**Meer dan een kwart van de Belgische organisaties
in de afgelopen twee jaar in de problemen door phishing-e-mails**

Brussel, 13 maart 2019 – **Meer dan een kwart (28 procent) van de Belgische organisaties is in de afgelopen twee jaar in de problemen geraakt door phishing-aanvallen, terwijl 38 procent zei dat ze gevallen hebben geïdentificeerd van medewerkers die op ongevraagde e-mails reageren of op links in die berichten klikken. Zo blijkt uit onderzoek voor Sophos, leider op het gebied van netwerk- en endpointbeveiliging.**

Sophos' onderzoek onder 906 IT-directors in West-Europa, uitgevoerd door [Sapio Research](https://sapioresearch.com/), onthulde dat grotere bedrijven het meest waarschijnlijk zijn aangetast door phishing-aanvallen, hoewel ze ook de meeste kans hebben om bedreigingbewustmakingscursussen te volgen op het gebied van phishing en cybersecurity.

Wat phishing betreft, presteerden organisaties in België aanzienlijk beter (28%) dan hun buren in Frankrijk en Nederland, waar respectievelijk 49% en 44% van de respondenten toegaf het slachtoffer te zijn geweest van phishing in de onderzochte periode.

Erik Farine, Regional Director Benelux bij Sophos, verklaart: “Criminelen zijn bedreven in het gebruik van social engineering om menselijke zwakheden uit te buiten, terwijl goed opgeleide werknemers een uitstekend afschrikmiddel zijn, zelfs de beste eindgebruiker kan al eens verstek geven. Organisaties moeten ervoor zorgen dat werknemers waakzaam blijven voor de bedreigingen van phishing-aanvallen; Permanente training moet daar onderdeel van zijn om medewerkers te controleren en ervoor te zorgen dat ze correct reageren en de richtlijnen blijven volgen die ze hebben gekregen.”

“Phishing beïnvloedt iedereen en is een van de meest gebruikte toegangsroutes voor cybercriminelen. Naarmate organisaties groeien, neemt hun risico om slachtoffer te worden toe. Ze worden lucratiever en bieden hackers meer potentiële toegangspunten. Gezien de frequentie van deze aanvallen zullen organisaties zonder basisinfrastructuur om partijen met schadelijke e-mails te identificeren, nog grote problemen tegenkomen.”

“Organisaties moeten schadelijke links, bijlagen en bedriegers blokkeren voordat ze de inbox van eindgebruikers bereiken. Ze moeten ook de nieuwste cyberbeveiligingstools gebruiken om ransomware en andere geavanceerde bedreigingen op apparaten te stoppen, zelfs als een gebruiker op een schadelijke link klikt of een geïnfecteerde bijlage opent.”

● In heel West-Europa vertelde 54 procent van de IT-directors bij bedrijven met tussen 500 en 1.000 mensen aan de onderzoekers van Sophos dat hun organisaties de afgelopen twee jaar het slachtoffer waren geworden van phishingaanvallen
● Dit in vergelijking met 39 procent van 250 tot 499 persoonsbedrijven en slechts 14 procent van bedrijven met minder dan 250 werknemers
● 50 procent van de bedrijven met minder dan 250 mensen bood training aan om werknemers te helpen aanvallen te herkennen, vergeleken met 78 procent van degenen met tussen 500 en 1.000 mensen
● 52 procent van de Belgische bedrijven voert al regelmatig bewustmakingscursussen voor cyberdreigingen uit, terwijl 38 procent van plan is dit in de toekomst aan te bieden

**Nota voor redacteuren**

**Methodologie**

In augustus en september 2018 interviewde marktonderzoeksbureau Sapio Research 906 IT-directeuren en managers bij bedrijven met maximaal 1.000 werknemers over hun ervaringen met cybercriminaliteit en benaderingen voor het beheren van cyberbeveiliging. De interviews werden online afgenomen met mensen in het VK, Ierland, Frankrijk, België en Nederland.

*Read the latest security news and views on our award-winning* [*Naked Security News*](http://nakedsecurity.sophos.com/) *and read more about Sophos on our* [*News blog*](https://blogs.sophos.com)*.*

[*Lees het laatste beveiligingsnieuws en nieuws over ons bekroonde Naked Security News*](https://nakedsecurity.sophos.com/) *en lees meer over Sophos op onze [Nieuwsblog](https://news.sophos.com/nl-nl/).*

*Lees* [*The Top Ten Phishing Emails That Hook Us*](https://www.sophos.com/en-us/medialibrary/pdfs/other/sophos-the-top-ten-phishing-emails-that-hook-us-arna.pdf)*.*

*Connecteer met Sophos via* [*Twitter*](http://twitter.com/sophos)*,* [*LinkedIn*](http://soph.so/Cfv36)*,* [*Facebook*](http://soph.so/CfvaA)*,* [*Spiceworks*](http://soph.so/Cgbwa%20)*,* [*YouTube*](http://www.youtube.com/user/sophoslabs)*,* [*Google+*](https://plus.google.com/%2Bsophos)

**Voor meer informatie, contacteer:**

Sandra Van Hauwaert, Square Egg Communications, sandra@square-egg.be, GSM 0497251816.

**Over Sophos**

Meer dan 100 miljoen gebruikers in 150 landen rekenen op Sophos voor de beste bescherming tegen complexe bedreigingen en dataverlies. Sophos levert security- en databeschermingsoplossingen die eenvoudig in te zetten, te beheren en te gebruiken zijn. Zo biedt Sophos prijswinnende oplossingen aan voor endpoint security, web security, e-mail security, network security, mobile security en encryptie. Deze worden ondersteund door Sophos Labs, een wereldwijd netwerk van threat intelligence centra. Het hoofdkwartier van Sophos bevindt zich in Oxford (UK) en in Boston (VS). Meer informatie over Sophos op: [www.sophos.com](http://www.sophos.com).