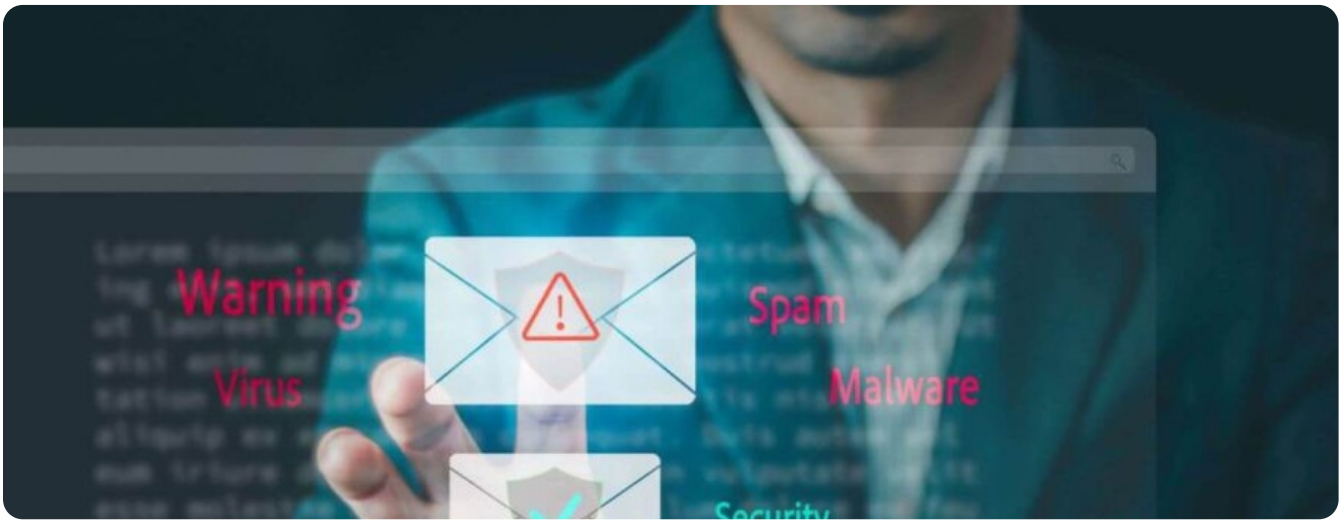
Blog • Security

Jij bent de zwakste schakel in cybercrimepreventie

Interstellar Team
18.03.2025 • 6 minuten leestijd



Jij bent de zwakste schakel. Dat is niet leuk om te horen, maar als het gaat om cybercriminaliteit, dan veroorzaakt de menselijke factor nog altijd de meeste problemen. Daarom is het zaak om medewerkers binnen alle lagen van de organisatie bewust te maken hoe we met elkaar die cyberaanvallen grotendeels kunnen voorkomen. Preventieve security-awareness trainingen zijn hierbij de sleutel.

Je kunt je organisatie nog zo goed beveiligd hebben tegen cybercriminaliteit, zonder opgesteld beleid en gedragsregels in combinatie met leermomenten van bewustwording

kosten die securitymaatregelen (firewalls, antivirusprogramma's, netwerksegmentaties) alleen maar een hoop geld. Mensen leren juist achterdochtig en voorzichtig te worden zodra ze bewust zijn dat ze een keer fout geklikt hebben. En dat is precies de gedragsverandering die nodig is.

Security-awareness trainingen zijn dé oplossing om de benodigde gedragsverandering te bewerkstelligen. Met awareness trainingen wordt iedereen preventief bewust van digitale gevaren, waarna aantoonbaar het percentage aan fout geklikte situaties daalt.

De volgende veranderingen kun je nu al in je organisatie doorvoeren om de cybersecurity via je medewerkers te verbeteren:

Open geen bijlagen en links in onbekende e-mails
Cybercriminelen doen zich geregeld voor als een vertrouwd contact. Ze proberen je te verleiden om gegevens achter te laten via een link of om malware naar je apparaat te downloaden. Deze links en bijlagen worden veelal via de e-mail verstuurd. Er worden vaak psychologische trucs uitgehaald op het gebied van geloofwaardigheid, angst en tijdsdruk om je in deze zogeheten phishing-(aan)val te lokken. Misschien ken je die zogenaamde mails van je bank nog wel: heb jij nooit de druk gevoeld om actie te ondernemen na het lezen van een dergelijk bericht?

Maak jij het geld direct nog even over?
Volgens het Global Risk Report 2021 van World Economic Forum heeft ongeveer 75% van de organisaties in 2020 te maken gehad met een vorm van phishing. Whaling, een vorm van spear phishing, zit zelfs in de lift: een kwaadwillende doet zich voor als de CEO of CFO van je organisatie en vraagt een medewerker van de financiële afdeling om geld over te maken naar een rekening van de kwaadwillende. Door de toegenomen populariteit van (zakelijke) sociale netwerken als LinkedIn weten hackers steeds beter wie ze hiervoor moeten benaderen.

Inzage krijgen in de factuurstromen is vrij eenvoudig als een crimineel eenmaal inloggegevens van iemand heeft ontvangen. Lukt het om een eigen account te krijgen binnen een organisatie, dan kan de fraudeur proberen om daarna de Administrator rechten te krijgen. Met die rechten kan de fraudeur alles.

Hoe kun je phishing voorkomen?
In één woord: preventie. Maak medewerkers continu bewust van de risico's van phishing en voer praktijktesten uit om dit soort aanvallen te herkennen. Leer ze de volgende punten standaard te controleren:

1. De naam van de afzender en het e-mailadres. Is de persoon daadwerkelijk de persoon die hij/zij zegt dat hij/zij is? Benader bij twijfel altijd de persoon zelf;
2. Hoe word je aangesproken in de aanhef? Hoe onpersoonlijker, hoe groter de kans dat het gaat om een phishing-bericht;
3. De toegevoegde link voordat hierop wordt geklikt. Komt het webadres overeen met die van het bedrijf in kwestie of is deze fout verkort?;
4. Worden je persoonlijke gegevens opgevraagd om deze enkel te verifiëren? Dan moet er direct een rode vlag gaan wapperen. Bedrijven zullen NOOIT vragen om persoonlijke gegevens te verifiëren. Twijfel je toch? Neem dan eerst contact op met het bedrijf om na te gaan hoe het zit.

Gebruik geen USB-sticks

Je staat op een beurs en je hebt haast. Er moet een offerte van de ene laptop op een andere gezet worden en je hebt toevallig een USB-stick ergens gevonden. Hoe verleidelijk het ook is, zie toch maar af van het gebruik van deze stick. Beter nog: gooi hem voor ieders welzijn weg. Voor je het weet heb je malware op je laptop staan en worden er bestanden versleuteld. Hier kom je pas achter op het moment dat het te laat is en je dringend wordt verzocht om te betalen als je jouw bestanden nog terug wil hebben. Zonder goede back-up lijkt betalen haast de enige optie, aangezien je anders volledig opnieuw moet beginnen.

Verander met enige regelmaat je wachtwoord

Deze verandering wordt waarschijnlijk niet met open armen ontvangen, maar om de veiligheid van je organisatie te versterken, raden wij sterk aan om medewerkers minimaal eens in de 3 maanden hun wachtwoord te laten wijzigen. Om ervoor te zorgen dat medewerkers daadwerkelijk hun wachtwoord wijzigen, kun je dit proces automatiseren. Iedereen krijgt op een bepaald moment de mededeling dat het wachtwoord aangepast dient te worden. Stel direct in waar een wachtwoord aan moet voldoen. Een afwisseling van letters, cijfers en tekens maakt het voor een hacker lastiger om het wachtwoord te kraken.

Vermijd bezoekjes aan onveilige sites

Staat er geen slotje voor de URL? Dan heb je te maken met een onbeveiligde site zonder SSL-certificaat. Zonder dit certificaat wordt het dataverkeer tussen een browser en webserver niet versleuteld, waardoor het voor cybercriminelen kinderspel wordt om data als persoonsgegevens of creditcardinformatie te onderscheppen. Daarom is het verstandig om in je veiligheidsbeleid op te nemen dat medewerkers dit soort sites niet mogen bezoeken met hun zakelijke device.

Iedereen maakt fouten

Het kan altijd voorkomen dat een medewerker toch per ongeluk op een link klikt of een bestand opent dat dicht had moeten blijven zitten. Zorg er daarom voor dat iedereen weet bij wie hij/zij terecht kan om een dergelijke situatie aan te kaarten. Alleen dan kan er direct actie ondernomen worden en kan de schade beperkt blijven.

Wil je jouw organisatie slim beschermen tegen cybercriminaliteit door middel van preventieve security-awareness trainingen? Neem via het formulier contact op voor meer informatie.

DEEL ARTIKEL

DO YOU WANT TO TALK SECURITY?

Interstellar Team

KOM IN CONTACT