BDO RISK ADVISORY SERVICES

# CYBERSECURITY AWARENESS EN PREVENTIE VOOR LOKALE OVERHEDEN

# DE BEHOEFTE AAN CYBERBEVEILIGINGSMAATREGELEN

De dienstverlening van de lokale overheden is in continue beweging, dit als antwoord op een veranderende vraag en verwachting van de burgers. Steden en gemeenten willen de dienstverlening meer online brengen, met een ruime informatievoorziening die minder gebonden is aan kantoortijden. Daarnaast begeven steden en gemeenten zich ook vaker in samenwerkingsverbanden en netwerken van organisaties waarmee informatie wordt uitgewisseld. Samen met deze duidelijke tendens van toenemende digitalisering en connectiviteit, zien we helaas ook meer cybercriminaliteit.

Vertrouwen is belangrijk in ons dagdagelijks leven: de burger vertrouwt erop dat organisaties en overheden zorgvuldig met zijn/haar gegevens omgaan, op haar beurt vertrouwt de lokale overheid op partners om haar doelstellingen waar te maken. Door de toenemende connectiviteit is vertrouwen de optelsom van steeds meer schakels in de keten. Sommige van de schakels kennen we beter dan andere, soms vervallen we daardoor in vertrouwde gewoontes en schatten we potentiële risico's onvoldoende in. Zoals altijd is 'vertrouwen' goed, maar niet in elke context. Bij 82% van alle datalekken en cyberincidenten ligt een menselijke fout aan de oorsprong, een medewerker die vanuit zijn vertrouwen op de verkeerde link klikt, of de verkeerde bijlage opent. Een kleine handeling die een enorme impact kan hebben in deze intergeconnecteerde wereld. Ook uit audits door Audit Vlaanderen rond informatieveiligheid evenals andere publicaties rond cyberveiligheid is gebleken dat gebruikers een heel groot aandeel hebben in de cyberveiligheid van een organisatie. Vaak zijn zij de zwakste schakel in de beveiliging van onder andere openbare besturen.

Goed opgeleide medewerkers spelen een belangrijke rol in het voorkomen en snel detecteren van een cyberaanval of inbreuk op informatieveiligheid. Het is dan ook van belang om te  investeren in bewustmaking en training rond de basisprincipes van cyber- en informatieveiligheid.

Hoewel de technologie phishing voortdurend bestrijdt, beschermt zij alleen niet afdoende tegen dergelijke aanvallen. Voortdurende training van je medewerkers is daarom cruciaal, zodat zij social engineering-aanvallen kunnen herkennen en er adequaat op kunnen reageren.

Het is belangrijk dat de training herhaaldelijk wordt aangeboden, zodat je medewerkers de juiste reflex aannemen. In deze context biedt BDO een geautomatiseerd AI-gestuurd Phishing-awareness-as-a-Service programma aan dat wordt aangestuurd door het gedrag van de beoogde werknemers en hun reactievermogen op phishing. Door trainingen op maat van de medewerker te geven en hen voortdurend te sensibiliseren, zorgen we voor een aanzienlijke verbetering van je cyberveiligheid.

# ONZE CYBER AWARENESS DIENSTEN AFGESTEMD OP JOUW BEHOEFTEN

Cybersecurity is een complex onderwerp, waarbij veel factoren en maatregelen een rol spelen.
Sterker nog, dit is waarschijnlijk één van de redenen waarom zoveel organisaties er niet in slagen om hun personeel afdoende op te leiden binnen dit domein.

Perfecte beveiliging bestaat helaas niet, daarom is het belangrijk om onze medewerkers bewust te maken van de risico's, hen voor te bereiden op een mogelijke aanval en een gepaste reactie strategie aan te leren.
Daarbij helpen wij je graag.

## ONZE AANPAK

### 1 Bepalen van de scope

Samen met jou configureren we de verschillende parameters en instellingen van de phishing AI. Daarna wordt het platform door ons beheerd om de werkdruk op je interne IT-afdeling te verminderen. Het grote verschil in het gebruik van AI om je (cyber) zelfverdediging te verhogen, vergeleken met een traditionele eenmalige phishing campagne, is dat een breed scala aan verschillende e-mails wordt verzonden naar de werknemers op basis van hun bewustzijn profiel en hun resultaten op eerdere simulaties. Elke medewerker doorloopt een individueel traject. Bovendien worden de e-mails verspreid over de tijd om het risico te beperken dat werknemers van een lopende phishing simulatie op de hoogte worden gebracht door een collega.

### 2 Phishing simulaties

Behalve voor de whitelisting van ons phishing platform, vereist een simulatie geen tussenkomst van je interne IT-afdeling. De AI verstuurt phishing e-mails naar de medewerkers op basis van hun bewustzijnsniveau (en op het bereik). Naast de handmatige import van een "doellijst" van werknemers, kan deze ook met behulp van, een integratie met de Active Directory van het bedrijf automatisch geimporteerd en up-to-date gehouden worden. Op deze manier kan ook het gebruik van je licenties geoptimaliseerd worden.

### 3 Analyse en reporting

Er wordt gewerkt met niet-agressieve phishing simulaties, wat betekent dat er geen gegevens geregistreerd worden (wachtwoord en gebruikersnaam) wanneer deze zouden worden ingevoerd. Onze simulaties zijn volledig gericht op het monitoren van gedrag en de evoluties ervan.
Om de anonimiteit van de werknemers te beschermen, wordt een geaggregeerde rapportage gebruikt.
Er is daar naast een diepgaande rapportering beschikbaar op het niveau van bedrijf, afdeling, gebruiker, locatie, tijd en apparaattype. Per gebruiker is informatie raadpleegbaar over hun phishing bewustzijnsniveau, progressie, de ontvangen ontvangen, geopend, phished ratio, gegevensinvoer, enz. Het gebruik van gedetailleerde rapportage stelt je in staat om in te grijpen en bij te sturen waar nodig.

### 4 Security awareness creatie

Naast de simulaties krijgen de werknemers trainingen aangeboden die hen helpen om dergelijke aanvallen beter kunnen herkennen en ze aan IT kunnen melden. Afhankelijk van het door de AI bepaalde bewustzijnsniveau van de gebruiker, krijgt de gebruiker aanvullende trainingsinitiatieven gericht op zijn bewustzijnsniveau. De aangeboden trainingen zullen kort zijn, in de taal van de werknemer en to the point. De nadruk ligt op het automatiseren van de juiste reactie wanneer ze geconfronteerd worden met een phishing-poging.

### 5 Continue herhaling van de cyclus

Bij BDO geloven we dat het creëren van veiligheidsbewustzijn een continu proces is, niet een eenmalige gebeurtenis. Door de implementatie van geautomatiseerde AI-gebaseerde phishing-simulaties, aangepast aan de steeds veranderende cyberwereld, blijven we het beveiligingsbewustzijn continue meten en aanpassen. Op deze manier, blijven medewerkers zich bewust van de bedreigingen en zijn ze minder geneigd om te reageren op een echte aanval van buitenaf.

# WAT KAN JE VAN ONS VERWACHTEN?

**Vinger aan de pols** – als onafhankelijke experts evalueren we je bestaande IT omgeving, rekening houdende met de specifieke context van je organisatie.

**Sterke en zwakke punten** – we brengen zowel de sterke als zwakke punten in kaart en maken daarbij gebruik van eenvoudige, niet-technische taal. Zo heb je een goed beeld van de bestaande en/of potentiële risico's.

**Het belangrijkste eerst** –onze aanpak is geleidelijk, eerst zorgen we ervoor dat de grootste kwetsbaarheden in de bestaande beveiliging aangepakt worden. Pas als er een solide basis is gelegd, gaan we een stap verder met de definitie van aanvullende controles.

**Klankbord** – het is niet eenvoudig voor niet-technische mensen om inzicht te krijgen in daadwerkelijke cyberrisico's. In onze rol als onafhankelijke experts zijn we een klankbord voor het management en zorgen we ervoor dat je door de bomen het bos blijft zien.

**Cyberdarwinisme** – terwijl de evoluties vroeger steeds traag waren, is het tempo in de wereld van vandaag razend. Het uitgangspunt blijft echter hetzelfde: alleen wie zich kan aanpassen, zal overleven. We begeleiden je graag bij het maken van de juiste keuzes in je cyberevolutie.


## Interesse?

Neem contact op met:

**STEVEN CAUWENBERGHS**
Partner Risk Advisory Services

**E-mail:** steven.cauwenberghs@bdo.be
**Tel.:** +32 497 05 12 23

**FRANCIS OOSTVOGELS**
Senior Manager Risk Advisory Services

**E-mail:** francis.oostvogels@bdo.be
**Tel.:** +32 474 92 08 00

**NICK HUYSMANS**
Senior Manager Risk Advisory Services

**E-mail:** nick.huysmans@bdo.be
**Tel.:** +32 486 31 90 45

▶ Follow us
▶ www.bdo.be