



Menschliche Gefahr

Fehlende Security-Awareness der Mitarbeiter gilt als größtes Sicherheitsrisiko.

42%



IT-Security-Strategie

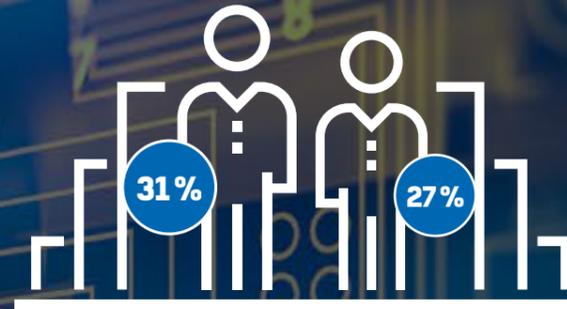
Während 84 Prozent der Unternehmen über eine IT-Security-Strategie verfügen, bleiben zehn Prozent bei isolierten Einzelmaßnahmen stehen.

84%

10%

Aufgabe der IT

Hauptsächlich CIOs und IT-Leiter sind für die Entwicklung der Security-Strategie und die Umsetzung der Sicherheitsarchitektur verantwortlich.



CIO / IT-Vorstand

IT-Leiter



Bericht an den CEO

In 48 Prozent der Firmen ist der Verantwortliche für Informationssicherheit direkt dem Geschäftsführer unterstellt. Bei kleinen Unternehmen liegt der Anteil bei extrem hohen 93 Prozent.



Externe Hilfe

Aufbau und Pflege der Sicherheitsarchitektur oder Penetrations-Tests gehören zu den wichtigsten Gebieten, bei denen Unternehmen auf externe IT-Security-Dienstleister setzen. Nur 20 Prozent der Firmen nehmen ihre IT-Security selbst in die Hand.

Künftige Bedrohungen

Unternehmen fürchten vor allem Cyber-Angriffe wie Ransomware und das Risiko durch die Nachlässigkeit interner Mitarbeiter.



Management Summary

Die Key Findings im Überblick

Zusätzliche Investitionen im Bereich IT-Security



80%

der Befragten fordern mehr Geld.

26%

(Eher) keine Investitionen geplant

29%

Nennenswerte Investitionen geplant



Partnerwahl

Die Hälfte der Unternehmen achtet bei der Wahl des IT-Security-Dienstleisters auf technisches Know-how und Prozesswissen.

Verantwortlicher

Vor allem große Unternehmen verfügen über eine Person oder Abteilung, die ausschließlich und alleine für Informationssicherheit zuständig ist.



73%

Großunternehmen

58%

Durchschnitt

51%

Kleine Unternehmen



Nur wenige CISOs

40 Prozent der Firmen haben die Position des Chief Security Information Managers (CISO) etabliert. In großen Unternehmen sind es immerhin 56 Prozent.