Capterra

/ Der Stand der IT-Sicherheit in deutschen KMU

44% der Unternehmen waren bereits Opfer eines Cyberangriffs

Inhaltsverzeichnis

/ Einführung

Die wachsende Gefahr von Cyberattacken: Studie zum Stand der IT-Sicherheit in deutschen KMU

Deutsche Unternehmen sind ein begehrtes Ziel für Cyberangriffe. Kleine und mittelständische Unternehmen (KMU) werden häufig als leichte Beute betrachtet, da sie über geringere Sicherheitsvorkehrungen als Großunternehmen verfügen. Die weltweite Pandemie hat zusätzlich für mehr Angriffsfläche gesorgt. Cyberkriminelle nutzen gerade die Krise und die niedrigen Sicherheitsbedingungen der remote arbeitenden Belegschaft für ihre Angriffe.

Capterra führte eine Studie unter 202 IT-Entscheidern aus deutschen kleinen und mittelständischen Unternehmen durch, um einen Einblick in die größten IT-Risiken, die Entwicklung der Angriffe in der Krise und den derzeitigen Sicherheitsstandard zu bekommen.

Befragt wurden dafür Voll-oder Teilzeitbeschäftigte, aus einem kleinen und mittelständischen Unternehmen (mit 2-250 Mitarbeitern), die für Entscheidungen über IT-Richtlinien in Ihrem Unternehmen teils oder voll verantwortlich sind.

Highlights der Studie

44 % der Unternehmen waren bereits Opfer eines Cyberangriffs

23 % der IT-Verantwortlichen haben bereits auf einen bösartigen Link in einer Phishing-E-Mail geklickt

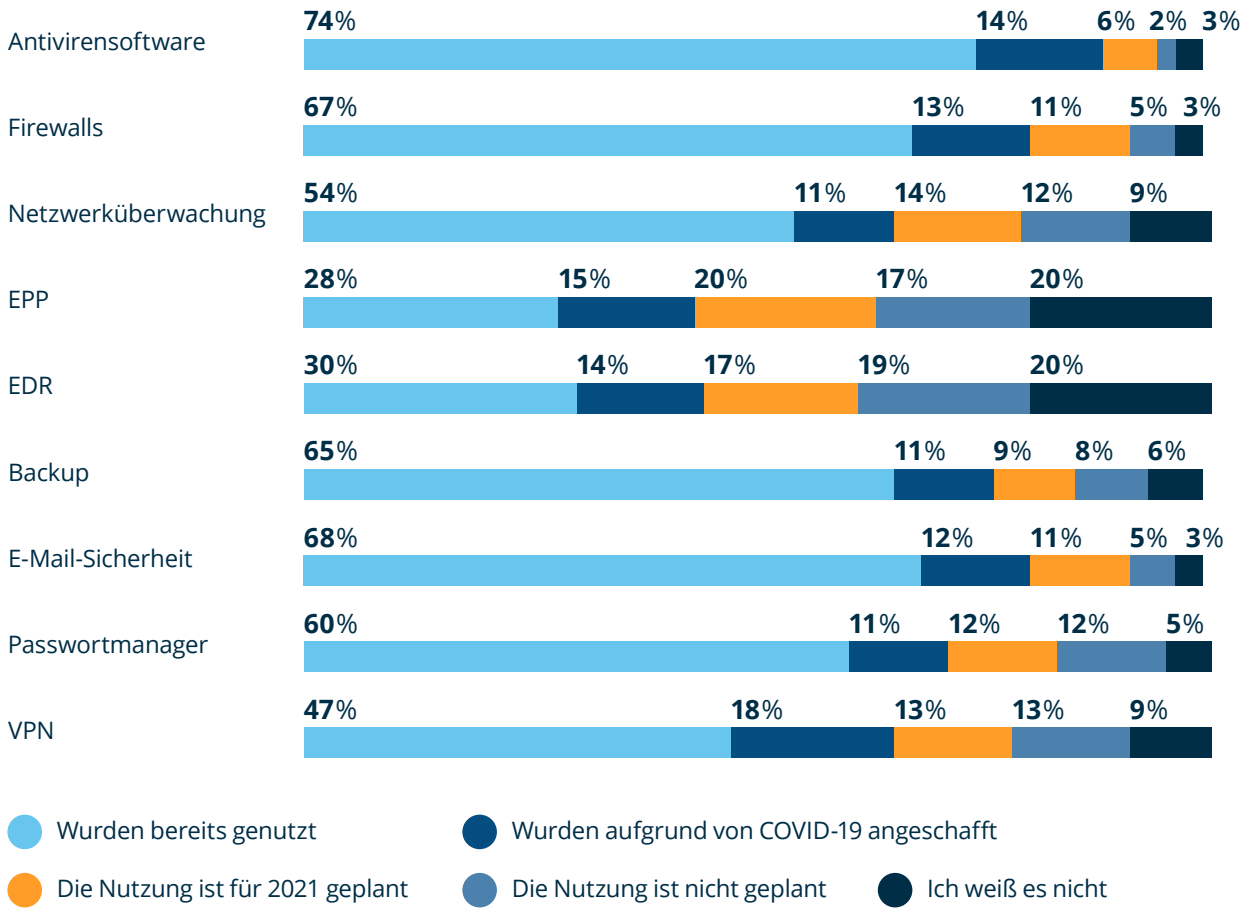
39 % der Angestellten haben Zugriff auf mehr Daten, als unbedingt zur Erfüllung ihrer Aufgaben erforderlich ist

36 % nutzen künstliche Intelligenz für ihre IT-Sicherheit

/ Umfrageergebnisse

Die meistgenutzten Sicherheitsanwendungen sind Antivirensoftware, E-Mail-Sicherheitssoftware und Firewalls

Die Nutzung von Sicherheitsanwendungen in deutschen KMU



Die Krise hat dazu geführt, dass viele Anwendungen erstmalig eingesetzt wurden. Vor allem VPN Software erhielt einen großen Anstieg. Auch Anwendungen wie Endpoint Protection Platform (EPP) und Endpoint Detection and Response (EDR), die vorher wenig genutzt wurden, wurden während COVID-19 angeschafft.

44 % der Unternehmen waren bereits Opfer eines Cyberangriffs

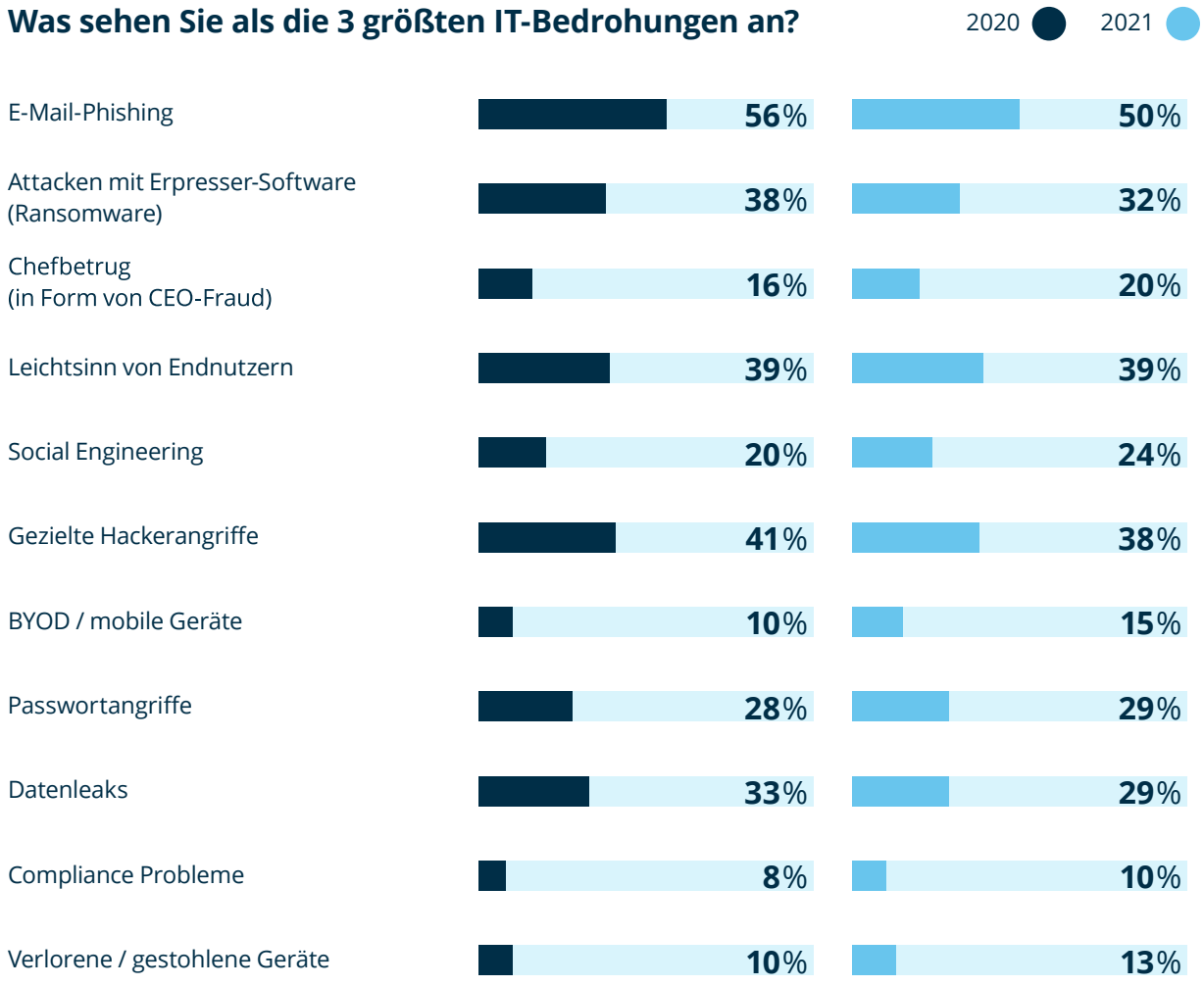
Fast jedes zweite Unternehmen fiel bereits einer Cyberattacke zum Opfer. Diese Zahl ist immens hoch. Unentdeckte Attacken sind darin nicht enthalten. Die Auswirkungen von Cyberangriffen sind fatal. Ein Unternehmen teilte uns auf die Frage, was die mit dem Cyberangriff verbundenen Ausfallzeiten und finanziellen Verluste waren, mit: “damals konnten wir unsere Systeme für 12 Stunden nicht nutzen und wir gehen aufgrund von Kundenverlusten von mindestens 50.000 Euro Verlust aus.” Ein anderes Unternehmen meinte: “Wir konnten nicht mehr auf unsere PCs zugreifen und haben 100.000 Euro Verlust gemacht”

Es gab jedoch auch positive Rückmeldung der IT-Abteilungen, “geringe bis keine Ausfallzeit, da der Angriff bemerkt wurde und umgehend Maßnahmen getroffen werden konnten, daher ebenfalls nur keine bis geringe finanzielle Verluste”. Ein anderer IT-Verantwortlicher meinte zu uns “Alles war gut gesichert, daher konnte weiter gearbeitet werden. Es hat jedoch etwa eine Woche gedauert, bis alles wie vorher war.”

/ Die größten IT-Bedrohungen 2020 und 2021

IT-Verantwortliche sollten definitiv die Bedrohungen, die auf menschlichen Fehlern beruhen im Auge behalten wie Phishing-E-Mails, Chef-Betrug und Social Engineering. Diese sind weiterhin eine große Gefahr für Unternehmen – vor allem, wenn sie nicht darauf vorbereitet sind. Vor allem der Chefbetrug sowie Social Engineering werden von den IT-Verantwortlichen als wachsende Gefahr in diesem Jahr angesehen.

Was sehen Sie als die 3 größten IT-Bedrohungen an?

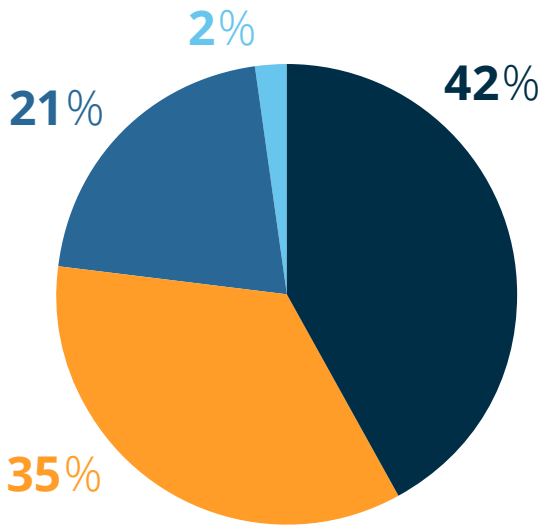


Bei dieser Frage standen mehrere Antwortmöglichkeiten zur Verfügung, daher weicht die Gesamtsumme von 100 Prozent ab.

Die Zahl der Phishing-Angriffe steigt während der Krise

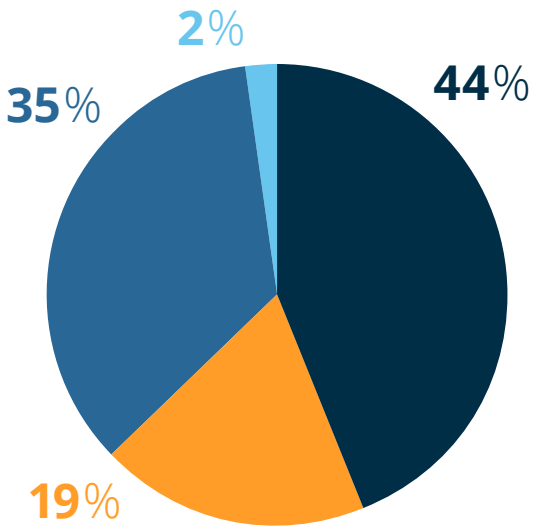
77 % der Unternehmen haben bereits eine Phishing-E-Mail erhalten. Von diesen Unternehmen geben 44 % an, dass sie während der Krise mehr Phishing-E-Mails als gewöhnlich erhalten.

Haben Sie oder jemand anderes in Ihrem Unternehmen jemals eine Phishing-E-Mail erhalten?



- Ja, ich selbst
- Ja, andere in meinem Unternehmen
- Nein, ist mir nicht bekannt
- Ich weiß es nicht

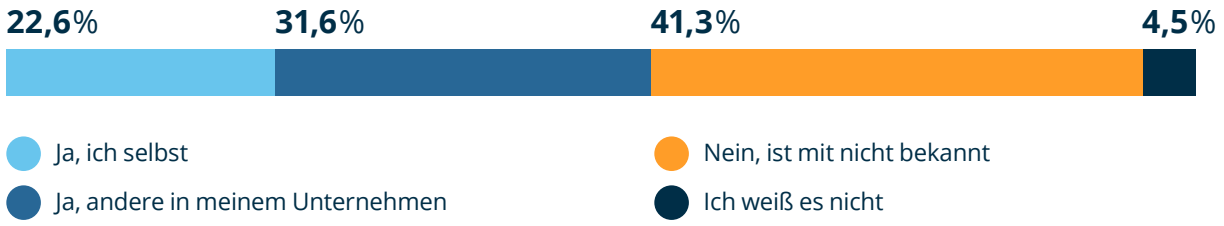
Hat ihr Unternehmen mehr Phishing-E-Mails während der COVID-19-Krise erhalten?



- Ja, wir haben mehr Phishing-E-Mails als gewöhnlich erhalten
- Nein, wir haben weniger Phishing-E-Mails als gewöhnlich erhalten
- Wir haben ungefähr gleich viele Phishing-E-Mails erhalten
- Wir haben keine Phishing-E-Mails während der COVID-19-Krise erhalten

23 % der IT-Verantwortlichen haben bereits auf einen bösartigen Link in einer Phishing-E-Mail geklickt

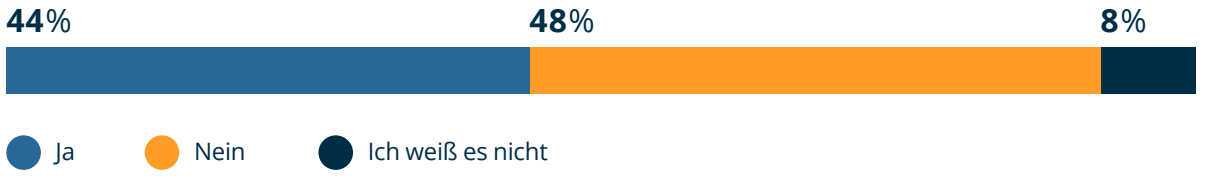
Haben Sie oder jemand anderes in Ihrem Unternehmen jemals auf einen bösartigen Link in einer Phishing-E-Mail geklickt?



Selbst 23 % der IT-Verantwortlichen geben an, schon auf einen Link in einer Phishing-E-Mail geklickt zu haben.

Unternehmen wird dringend geraten einen Phishing-Test durchzuführen, bei denen alle Angestellten eine gefälschte E-Mail erhalten, um herauszufinden, ob jemand auf den Link klickt oder einen Anhang öffnet. Diese Tests können von Ihrer internen IT-Abteilung entworfen oder von einem externen Sicherheitsunternehmen durchgeführt werden.

Hat Ihr Unternehmen Phishing-Tests durchgeführt?

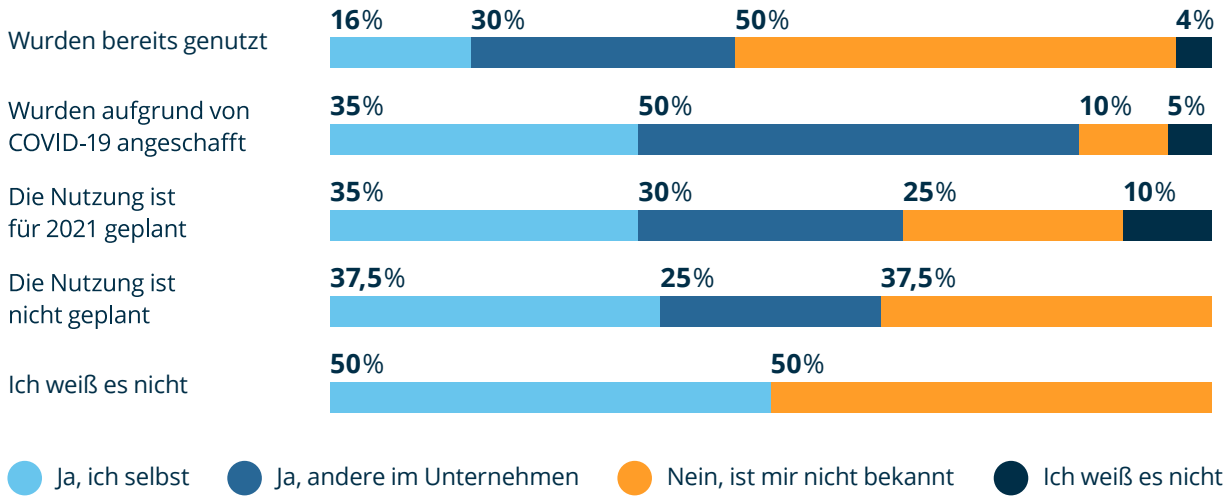


Die Anzahl an Unternehmen, die Phishing-Tests durchführen hat sich seit 2019 mehr als verdoppelt. In einer vorigen Capterra Umfrage haben wir ermittelt, dass vor der Krise lediglich 20 % der Unternehmen einen solchen Test durchgeführt haben.

E-Mail-Sicherheitssoftware verringert das Phishing-Risiko

E-Mail-Sicherheitslösungen erkennen schädliche Mails und sortieren diese aus. Ebenfalls können sie die in den E-Mails enthaltenen Links überprüfen und dadurch schädliche Webseiten identifizieren. 81 % der deutschen KMU sind sich den Gefahren bewusst und haben E-Mail-Sicherheit implementiert.

Einsatz von E-Mail-Sicherheitssoftware vs. Klicks auf Phishing-E-Mails

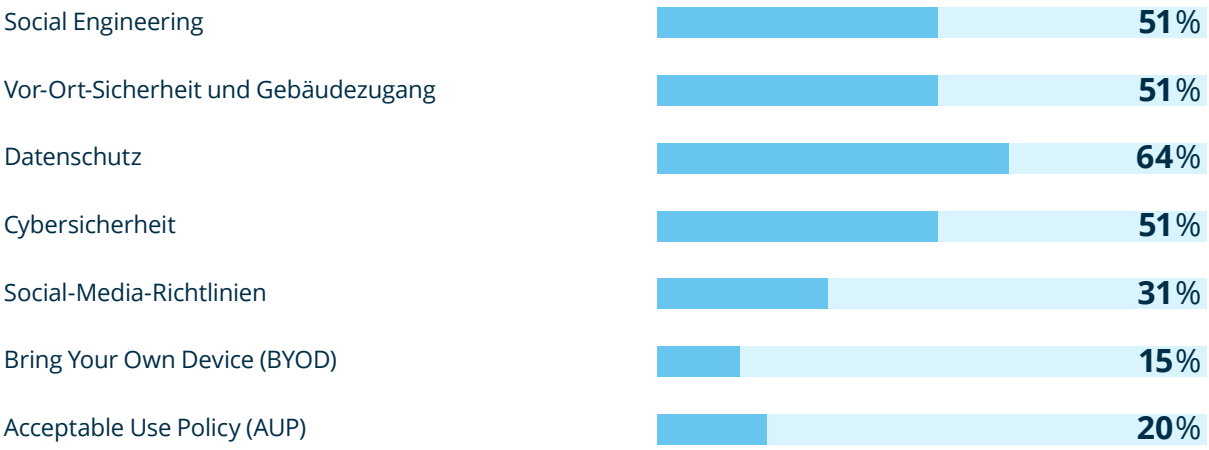


In Unternehmen, die E-Mail-Sicherheit nutzen, haben 16 % der IT-Verantwortlichen auf einen bösartigen Link in einer Phishing-E-Mail geklickt. In Unternehmen, die momentan keine E-Mail-Sicherheit nutzen, die Nutzung jedoch für 2021 planen, waren es ganze 35 %. Ohne E-Mail-Sicherheit ist das Risiko in Unternehmen auf Phishing-E-Mails zu klicken demnach deutlich höher.

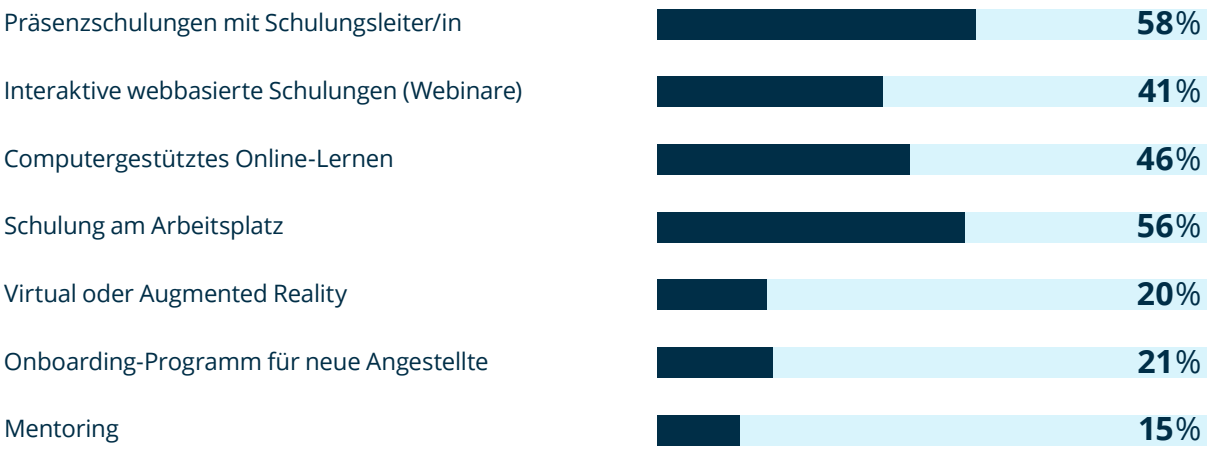
51 % der Unternehmen bieten Schulungen im Bereich der IT-Sicherheit an

Neben dem Einsatz von Software sind Mitarbeiter-Schulungen entscheidend, um die Risiken von Cyberangriffen wie beispielsweise Klicks auf Phishing E-Mails zu verringern.

In welchen der folgenden Bereichen bietet Ihr Unternehmen Schulungen an?



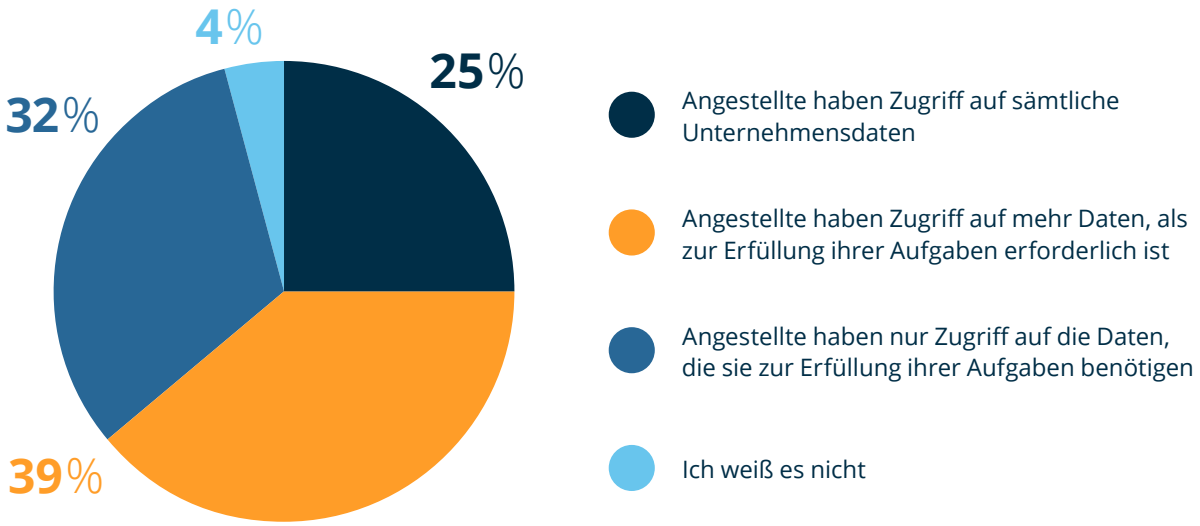
Welche der folgenden Methoden nutzt Ihr Unternehmen für Schulungen?



Bei dieser Frage standen mehrere Antwortmöglichkeiten zur Verfügung, daher weicht die Gesamtsumme von 100 Prozent ab.

39 % der Angestellten haben Zugriff auf mehr Daten, als unbedingt zur Erfüllung ihrer Aufgaben erforderlich ist

Wie viel Zugriff haben die Angestellten in Ihrem Unternehmen auf Unternehmensdaten?



Knapp zwei Drittel aller Unternehmen ermöglicht ihren Mitarbeitern den Zugriff auf mehr Daten, als sie für ihre Arbeit benötigen bzw. Zugriff auf sämtliche Unternehmensdaten. Dies gefährdet die Datensicherheit, erschwert die Einhaltung von Vorschriften und bietet unnötige Möglichkeiten für Insider-Bedrohungen.

Authentifizierungswerkzeuge können vor Cyberangriffen schützen

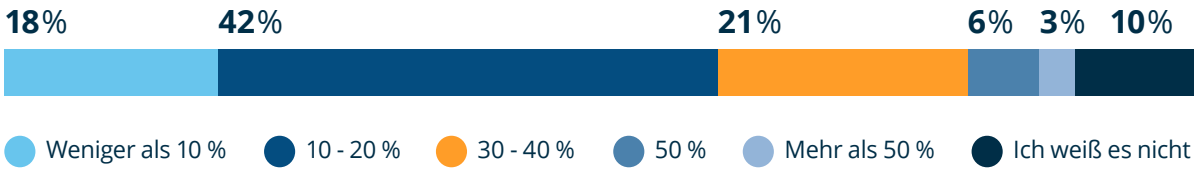
Nutzt Ihr Unternehmen Authentifizierwerkzeuge für Geschäftsanwendungen?	✓	✗	?
Zwei-Faktor-Autorisierung (2FA)	66%	28%	6%
Biometrische Sicherheitsmaßnahmen (Biometric security measures)	50%	47%	3%

Authentifizierungswerkzeuge überprüfen die Identität von Personen, die Zugang zu Ihren Unternehmensressourcen suchen. Die Zwei-Faktor-Authentifizierung erfordert zwei Identifizierungsmethoden und verhindert viele der häufigsten Cyberangriffe und Datenverletzungen. Die biometrische Authentifizierung ist die Verwendung eines physischen Merkmals, wie z.B. eines Fingerabdrucks oder eines Iris-Scans, um Zugang zu einer sicheren Einrichtung zu erhalten. Die Technologie ist eine kostspieligere Investition und wird daher vermutlich weniger genutzt.

Die Nutzung von Authentifizierungswerkzeugen ist jedoch stark durch die Krise gestiegen. Einer vorigen Capterra Studie zufolge, lag 2019 die Nutzung von Zwei-Faktor-Autorisierung noch bei 55 %, die von biometrischen Sicherheitsmaßnahmen lediglich bei 20 %.

Knapp die Hälfte der Unternehmen investiert aufgrund von COVID-19 mehr in IT-Sicherheit

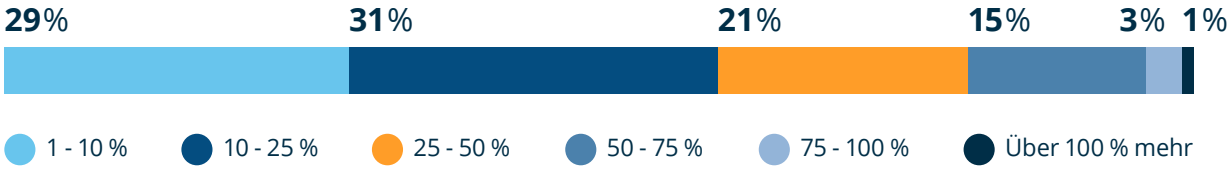
Wie viel des IT-Budgets in Ihrem Unternehmen wird für IT-Sicherheit ausgegeben?



Unternehmen in Deutschland verwenden immer noch einen geringen Prozentsatz für die IT-Sicherheit. 60 % der Unternehmen geben unter 20 % des IT-Budgets für Sicherheit aus.

Hat ihr Unternehmen aufgrund von COVID-19 mehr in IT-Sicherheit investiert?

Wie viel mehr hat ihr Unternehmen aufgrund von COVID-19 in IT-Sicherheit investiert?

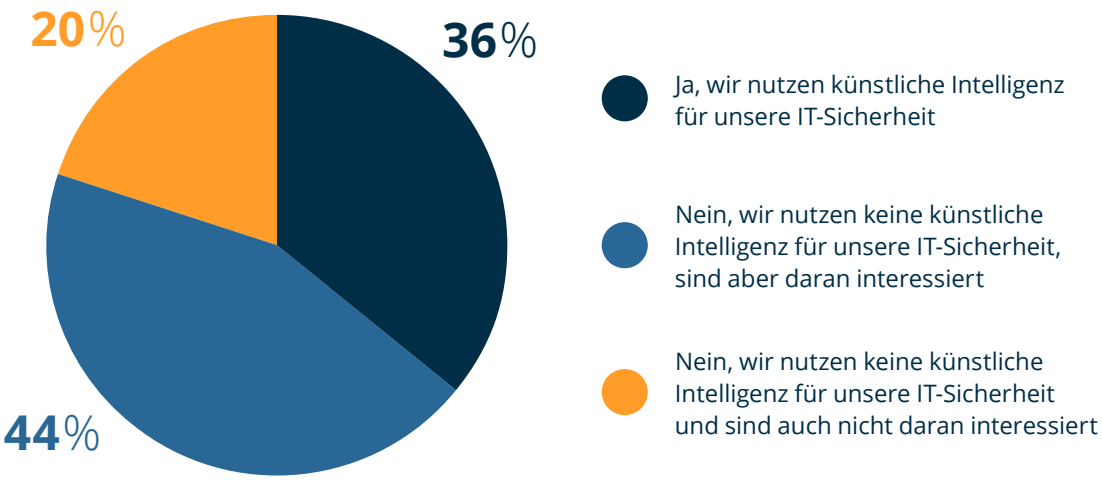


Das IT-Sicherheitsbudget ist jedoch in knapp der Hälfte der Unternehmen in der Krise erhöht worden. 81 % dieser Unternehmen haben um bis zu 50 % mehr für IT-Sicherheit ausgegeben.

Künstliche Intelligenz für die Verbesserung der IT-Sicherheit in Unternehmen

Die künstliche Intelligenz ist die Zukunft der IT-Sicherheit. 80 % der Unternehmen setzen sie bereits ein bzw. sind an der Technologie interessiert.

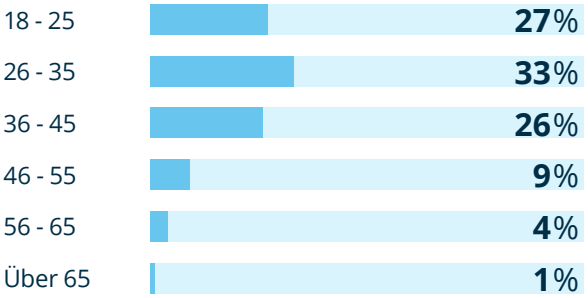
Nutzen Sie künstliche Intelligenz für die IT-Sicherheit Ihres Unternehmens oder sind Sie daran interessiert?



Cyberangriffe treten nicht nur häufiger auf, sondern werden auch immer komplexer. Die künstliche Intelligenz kann Anomalien schneller erkennen, Risiken und Risikobereiche vorhersagen und den Cybersicherheitsplan robuster gestalten.

/ Teilnehmerstruktur

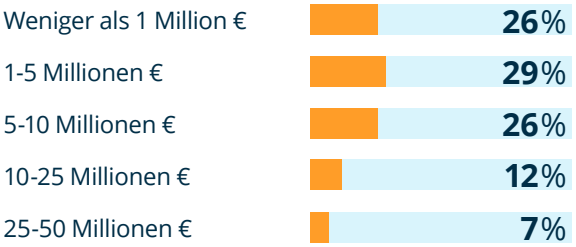
Alter



Geschlecht

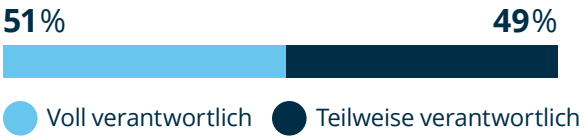
Beschäftigte

Jahresumsatz des Unternehmens



Beschäftigungsstatus

Verantwortlichkeit über Entscheidungen zu IT-Richtlinien



Branche

Bildung und Wissenschaft	7%
Handel	9%
Gesundheitswesen, Medizin und Sozialbereich	6%
Banken und Finanzdienstleister	7%
Herstellung und Produktion	10%
Wirtschaftsprüfung, Steuern und Recht	4%
Transport und Logistik	6%
Design, Architektur	5%
Tourismus und Gastgewerbe	1%
Landwirtschaft und Nahrungsmittel	1%
Medien, Informationen, Kommunikation	4%
Immobilienbranche	1%
Internet, Computer und IT	29%
Bausektor	4%
Sonstige Branchen:	5%

/ Methodik der Datenerfassung

/ Studienmethodik

Die Befragung wurde im Dezember 2020 durchgeführt. Teilnehmer wurden per Online-Fragebogen zur Teilnahme eingeladen. Insgesamt qualifizierten sich 202 Personen für die Befragung.

Für die Umfrage haben sich folgende Teilnehmer qualifiziert:

- Über 18 Jahre alt,
- teil- oder vollzeitbeschäftigt,
- in einem kleinen und mittelständischen Unternehmen mit 2-250 Mitarbeitern und einem Jahresumsatz von unter 50 Millionen Euro beschäftigt,
- teilweise verantwortlich oder voll verantwortlich für Entscheidungen über IT-Richtlinien in ihrem Unternehmen.

Hinweise

- Durch Rundungen der Prozentwerte kann die Gesamtsumme von 100 Prozent abweichen.
- Bei einigen Fragen standen mehrere Antwortmöglichkeiten zur Verfügung, daher weicht die Gesamtsumme von 100 Prozent ab.

Capterra

/ Über Capterra

Capterra hilft Unternehmen weltweit, die richtige Software für ihre Anforderungen zu finden. 1999 gegründet, bietet Capterra mit seiner globalen Produktpräsenz, verifizierten Nutzerbewertungen, unabhängigen Testberichten und maßgeschneiderten Vergleichstools jeden Monat mehr als fünf Millionen Käufern Zuversicht bei der Softwareauswahl.

Softwareauswahl leicht gemacht

- 1.375.000 verifizierte Software-Bewertungen
- In über 800 Kategorien
- 60.000+ Tools im Vergleich

ERFAHRE MEHR AUF CAPTERRA.COM.DE