CYBER SECURITY AWARENESS

Training voor medewerkers om cyber dreigingen te herkennen

OBI Hét ICT Team

ZORGT DAT ICT WERKT. ALTIJD. OVERAL.

CYBER SECURITY AWARENESS

Voor organisaties die hun medewerkers willen trainen om cyber dreigingen te herkennen en te voorkomen.

INHOUD

OBI Automatisering | www.obi.nl | support@obi.nl

Tel. +31 (0)88 9008100 | De Hooge Akker 10b, 5661 NG Geldrop

KVK nr. 17130973 | BTW nr. NL 8093.61.048.B01 | IBAN NL73ABNA0588512311

NIEMAND ONTSNAPT AAN CYBERAANVALLEN

68 PROCENT BEDRIJVEN IN NEDERLAND HEEFT TE MAKEN MET CYBERAANVALLEN

In 2020 jaar was het percentage bedrijven dat te maken kreeg met een cyber event flink meer dan een jaar eerder (61 procent wereldwijd en 68 procent in Nederland). Ook vallen dit jaar de kosten van een incident of een lek fors hoger uit. Het Amerikaanse bedrijf Hiscox* onderzocht bijna tweeduizend bedrijven die te maken hebben gehad met cyberincidenten en lekken.

> ***"Productie VDL dagenlang opgeschort na cyberaanval"***
>
> *- VDL groep*
>
> ***"Gemiddeld 74.000 dollar afpersing per getroffen organisatie in Nederland"***
>
> *- Hiscox*

In 2020 lagen in Nederland per getroffen organisatie de gemiddelde kosten op 74.000 dollar. Een forse stijging ten opzichte van 2019. Alle gerapporteerde cyber events wereldwijd samen kostten totaal 1,8 miljard dollar. Aanzienlijk meer dan in 2019, toen het aantal events hoger lag, maar de kosten uitkwamen op 1,2 miljard dollar. Kort gezegd, hoe groter het bedrijf, hoe hoger het bedrag dat is betaald voor een cyber event. Het grootste bedrag dat een Nederlands bedrijf, dat werd ondervraagd, betaalde voor een incident of lek was 600.000 dollar.

* Bron: https://www.hiscox.co.uk/sites/uk/files/documents/2020-06/Hiscox_Cyber_Readiness_Report_2020_UK.PDF

MEER DAN 99 PROCENT CYBERAANVALLEN VEREIST MENSELIJKE INTERACTIE

Cybercriminelen richten zich nadrukkelijk op personen, omdat het relatief eenvoudig voor hen is om frauduleuze e-mails te versturen, referenties te stelen en kwaadaardige bijlagen naar cloudapplicaties te uploaden. Het is gemakkelijker en winstgevender dan dure, tijdrovende exploitaties van veiligheidsgaten te creëren, die ook nog een grote kans op mislukking hebben. Meer dan 99 procent van de cyberaanvallen heeft menselijk handelen nodig om te werken.* Hierdoor worden individuele gebruikers de laatste verdedigingslinie van een organisatie. Om de risico's aanzienlijk te verminderen, hebben organisaties een mensgerichte cyber security-benadering nodig. Deze moet onder meer effectieve bewustwordingstrainingen en een gelaagde bescherming omvatten die aangeeft wie de meest kwetsbare gebruikers binnen een organisatie zijn.

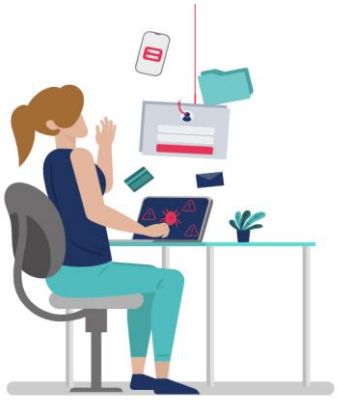
*Bron: https://www.infosecuritymagazine.nl/nieuws/meer-dan-99-procent-van-cyberaanvallen-vereist-menselijk-handelen

VOORKOM EEN CYBERAANVAL MET CYBER SECURITY AWARENESS

BEGIN BIJ DE ZWAKSTE SCHAKEL: DE EINDGEBRUIKER

Jarenlang gingen haast alle corporate inspanningen voor een goede cyber securitystrategie naar de technische middelen. Firewalls, antivirusprogramma's, antispam, etc. Deze technische maatregelen bereikten een dusdanig hoge efficiëntie dat cybercriminelen hun heil elders moesten gaan zoeken: bij de menselijke factor.

Vandaag de dag heeft het grootste gedeelte van alle cyberaanvallen een menselijke interactie nodig. Een medewerker klikt onbedoeld op een link in een nep e-mail (phishing), waarna ransomware het bedrijf overneemt, waarna een hacker losgeld zal eisen om de gegijzelde (versleutelde) bestanden weer vrij te geven. Het gebeurt vaker dan je zou vermoeden. Daarom is er het besef nodig dat een investering in een 'menselijke firewall' even noodzakelijk is als investeren in technische infrastructuur.



"Meer dan 99 procent van de waargenomen aanvallen vereiste menselijke interactie om te werken"

"Microsoft-gerelateerde aanvallen bleven het populairst"

- Proofpoint

CREËER EEN MENSELIJKE FIREWALL

OBI helpt organisaties een eigen Menselijke Firewall te bouwen, maar wat betekent dat, en waarom is het belangrijk? De traditionele cyber security awareness training met een Powerpoint presentatie voldoet niet langer aan de vereisten om de kwetsbare groep medewerkers weerbaar te maken tegen een cyberaanval. Er ontbreken namelijk enkele basisingrediënten: Het regelmatig 'updaten' van het kennisniveau, het controleren en 'monitoren' van eventuele zwakke schakels of lekken in de beveiliging.

OBI heeft in samenwerking met een softwarebedrijf een programma opgezet waarbij er **continue wordt gemeten waar de zwakste schakel zit in de menselijke firewall door het simuleren van cyberaanvallen met nep e-mails, waarna er direct een maatwerk online training wordt geboden aan de betreffende eindgebruiker.**

ALLEEN DAAR TRAINEN WAAR NODIG

Medewerkers zijn al druk genoeg en trainen is goed, maar liever niet ten koste van de productiviteit van de organisatie. Daarom meet OBI eerst wíe er behoefte heeft aan cyber security trainingen door periodiek een phishing aanval te simuleren.
De medewerkers die onverhoopt op een link klikken tijdens een gesimuleerde phishing aanval, krijgen vervolgens extra maatwerk online training aangeboden in de vorm van een korte instructie video die is afgestemd op het specifieke type aanval.
Indien nodig kunnen uw medewerkers extra worden getraind door middel van een workshop via Teams, of bij u op locatie door uw persoonlijke Security Officer van OBI.

HET CYBER SECURITY AWARENESS TOTAALCONCEPT VAN OBI

GEAUTOMATISEERDE AANVAL MET NEP E-MAIL (PHISHING) SIMULATIES

Cyber security awareness voor medewerkers door middel van een gesimuleerde aanval met nep e-mail (phishing) is een nieuwe oplossing gebaseerd op cloud software. Dit betekent dat OBI met behulp van een speciaal software programma nep e-mail simuleert en deze verstuurt naar de medewerkers, zonder de gevaren van echte hackers.
Door medewerkers in contact te laten komen met alle mogelijke phishingvarianten, in een veilige en gecontroleerde omgeving, herkennen zij de echte gevaren wanneer die zich voordoen.

De softwarematige phishing simulator is ingebouwd met een zelflerende module die rekening houdt met het gedrag van elk individu en daardoor zijn aanpak aanpast bij elke simulatie op basis van klikgedrag van de gebruiker. De simulator verstuurt periodiek volledig geautomatiseerde phishingsimulaties, die zowel qua timing als qua inhoud zijn afgestemd op de ontvanger.

PERSOONLIJKE ONLINE MICRO-LEARNING MET VIDEO NA NEP E-MAIL SIMULATIE

Vroeg of laat hapt iedere werknemer toe. Medewerkers die in de val lopen door op een link te klikken in een nep e-mail, krijgen maatwerk online trainingen aangeboden via de pagina die wordt geopend nadat ze op de link hebben geklikt. Door middel van korte krachtige filmpjes van enkele minuten met uitleg die passen bij het soort nep e-mail waarbij ze in de val zijn gelopen, krijgen medewerkers effciënt maatwerk training aangeboden. Zonder dat dit teveel ten koste gaan van de productiviteit.

> ***“Medewerkers zijn al druk genoeg en trainen is goed, maar liever niet ten koste van de productiviteit van de organisatie.”***

OUTLOOK ‘NEP E-MAIL TEST’ KNOP

Met de ‘Nep e-mail knop’ in Outlook kunnen ontvangers gemakkelijk potentiële nep e-mails (of nep e-mail simulaties) controleren door eenvoudig op een knop te drukken. Hierna zal een melding komen óf het een simulatie is of de kans dat het een echte nep e-mail is. Indien nodig kan de medewerker hierna zelf beoordelen of het een nep e-mail is, of hulp inschakelen door te bellen met de persoonlijke Security Officer van OBI.

BEWUSTWORDING WORKSHOPS

Tijdens de workshop Cybercrime en Cyber Security Awareness worden verschillende groepen medewerkers binnen een organisatie bewuster gemaakt van cybercrime. Een aanvulling op de online training waar nodig. Dit kan via Teams of bij opdrachtgever op locatie.

RAPPORTAGE

RAPPORTAGE EN EVALUATIE

Periodiek zal er door OBI uitgebreide rapportering plaatsvinden op basis van gedragsanalyses per afdeling, ontvanger, functie en locatie. Op deze manier kan met de opdrachtgever worden afgestemd of er extra begeleiding nodig is voor een kwetsbare groep gebruikers of afdeling binnen de organisatie.
Daarnaast kan de rapportage gebruikt worden om externe audits van de klant te ondersteunen als bewijslast.

ISO 27001

OBI helpt organisaties voldoen aan cyber securitycertificeringen, zoals de ISO 27001-normen. Anti-phishingtraining vormt een belangrijke manier om de staat en evolutie van cyber security awareness maatregelen te evalueren en te verbeteren (PDCA). Bovendien draagt de online training module bij tot het behalen van de ISO-norm rond permanente bijscholing over informatiebeveiliging en maakt deze het makkelijk om de stand van zaken te meten, bij te houden, te documenteren en te verbeteren binnen de organisatie.

AVG/GDPR PRIVACY

De AVG privacy wetgeving stelt dat organisaties technische en organisatorische maatregelen moeten nemen om de kans op datalekken te voorkomen. Dit Cyber Security Awareness programma valt onder de categorie organisatorische maatregelen.

WERKWIJZE EN PLANNING

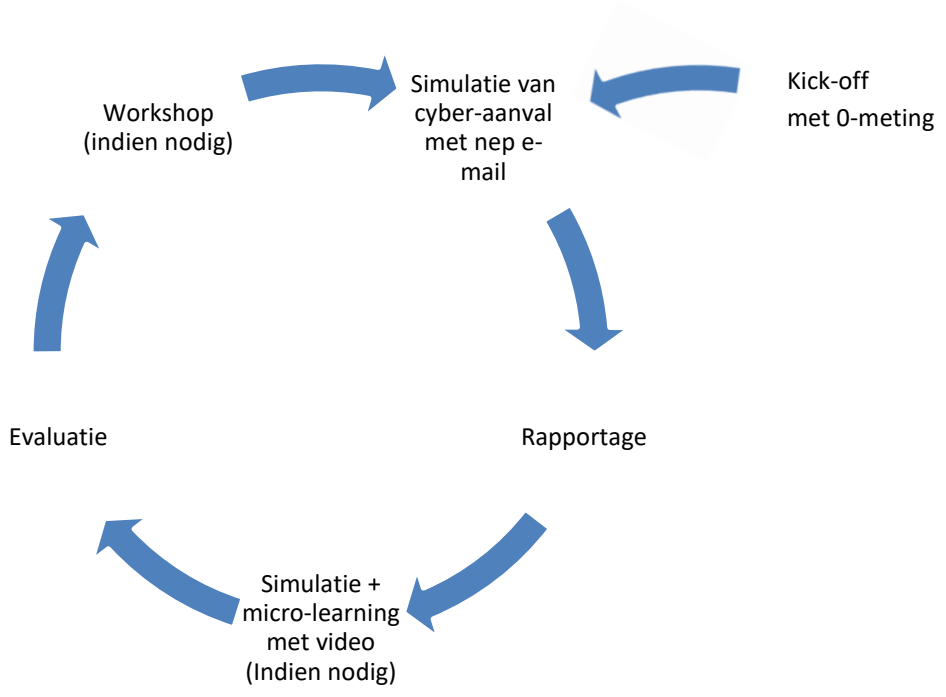
Kick-off en onboarding van organisatie

1. Kennismakingsgesprek (via Teams of op locatie)
2. Demonstratie (via Teams)
3. Offerte en akkoord
4. Setup simulatie software t.b.v. Cyber Security Awareness campagne
   (Inclusief inrichten nep e-mail sjablonen, gebruikers aanmaken, rapportage inrichten)
5. 0-meting met eerste simulatie van een nep e-mail aanval
   (Meting van kennisniveau eindgebruikers door eerste ronde van nep e-mail simulatie)
6. Evaluatie 0-meting met rapportage naar centrale contactpersoon (via Teams)
7. Kick-off Cyber Security Awareness campagne naar eindgebruikers
   (Introductie naar eindgebruikers per e-mail via centrale contactpersoon opdrachtgever)

Awareness programma voor gebruikers

Onderstaand programma kan eenmalig op afroep worden ingezet óf als continue proces worden ingericht

1. Periodieke simulatie met nep e-mail aanval
2. Rapportage naar centrale contactpersoon (per e-mail)
3. Periodieke evaluatie (via Teams) en bijsturen indien nodig
4. Nep e-mail aanval simulatie (geautomatiseerd), 12x per kwartaal
5. Rapportage uitkomsten van simulatie, 1x per maand
6. Rapportage evalueren en bespreken (via Teams), 1x per kwartaal
7. Workshop “Cyber Security en nep e-mail” (via Teams), 1x per kwartaal (vaker mogelijk op afroep)
8. Online leerplatform met korte instructie video’s



OVER OBI

OBI is gespecialiseerd in **volledige outsourcing van uw ICT**, ook wel 'Managed Services' genoemd. **Managed services** is het overhevelen van bedrijfsprocessen naar een externe partij, met als doel een hogere efficiëntie of lagere kosten. Met andere woorden, het volledige bedrijfsproces uitbesteden.

OBI is gespecialiseerd in het **bouwen**, **beheren** en **bewaken** van uw **ICT omgeving** bij u in-house in combinatie met de laatste cloud-ontwikkelingen op gebied van Microsoft 365 en Microsoft Azure.

Daarnaast ondersteunt OBI uw ICT met organisatorische maatregelen zoals het helpen **voldoen aan de AVG privacywetgeving** met behulp van avgonline.nl, het **Cyber Security Awareness programma** en het vormen van een IT-beleid.

Wij ondersteunen uw ICT met ticketsoftware en server bewaking- en monitoringsystemen om een optimale veiligheid van uw computernetwerk te garanderen. OBI bestaat 21 jaar en is **ISO27001 gecertificeerd,** wat een hoge continuïteit van dienstverlening garandeerd. OBI heeft een brede klantenkring opgebouwd van organisaties tussen de 20 en 200 computerwerkplekken en is sterk in **industrie- en kantoorautomatisering**.

Microsoft 365 Microsoft Azure

OBI Automatisering | www.obi.nl | support@obi.nl
Tel. +31 (0)88 9008100 | De Hooge Akker 10b, 5661 NG Geldrop
KVK nr. 17130973 | BTW nr. NL 8093.61.048.B01 | IBAN NL73ABNA0588512311

ISO 27001:2017 Gecertificeerd door Brand Compliance MGMT. SYS. RvA C 548

JAAR 20