LastPass

De top 4 cyberrisico's
die u moet kennen

RISICO 1 Aanvallen met wachtwoorden

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

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 malware[1]

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

RISICO 3 Phishing

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

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 gehad 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/