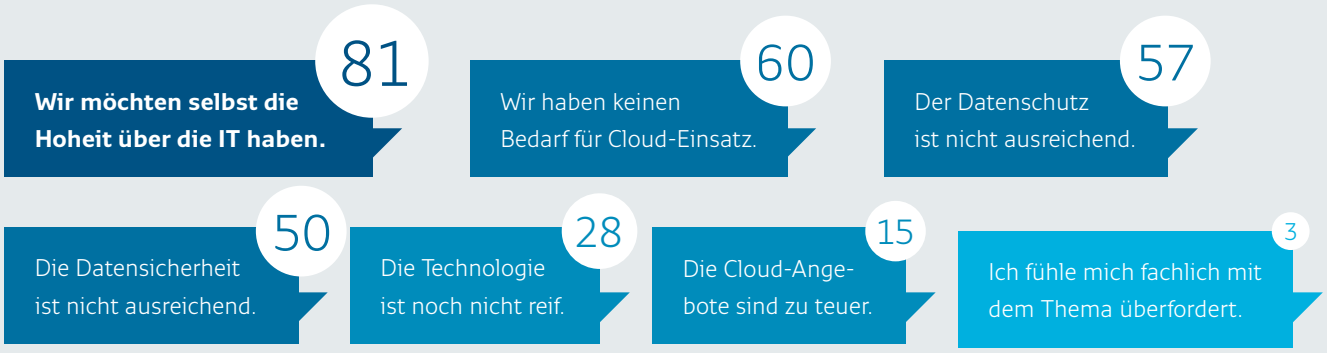
Am zweithäufigsten wird der mangelnde Bedarf für die Nutzung von Cloud-Angeboten genannt: drei von fünf Nichtnutzern geben an, dass sie solche Cloud-Services nicht brauchen. Bei den Großunternehmen ist dieser Anteil mit 32 Prozent allerdings deutlich geringer als bei kleinen Unternehmen (63 Prozent).

An dritter und vierter Stelle folgen Bedenken bei der Gewährleistung von Datenschutz und Datensicherheit: Viele Nichtnutzer trauen den Cloud-Anbietern keine ausreichende Gewährleistung von Datenschutz (57 Prozent) bzw. Datensicherheit (50 Prozent) zu. Vor allem große Unternehmen sind hier skeptisch (71 Prozent bzw. 63 Prozent).

Dass die Cloud-Technologie noch nicht ausgereift sei, meinen fast drei von zehn Unternehmen, die auf die Nutzung von Cloud-Angeboten verzichten.

Der Kostenaspekt wird nur von einer kleinen Minderheit (15 Prozent) als Begründung für ihre Ablehnung von Cloud-Services genannt, noch seltener wird sie mit der eigenen fachlichen Überforderung bei diesem Thema begründet (3 Prozent).

### Gründe gegen Cloud-Nutzung: Unternehmen möchten ihre IT in der Regel selbst in der Hand haben.




**Frage:** Warum nutzen Sie bislang keine Cloud-Angebote?

**Basis:** Unternehmen, die keine Cloud-Angebote nutzen und dies auch nicht planen. Mehrfachnennungen möglich.

## 8 Einsatz von Mitarbeiterausweisen

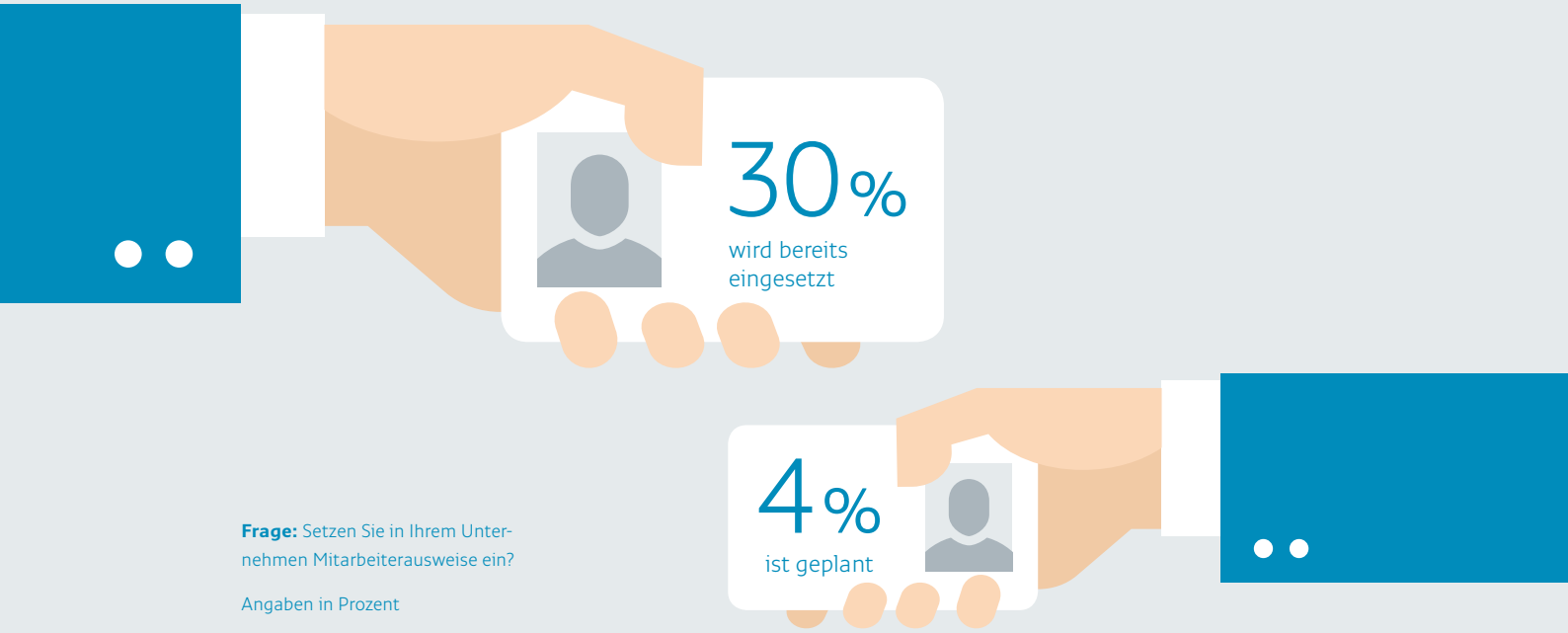
**Mitarbeiterausweise können insbesondere beim Schutz vor dem sogenannten Social Engineering durch Fremde auf dem eigenen Betriebsgelände eine wichtige Rolle spielen, da sie Unternehmensmitarbeiter entweder sichtbar oder elektronisch als solche identifizieren bzw. von Betriebsfremden unterscheiden.**

Sie reihen sich damit ein in die Liste der für Unternehmen verfügbaren IT-Sicherheitsmaßnahmen zum Schutz vor Sicherheitsvorfällen – insbesondere, wenn die Ausweise etwa über einen eingebauten Chip auch als elektronische Zutrittskontrolle zu Gebäuden, für die Anmeldung am Computer oder als digitale Signatur verwendet werden können.

Allerdings sind Mitarbeiterausweise in den Unternehmen in Deutschland nicht sehr weit verbreitet: Nur in drei von zehn Unternehmen gibt es für Mitarbeiter persönliche Identifikationsausweise. Weitere 4 Prozent der Unternehmen planen eine Einführung.

Während in kleinen Unternehmen mit weniger als 100 Beschäftigten nur jedes vierte Unternehmen solche Mitarbeiterausweise eingeführt hat, ist dies in größeren Unternehmen eher die Regel: 57 Prozent der mittelgroßen Unternehmen mit mindestens 500 und weniger als 2.000 Beschäftigten verwenden Mitarbeiterausweise, bei den noch größeren Unternehmen sind es sogar 70 Prozent.

### Jedes dritte Unternehmen setzt Mitarbeiterausweise ein oder plant eine Einführung




**Frage:** Setzen Sie in Ihrem Unternehmen Mitarbeiterausweise ein?

Angaben in Prozent

## Kurzzusammenfassung

**Die große Mehrheit der Unternehmen in Deutschland ist sich der Sicherheitsrisiken durch eine fortscheitende Digitalisierung bewusst und sieht IT-Sicherheit als Basis für eine erfolgreiche Digitalisierung.**

Bisher haben nur knapp 40 Prozent der Unternehmen ihre Produktionsprozesse bereits digitalisiert. Die anstehende digitale Transformation wird von den IT-Entscheidern in den Unternehmen jedoch bereits als große Herausforderung gesehen: Nicht einmal jeder dritte IT-Sicherheitsverantwortliche sieht sein eigenes Unternehmen schon jetzt gut gerüstet für die digitale Transformation. Jedem sechsten Unternehmen geht Umsatz verloren, weil es aus Angst vor IT-Sicherheitsvorfällen seine Digitalisierung langsamer als möglich vorantreibt (Vorjahr: 21 Prozent).

Dabei wird das Thema IT-Sicherheit von den Unternehmen noch zu häufig als reiner Kostenfaktor gesehen: In nur drei von zehn Unternehmen wird IT-Sicherheit unternehmenspolitisch eher als Wettbewerbsvorteil gegenüber der Konkurrenz statt als Kostenfaktor wahrgenommen. In jedem sechsten Unternehmen werden notwendige IT-Sicherheitsmaßnahmen aus Kostengründen nur begrenzt umgesetzt. Dennoch wird dem Thema IT-Sicherheit in den deutschen Unternehmen insgesamt große Bedeutung beigemessen.

Vier von fünf Unternehmen geben an, dass IT-Sicherheit einen hohen oder sogar sehr hohen Stellenwert in ihrem Unternehmen habe, quer über alle Unternehmensgrößen hinweg.

Die hohe Bedeutung der IT-Sicherheit in den Unternehmen spiegelt sich auch in deren Budgetplanungen wider: So beabsichtigt die Mehrheit der Unternehmen, dieses Jahr mehr in ihre IT-Sicherheit zu investieren als im Vorjahr. Jedes fünfte erwartet sogar eine starke Zunahme.

In fast vier von fünf Unternehmen in Deutschland fällt die Geschäftsführung die strategischen Entscheidungen im Hinblick auf die IT-Sicherheit. Mit zunehmender Größe der Unternehmen wird immer häufiger auch eine eigene IT-Abteilung an sicherheitsstrategischen Entscheidungen beteiligt. Zwei von fünf Unternehmen lassen sich dabei aber auch von externen Dienstleistern im Bereich der IT-Sicherheit beraten.

Vor allem kleinere Unternehmen, denen oft kein geeignetes Personal zur Verfügung steht, das auf IT-Sicherheit spezialisiert ist, lassen sich verhältnismäßig häufig durch externe Dienstleister hinsichtlich der IT-Sicherheit strategisch beraten. Ein Grund dafür ist sicherlich auch die Überforderung mit den gesetzlichen Regelungen rund um IT-Sicherheit und Datenschutz, die die Mehrheit der IT-Entscheider in deutschen Unternehmen beklagt, vor allem in kleineren Unternehmen.

Allerdings entscheidet in fast jedem dritten kleinen Unternehmen die Geschäftsführung allein über die IT-Sicherheitsstrategie, also ohne Beratung durch interne oder externe Spezialisten. Zwar lässt sich die Mehrheit der Unternehmen beim Thema IT-Sicherheit von externen Spezialisten beraten, externe IT-Sicherheits-Zertifizierungen nimmt aber nicht einmal jedes zweite Unternehmen in Anspruch. Bei der Zusammenarbeit mit externen Dienstleistern bevorzugen die meisten externe IT-Sicherheitslösungen und entsprechende Beratung aus einer Hand.

Bei der Umsetzung technischer und organisatorischer IT-Sicherheitsmaßnahmen zeigt sich, dass zwar essenzielle technische Maßnahmen der IT-Sicherheit wie etwa Netzwerkverschlüsselungen weit verbreitet sind, darüber hinausgehende Sicherheitsmaßnahmen wie regelmäßige Sicherheits-Audits aber nur von einer Minderheit der Unternehmen eingesetzt werden. Die physische Infrastruktur wie Datenträger, IT-Anlagen, Maschinen oder Gebäude sind zudem oft deutlich schlechter gesichert als die virtuelle Infrastruktur wie etwa Netzwerke.

Beunruhigend ist der Befund, dass nicht einmal die Hälfte der befragten Unternehmen regelmäßige Schulungen ihrer Mitarbeiter zu Themen der IT-Sicherheit durchführt. Allerdings plant fast jedes fünfte Unternehmen die Einführung solcher Schulungen.

Bei den IT-Sicherheitsmaßnahmen sieht sich die Mehrheit der Unternehmen in Deutschland insgesamt gut aufgestellt, je nach Maßnahmenbereich sagen aber immerhin drei bis vier von zehn Unternehmen, dass die bisher im eigenen Unternehmen umgesetzten IT-Sicherheitsmaßnahmen verbessert werden müssen, vor allem die technischen Maßnahmen.

## Kleine Unternehmen mit weniger als 100 Mitarbeitern sind insgesamt deutlich schlechter durch Sicherheitsmaßnahmen vor IT-Sicherheitsvorfällen geschützt als große Unternehmen. Sie machen jedoch das Gros der deutschen Wirtschaft aus.

Was externe Cloud-Angebote angeht, so werden diese bisher nur von einer Minderheit genutzt. Jedes sechste deutsche Unternehmen nimmt bereits externe Cloud-Services in Anspruch. Dabei ist das mit Abstand wichtigste Kriterium für die Wahl eines Cloud-Anbieters Datensicherheit, gefolgt von der Bedingung, dass der Cloud-Anbieter seinen Sitz in Deutschland hat oder sich zumindest die Cloud-Server in Deutschland befinden, sodass etwa das Datenschutzniveau den deutschen Vorschriften entsprechen muss.

Bei den meisten Unternehmen hat sich die Nutzung von Cloud-Angeboten bisher jedoch noch nicht durchgesetzt. Am häufigsten wird dies damit begründet, dass man selbst die Kontrolle über die IT behalten wolle. Viele Nichtnutzer trauen den Cloud-Anbietern zudem auch keine ausreichende Gewährleistung von Datenschutz bzw. Datensicherheit zu.

BUNDES DRUCKEREI

## Kontakt

**Bundesdruckerei GmbH**
Kommandantenstraße 18
10969 Berlin
Tel.: +49 (0) 30 – 25 98 – 28 10
Fax: +49 (0) 30 – 25 98 – 22 05
marc.thylmann@bdr.de
www.bundesdruckerei.de