Bundesamt
für Sicherheit in der
Informationstechnik

Allianz für
Cyber-Sicherheit

Cyber-Sicherheits-Umfrage 2017

Cyber-Risiken, Meinungen und Maßnahmen

Cyber-Sicherheits-Umfrage

Die Cyber-Sicherheits-Umfrage 2017 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 subjektive Gefährdungslage und Betroffenheit deutscher Institutionen durch Cyber-Angriffe sowie den Umsetzungsstand entsprechender Schutzmaßnahmen.

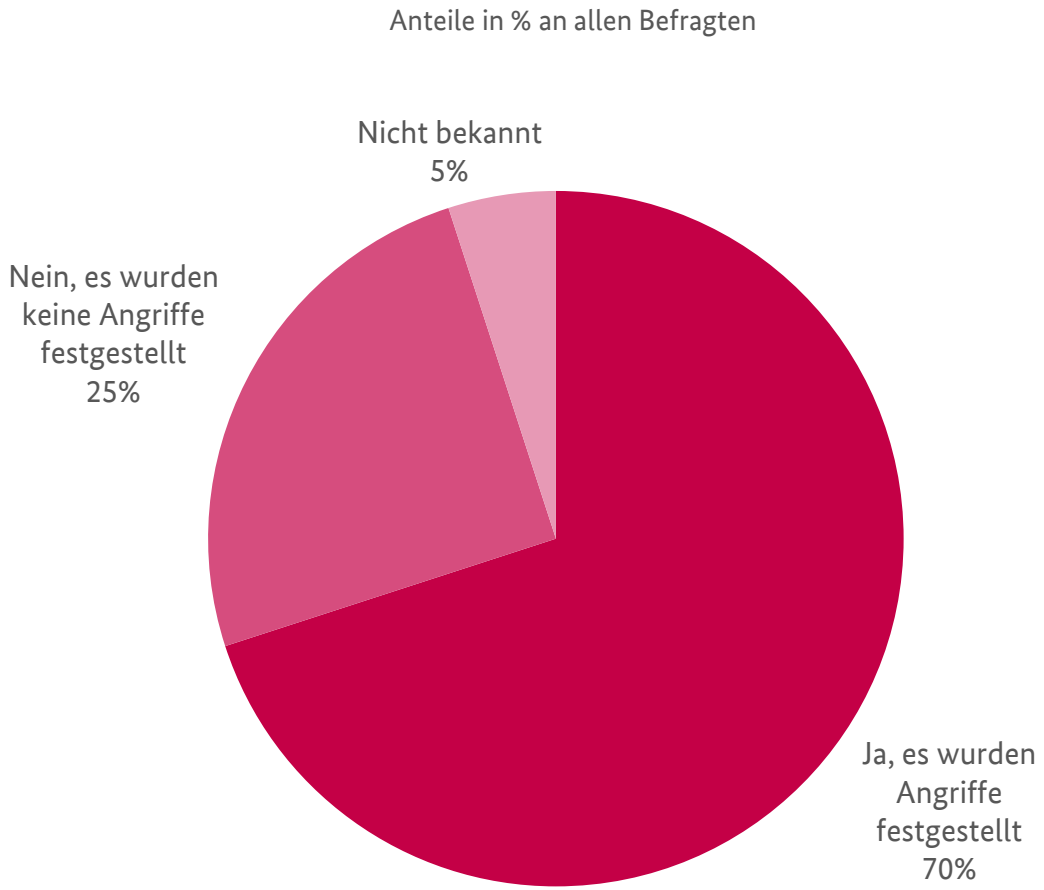
Aus den Ergebnissen der Umfrage lassen sich unter anderem praxisbezogene Lösungsansätze und Empfehlungen sowie Beratungsschwerpunkte ableiten, die das BSI im Rahmen der Allianz für Cyber-Sicherheit einbringt und auch anderen Unternehmen bzw. Institutionen zur Verfügung stellt. Zudem fließen die Ergebnisse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

Aktuelle Bedrohungslage und Risikobewertung

Betroffenheit durch Cyber-Angriffe

Rund 70% der Befragten gaben an, in den Jahren 2016 und 2017 Opfer von Cyber-Angriffen geworden zu sein.

In etwa der Hälfte der Fälle waren die Angreifer erfolgreich, d. h. sie konnten sich zum Beispiel Zugang zu IT-Systemen verschaffen, die Funktionsweise von IT-Systemen beeinflussen, Internet-Auftritte von Firmen manipulieren usw. Die übrigen Befragten gaben an, alle Angriffe erfolgreich abgewehrt zu haben.

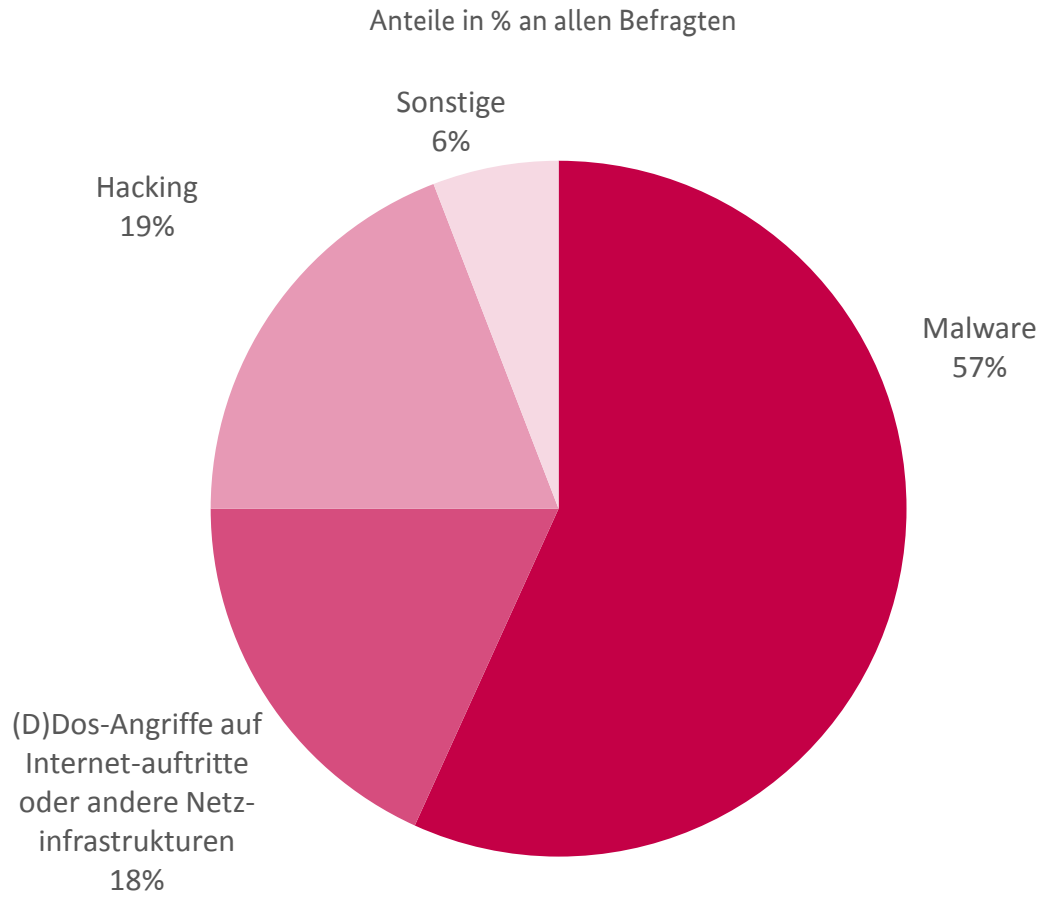


Bundesamt
für Sicherheit in der
Informationstechnik

Art der Cyber-Angriffe

Von den verschiedenen Angriffsarten fanden Malware-Infektionen am häufigsten statt.

Knapp 57% der berichteten Angriffe waren Malware-Infektionen, bei denen Schadprogramme in betriebliche IT-Systeme eindrangen, um schädliche Operationen durchzuführen. Hacking-Angriffe wie beispielsweise die Sabotage von industriellen Steuerungssystemen, Datendiebstahl oder die Manipulation von Internet-Auftritten machten 19%, (D)Dos-Attacken, die durch Überlastung zum Ausfall von Webseiten und anderen Netzinfrastrukturen führen, machten 18% der erfolgreichen Angriffe aus.

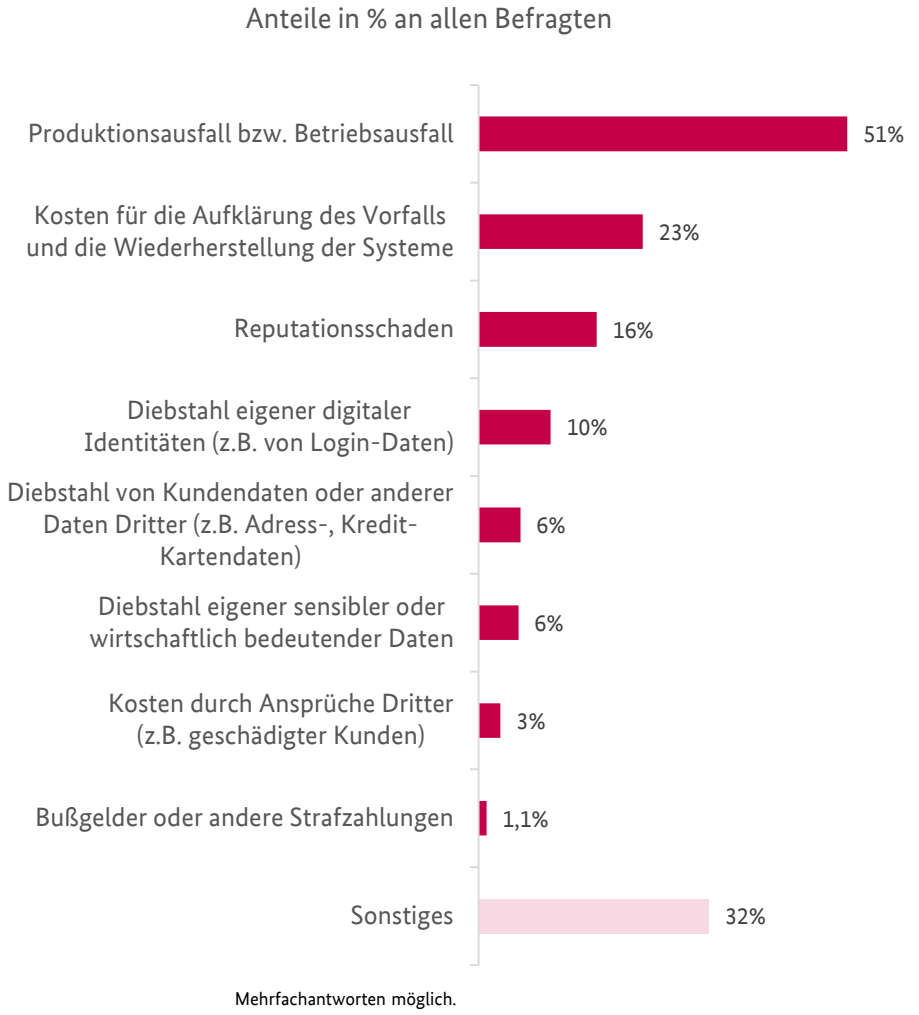


Bundesamt
für Sicherheit in der
Informationstechnik

Art der Schäden durch erfolgreiche Cyber-Angriffe

Cyber-Angriffe hatten teils erhebliche Konsequenzen für die Betriebe.

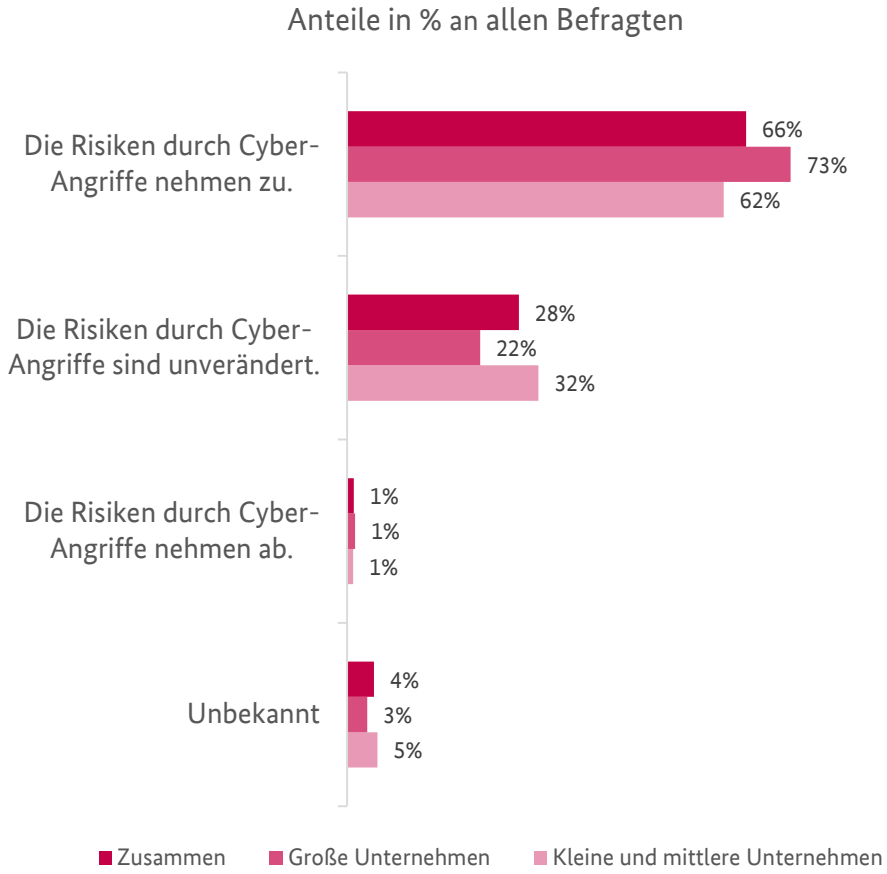
So gab jeder zweite betroffene Betrieb an, dass es 2016/2017 zu Produktions- bzw. Betriebsausfällen aufgrund von Cyber-Angriffen kam (gut 51%). Hinzu kamen häufig noch Kosten für die Aufklärung der Vorfälle und die Wiederherstellung der IT-Systeme (bei knapp 23% der Befragten) sowie Reputationsschäden (bei 16,5% der Befragten).



Risikobewertung

Zwei von drei Befragten gingen davon aus, dass die Risiken durch Cyber-Angriffe zunehmen.

Dabei fällt auf, dass kleine und mittlere Unternehmen die Lage weniger kritisch beurteilten, als Großkonzerne. Während ca. 73% der Großkonzerne damit rechneten, dass die Gefahren aus dem Cyber-Raum zunehmen, traf dies nur auf gut 62% der kleinen und mittleren Unternehmen zu.



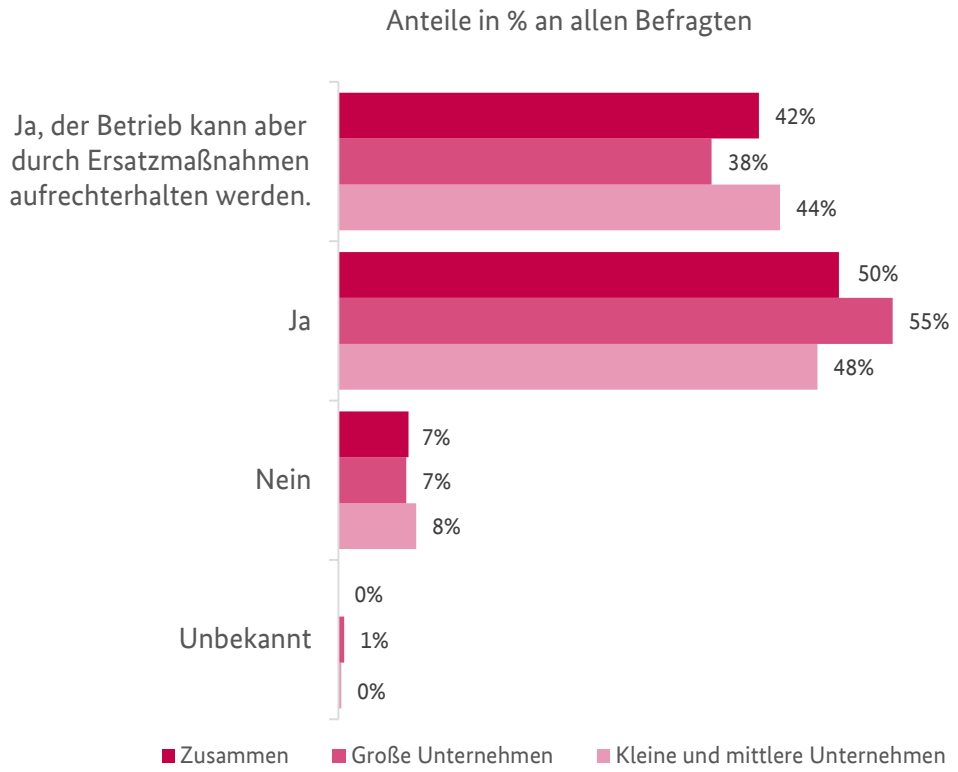
Bundesamt
für Sicherheit in der
Informationstechnik

Gefährdung der Betriebsfähigkeit durch Cyber-Angriffe

Das Bewusstsein für die Gefahren, die den Betrieben aus dem Cyber-Raum drohen, ist hoch.

So schätzten insgesamt rund 92% der Befragten die Gefahren aus dem Cyber-Raum als kritisch für die Betriebsfähigkeit ihrer Institution ein. Nur knapp 42% der Befragten gingen davon aus, dass der Betrieb im Fall eines Cyber-Angriffs durch Ersatzmaßnahmen aufrechterhalten werden könnte. Als besonders gefährdet betrachteten sich große Konzerne. Nur knapp 38% von ihnen glaubten, dass der Betrieb im Fall eines Cyber-Angriffs fortgeführt werden könnte.

Stellen Cyber-Angriffe eine relevante Gefährdung der Betriebsfähigkeit Ihrer Institution dar?



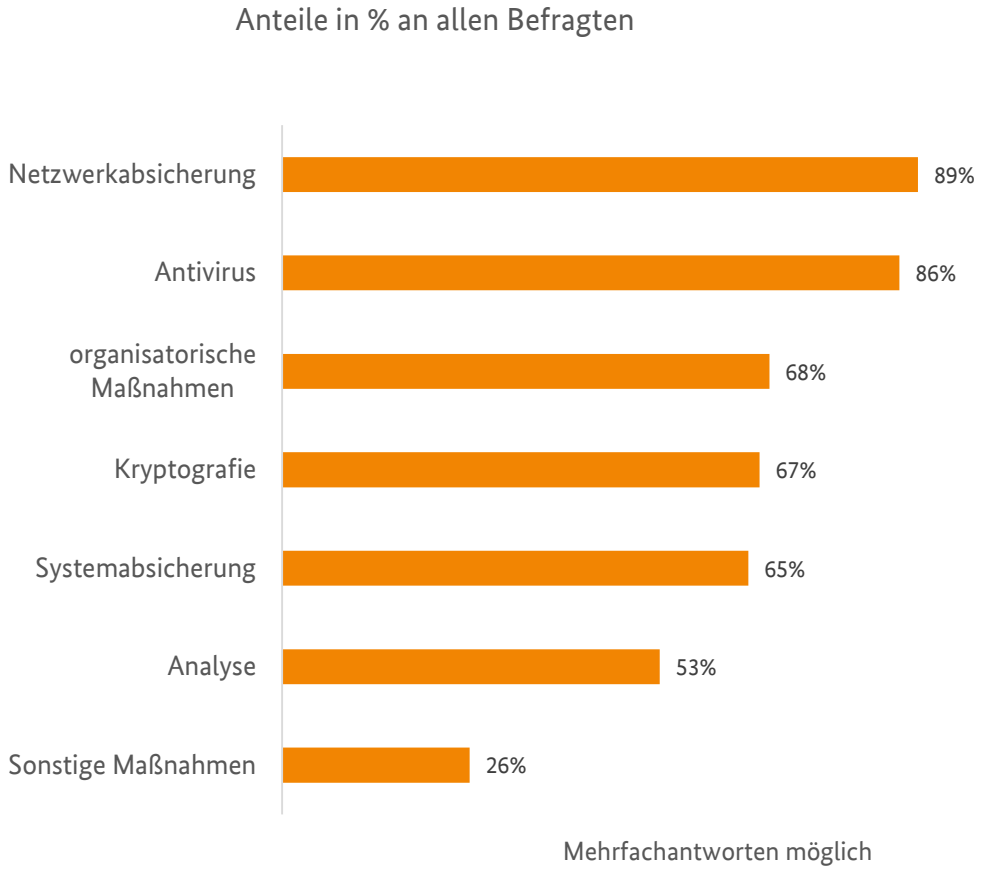
Bundesamt für Sicherheit in der Informationstechnik

Cyber-Sicherheits-Maßnahmen in Unternehmen bzw. Institutionen

Aktuelle Cyber-Sicherheitsmaßnahmen

Entsprechend ihrem Gefahrenbewusstsein hatten viele Betriebe bereits umfassende Cyber-Sicherheitsmaßnahmen eingeleitet.

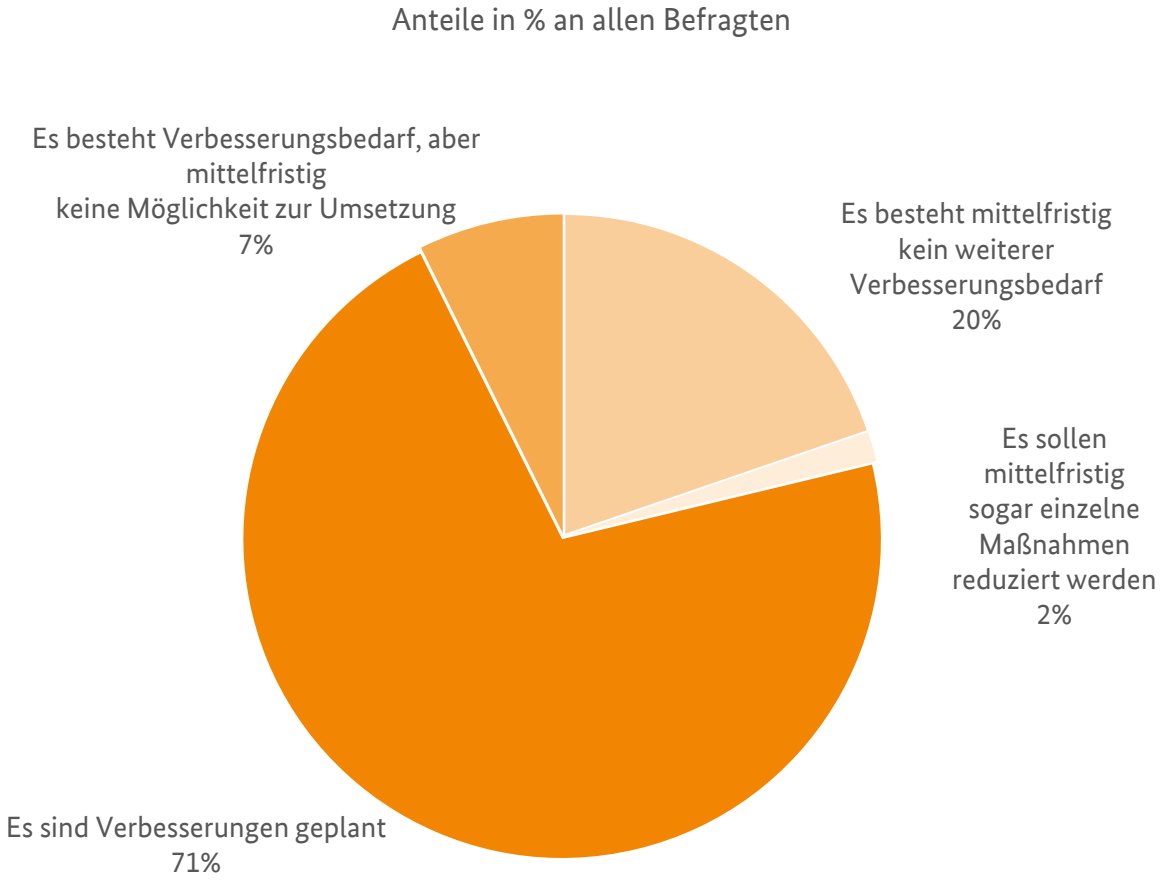
Von den Befragten gaben 89% an, dass Maßnahmen wie Segmentierung oder die Minimierung von Netzübergängen ergriffen wurden, um die Netze abzusichern. Auch Maßnahmen zur Abwehr von Viren fanden häufig Anwendung (86%). Dabei kamen sowohl Maßnahmen zur zentralen Detektion, wie etwa Scans am Sicherheitsgateway, Mailservern usw., als auch dezentrale Maßnahmen wie Scans auf Client-/Server-Systemen zum Einsatz.



Verbesserungsbedarf bei Cyber-Sicherheitsmaßnahmen

In vielen Betrieben sind Verbesserungen bei den Cyber-Sicherheitsmaßen geplant (71%).

Unter ihnen gaben rund 13% an, dass sogar kurzfristig dringende Verbesserungen in kritischen Bereichen geplant sind. Jeder fünfte Teilnehmer bewertete die Cyber-Sicherheitsmaßnahmen in seinem Betrieb als ausreichend (20%), sodass kein weiterer Verbesserungsbedarf bestehe.

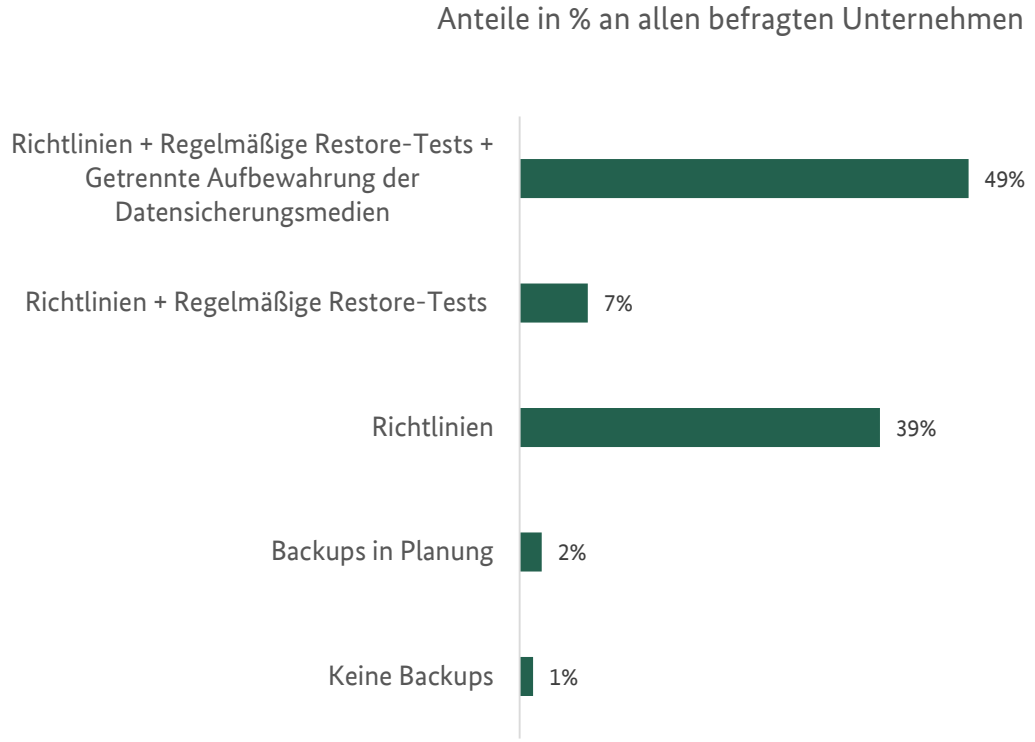


Prävention (Auswahl)

Umgang mit Backups

Die weitaus meisten Unternehmen (96%) verfügen über Richtlinien für das Sichern und Wiederherstellen von Daten.

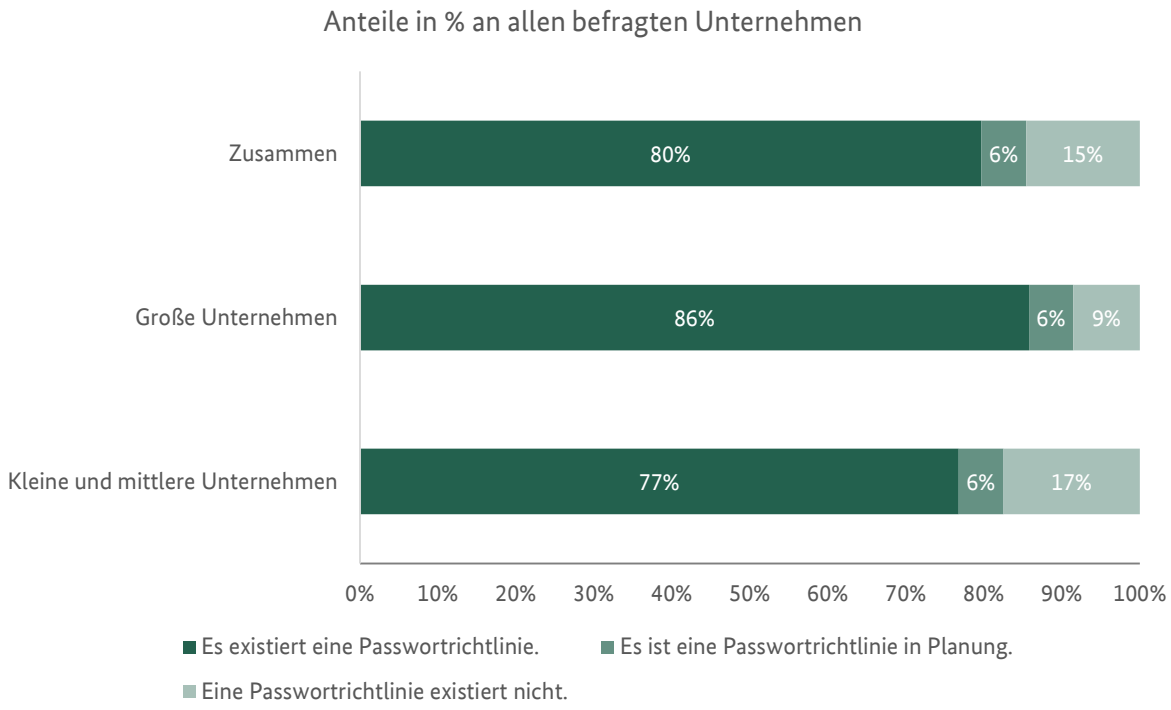
Fast die Hälfte der Unternehmen gab darüber hinaus an, dass auch regelmäßige Restore-Tests für die Wiederherstellung von Daten durchgeführt werden und Backups aus Sicherheitsgründen zudem örtlich von den übrigen Datenbeständen getrennt aufbewahrt werden (49%).



Passwortrichtlinien

Ein Großteil der Unternehmen hat Richtlinien für sichere Passwörter aufgestellt.

Im Jahr 2017 gaben rund 80% der Unternehmen an, über eine Passwortrichtlinie zu verfügen. Bei großen Unternehmen lag der Wert sogar bei 86%. Nachholbedarf wiesen kleine und mittlere Unternehmen auf, von denen 77% eine solche Richtlinie vorweisen konnten.

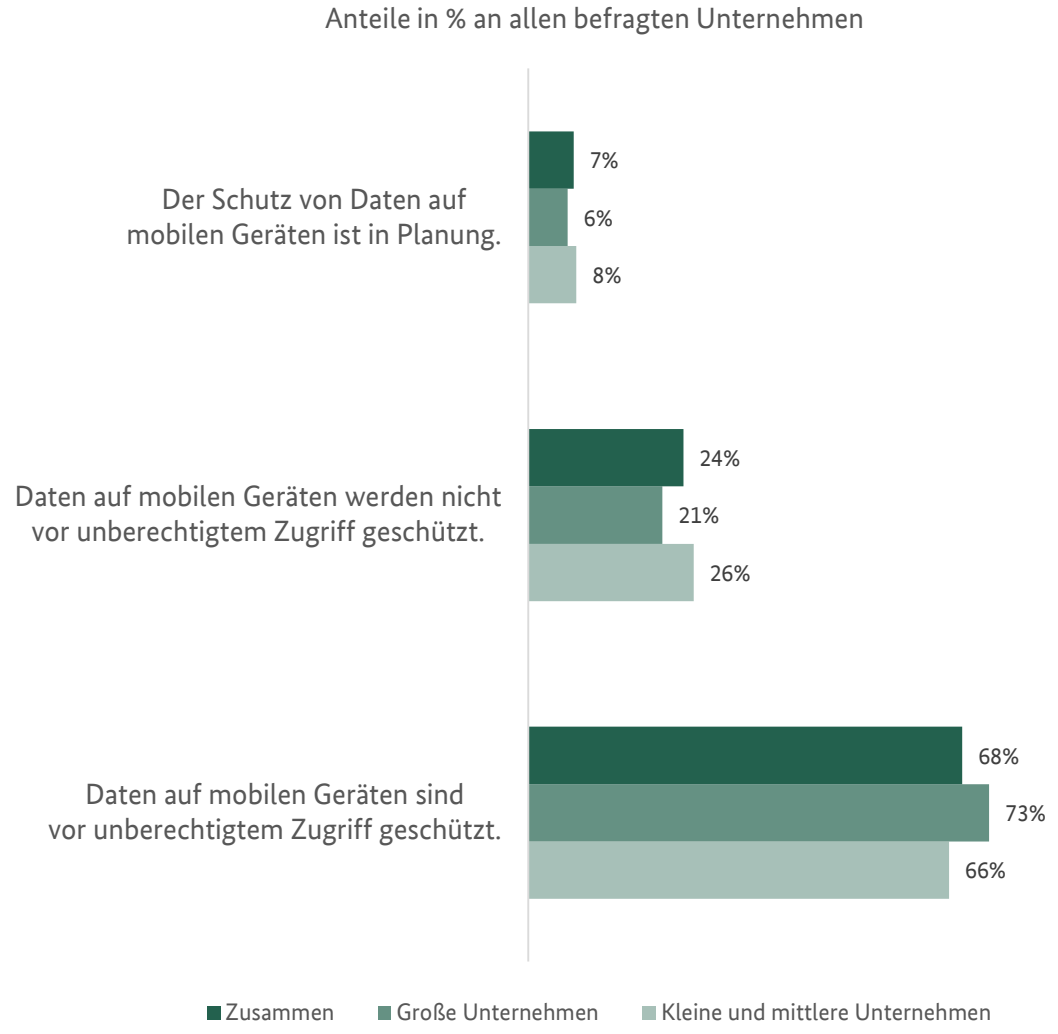


Bundesamt
für Sicherheit in der
Informationstechnik

Schutz mobiler Endgeräte

Gut zwei Drittel aller Unternehmen wenden Maßnahmen zum Schutz der Daten auf mobilen Endgeräten an.

Dabei schnitten die großen Unternehmen mit rund 73% besser ab als die kleinen und mittleren Unternehmen mit 66%. Fast ein Viertel der befragten Unternehmen gab an, Daten auf mobilen Endgeräten nicht vor unberechtigtem Zugriff zu schützen.



Bundesamt für Sicherheit in der Informationstechnik

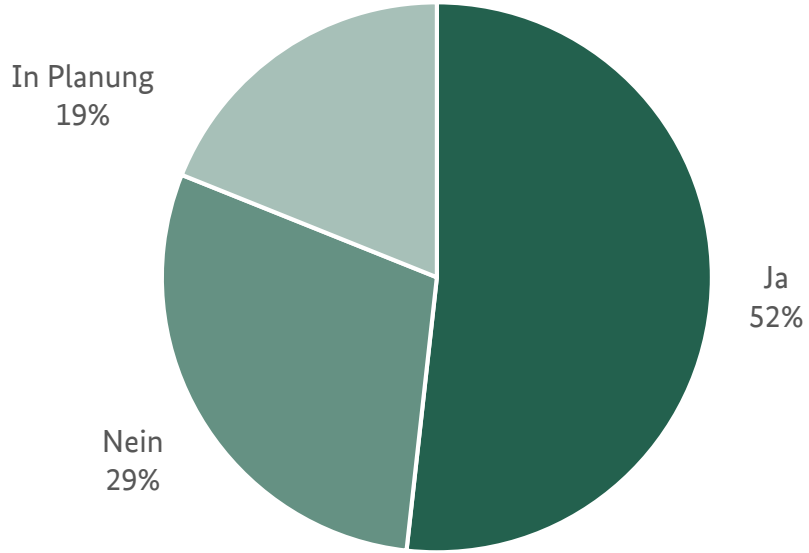
Schulung von Beschäftigten zur IT-Sicherheit

Viele Unternehmen haben die essenzielle Bedeutung der Qualifizierung und Sensibilisierung ihrer Beschäftigten erkannt.

So gaben mehr als die Hälfte der Unternehmen an, dass regelmäßige Schulungen für Beschäftigte zu Fragen der Cyber-Sicherheit durchgeführt werden (52%). Weitere knapp 20% der befragten Unternehmen berichteten, dass regelmäßige Schulungsmaßnahmen in Planung sind. Allerdings sagten knapp 30% der Befragten, dass IT-Sicherheits-Schulungen nicht stattfinden und auch nicht geplant sind.

Wird das Personal in regelmäßigen Abständen in Bezug auf IT-Sicherheit geschult?

Anteile in % an allen befragten Unternehmen



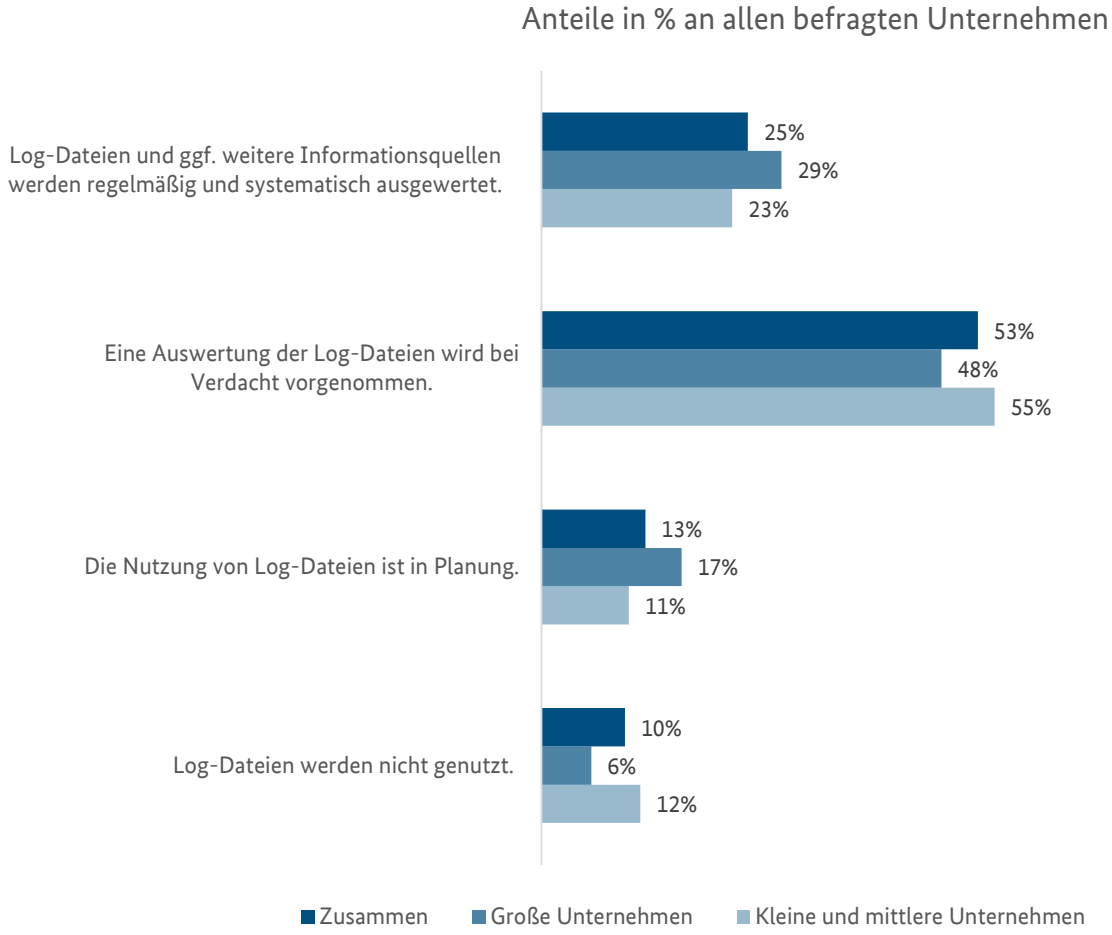
Bundesamt
für Sicherheit in der
Informationstechnik

Detektion

Erkennung von Cyber-Angriffen

Ein Viertel der befragten Unternehmen verfügt heute über ein Cyber-Sicherheits-Monitoring.

29% der großen Unternehmen und 23% der kleinen und mittleren Unternehmen werten Log-Dateien regelmäßig und systematisch aus. Gut die Hälfte aller Unternehmen untersucht Log-Files nur bei konkreten Anlässen. Nachholbedarf kleiner und mittlerer Unternehmen lässt sich bei den Planungsaktivitäten erkennen. Während rund 17% der großen Unternehmen die Nutzung von Log-Daten plant, trifft dies nur auf 11% der kleinen und mittleren Unternehmen zu.



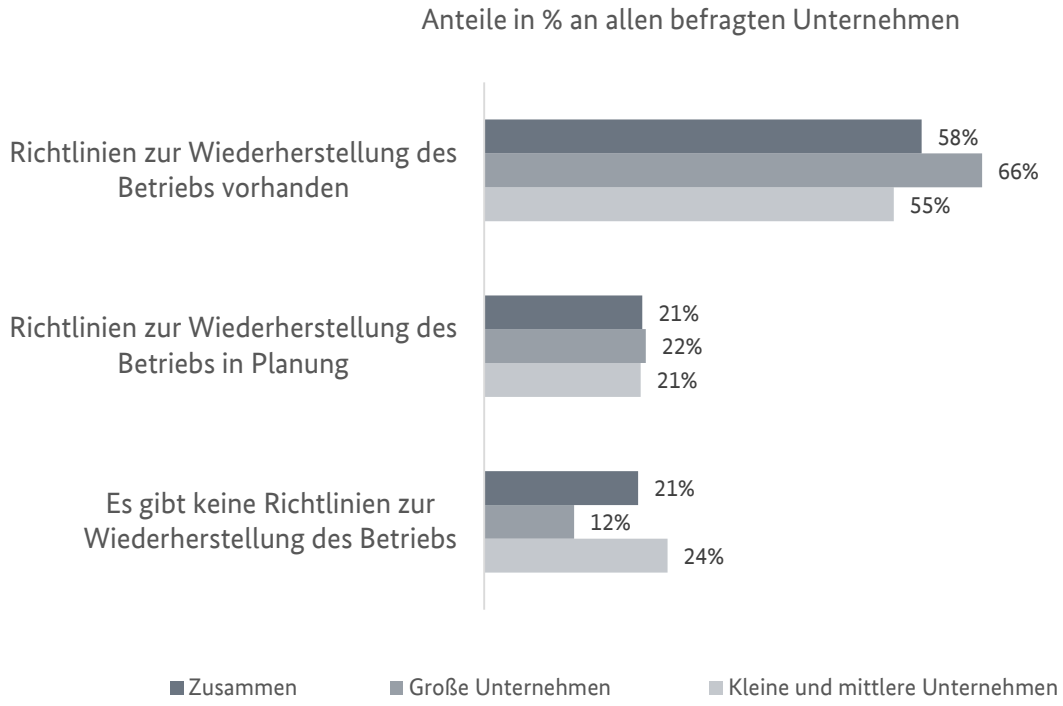
Bundesamt
für Sicherheit in der
Informationstechnik

Reaktion

Richtlinien zur Wiederherstellung des Betriebs nach einem Störfall

Besondere Aufmerksamkeit widmen die Unternehmen nach eigenen Angaben reaktiven Maßnahmen für den Fall eines Cyber-Angriffs.

So gaben rund 58% der Befragten an, dass Richtlinien wie etwa Notfallpläne oder Störfallanweisungen existieren, die die Wiederherstellung des Betriebs nach einer schwerwiegenden Betriebsstörung beschreiben. Dabei traten deutliche Unterschiede zwischen kleinen, mittleren und großen Unternehmen zutage. Während 66% der großen Unternehmen über eine solche Richtlinie verfügen, traf dies nur auf gut 55% der kleinen oder mittleren Unternehmen zu.



Bundesamt
für Sicherheit in der
Informationstechnik

Angaben zur Datenbasis und zum Teilnehmerfeld

Datenbasis

Die Cyber-Sicherheits-Umfrage 2017 wurde durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) im Rahmen der Allianz für Cyber-Sicherheit durchgeführt. An der Erstellung des Fragenkatalogs war Dr. Thiele IT-Beratung, ein Partner der Allianz für Cyber-Sicherheit, beteiligt.

- Umfragezeitraum: 04.10.2017 bis 30.11.2017
- 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: 879 teilnehmende Institutionen

Teilnehmerfeld

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

- **Kleine und mittlere Unternehmen bzw. Institutionen** mit 1 bis 499 Beschäftigten: etwa zwei Drittel
- **Große Unternehmen bzw. Institutionen** mit mehr als 500 Mitarbeiterinnen und Mitarbeitern: etwa ein Drittel

An der Umfrage beteiligten sich Institutionen aus den folgenden Wirtschaftsfeldern (eigene Angaben):

- **Anwenderunternehmen**: ca. 49 Prozent
- **IT-Dienstleister, -Hersteller, -Provider**: ca. 20 Prozent
- **Öffentlicher Dienst**: ca. 14 Prozent
- Sonstige: ca. 17 Prozent

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 mehr als 2.500 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 Erstberatung, Penetrationstests und vieles mehr, bereitgestellt durch die Partner der Allianz für Cyber-Sicherheit.

Weitere Informationen zur kostenfreien Mitgliedschaft unter: www.allianz-fuer-cybersicherheit.de

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) 228 99 9582 5977
www.allianz-fuer-cybersicherheit.de

Bundesamt
für Sicherheit in der
Informationstechnik