

Vier Cyberrisiken, die Sie kennen sollten



RISIKO 1 Passwortdiebstahl

1

Was bedeutet das? Hacker nutzen gestohlene Zugangsdaten, um ins Unternehmensnetz oder an Admin-Rechte zu gelangen oder in Mitarbeiterkonten einzudringen.



80%
der Datendiebstähle erfolgen über gestohlene und schwache Passwörter.¹

2022 waren die durchschnittlichen Kosten für Datendiebstähle so hoch wie nie:

4,45 Mio. USD²



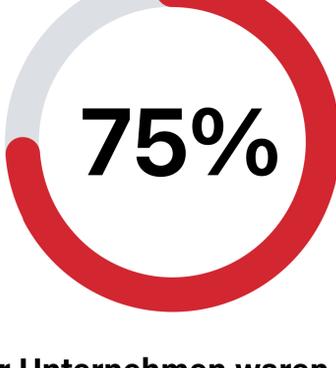
RISIKO 2 Malware

2

Was bedeutet das? Bösartige Software, die sich stillschweigend auf einem Gerät einnistet und Hackern Zugriff auf Daten oder Konten gibt.



30%
der KMUs sind Opfer von Malware-Angriffen.¹



75%
der Unternehmen waren Ziel einer Verbreitung von Malware von Mitarbeiter zu Mitarbeiter.³

RISIKO 3 Phishing

3

Was bedeutet das? Der Versuch, an Zugangsdaten oder andere wertvolle Informationen zu gelangen, indem Nutzer zum Aufrufen betrügerischer Websites oder Apps gebracht werden.

Über 255 Millionen

Phishing-Angriffe gab es 2022.¹



Ein Unternehmen mit 10.000 Mitarbeitern verliert im Schnitt

65.343 Stunden

jährlich aufgrund von Phishing.³

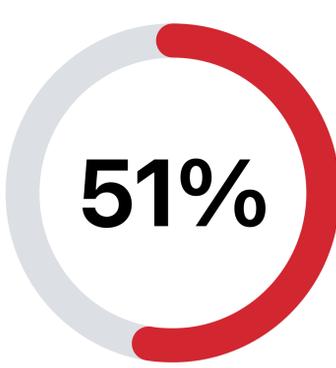
RISIKO 4 Ransomware

4

Was bedeutet das? Eine Malware, mit der Daten gestohlen und verschlüsselt werden. Für die Herausgabe wird vom Opfer ein Lösegeld gefordert.



11%
der KMUs sind Opfer von Ransomware-Angriffen.



51%
der von einem Ransomware-Angriff betroffenen KMU zahlen Lösegeld.³



Beugen Sie den wichtigsten Cyberbedrohungen vor.
LastPass unterstützt Sie dabei.

[Mehr erfahren](#)

Quellen:

(1) <https://www.verizon.com/business/en-gb/resources/2022-data-breachinvestigations-report-dbir.pdf>

(2) <https://www.swktech.com/costs-of-a-cyber-attack-for-smbs/>

(3) <https://www.comparitech.com/antivirus/malware-statistics-facts/>