ateron®

WHITEPAPER

Wat maakt een security awareness programma succesvol? En waarom schieten ze toch vaak tekort?

Het belangrijkste doel van een security awareness programma is om een veiligere werkomgeving te creëren waarin medewerkers zich bewust zijn van hun rol en verantwoordelijkheden als het gaat om informatiebeveiliging. In deze whitepaper behandelen we - onder andere op basis van onze eigen ervaringen - hoe organisaties het gedrag van hun medewerkers op het gebied van informatiebeveiliging kunnen veranderen en verbeteren. Wat zijn succesfactoren en waarom voldoen security awareness programma's toch vaak niet aan de verwachtingen?

Om gedragsverandering te realiseren is er meer nodig dan het verstrekken van informatie over risico's en uitleggen wat het juiste gedrag is. Allereerst moet men in staat zijn om de adviezen te begrijpen en toe te passen en ten tweede moet er de wil zijn om de adviezen te begrijpen en toe te passen. Hiervoor is een verandering in houding en intentie nodig. Wat zijn volgens ons de essentiële punten om dit te realiseren en wat zijn de factoren die vaak leiden tot het mislukken van een campagne?

Essentiële componenten van een Security Awareness programma

1. Interne communicatie

Een goed begin is het halve werk. Een belangrijke factor van een succesvol awareness programma is de manier waarop het binnen de organisatie gecommuniceerd wordt. Denk hierbij aan nieuwsbrieven, blogs en andere manieren waarop er intern gecommuniceerd wordt. Een andere manier is door het verspreiden van grappige posters, cartoons, een introductievideo door de directie of andere gimmicks. Geef aan waarom informatiebeveiliging zo belangrijk is en wat medewerkers de komende periode kunnen verwachten.

2. Computer based training

Het grootste deel van alle werknemers heeft beschikking over een computer. Daarom pleiten wij er altijd voor om computer based training een belangrijk onderdeel van een awareness programma te maken. Uit onderzoek onder werknemers blijkt dat een online training op basis van video's de voorkeur geniet ten opzichte van games en trainingen gebaseerd op tekst. De combinatie van gesproken tekst en visuele beelden hebben een positieve invloed op het leereffect. Andere voordelen zijn de schaalbaarheid voor grotere organisaties en de mogelijkheid voor medewerkers om de training in hun eigen tempo te volgen.

3. Fysieke bijeenkomsten

Goed georganiseerde bijeenkomsten en events laten het onderwerp echt leven binnen de organisatie en zorgen dat medewerkers meer betrokken raken bij informatiebeveiliging. Door middel van een dergelijke spreeksessie kan je goed overbrengen waarom het onderwerp aandacht behoeft.

4. Alles makkelijk toegankelijk

Beperk de drempels voor de medewerker om de juiste informatie te kunnen vinden. Een algemeen toegankelijk systeem dient als een kennisbank, waarin alle benodigde informatie gevonden kan worden over de verschillende onderwerpen binnen informatiebeveiliging. Naast het toepassen van de materie op situaties op de werkvloer, is het ook van groot belang om informatie en tips te geven over privé situaties, zoals het beveiligen van social media accounts en het online beschermen van zijn of haar kinderen.

5. Testen van gedrag en het creëren van leerzame momenten

Social engineering onderzoeken, zoals het versturen van een gesimuleerde phishingmail of een bezoek van een mystery guest, zijn belangrijke leermomenten. Door medewerkers het gevaar te laten ervaren zal de leerbereidheid groeien. Door resultaten van deze onderzoeken te verwerken in een spreeksessie wordt het belang van aandacht voor het onderwerp nog eens extra versterkt.

Deze onderzoeken behoeven wel wat voorzichtigheid. Je wilt geen angstcultuur creëren en je wilt niet dat men het als treiterig ervaart. Een goed voorbeeld is de phishing test van een grote Nederlandse bank. Zij stuurden een nep-phishingmail met een verheugend bericht over de terugkeer van het vorig jaar geschrapte kerstpakket. Dit schoot bij veel medewerkers in het verkeerde keelgat en creëerde dus een averechts effect.

6. Gebruik de taal van de medewerker

Wat op het eerste gezicht een gebrek aan motivatie lijkt, kan in werkelijkheid een gebrek aan leervermogen zijn. Het is aan de opleiders, ontwikkelaars en andere Security Awareness professionals om complexe materie te vertalen naar makkelijk te begrijpen lesstof en praktische handvatten die direct zijn toe te passen.

Waarom sommige programma's toch tekort schieten

1. Medewerkers begrijpen niet wat Security Awareness echt inhoudt

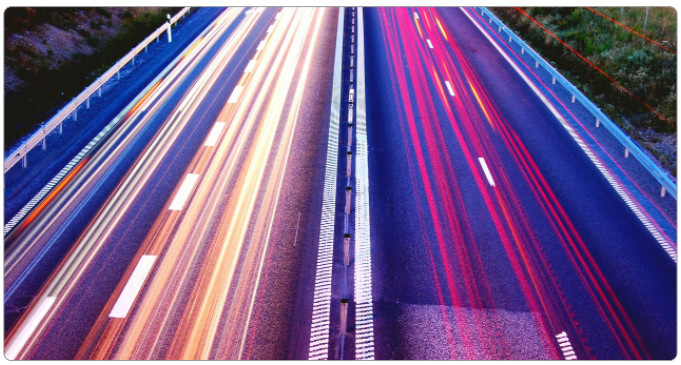
Om medewerkers te laten begrijpen wat security awareness inhoudt moet informatie op een manier worden overbracht die overeenkomt met hoe mensen in de praktijk denken en handelen. Men moet zich herkennen in situaties en snappen hoe de opgedane kennis van invloed kan zijn op hun acties. security awareness is een unieke discipline. Een goede security awareness professional stelt doelen en kan de materie op een juiste manier voor de medewerker vertalen. Daarnaast heeft hij een goede kijk op het inzetten verschillende leermethoden om bewustzijn te creëren en gedragsverandering te realiseren.

2. Het kunnen zetten van een vinkje

Wij zien vaak dat organisaties alleen iets aan security awareness doen om een vinkje te kunnen zetten dat ze het onderwerp hebben behandeld. Denk aan het versturen van een interne mailing met wat informatie en tips of een eenmalige training. Je hebt dan wat gedaan aan security awareness, maar je realiseert absoluut geen gedragsverandering en je creëert gegarandeerd geen duurzame en informatiebewuste werkomgeving.

3. Het mag niet te veel tijd kosten

De effectiviteit van een programma wordt bepaald door de middelen die je er als organisatie aan toekent. Er zit een groot verschil tussen een eenmalige actie en een doorlopend proces van bewustwording met verschillende leermethoden. Geef het daarom de aandacht die het nodig heeft om het gewenste gedrag te realiseren. Wij zien vaak dat organisaties security awareness als eenmalige actie zien. Zij denken er dan te zijn met een enkele phishing simulatie, omdat het anders te veel tijd kost.



4. Gebrek aan boeiende, afwisselende en geschikte leermaterialen

Alleen informeren over een specifiek onderwerp of risico's maakt nog geen training. Er is meer nodig om de interesse van medewerkers te wekken en vast te houden. Zorg voor afwisselende leermethoden en maak het leerproces interactief.

5. Niet monitoren van het programma

Door regelmatig het veiligheidsniveau te meten en de voortgang en resultaten van medewerkers te monitoren kan je het programma aanpassen waar nodig. Ook kan je bepalen welke leermethoden wel en niet werken binnen de organisatie. Voor een zo goed en volledig mogelijk beeld adviseren wij om vooraf een meting te doen, tussentijds te meten door middel van phishing simulaties of andere social engineering onderzoeken en een evaluatiemeting uit te voeren.

6. Onredelijke verwachtingen

Geen enkele maatregel op het gebied van informatiebeveiliging zal 100% veiligheid bieden. Verwacht dus niet dat alle incidenten voorkomen worden. Iedereen maakt wel eens een foutje en criminelen ontwikkelen alsmaar nieuwe technieken en methoden om mensen te misleiden.

Conclusie

Een succesvol security awareness programma bestaat uit een combinatie van leermethoden. Er is niet één opzichzelfstaande leermethode die per definitie het best is, het is de versterking tussen middelen en de manier waarop het verhaal verteld wordt die bepalen of een security awareness programma succesvol is.

Ons advies is om security awareness niet als een eenmalige activiteit te zien, maar als doorlopend proces. Houd daarbij rekening met de taal van de medewerker, maak het interactief en wees vooral creatief. Je kan al heel veel zelf doen om het onderwerp kracht bij te zetten!

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