

De top 4 cyberrisico's die u moet kennen



RISICO 1 Aanvallen met wachtwoorden

1

Het gevaar: Hackers gebruiken gestolen aanmeldingsgegevens om toegang te krijgen tot een bedrijfsnetwerk, beheerdersrechten te krijgen of accounts van medewerkers over te nemen.



80% van de gegevenslekken door hacking is te herleiden tot zwakke, hergebruikte en gestolen wachtwoorden.¹

In 2022 stegen de gemiddelde kosten van een gegevenslek tot een nieuw record van **4,45 miljoen dollar**



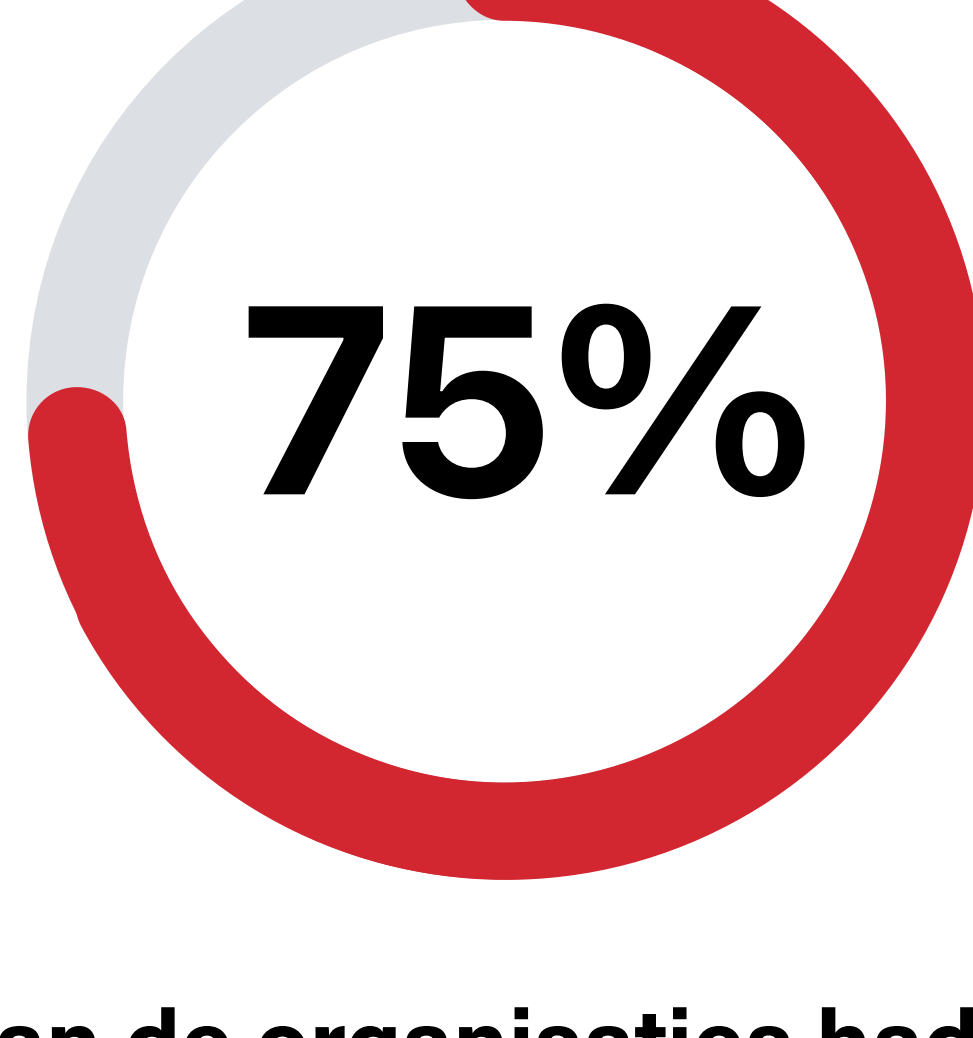
RISICO 2 Malware

2

Het gevaar: Illegale software wordt ongemerkt geïnstalleerd op een apparaat om hackers toegang te geven tot gegevens of accounts.



van de MKB-ers had te maken met aanvallen met malware¹



van de organisaties had te maken met malware die onderling door medewerkers werd verspreid.³

RISICO 3 Phishing

3

Het gevaar: Internetcriminelen lokken gebruikers naar nep-websites en apps om aanmeldingsgegevens of andere waardevolle informatie te stelen.

In 2022 werden **ruim 255 miljoen** phishing-aanvallen gemeld.¹



Een bedrijf met 10.000 medewerkers verliest gemiddeld **65.343 uur** per jaar door phishing-aanvallen.³

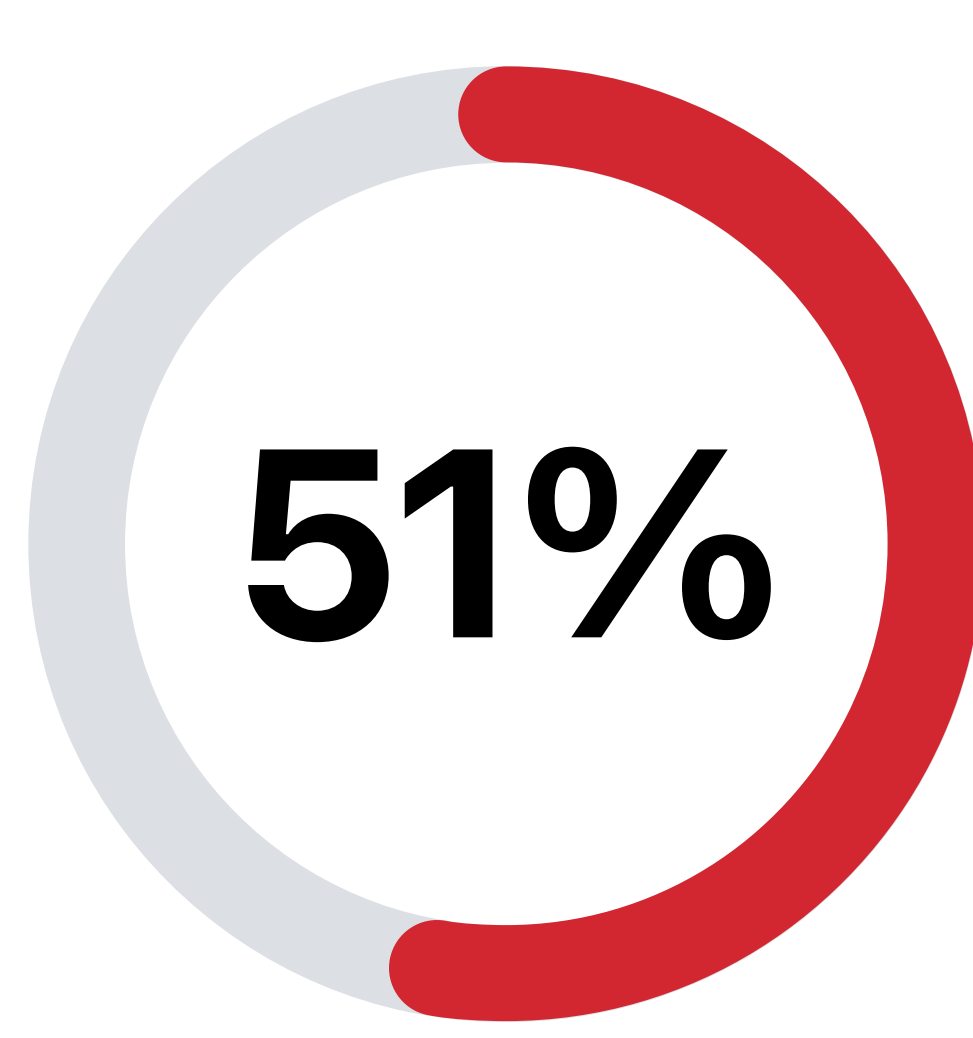
RISICO 4 Ransomware

4

Het gevaar: Met gijzelsoftware stelen en versleutelen hackers gegevens van hun doelwit, waarna ze losgeld eisen om systemen en gegevens weer toegankelijk te maken.



van het MKB heeft te maken met ransomware-aanvallen.



van de kleine bedrijven die worden getroffen door ransomware, betalen het losgeld.³



LastPass kan helpen om de meest voorkomende soorten cyberaanvallen te voorkomen.

[Meer informatie](#)

Bronnen:

(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/>