Het mkb is kwetsbaar voor phishing

Het probleem / aanleiding

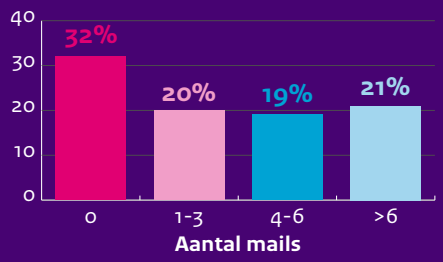
- De afgelopen jaren is er een sterke toename van cybercriminaliteit.
- Phishing is één van de meest voorkomende vormen en is vaak het begin van andere cyberaanvallen (zoals malware en ransomware).
- Ruim een kwart van de medewerkers binnen het mkb heeft afgelopen jaar een phishingmail ontvangen.
- MKB heeft niet altijd het besef van de urgentie en de juiste kennis en vaardigheden in huis om hun bedrijf weerbaar(der) te maken tegen cybercriminaliteit.
- Veel bedrijven zijn onderdeel van grotere ketens van kritische processen. Eén kwetsbaar bedrijf kan grote gevolgen hebben voor vele andere organisaties.

De onderzoeksopzet en de resultaten

Aantal deelnemers
33.000+ medewerkers
bij **650+** bedrijven.

Ruim **1 op de 5** medewerkers (22%) werkzaam binnen het mkb klikte op een onbetrouwbare link in een generieke phishingmail.

Medewerkers die aangaven de afgelopen **12 maanden** géén phishingmail te hebben ontvangen, klikten gemiddeld vaker op de link dan medewerkers die aangaven één of meerdere phishingmails te hebben ontvangen.



Medewerkers die een maand eerder een phishingmail hebben ontvangen, klikten minder vaak op een tweede phishingmail dan medewerkers die nog niet een eerste phishingmail hadden ontvangen (9,9% t.o.v. 19,8%). Er was geen effect op (middel)lange termijn.

Dit kun je doen om je digitale veiligheid te verbeteren

Train medewerkers en collega's om phishing te herkennen

Zet een **bewustwordings-campagne** op

Zorg voor veilige **e-mail instellingen** en beveiligingsstandaarden

Maak duidelijke afspraken met je **IT-leverancier**

Bekijk digitaltrustcenter.nl voor meer tips en tools om aan de slag te gaan met jouw digitale veiligheid.