Bundesamt
für Sicherheit in der
Informationstechnik

Allianz für
Cyber-Sicherheit

Cyber-Sicherheits-Umfrage – Cyber-Risiken & Schutzmaßnahmen in Unternehmen

Betrachtungszeitraum 2018

Cyber-Sicherheits-Umfrage

Die Cyber-Sicherheits-Umfrage wurde durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) im Rahmen der Allianz für Cyber-Sicherheit durchgeführt.

Mit der Cyber-Sicherheits-Umfrage untersucht das BSI seit 2014 jährlich die Gefährdungslage und Betroffenheit deutscher Institutionen durch Cyber-Angriffe sowie den Umsetzungsstand entsprechender Schutzmaßnahmen.

Aus den Ergebnissen der Umfrage lassen sich unter anderem praxisbezogene Lösungsansätze und Empfehlungen sowie Beratungsschwerpunkte ableiten, die das BSI im Rahmen der Allianz für Cyber-Sicherheit Unternehmen, Behörden und anderen Institutionen zur Verfügung stellt. Zudem fließen die Ergebnisse der Umfrage in die Erstellung und kontinuierliche Pflege des Lagebilds der Cyber-Sicherheit in Deutschland ein.

Unternehmen, Behörden und andere Institutionen können die Ergebnisse für die eigene Strategieentwicklung nutzen, zum Beispiel als Benchmarking im Bereich Cyber-Sicherheit.

Das BSI fragt – IT-Sicherheits-Experten antworten

Die Cyber-Sicherheits-Umfrage für den Betrachtungszeitraum 2018 wurde als Online-Erhebung im Zeitraum vom 21.02.2019 bis 07.03.2019 realisiert. Die Einladung zur Teilnahme erfolgte über die Kommunikationskanäle des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

Es ist davon auszugehen, dass insbesondere Organisationen teilgenommen haben, die eine erhöhte Affinität zur IT-Sicherheit aufweisen und die mit den Cyber-Sicherheits-Empfehlungen des BSI vertraut sind.

Gut drei Viertel der Befragten waren IT-Sicherheitsverantwortliche in ihren Institutionen.

Meinungen

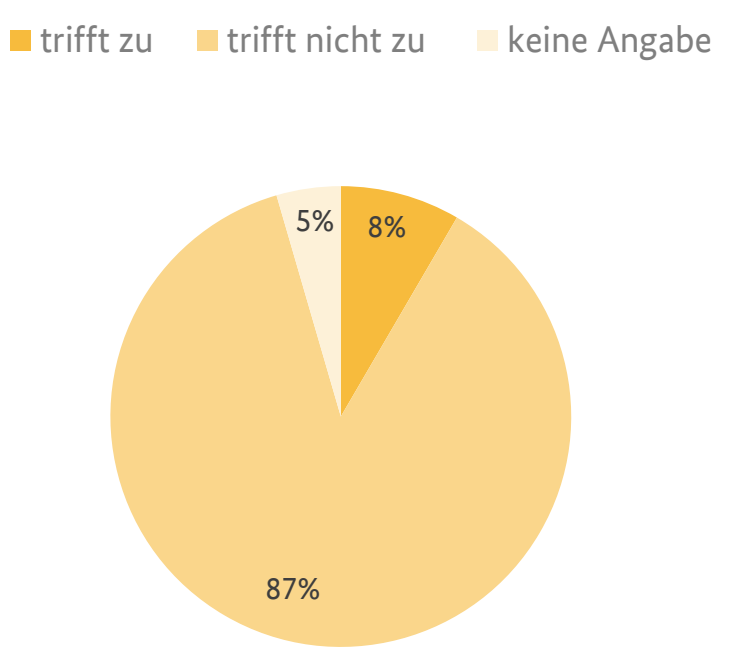
Cyber-Sicherheit als Faktor für den täglichen Betrieb

Nur jeder zwölfte Teilnehmende sieht Cyber-Bedrohungen als relevante Gefährdung

8% der Befragten sehen in Cyber-Angriffen das Potenzial, die betrieblichen Prozesse zu beeinflussen.

87% gehen nicht davon aus, dass Cyber-Vorfälle zu Störungen und/oder Ausfällen des Betriebsablaufes führen können.

Cyber-Angriffe stellen eine relevante Gefährdung der Betriebsfähigkeit dar.
Anteil in % an allen Befragten je Kategorie



Bundesamt für Sicherheit in der Informationstechnik

Cyber-Sicherheit als Voraussetzung für eine erfolgreiche Digitalisierung

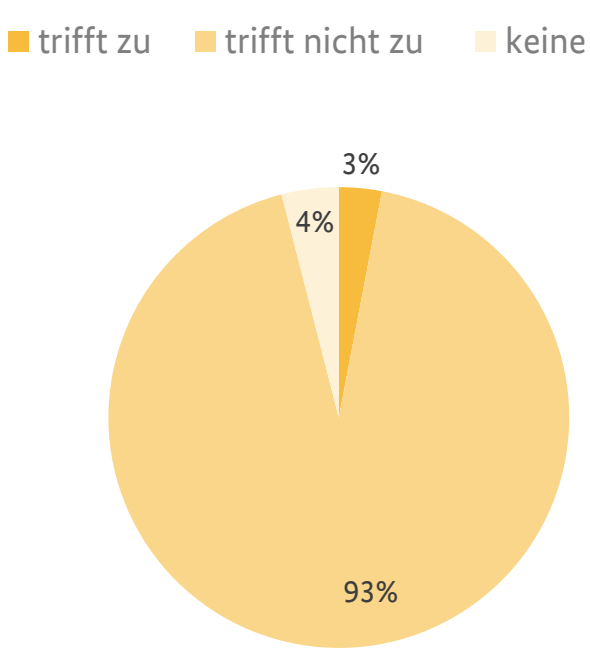
Neun von zehn Unternehmen erwarten von der Digitalisierung keine Veränderung der Bedrohungslage

Nur 3 % der Teilnehmenden befürchten, dass mit der Digitalisierung zusätzliche Cyber-Risiken einhergehen.

93 % gehen davon aus, dass keine zusätzlichen Gefährdungen entstehen.

Mit der Digitalisierung wächst die Angriffsfläche für Bedrohungen aus dem Cyber-Raum.

Anteil in % an allen Befragten je Kategorie



Bundesamt für Sicherheit in der Informationstechnik

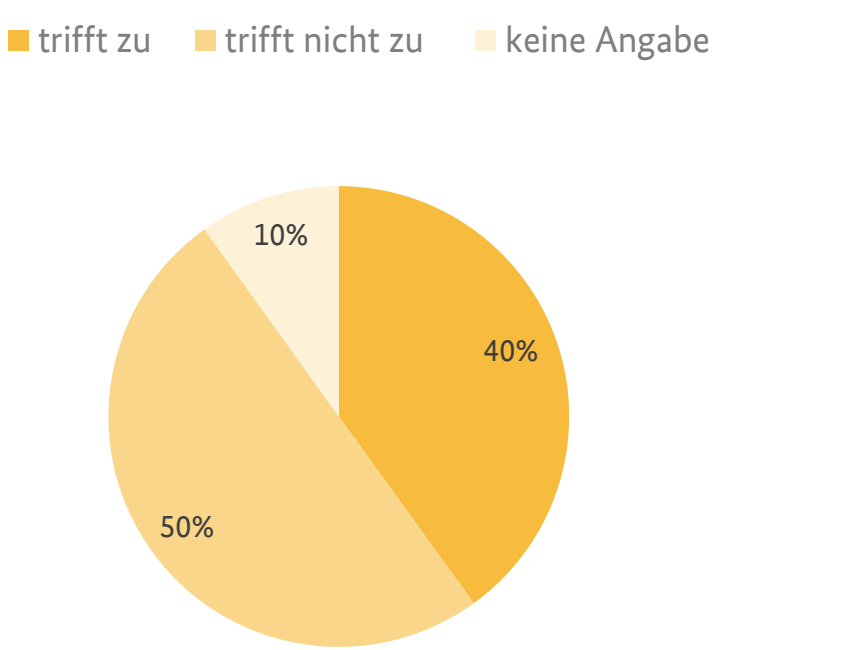
Cyber-Sicherheit als Wettbewerbsvorteil

Eine große Anzahl der Unternehmen verstehen Cyber-Sicherheit als Chance für Innovation

40% der befragten Institutionen erkennen Cyber-Sicherheit als Wettbewerbsvorteil.

50% versprechen sich keinen Mehrwert von Cyber-Sicherheit.

Cyber-Sicherheit ist für uns ein Innovationstreiber, mit dem wir uns vom Wettbewerb abheben.
Anteil in % an allen Befragten je Kategorie



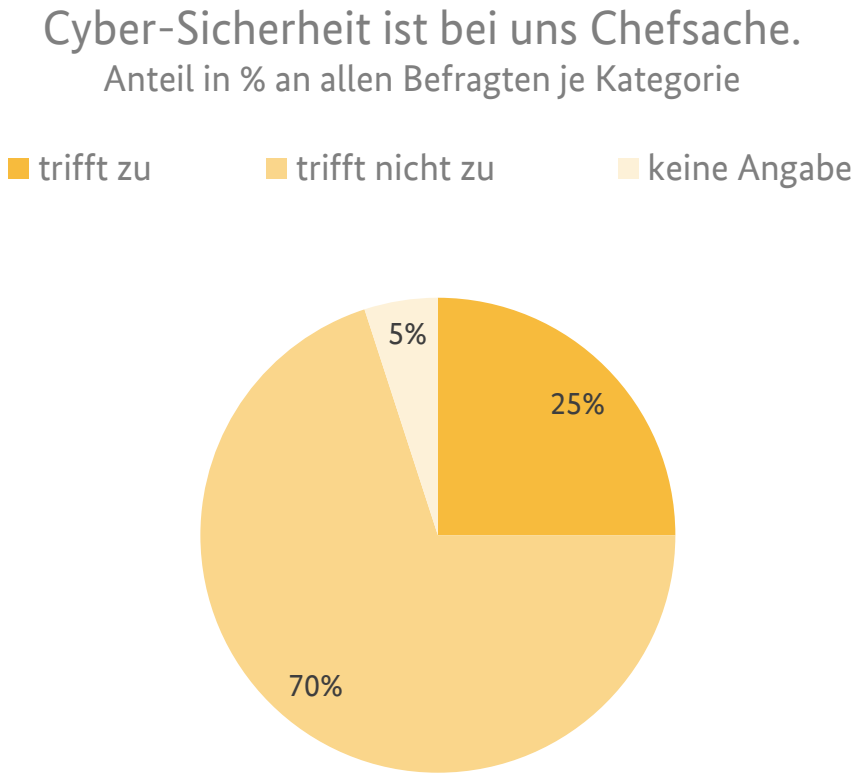
Bundesamt für Sicherheit in der Informationstechnik

Cyber-Sicherheit als Chefsache

Nur ein Viertel der Unternehmen sehen die Leitung in der Verantwortung für Informationssicherheit

Von den Befragten unterschrieben 25% die Aussage: „Cyber-Sicherheit ist Chefsache.“

In 70% der Unternehmen trifft die Aussage (eher) nicht zu.



Bundesamt für Sicherheit in der Informationstechnik

Aktuelle Bedrohungslage

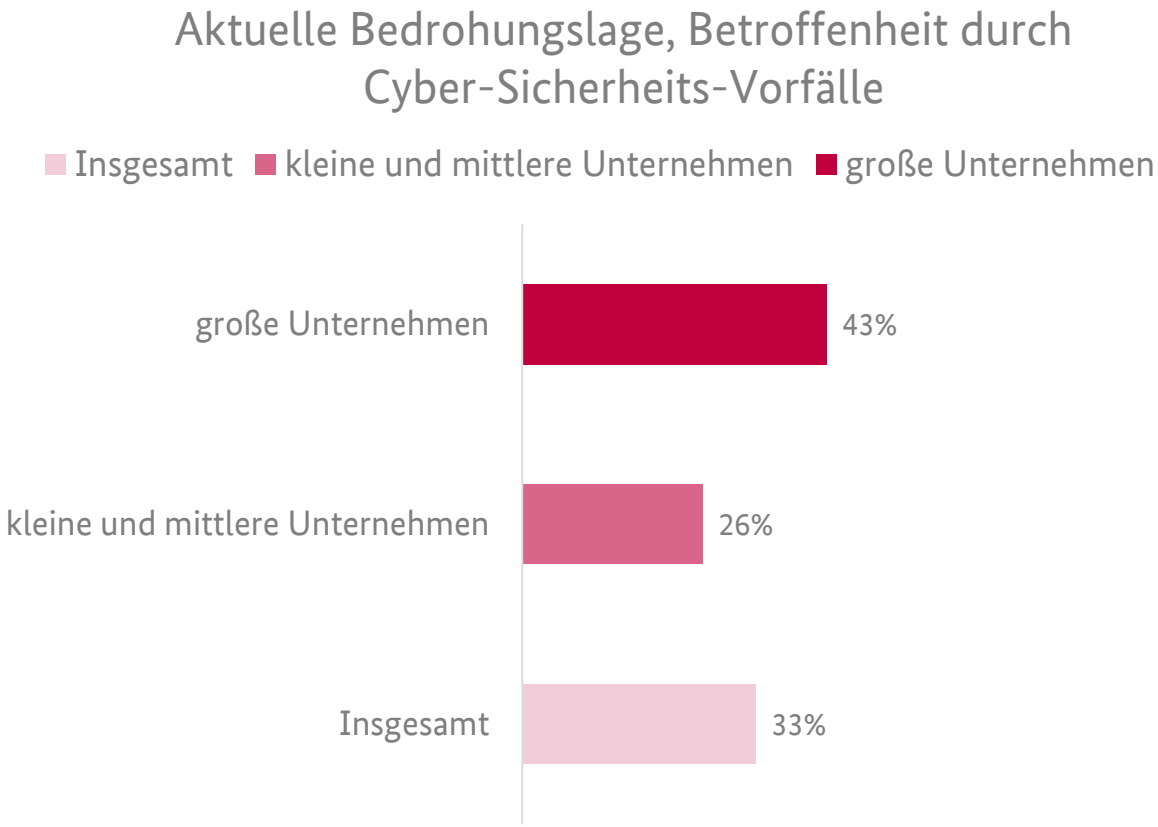
Betroffenheit durch Cyber-Sicherheits-Vorfälle

Große Unternehmen am stärksten von Cyber-Sicherheits-Vorfällen betroffen

Unter den befragten Organisationen gaben 43 % der großen Unternehmen an, 2018 von Cyber-Sicherheits-Vorfällen betroffen gewesen zu sein. Bei den kleinen und mittelständischen Unternehmen lag der Wert bei 26%.

In der Hälfte der Fälle waren die Angreifer erfolgreich, d. h. sie konnten sich zum Beispiel Zugang zu IT-Systemen verschaffen, deren Funktionsweise beeinflussen oder Internet-Auftritte von Firmen manipulieren.

Hinweis: In der Regel wird nur ein Teil der Angriffe erkannt, daher sind nur detektierte Vorfälle berücksichtigt.



Bundesamt für Sicherheit in der Informationstechnik

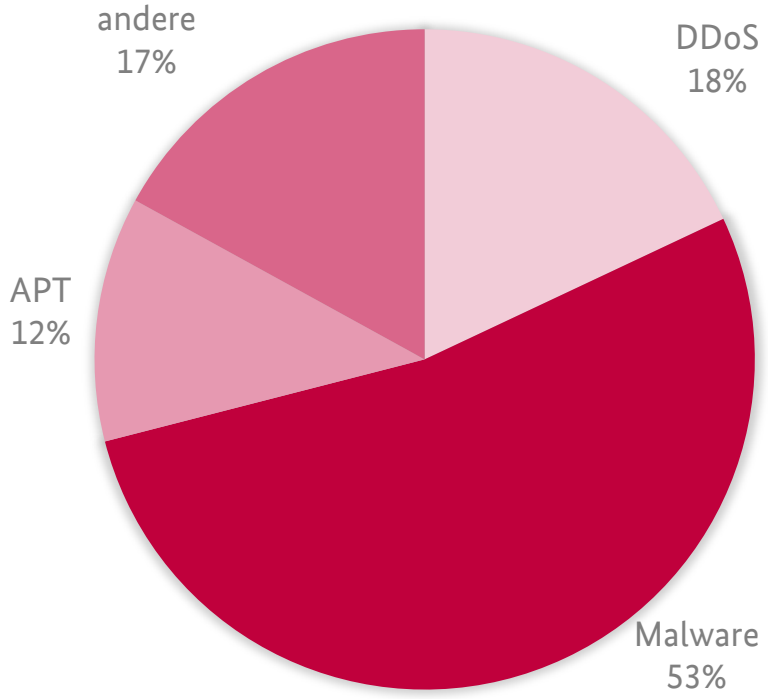
Art der Cyber-Angriffe

Malware auch 2018 wieder die häufigste Angriffsart

In 53% der berichteten Angriffsfälle handelte es sich um Malware-Infektionen, bei denen Schadprogramme in betriebliche IT-Systeme eindrangen (DDoS-Attacken 18%, gezieltes Hacking 12%).

90% der Schadprogramme wurden als Anhang oder Link in einer E-Mail verteilt. In der Hälfte der Fälle verhinderten technische Maßnahmen eine Infektion, in den übrigen Fällen war die Awareness der Beschäftigten der Erfolgsfaktor.

Anteile in % an allen berichteten Angriffen



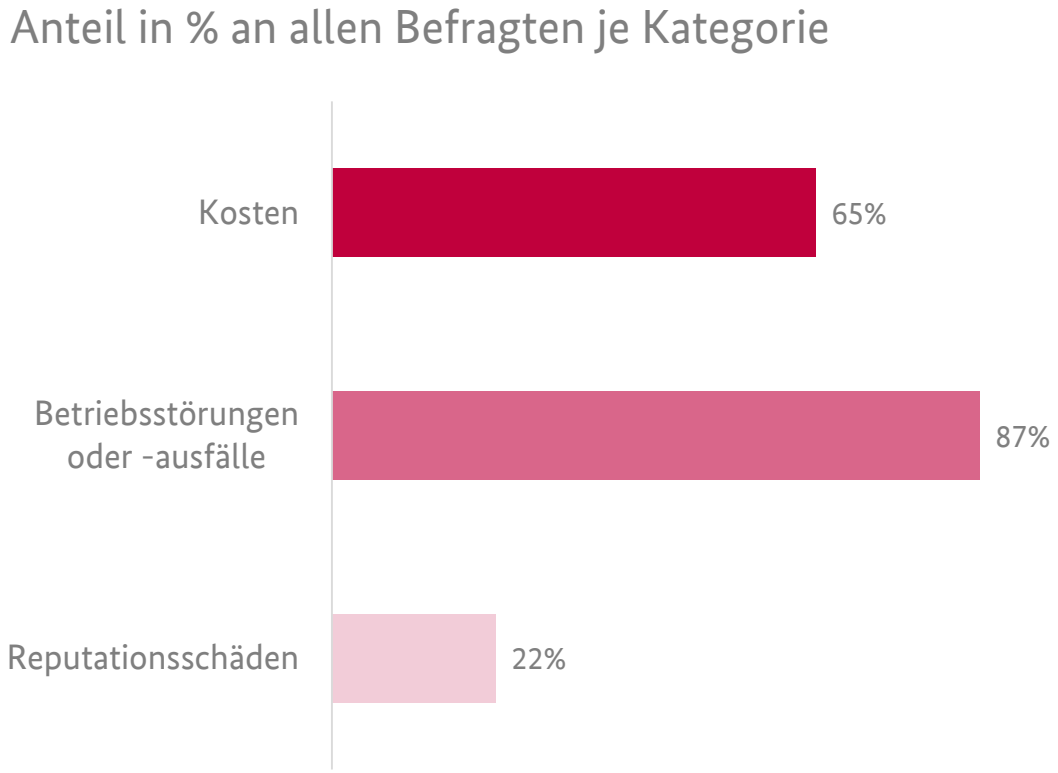
Bundesamt
für Sicherheit in der
Informationstechnik

Art der Schäden durch erfolgreiche Cyber-Angriffe

Cyber-Angriffe hatten erhebliche Konsequenzen für die Betriebe

So gaben 87% der Betroffenen an, dass es 2018 zu Betriebsstörungen oder –ausfällen kam.

Hinzu kamen häufig noch Kosten für die Aufklärung der Vorfälle und die Wiederherstellung der IT-Systeme (bei 65% der Betroffenen) sowie Reputationsschäden (bei 22% der Betroffenen).



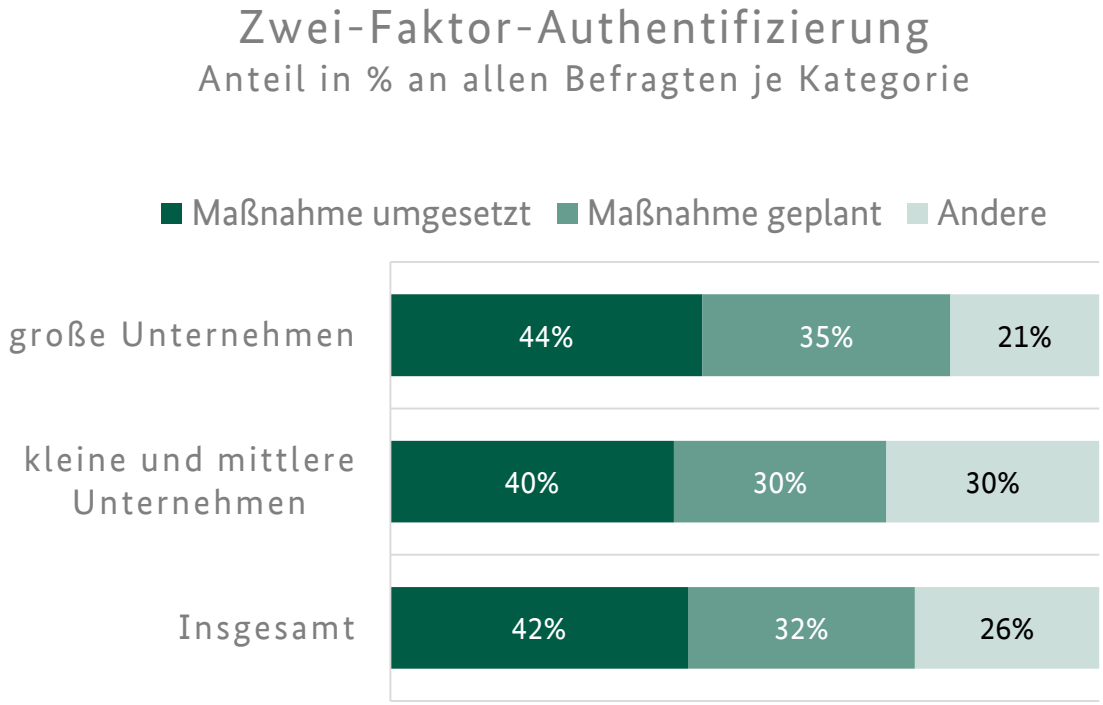
Bundesamt für Sicherheit in der Informationstechnik

Prävention (Auswahl)

Zwei-Faktor-Authentifizierung im Trend

Rund 42% der Befragten verwendeten Zwei-Faktor-Authentifizierung zur Kontrolle der Zugriffe auf ihre Netzwerke und zur Absicherung gegen unbefugtes Eindringen in Systeme. Ein knappes Drittel der Befragten gab an, entsprechende Maßnahmen zu planen.

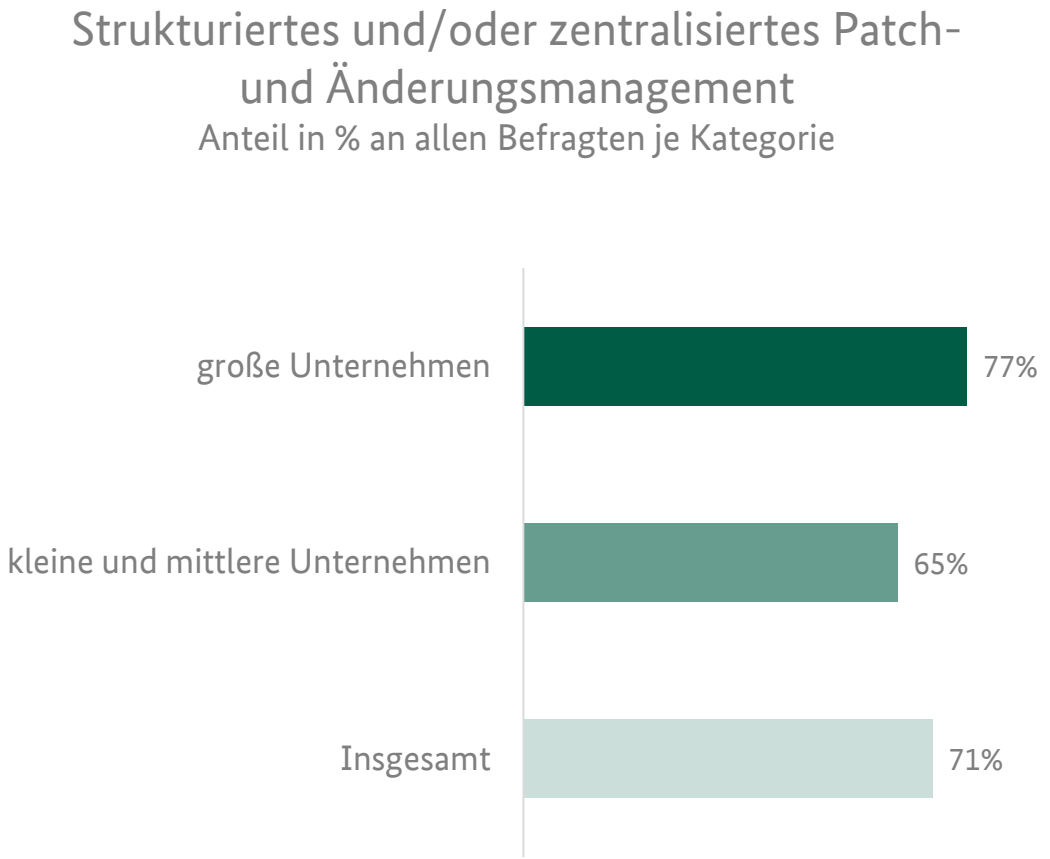
Der Anteil der Befragten, die Zwei-Faktor-Authentifizierung bereits einsetzen, lag in großen Unternehmen bei 44%, in kleinen und mittleren Unternehmen bei 40%.



Strukturiertes Patch-Management an der Tagesordnung

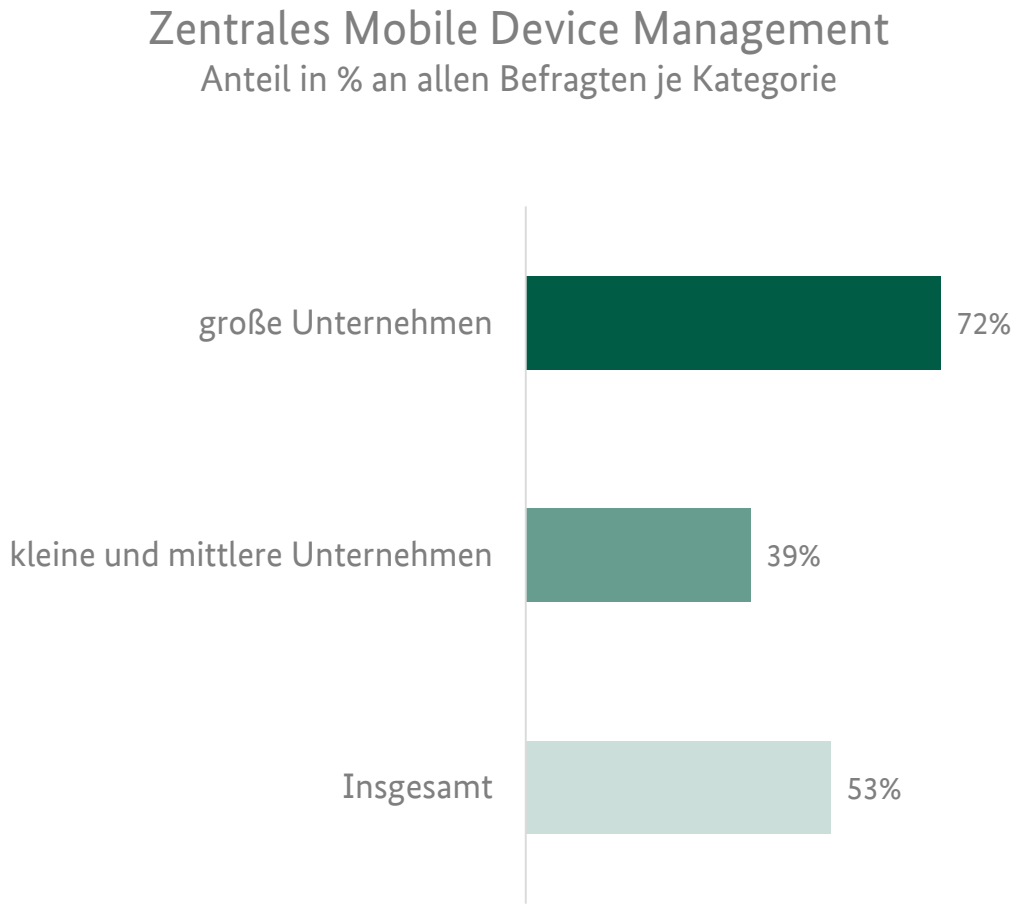
Insgesamt verfügten 71% der befragten Institutionen 2018 über ein strukturiertes Patch-Management, um auf bekannt gewordene Sicherheitslücken schnell reagieren zu können.

Während 77% der großen Unternehmen strukturiert und zentralisiert patchten, waren es unter den kleinen und mittelständischen Unternehmen 65%.



Beim zentralen Mobile Device Management haben große Unternehmen die Nase vorn

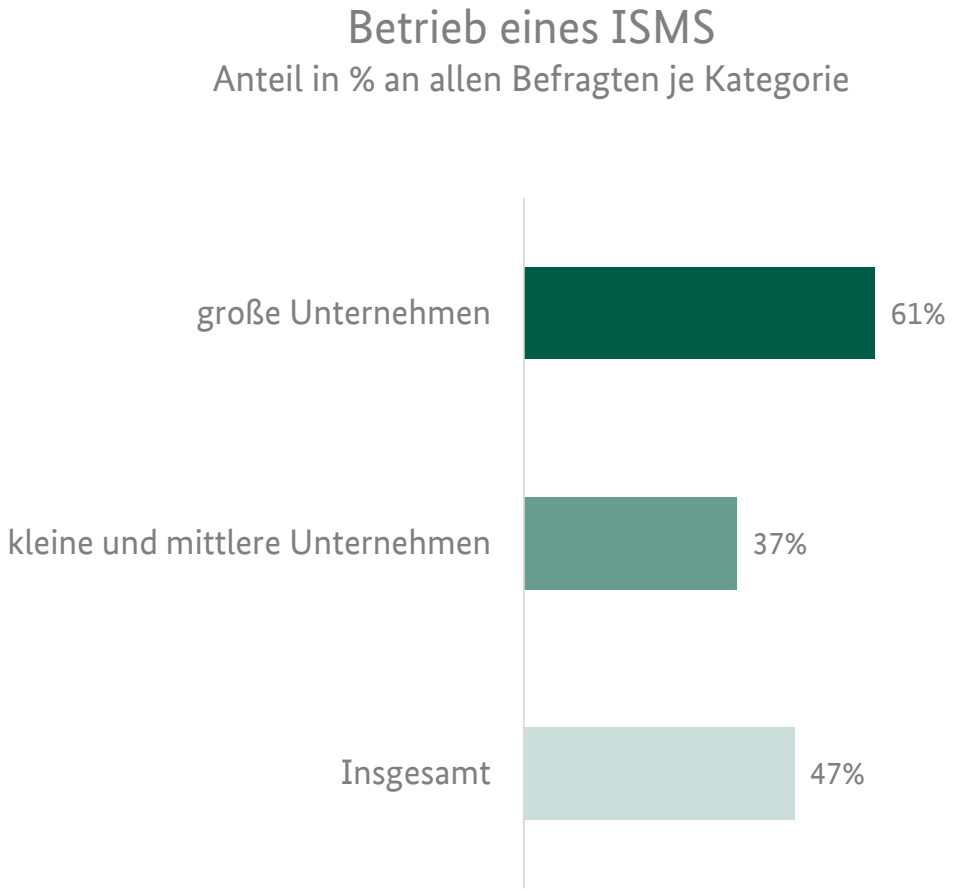
Während rund 72% der befragten großen Unternehmen über ein zentrales Management für die Sicherheit mobiler Endgeräte verfügten, waren es bei den kleinen und mittelständischen Unternehmen 39%.



Nachholbedarf beim Thema ISMS

Gut 47% aller Befragten verfügten 2018 über ein Managementsystem für Informationssicherheit (ISMS).

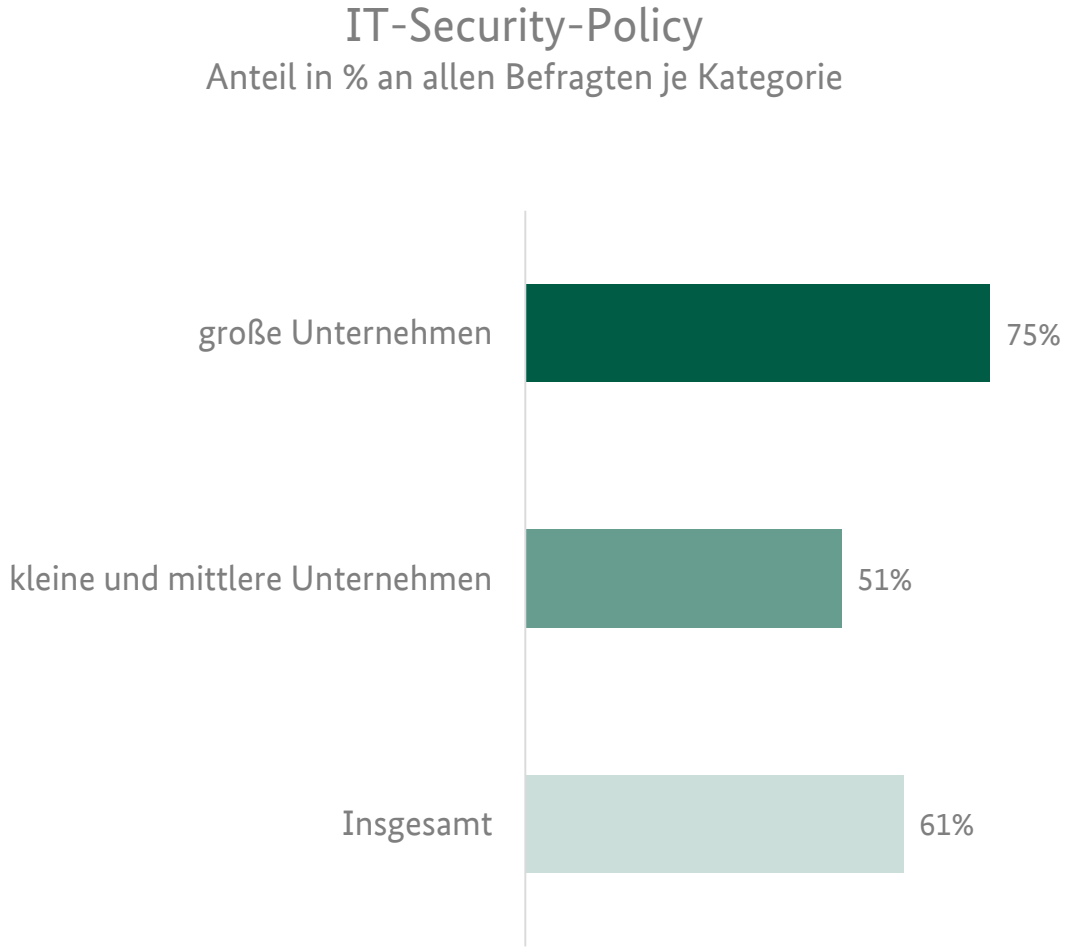
Von den großen Unternehmen betrieben 61% ein solches System, von den kleinen und mittelständischen Unternehmen waren es 37%.



IT-Security-Policy unter großen Unternehmen weit verbreitet

Insgesamt 61% der Befragten gaben an, dass in ihren Institutionen eine Richtlinie zur Umsetzung der Informationssicherheit existiert.

Drei von vier der großen Unternehmen besaßen 2018 eine solche Policy. Unter den kleinen und mittelständischen Unternehmen waren es gut die Hälfte.



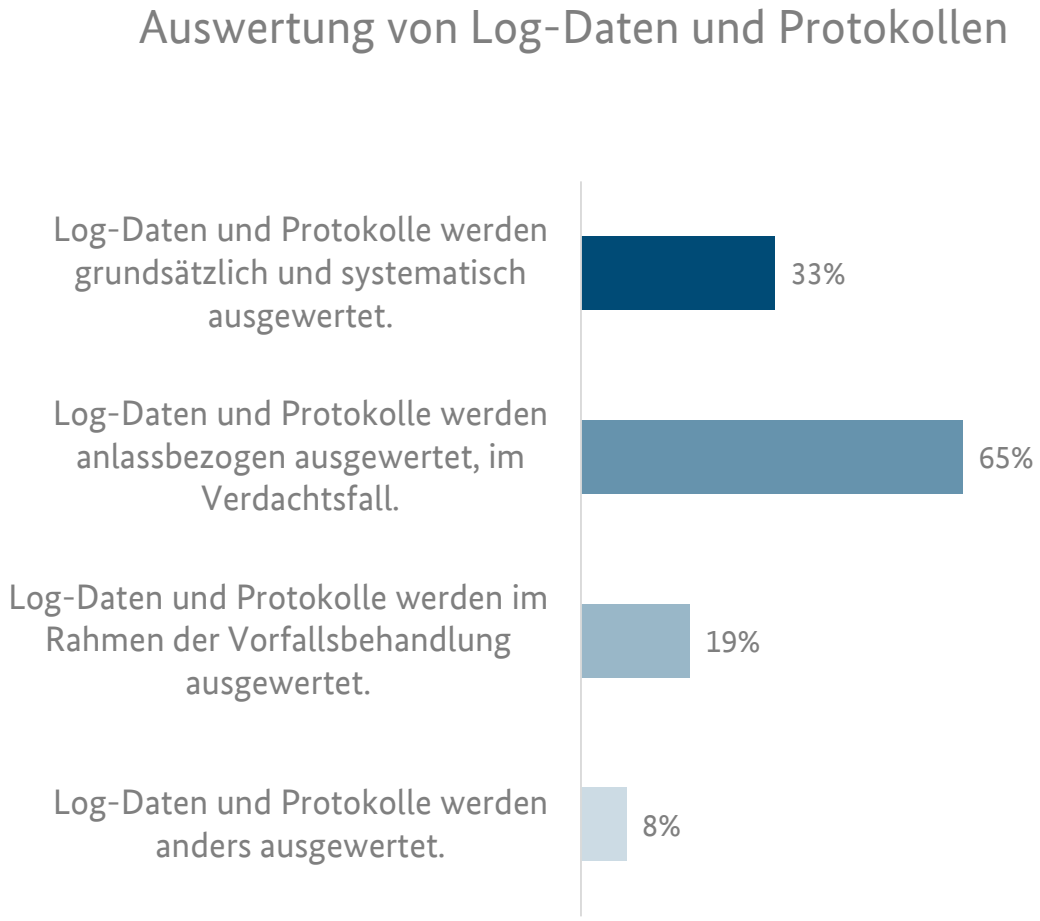
Detektion

Erkennung von Cyber-Angriffen

Mehrzahl der Betriebe werten Log-Daten und Protokolle aus

Ein gutes Drittel der Befragten gab an, Log-Daten und Protokolle auch grundsätzlich und systematisch auf Indizien für Cyber-Sicherheits-Vorfälle zu untersuchen.

In knapp zwei Drittel der Betriebe fanden Prüfungen von Log-Daten und Protokolldateien statt, wenn ein Anfangsverdacht bestand.



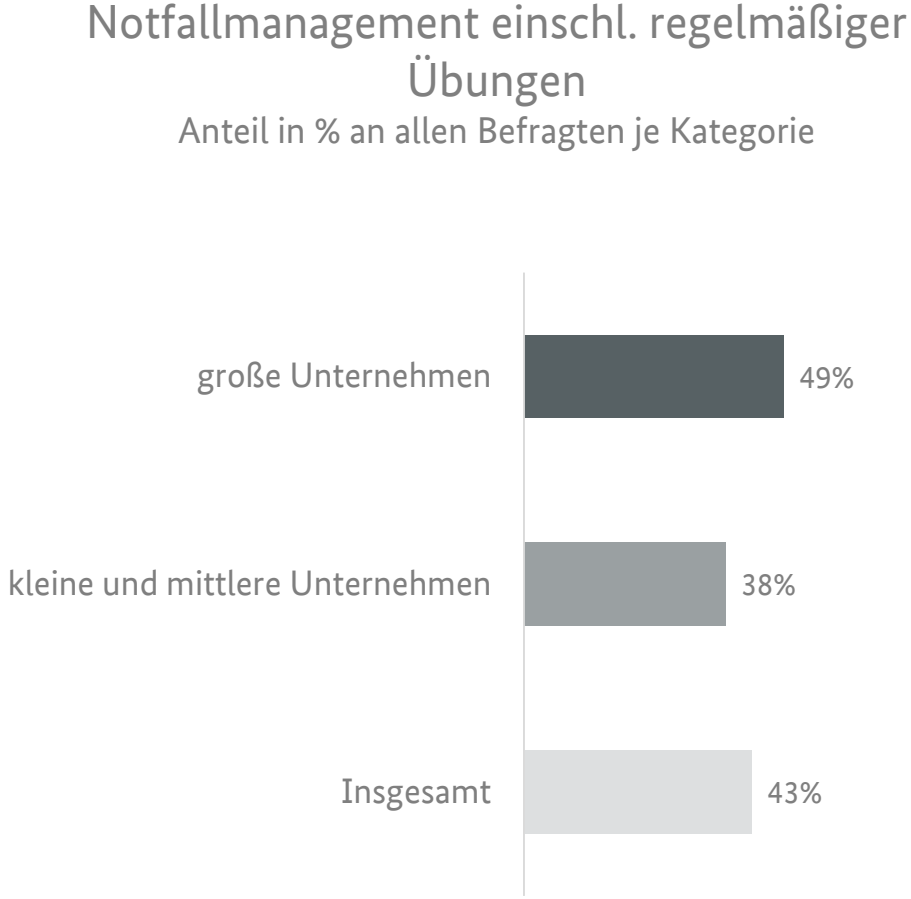
Bundesamt für Sicherheit in der Informationstechnik

Reaktion

Notfallmanagement und regelmäßige Übungen sind noch nicht überall Standard

Im Jahr 2018 lag der Anteil der Befragten, die ein Notfallmanagement einschl. regelmäßiger Übungen betreiben, um bei einem Cyber-Vorfall schnell handlungsfähig zu sein, bei 43%.

Mit 49% war der Anteil der Betreiber eines solchen Systems unter den großen Unternehmen deutlich höher als unter den kleinen und mittelständischen Unternehmen mit 38%.



Datenbasis und Teilnehmerfeld

Datenbasis

Die Cyber-Sicherheits-Umfrage wurde durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) im Rahmen der Allianz für Cyber-Sicherheit durchgeführt.

- Umfragezeitraum: 21.02.2019 bis 07.03.2019
- Betrachtungszeitraum: 2018
- Öffentliche Online-Umfrage auf www.allianz-fuer-cybersicherheit.de
- Die Umfrage war anonym, ein Rückschluss auf die teilnehmenden Institutionen ist nicht möglich.
- Datenbasis der Umfrage: 1039 teilnehmende Institutionen

Teilnehmerfeld

Unternehmensgröße nach Anzahl der Beschäftigten in den Institutionen laut Angaben der Befragten:

- **Kleine und mittlere Unternehmen bzw. Institutionen** mit 1 bis 249 Beschäftigten: 57%
- **Große Unternehmen bzw. Institutionen** mit 250 oder mehr Beschäftigten: 43%

Branchen der beteiligten Institutionen (eigene Angaben):

- **Information und Kommunikation:** 18%
- **Energieversorgung**: 17%
- **Öffentliche Verwaltung**: 11 %
- **Andere:** 54%

Funktionen der Befragten (Mehrfachnennungen möglich):

- **IT-Sicherheitsverantwortliche**: 77%
- **IT-Spezialisten (z. B. Admins):** 42%
- **IT-Anwender/innen:** 27%

Allianz für Cyber-Sicherheit

Mit der 2012 gegründeten Allianz für Cyber-Sicherheit verfolgt das BSI das Ziel, die Widerstandsfähigkeit des Standortes Deutschland gegenüber Cyber-Angriffen zu stärken. Inzwischen gehören der Initiative rund 3.500 Institutionen an.

Das Angebot der Allianz für Cyber-Sicherheit umfasst:

- **Verlässliche Informationen** – Aktuelle Warnmeldungen, Lageberichte zur Cyber-Sicherheit in Deutschland, Lösungshinweise und praktische Anleitungen.
- **Wissens- und Erfahrungsaustausch** – Thematische Cyber-Sicherheits-Tage, Erfahrungs- und Expertenkreise.
- **Ausbau von Sicherheitskompetenz** – Schulungen und Workshops, Analysen und Erstberatungen, Penetrationstests und vieles mehr, bereitgestellt durch die Partner der Allianz für Cyber-Sicherheit.

Informationen zur kostenfreien Teilnahme: www.allianz-fuer-cybersicherheit.de/ACS/Registrierung

Vielen Dank für Ihr Interesse

Kontakt

Geschäftsstelle der Allianz für Cyber-Sicherheit
c/o Bundesamt für Sicherheit in der Informationstechnik (BSI)

Godesberger Allee 185 – 189
53175 Bonn

info@cyber-allianz.de

Tel. +49 (0) 800 2741000
www.allianz-fuer-cybersicherheit.de

Bundesamt
für Sicherheit in der
Informationstechnik