ateron®

WHITEPAPER

Creëer Bewustwording voor Bewustwording bij Management

De mens wordt vaak als de zwakste schakel gezien als het gaat om informatie-beveiliging. Desondanks is er nog vaak, volledig onterecht, weinig bereidheid bij het management om dit te veranderen. Informatiebewustwording is juist extra belangrijk voor managementleden, omdat zij toegang hebben tot de kroonjuwelen van een organisatie. Criminelen kunnen veel eenvoudiger een gebruiker ‘hacken’ dan een computernetwerk. CEO-fraude is hier een goed voorbeeld van. En het management zou ook een voorbeeldfunctie moeten vervullen.

De menselijke factor van informatiebeveiliging krijgt steeds meer aandacht. En niet zonder reden, het grootste deel van alle incidenten wordt nog altijd veroorzaakt door de eigen medewerkers. Ondanks deze wetenschap blijkt het nog steeds moeilijk om het management te overtuigen om een security awareness traject te starten. Vaak blijft het bij een eenmalige actie, zoals een phishing simulatie of lunchbijeenkomst, terwijl een dergelijke aanpak geen effect heeft op de lange termijn en echt geen gedragsverandering onder medewerkers zal creëren.

Welke oorzaken liggen ten grondslag aan de lage bereidheid van het management om te investeren in security awareness? En op welke manieren creëer je dan wel draagvlak?

OORZAKEN VAN EEN LAGE BEREIDHEID.

1. GEBREK AAN INTERESSE

Een simpel gebrek aan interesse is vaak de oorzaak van een lage bereidheid bij het management, maar ook bij medewerkers. Het is in dit geval nog niet helemaal doorgedragen dat security een taak van iedereen is en dat iedereen een doelwit kan zijn. Van deze gedachtegang is vooral sprake binnen het mkb. Het mkb realiseert zich vaak niet dat criminelen op zoek zijn naar zwak beveiligde organisaties en in de praktijk is dit vaak het mkb. Zelfs bij kleine organisaties valt een hoop te halen en met relatief weinig moeite voor de crimineel. Maar gelukkig vindt hier de laatste jaren wel een verschuiving plaats, want steeds vaker nemen mkb-bedrijven cybersecuritymaatregelen, zo blijkt ook uit de Cybersecuritymonitor 2019 van het CBS.

2. ANDERE PRIORITEITEN

In de praktijk merken we regelmatig dat security awareness een lage prioriteit krijgt bij het management. Er zijn, volgens het management, tal van andere zaken die belangrijker zijn. Het is dan makkelijk om security awareness te schrappen om budget vrij te maken. Een veelgehoord excuus is dan: ”het mag niet ten koste gaan van de arbeidsproductiviteit.” Tijd is immers geld en de kosten van een security awareness traject gaan vaak zitten in de tijd die medewerkers kwijt zijn aan het volgen van een (online) training.

3. ER IS GEEN NOODZAAK

Vaak is er (nog) geen noodzaak om te investeren in security awareness, want er hebben nog geen

grote incidenten plaatsgevonden. Het heeft dus allemaal niet zoveel haast. Totdat er wel iets gebeurt. En dan ben je te laat!

"Zelfs bij kleine organisaties valt een hoop te halen en met relatief weinig moeite voor de crimineel."

4. GEEN DIRECT RESULTAAT

Security awareness is moeilijk om hard te maken. Het management wil cijfers zien over de ROI van een investering. Het directe resultaat is van een investering is ook moeilijk meetbaar, want je weet nooit hoeveel schade een potentieel incident zou hebben gedaan. Een hoop afgeweerde incidenten zullen ook nooit aan het licht komen. In feite lijkt security awareness alleen maar geld te kosten.

DRAAGVLAK CREËREN BIJ HET MANAGEMENT.

De uitdaging voor de personen die security awareness in hun portefeuille hebben is dus: hoe creëer je draagvlak voor het onderwerp security awareness?

1. TOON NOODZAAK AAN

Het aantonen van noodzaak is makkelijker gezegd dan gedaan. Op het moment dat er echt iets gebeurt, zoals een datalek of ransomware-infectie, zal security awareness automatisch hoger op de agenda komen. Maar het is natuurlijk de taak van de security awareness manager om incidenten te voorkomen en niet te wachten op een incident.

"Wachten op een incident is geen optie"

Je kunt natuurlijk wel een incident simuleren. Door een veilige phishing test, of door andere social engineering onderzoeken uit te voeren (mystery guest, telefonische phishing en dergelijke), kan aangetoond worden hoe eenvoudig een cybercrimineel aan vertrouwelijke gegevens kan komen. Dergelijke onderzoeken hoeven niet veel te kosten en het kost sowieso veel minder dan een echte cyberaanval!

2. COMPLIANCY

Vanuit compliancy oogpunt (ISO, NEN, BIO, AVG) worden eisen gesteld om 'redelijke maatregelen' te treffen om incidenten te voorkomen. Maar wat zijn 'redelijke maatregelen' precies? Dit wordt niet nauwkeurig gespecificeerd, maar verschilt natuurlijk per organisatie. In de zorg zullen andere eisen gesteld worden dan bij de kledingwinkel om de hoek.

In de praktijk zien we dat veel incidenten toch te wijten zijn aan onvoldoende maatregelen, waarna waarschuwingen, sancties of aansprakelijkheid volgen. Natuurlijk is 100% veiligheid niet mogelijk. Het is dan ook zaak om aan de autoriteiten aan te kunnen tonen dat er alles aan gedaan is om risico's te verkleinen. Het adequaat trainen van medewerkers is daar één onderdeel van. Als na een incident niet aangetoond kan worden wat er gedaan is, zeg je als organisatie in feite dat het onderwerp niet belangrijk genoeg was.

3. EEN VEILIGE WERKOMGEVING

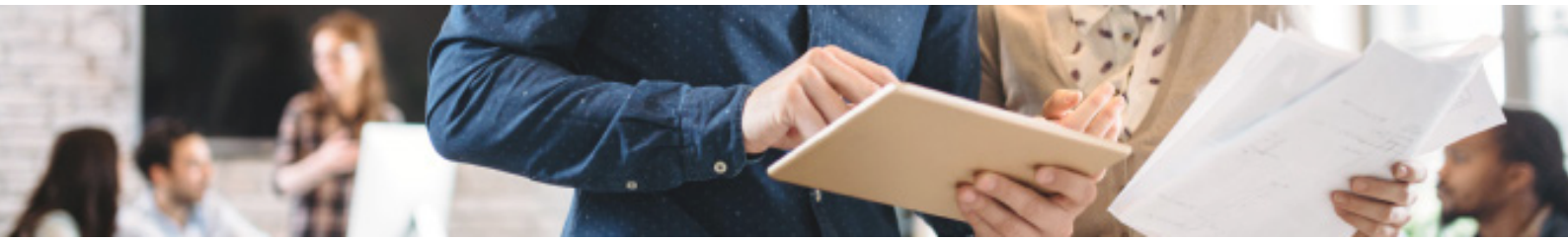
Welke organisatie wil nou geen veilige werkomgeving waarin zorgvuldig omgegaan wordt met de informatie waarover zij beschikken? Informatie is goud waard voor criminelen en dat wil je dat toch zo goed mogelijk beschermen?

Door het trainen van medewerkers zorg je ervoor dat medewerks bewust worden van hun rol en verantwoordelijkheden op het gebied van informatiebeveiliging binnen hun organisatie. Ze zullen zich meer bewust worden van de waarde van informatie en zorgvuldiger en alerter te werk gaan. Daarnaast kunnen medewerkers de kennis ook in hun privésituatie gebruiken, zodat ze ook daar digitaal weerbaar worden.

4. REPUTATIE EN IMAGO

Steeds vaker vragen (potentiële) klanten aan organisaties welke maatregelen zij treffen op het gebied van informatiebeveiliging. Klanten vertrouwen je immers hun data toe en het trainen van medewerkers is natuurlijk een maatregel die klanten vertrouwen geeft. Het laat zien dat je als organisatie goed zorgt voor de gegevens van klanten, medewerkers, burgers, et cetera. Het aantoonbaar zorgvuldig omgaan met gegevens kan reputatieverhogend werken en je net dat stukje voorsprong geven ten opzichte van de concurrentie.

“Security awareness kan je net dat extra stukje voorsprong geven ten opzichte van de concurrentie”



OVER ATERON.

Organisaties worstelen vaak met de betrokkenheid van medewerkers op het gebied van informatiebeveiliging en privacy. 70% van alle informatiebeveiligingsincidenten wordt immers veroorzaakt door menselijk handelen. Awaretrain is specialist in het creëren van bewustwording en gedragsverandering rondom informatiebeveiliging.

Wij testen het gedrag van medewerkers, geven inzicht in het veiligheidsniveau en trainen uw medewerkers. Dit doen we met security awareness programma’s en -meetmethoden. Leer medewerkers beveiligingsrisico’s herkennen, maak van hen de sterkste schakel in informatiebeveiliging en creëer een (cyber)veilige werkomgeving.

CONTACT

Ateron
Bergerweg 170
6135 KD SITTARD

+31 (0)46 475 93 05
info@**ateron**.nl