Cybersecurity Awareness Training

Maak jouw medewerkers de sterkste schakel.

Portiva.

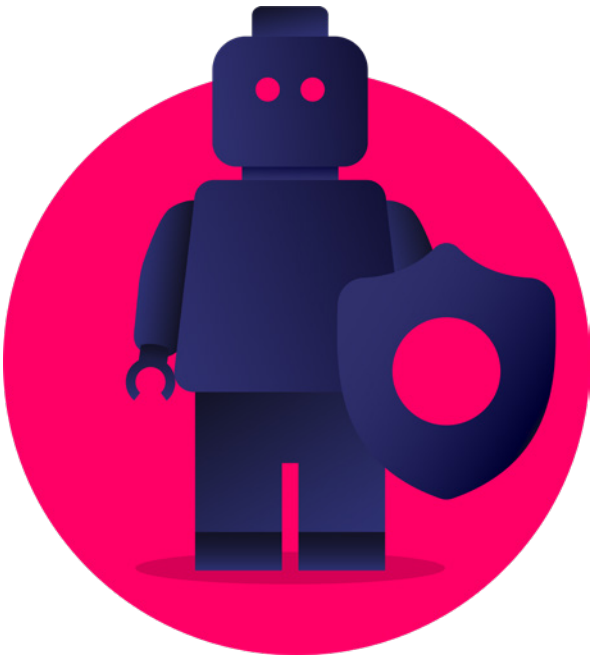
Het waarom, wat en hoe van user awareness training.

Om je IT-omgevingen te beschermen tegen hackers, ransomware en fraude zijn er enorm veel technische oplossingen beschikbaar. Bij Portiva helpen we dagelijks met veel plezier bedrijven met het implementeren daarvan. Maar tegelijkertijd: 98% van de cyberaanvallen maakt op een of andere manier gebruik van de onoplettendheid of het vertrouwen van medewerkers. Hoe verander je die medewerkers van veiligheidsrisico in een robuuste verdedigingslinie?

Voor elke organisatie bestaat een goed ontruimingsplan. Er zijn BHV'ers, hun reflecterende hesjes hangen klaar, portofoons staan gereed en ontruimingen worden regelmatig geoefend.

Maar het lijkt soms of voor digitale veiligheid andere regels gelden. Er wordt juist weinig geoefend. Terwijl die oefening inzichtelijk maakt wat er goed gaat en waar het beter kan. Helaas: zolang alles lekker draait is er ook geen noodzaak om te veranderen. Tot het wél mis gaat. Of totdat een toezichthouder lastige vragen komt stellen.

Al met al zijn er heel weinig bedrijven waar security geen hoge prioriteit meer heeft. Dat is een positieve ontwikkeling van de laatste jaren. Maar dat neemt niet weg dat er in heel veel organisaties, technisch maar vooral op het gebied van awareness, nog veel te verbeteren is.



De dreiging in beeld: feiten en cijfers.

Hoe groot is de veiligheidsdreiging eigenlijk? En wat is de rol van gebruikers daarin? We geven je een paar cijfers:

98%
van de cyberaanvallen gebruikt social engineering: onderzoek (bijvoorbeeld op social media) naar hoe gebruikers communiceren en imitatie daarvan

Phishing-aanvallen zijn in 2019 met
54%
toegenomen. Impersonation attacks, zoals CEO-fraude, namen zelfs met 67% toe
(Mimecast State of Email Security Report, 2019)

75%
van de bedrijven die slachtoffer werden van ransomware hadden hun technische beveiliging op orde

30%
van de phishing-berichten wordt door gebruikers geopend
(Verizon Data Breach Investigations Report 2019)

40%
van de ransomware-slachtoffers betaalden uiteindelijk losgeld

De kosten van cybercrime zijn wereldwijd
6 biljoen dollar.
Een belangrijk deel daarvan komt voort uit phishing en ransomware
(*Ventures Cybersecurity Almanac, 2019)*

Er worden iedere maand
1,5 miljoen
nieuwe phishingsites gelanceerd
(Bron: Purplesec)

“You might have an incredibly talented, diverse group of professionals at your organization. But cybersecurity’s dirty little secret is that no matter how skilled your employees are, they still usually represent your biggest risk. Research shows that human error ranks even higher for cyber risk than software flaws and vulnerabilities. So high, in fact, that it’s a contributing factor in more than 90% of breaches.”
(2018 Cost of a Data Breach Study by Ponemon)

Mogelijke datalekken door menselijk gedrag

De rode draad in veel van deze onderzoeken is dat datalekken en gebruikersfouten heel divers zijn en ook tot een diversiteit aan problemen kunnen leiden. Een paar voorbeelden van mogelijke datalekken als gevolg van menselijk gedrag:

- Het onbeheerd achterlaten van een laptop
- Een verloren USB-stick
- Gevoelige data printen en dat niet gelijk van de printer halen
- Met gevoelige data werken terwijl gasten mee kunnen kijken op je scherm
- Data naar een verkeerde persoon sturen door een typefout in het mailadres of door het onachtzaam gebruik van de mooie autocomplete functie van Outlook
- Forwarden van een gevoelige mail naar een te grote groep mensen
- Iets posten op sociale media wat gevoelig ligt voor de organisatie

Andere veiligheidsrisico’s door menselijk gedrag:

- Niet herkennen van een impersonation- of CEO fraud-mail en geld overmaken
- Een onbekende die net aan komt rennen binnenlaten in het kantoor, omdat je uit beleefdheid de deur openhoudt
- Een bestand openen dat een ransomware-aanval in gang zet
- Klikken op een phishing-link en inloggegevens invoeren op een fakesite
- Slordig omgaan met wachtwoorden: te eenvoudig, in gebruik op diverse andere sites, te makkelijk te raden...

Het is duidelijk: je gebruikers kunnen de zwakste schakel zijn in je beveiligingsketen.

Of de sterkste. Want goed getrainde, bewuste en oplettende gebruikers kunnen je juist helpen om criminelen buiten de deur te houden. En dat brengt ons bij de kernvraag van deze whitepaper: **Waarom is user awareness training zo belangrijk?**

Waarom is user awareness training zo belangrijk?

In de Microsoft Cloud en rondom de digitale werkplek heb je een enorm palet aan de allerbeste security-oplossingen. Maar de cijfers laten zien dat het uiteindelijk de gebruiker is die, letterlijk of figuurlijk, de deur opendoet voor een cyber-aanval. De voorbeelden zijn talloos. Pathé, Universiteit van Maastricht, Cognizant, Flevoziekenhuis, allemaal recente voorbeelden van human error: menselijke fouten die voorkomen hadden kunnen worden, maar wel vergaande gevolgen hebben. In het geval van Pathé heeft het vele miljoenen gekost, in het geval van het Flevoziekenhuis gaat het 'slechts' om het verliezen van privacygevoelige informatie die op een onbeveiligde manier was opgeslagen.

Vaak is het gebruikersgedrag dat een sleutelrol speelt bij het falen van de beveiliging. Wat doe je hiermee als security officer of CISO? Hoe hou je je data veilig en hoe bescherm je de reputatie van de organisatie? Nog meer dichttimmeren? Dat werkt niet.

Het is tijd om je gebruikers van een risico in security assets te gaan veranderen. En dat kan alleen met goede training, die aansluit bij hun praktijk en die gebruikersgedrag effectief en blijvend verandert.

Wat is een goede training?

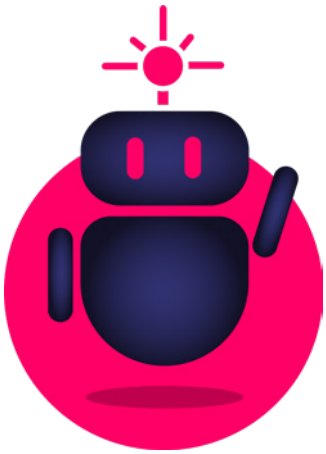
Steeds meer bedrijven zien de waarde van security awareness training en het aantal aangeboden trainingen groeit. Daarmee komt ook de kwaliteit onder druk te staan. Maar hoe ziet een goed security awareness-programma eruit? Een jaarlijks event met alle collega's? Ieder kwartaal een ochtend met het team? E-mails met tips? Veel experts hebben de afgelopen jaren effecten van user awareness training onderzocht. En ze zijn het redelijk eens over wat een goed security awareness-programma is:

- Maandelijkse online trainingen werken het beste. Continuïteit maakt het succes.
- Als medewerkers het programma als leuk en zinvol ervaren, stimuleren ze elkaar het steeds beter te doen.
- Het uitdelen van grappige beloningen aan de medewerker die het hoogst scoort blijkt vruchten af te werpen.
- Een training die dicht bij de dagelijkse praktijk van de mensen komt, over onderwerpen die leven, geeft herkenning en daardoor succes.
- Humor werkt. Het zorgt dat de boodschap beter blijft hangen. Iets wat reclamemakers al decennialang heel goed weten overigens...
- Het hoger management moet het programma ondersteunen en natuurlijk meedoen!

Het succes van een training uit zich in daadwerkelijke gedragsverandering. Daarvoor is alleen het overbrengen van droge kennis niet genoeg. Toch zijn veel awareness-trainingen lang en saai. Ze zijn bovendien vaak niet up-to-date. Zo wordt de training een 'moetje'. Een paar keer per jaar verzamel je je met je collega's in een vergaderzaal. Daar krijg je hetzelfde voorspelbare verhaal te horen, gevolgd door een paar onbenullige vragen. Uiteindelijk gaat het erom dat je je handtekening op de lijst zet, zodat je er weer voor een paar maanden vanaf bent, en je baas kan zeggen dat je 'getraind' bent in security awareness. Dit werkt natuurlijk niet.

Forrester vroeg in een recent onderzoek aan kenniswerkers wat zij vonden van security awareness trainingsprogramma's. 51% vond die trainingen zonde van de tijd, 45% vond ze te lang en 44% antwoordde 'security is saai en datzelfde geldt voor de trainingen'. Ideeën voor verbeteringen hadden ze ook:

- Programma's moeten meer 'engaging' zijn en leuker worden.
- Programma's moeten interactiever worden.
- Trainingen moeten accuraat en actueel zijn, zodat ze passen bij de dagelijkse praktijk.
- 91% van de ondervraagde deelnemers aan security awareness trainingen vraagt om humor in de training.



Niet te technisch

Wij als security-mensen vinden het misschien interessant om te praten over hoe phishing technisch in zijn werk gaat, maar de meeste medewerkers zitten daar niet op te wachten. Bovendien blijkt dat technische kennis weliswaar helpt, maar dat het veel beter werkt om mensen te vertellen wat ze moeten doen. Niet-technische, actiegerichte content geeft mensen houvast. Door situaties te laten zien die ze herkennen, leren ze hoe cybercrime er in het echt uitziet.

Gamification en *fun*

Bij Portiva bieden we de online trainingen van Mimecast aan. Mimecast ontdekte dat ook gamification een grote positieve invloed heeft op het resultaat van security awareness-trainingen. Publiceer bijvoorbeeld elk kwartaal de beste deelnemer en denk na over een kleine beloning voor de best presterende medewerker(s). Wij vinden de Mimecast-training zo goed, omdat mensen ze leuk vinden. Herkenbare personages worden gepresenteerd in alledaagse situaties, met humor. De filmpjes zijn kort en mensen kunnen ze kijken wanneer het hen uitkomt.

Het Amerikaanse Congres vroeg ooit aan Gregory Touhill, destijds Chief Information Security Officer van de Obama-regering, wat hij zou doen met extra budget voor databeveiliging. Zijn antwoord: 'I would spend it on better training my people. I find a very well-trained, well informed workforce is better prepared to help an organization buy down their cyber risk.'

Onderwerpen.

We zagen al dat dreigingen en gevaarlijk gedrag een enorme diversiteit kennen. Je awareness-programma moet daarop inspelen. Er zijn veel programma's die zich volledig concentreren op phishing-mails. Die slaan dus wat ons betreft de plank mis. Phishing is gevaarlijk maar het is maar één van de mogelijke dreigingen, zoals we hieronder laten zien.

Kantoorhygiëne

'*Office hygiëne*' of 'kantoorhygiëne' gaat niet over schoonmaken, maar over dingen als deurbeleid en omgang met bezoekers. Wat doe je als iemand roept: 'Houd de deur even voor me open,' terwijl je diegene niet persoonlijk kent? Laat je diegene binnen? Of vraag je toch maar even om een pasje? Ook mensen die er helemaal uitzien als echte onderhoudsmensen, kunnen verkeerde bedoelingen hebben. Maar het gaat ook over het werken met gevoelige data, terwijl er anderen op je scherm kunnen meekijken. Of het printen van gevoelige stukken en die dan niet meteen van de printer halen.

Impersonation

Impersonation, of 'CEO-fraude', is de techniek waarbij een crimineel e-mails verstuurt die van een hoge manager lijken te komen. Uiteindelijk wordt er daarin gevraagd om geld over te maken en dat aan niemand te vertellen. Dit is wat Pathé overkwam in 2018. Deze vorm van fraude is vrij makkelijk te voorkomen: bel gewoon even. Mail je terug, dan heb je kans dat je antwoord krijgt van de crimineel en niet van je CEO. Cybercriminelen rekenen erop dat mensen niet snel hun directeur persoonlijk zullen bellen om te vragen of een mail echt is. Door goede training zullen je medewerkers (en je CEO) weten dat dit juist wel de bedoeling is.

Ransomware

Virussen komen er op een moderne mailserver bijna niet meer door. Daar zijn de mailfilters te goed voor geworden. Daarom verstopt het gevaar zich nu in dingen die we niet blokkeren, omdat mensen ze dagelijks gebruiken. Denk daarbij aan Word-macro's. Een kwaadwillende macro kan, vanuit een onschuldig uitziend document, online gaan en daar stukje bij beetje de code van een stuk ransomware ophalen. Eenmaal in elkaar gezet, neemt deze software het hele netwerk over. De macro zelf is op geen enkele manier als malware te herkennen en kan dus ook niet door virusscanners worden geblokkeerd (tenzij je de macro als geheel blokkeert, maar daarvan worden niet al je gebruikers gelukkig). Alleen veilig gebruikersgedrag kan zo'n aanval tegenhouden.

Het grootste risico zit hem in gerichte aanvallen, uitgevoerd met zeer geraffineerde teksten. We zien steeds minder het patroon van dagenlange regens van phishing-mails, in de hoop dat één medewerker erop klikt. Steeds vaker zien we dat criminelen uitvoerig research doen en heel goed kunnen imiteren hoe collega's bij bepaalde bedrijven echt met elkaar communiceren.

Informatiebeveiliging en AVG

Documenten delen is makkelijk en samenwerken met externen gaat tegenwoordig naadloos. Maar dat levert risico's en verantwoordelijkheden op. Bovendien ben je als bedrijf gebonden aan de AVG, inclusief hoge boetes. Des te belangrijker dat medewerkers weten wat ze wel en niet moeten delen en hoe ze hier veilig mee om kunnen gaan.

De dreiging van morgen

De dreiging ontwikkelt zich continu, dus moet de training zich ook continu ontwikkelen. Een voordeel van online trainingen is, dat je op ieder moment content kunt toevoegen. De Mimecast-training die Portiva aanbiedt, wordt ieder jaar aangevuld met minimaal 12 nieuwe video's. Onze klanten kunnen ook zelf content toevoegen. Zo zorg je dat je up-to-date bent en je mensen ook traint voor nieuwe dreigingen.

Meetbare resultaten: grip is belangrijk.

Een nog belangrijker probleem van security awareness trainingen: meestal wordt niet gemeten of ze het gedrag van gebruikers ook echt verbeteren. De eerder genoemde Forrester-studie laat zien dat een derde van de onderzochte organisaties met awareness-trainingen geen dashboards of analytics heeft om te beoordelen of gedrag verbetert na training. Terwijl volgens dezelfde studie 31% van de gebruikers toegeeft onveilige dingen, ook na de training, te doen zoals ze dat altijd deden. Een dashboard laat je zien waar je staat en waar de zwakke plekken zitten. Begin daarbij altijd met een nulmeting. Als de trainingen eenmaal begonnen zijn, zie je de risicoscores teruglopen.

Het dashboard van onze online trainingen wordt automatisch gevuld met de resultaten van de tests die medewerkers regelmatig maken. Maar ook als we een phishing-campagne uitsturen om te kijken hoe mensen daarop reageren, verschijnen de resultaten meteen in het dashboard. Wie heeft er wel geklikt, en wie niet? Hoe snel klikken mensen? Zo weet je altijd hoe het ervoor staat met het menselijk risico in je organisatie: globaal, per training, per onderwerp, per afdeling of zelfs per gebruiker. Dit is het soort grip dat je als security officer of CISO nodig hebt als het gaat om security awareness.

De gegevens van het dashboard helpen je ook om de videocontent aan de juiste mensen aan te bieden. Want je wilt mensen de kennis aanbieden die ze nodig hebben, en ze niet lastigvallen met dingen die ze al weten.

Casus: Security bij de Politie

Dat *meer* technische security juist kan leiden tot *minder* daadwerkelijke dataveiligheid ondervond de Politie een paar jaar geleden. De meest gevoelige zaken stonden op fantastisch afgeschermde systemen in aparte werkruimtes. Het werken aan een zaak vereiste daardoor veel voorbereiding en toegangsautorisaties.

Het gevolg? Rechercheurs wisten een manier te vinden om dingen waar ze dagelijks aan moesten werken naar ‘gewone’ werkstations te kopiëren.

Zo konden ze ‘normaal’ werken, zonder steeds tijd te verliezen met allerlei beveiliging. Een averechts effect dus!

Adoptie.

De Mimecast-trainingen en het dashboard worden aangeboden als software as a service (SaaS), dus installatie en uitrol zijn technisch geen issue. Organisatorisch zijn er wel dingen waar je op moet letten. Je kunt bij geen enkel product verwachten dat je het 'aanzet', een mail rondstuurt met een link en dat iedereen het dan uit zichzelf optimaal gaat gebruiken. Goede adoptie van security awareness training hangt af van 3 factoren:

1. Executive buy-in. Zonder steun van het topmanagement wordt het nooit wat. Toch is dit vaak een probleem. Volgens de Forrester-studie heeft ongeveer de helft van de organisaties moeite om het hoger management te interesseren voor security awareness training. Vreemd, omdat juist die mensen zouden moeten weten hoe schadelijk datalekken zijn voor de reputatie van de organisatie.
2. Gebruikersengagement. Juist hierom is het zo belangrijk dat de content goed is!
3. Bewezen toegevoegde waarde. Als security awareness gezien wordt als een kostenpost, zonder dat daar meetbare resultaten tegenover staan, staat dat adoptie uiteraard in de weg. Goede analytics en dashboarding helpen hierbij. Maar het is ook belangrijk om een goed beeld te hebben van de risico's: de kosten van een hack of datalek zijn potentieel zo groot, dat het het einde van het bedrijf kan betekenen.

Meteen organisatiebreed uitrollen

Het is ook belangrijk dat je security awareness meteen over de hele organisatie uitrolt en niet gefaseerd. Want hoe ga je overzicht krijgen op je dashboard, als je maar één afdeling kunt monitoren?

Het is geen IT-dingetje

Maar ons belangrijkste advies is om dit niet exclusief bij IT neer te leggen. Security wordt vaak gezien als een IT-'dingetje'. Het budget ligt dus ook meestal bij de CIO, terwijl security awareness in principe een HR-uitdaging is. De HR-afdelingen moeten er dus ook nauw bij betrokken zijn. Ook Communicatie heeft uiteraard een functie bij het betrekken van medewerkers. Dit soort intensieve samenwerkingen, over silo's heen, zijn een typisch kenmerk van moderne IT-processen. Hoe groter de human factor wordt in IT, hoe belangrijker het wordt dat wij als IT'ers andere afdelingen betrekken bij wat we aan het doen zijn.

We helpen je.

We begrijpen heel goed dat het uitrollen van online trainingen, het monitoren van security awareness, het nadenken over topics, het rapporteren en bedenken van opvolgacties, dat dat allemaal wéér iets is dat bij je takenpakket komt. Daarom bieden we deze trainingen aan als managed service. Dat betekent dat we je het inrichten van dashboards, het finetunen van de templates, het inventariseren van de risico's en de kwartaalrapporten uit handen nemen.

We helpen je, op basis van de cijfers, ook met het uitkiezen van topics en het presenteren van de juiste content aan de juiste mensen. We begeleiden zo het hele proces van A tot Z en bespreken de voortgang met alle betrokkenen en verantwoordelijken.

Samen voor de beste beveiliging van jouw Microsoft 365-omgeving

Onderzoek toont aan dat organisaties die User Awareness training inzetten minder last hebben van fouten gemaakt door medewerkers. Samen gaan we voor de beste beveiliging door medewerkers te trainen. Vraag de gratis demo aan en zie waarom onze oplossing zorgt voor slimmere en meer betrokken medewerkers.

Vraag een gratis demonstratie aan

Neem contact op met *Marco Faasse:*
Account Manager Security
mfaasse@portiva.nl
06-51552419

Over Portiva | Onze bewezen oplossingen zorgen ervoor dat jij veilig kan werken in de cloud. Wij zijn ervan overtuigd dat oplossingen voor digitaal samenwerken, security en cloud infra & apps veiliger moeten zijn. Stabieler. Dit realiseren wij samen met onze klanten en Microsoft. Wij laten zien dat het anders kan: op een persoonlijke en eerlijke manier. Met wederzijds respect en plezier.