PULSE Lookout

Ransomware 2021

Ransomware-Angriffe, bei denen Kriminelle Daten mithilfe von Malware sperren, bis ein Lösegeld gezahlt wird, sorgen immer wieder für Schlagzeilen. Welche Erfahrungen haben Tech-Entscheidungsträger mit Ransomware gemacht?

Pulse hat mehr als 300 Entscheider für diesen „One-Minute Insight Report" befragt, um herauszufinden:

- Wie viele von ihnen Erfahrung mit Ransomware gemacht haben und wie die Angriffe ausgingen
- Was Unternehmen anfällig für Ransomware macht
- Warum Ransomware-Angriffe zugenommen haben

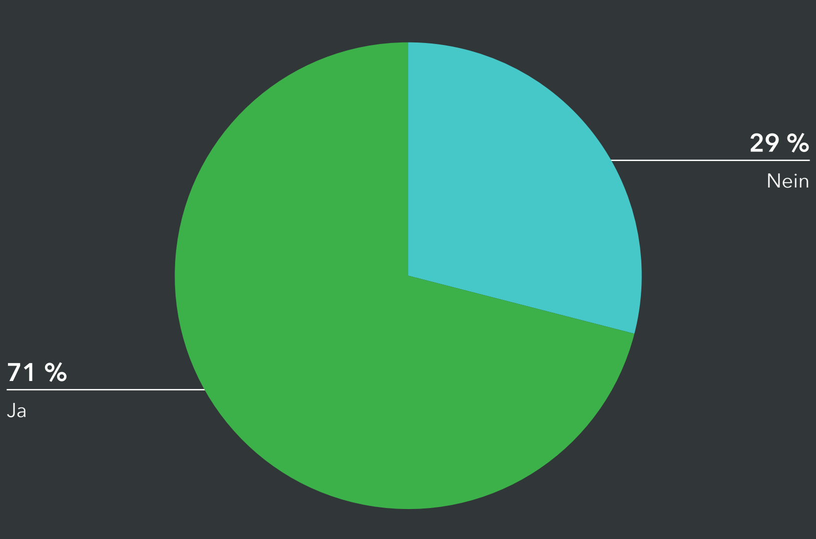
Daten erhoben vom 26. Juni bis 28. August 2021

Gesamtzahl der Teilnehmer: 331 Tech-Entscheidungsträger

Viele hatten in ihrer Laufbahn schon mit Ransomware zu tun, bei den meisten Angriffen erfolgte jedoch keine Zahlung und die Daten konnten in der Mehrheit der Fälle gerettet werden

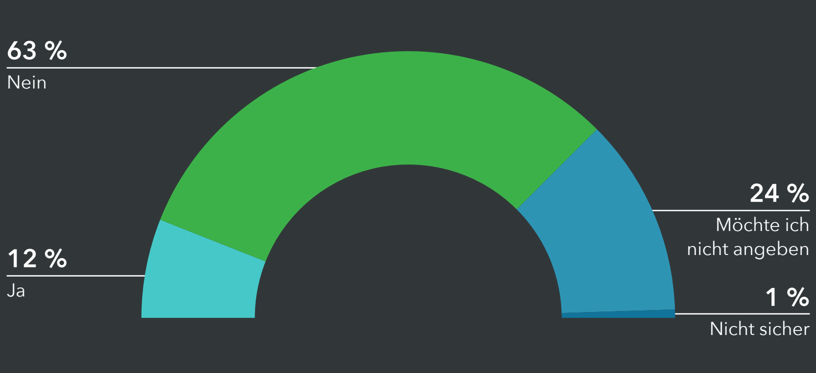
Fast drei Viertel (71 %) der Führungskräfte haben für Unternehmen gearbeitet, die schon einmal Opfer von Ransomware geworden sind.

Haben Sie jemals in einem Unternehmen gearbeitet, in dem es zu einem Angriff durch Ransomware kam?



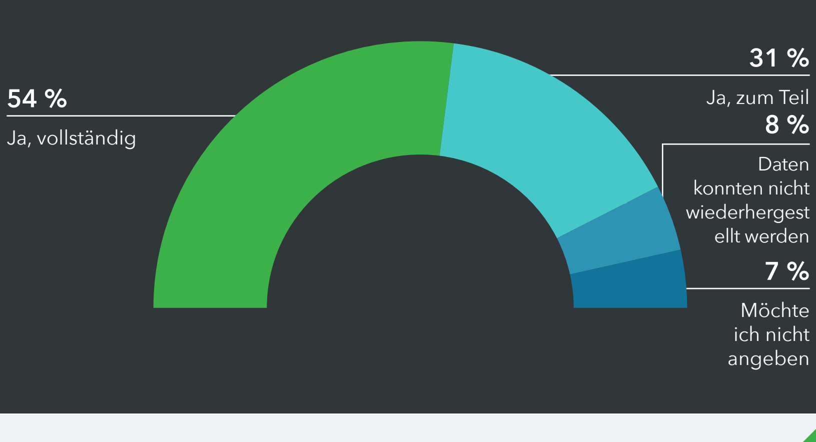
Bei mindestens 12 % dieser Ransomware-Fälle erfolgte eine Zahlung.

Wurde das Lösegeld für die Ransomware gezahlt?



Insgesamt gelang es 54 % der Führungskräfte, ihre Daten nach der Ransomware-Attacke vollständig wiederzuerlangen. Allerdings konnten nur 52 % der Unternehmen, die das Lösegeld zahlten (n = 29), alle Daten retten, während es bei den Unternehmen, die kein Lösegeld zahlten (n = 147), 65 % waren.

Konnten die von dem Angriff betroffenen Daten wiederhergestellt werden?



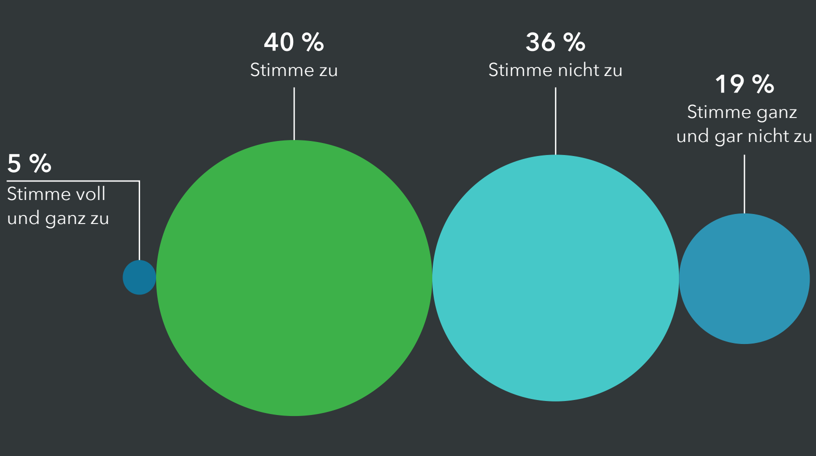
„Ransomware stellt sich weltweit als eine der größten Bedrohungen heraus und es ist wichtig, angemessen damit umzugehen."

– Leiter eines mittelgroßen Bergbauunternehmens

Führungskräfte sind uneinig, ob Ransomware-Zahlungen als Betriebskosten gelten sollten – für die meisten ist die Zahlung jedoch das letzte Mittel

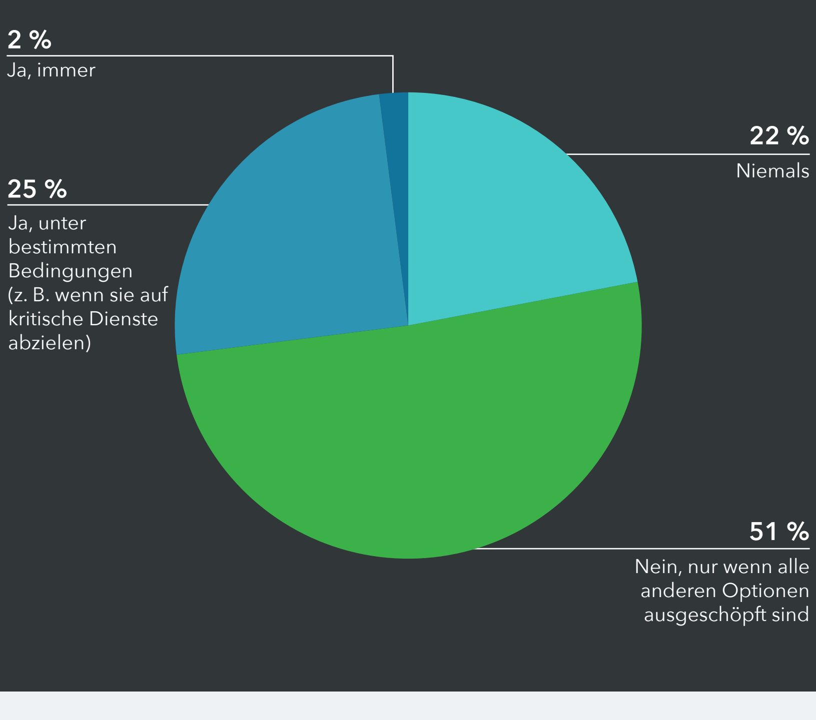
Insgesamt findet nur eine knappe Mehrheit der Führungskräfte (55 %), dass Unternehmen Ransomware-Zahlungen nicht als Betriebskosten ansehen sollten.

To what extent do you agree with the following:
Wie sehr stimmen Sie folgender Aussage zu:
„Unternehmen sollten Ransomware-Zahlungen als Betriebskosten ansehen."operating cost for businesses."



Die meisten (51 %) sind der Meinung, dass Ransomware-Forderungen erst dann gezahlt werden sollten, wenn alle anderen Optionen ausgeschöpft sind.

Sollten Unternehmen Ransomware-Forderungen zahlen?



„[Ransomware] ist ein hausgemachtes Problem. Versicherungen haben es noch verschlimmert, indem sie entsprechende Deckungen anbieten und das Verhalten der Erpresser ohne Konsequenzen [belohnen]."

– Vorstandsmitglied eines kleinen bis mittleren Bildungsunternehmens

„Wenn die Leute zahlen, gibt es einen Markt. Ich würde, offen gesagt, lieber die Strafe als die Kriminellen bezahlen."

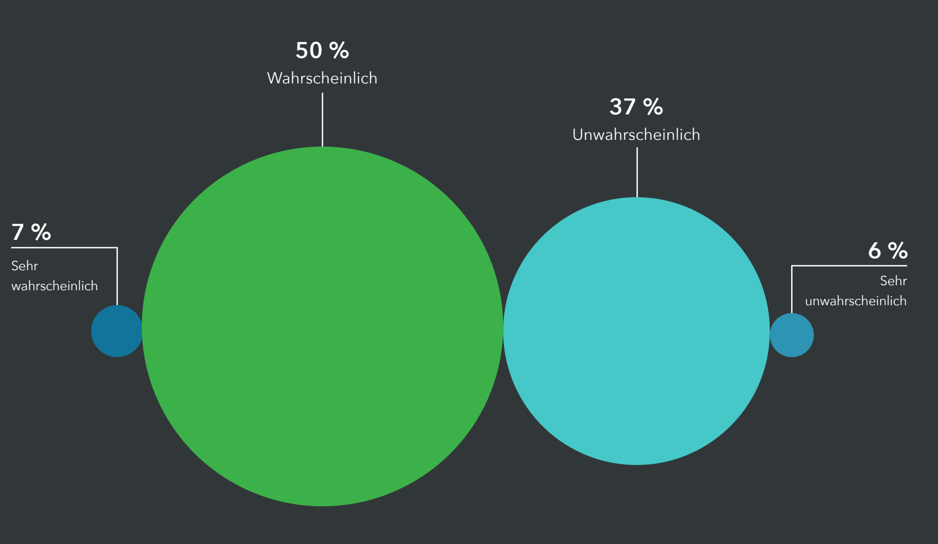
– VP eines großen Bildungsunternehmens

Die Mehrheit glaubt, dass ein Ransomware-Angriff auf ihr Unternehmen innerhalb des nächsten Jahres wahrscheinlich ist und fürchtet Reputationsschäden als Folge

Insgesamt gehen die meisten Führungskräfte (57 %) davon aus, dass ihr Unternehmen in den nächsten 12 Monaten wahrscheinlich von einem Ransomware-Angriff betroffen sein wird.

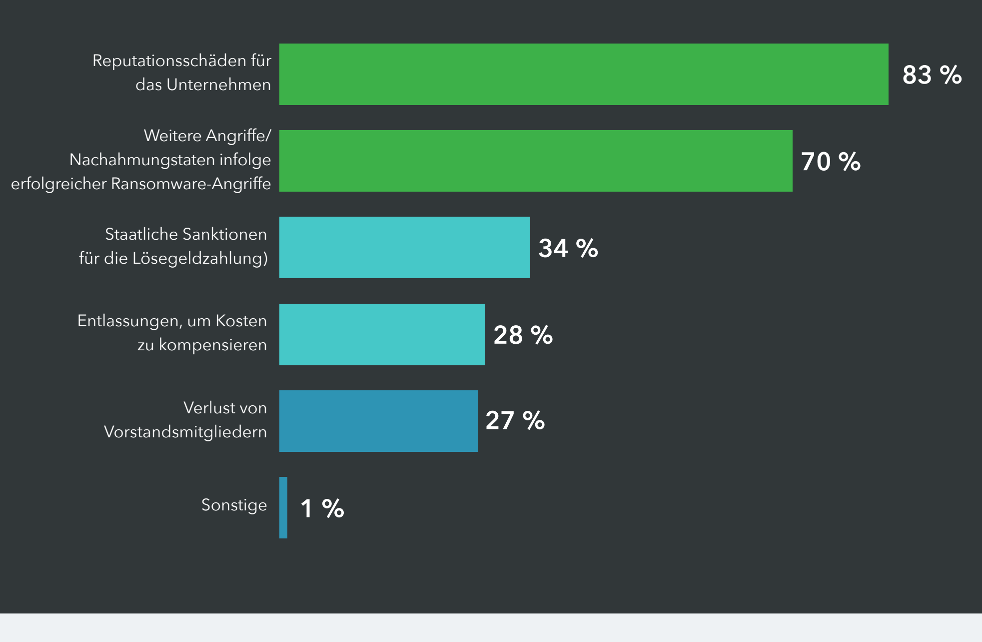
Allerdings halten 62 % derjenigen, die schon einmal einen Ransomware-Vorfall erlebt haben (n = 234), einen Angriff für wahrscheinlich. Unter den Befragten, die noch keine Ransomware-Attacke erlebt haben (n = 97), sind es lediglich 45 %.

Wie wahrscheinlich ist es, dass Ihr Unternehmen in den nächsten zwölf Monaten Opfer eines Ransomware-Angriffs werden könnte?



Was die negativen Auswirkungen anbelangt, gelten Reputationsschäden für das Unternehmen als schwerwiegendste Folge eines erfolgreichen Ransomware-Angriffs, gefolgt von der Angst, er könne weitere Attacken bzw. Nachahmungstaten nach sich ziehen (70 %).

Welche Folgen eines erfolgreichen Ransomware-Angriffs fürchten Sie für Ihr Unternehmen am meisten?



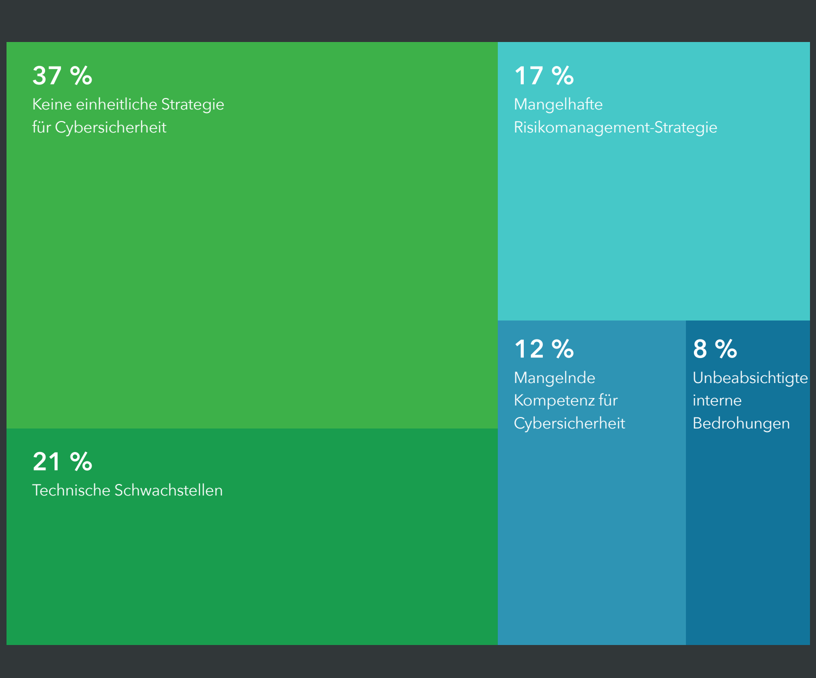
„Ransomware-Angriffe werden nicht gezielter, sondern beliebiger: Hacker werfen ein großes Netz aus, weil die meisten Unternehmen die gleichen Drittanbieter-Produkte nutzen."

– VP eines Software-Unternehmens

Das Fehlen einer einheitlichen Cybersicherheitsstrategie ist der am häufigsten genannte Grund, warum Unternehmen Ransomware zum Opfer fallen – und Mitarbeiter sind die größte Schwachstelle

Der Hauptgrund dafür, dass Unternehmen Opfer von Ransomware-Attacken werden, ist den Führungskräften zufolge das Fehlen einer einheitlichen Strategie für Cybersicherheit (37 %).

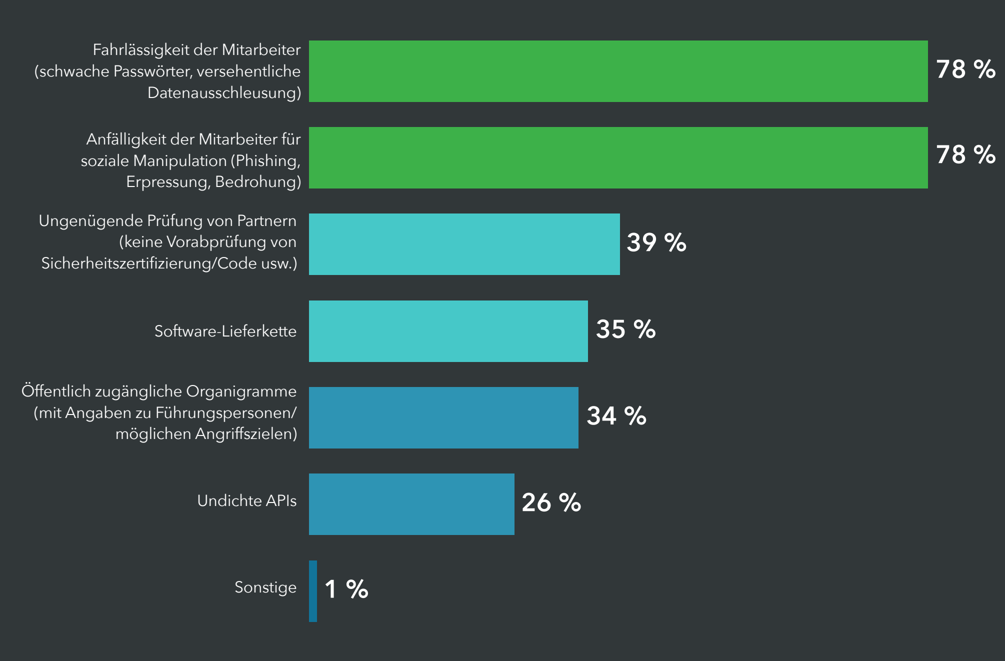
Was ist Ihrer Meinung nach der Hauptgrund dafür, dass Unternehmen einem Ransomware-Angriff zum Opfer fallen?



Bösartige interne Bedrohungen (**2 %**), verärgerte ehemalige Mitarbeiter (**1 %**), nichts davon (**1 %**), Sonstiges (**1%**)

Die größte Schwachstelle, die Ransomware-Angreifer ausnutzen, sehen Führungskräfte in den Mitarbeitern: Die beiden meistgenannten Schwachstellen sind Fahrlässigkeit der Mitarbeiter (78 %) und die soziale Manipulation von Mitarbeitern (78 %).

Welche Schwachstellen im Unternehmen nutzen bösartige Angreifer bei Ransomware-Attacken vorwiegend aus?



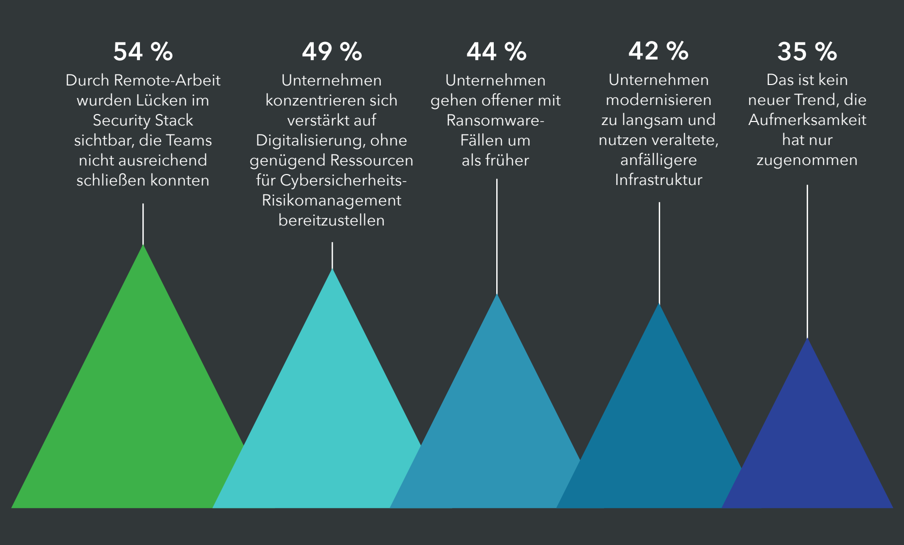
„Fast alle Angriffsvektoren für Cyber[-Attacken] haben an Bedeutung gewonnen – angetrieben von der Coronapandemie, der vermehrten Arbeit im Homeoffice und der geopolitischen Instabilität."

– Vorstandsmitglied eines mittelgroßen Gesundheitsunternehmens

Remote-Arbeit (und ein lückenhafter Security Stack) ist der Hauptgrund für Schlagzeilen über Ransomware – außerdem nennen Führungskräfte den Energiesektor und Gesundheitswesen als Hauptziele

Dass Ransomware in letzter Zeit häufiger für Schlagzeilen gesorgt hat, ist nach Ansicht der Führungskräfte vor allem darauf zurückzuführen, dass durch die Remote-Arbeit Lücken im Security Stack sichtbar wurden, die die Teams nicht schließen konnten (54 %).

Warum gab es in den letzten Monaten so viele Meldungen über prominente Ransomware-Fälle in den Nachrichten?



Finanzieller Anreiz von Ransomware ist größer als finanzieller Anreiz eines legalen Jobs als Cybersicherheitsexperte (**35 %**), Ausbreitung von Kryptowährungen erschwert Verfolgung von Cyberkriminellen (**34 %**), größere Angriffsfläche durch die Ausbreitung von Drittanbieter-SaaS (**22 %**), Zunahme staatlich geförderter Cyberkriminalität durch Verschlechterung internationaler Beziehungen (**19 %**), Sonstiges (**2 %**), nichts davon (**1 %**)

Die Branchen, die aus Sicht der Führungskräfte das größte Risiko haben, zum Ziel von Ransomware-Angriffen zu werden, sind der Energiesektor (79 %) und das Gesundheitswesen (72 %).

Welche Branchen halten Sie für die am stärksten gefährdeten Ziele für Ransomware-Angriffe?

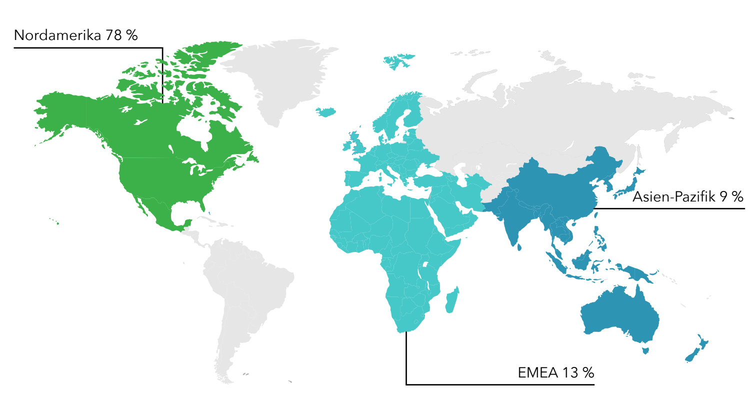
Lebensmittelverarbeitung (**24 %**), Sportverbände/-veranstaltungen (**11 %**), Sonstige (**1 %**)

„Solange Kryptowährungen nicht stärker reguliert werden (oder ihre Verwendung für Lösegeldzahlungen verboten wird), werden die Angriffe zukünftig nur weiter zunehmen."

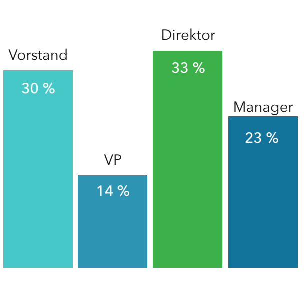
– Leiter eines großen Bildungsunternehmens

Details zu den Befragten

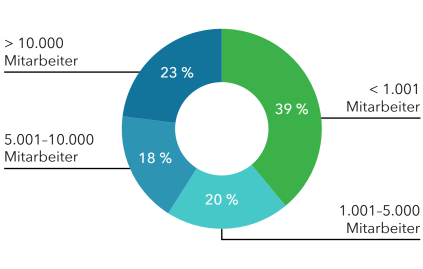
Region



Position



Firmengröße



Insights powered by PULSE