Veilig gedrag als de sleutel voor succesvolle bewustzijnsprogramma's

Minder dan 1% van alle investeringen in informatiebeveiliging wordt besteed aan mensen, terwijl 99% van de aanvallen menselijke fouten gebruikt om succesvol te zijn. Dit betekent dat het risicobewustzijn met betrekking tot informatie belangrijker is dan ooit. Maar door de onvolwassenheid van deze niche zijn veel bewustzijnsprogramma's niet effectief. Dit artikel bespreekt veelvoorkomende valkuilen en geeft een beknopt overzicht van een op data gebaseerde aanpak voor risicobewustzijn.

Doel

Door de toenemende druk van wet- en regelgeving en vooral ook (spear)phishing aanvallen, staat het risicobewustzijn van medewerkers met betrekking tot informatie hoog op het lijstje van menig Chief Information Security Officer. Het startpunt is dan vaak het trainen van personeel, maar zonder nauwkeurige planning en een methodische aanpak zal dit mislukken.

Een veelgemaakte fout is starten met het verkeerde doel. Ook al is bewustzijn met betrekking tot informatierisico's nuttig, het zou in geen geval het doel van een bewustzijns- of awarenessprogramma moeten zijn.

"Always start with the end in mind"

Stephen Covey

Volgens het Centrum voor Filantropie en Maatschappij van de Universiteit van Stanford "*is er een ruime hoeveelheid onderzoek wat aantoont dat mensen die alleen meer informatie krijgen, zelden hun overtuigingen of gedrag veranderen*" en "*wijst onderzoek uit dat bewustzijnscampagnes niet alleen tekortschieten en middelen verspillen wanneer ze slechts gericht zijn op het creëren van bewustzijn, maar soms zelfs meer schade toebrengen dan bijdragen.*"

Het ultieme doel van elk bewustzijnsprogramma binnen het kader van informatiebeveiliging, is het reduceren van het risico van menselijk handelen naar een acceptabel niveau. Daarbij is het niet kennis of bewustzijn dat een directe impact op risico heeft; het is *gedrag.* Kennis en bewustzijn zijn slechts randvoorwaarden.

Het stellen van veilig gedrag als doel heeft een enorme impact op het programma. Dat komt doordat meetpunten (KPI's) die het succes van het programma meten, direct worden afgeleid van dat doel. Door gedrag als doel te stellen meet men in plaats van slechts de betrokkenheid bij het programma, juist de impact van het programma op het risico van menselijk handelen. Met andere woorden, in plaats van het meten van deelname, toetsscores en voltooing van het curriculum, kan nu ook de impact van het programma op risico gemeten worden, zoals o.a.:

- gerapporteerde incidenten,
- door mensen veroorzaakte informatiebeveiligingsincidenten,
- deelnameratio van de afdeling Informatiebeveiliging in sleutelprojecten,
- percentage (juist) geclassificeerde documenten,
- verlaging van kosten applicatieontwikkeling

Naast een beter inzicht in de effectiviteit van het bewustzijnsprogramma zelf, is de waarde van het programma voor de organisatie op deze manier dus veel duidelijker aan te tonen.

Betrokkenheid

Een ander mogelijk obstakel naar een effectieve bewustzijnscampagne is een gebrek aan betrokkenheid van de doelgroep. In die gevallen waarbij dat een belangrijk criterium is, wordt er vaak gekozen voor een persoonlijke aanpak, zoals bij voorbeeld workshops of klassikale trainingen. Deze zijn uitstekend geschikt om mensen te motiveren en de boodschap persoonlijk te maken voor de trainee, maar het is ook duur en moeilijk te schalen bij grotere of geografisch verspreide aantallen.
Door gebruik te maken van online trainingen (of e-learning) wordt dat probleem opgelost. Maar hier is betrokkenheid weer een uitdaging. Zeker bij het gebruik van generieke trainingsmaterialen of als het curriculum onderwerpen behandeld die de doelgroep niet als direct relevant beschouwt.

Omdat het lastig is om de persoonlijke aanpak te laten schalen bij grote aantallen zonder de kosten significant te verhogen, is de vraag: Hoe vergroten we de betrokkenheid van de doelgroep bij e-learning?

Risicoanalyse

Net zoals het onderwijs eisen stelt aan nieuwe studenten om zorg te dragen voor een goede aansluiting met het curriculum, is het belangrijk de doelgroep grondig te analyseren. Omdat het doel van het programa veilig gedrag is, moet deze analyse zich richten op het identificeren van risicovol gedrag; wie het vertoont; waarom ze bestaan; en welke impact het heeft op de activiteiten van de organisatie.

De traditionele manier om een risicoanalyse uit te voeren is om de huidige situatie te vergelijken met de gewenste situatie of een norm. Het probleem is dat zelfs de meest gevestigde normenkaders vooral zijn gericht op technologie en processen. De basis voor een mensgerichte risicoanalyse op de traditionele manier is er dus niet.

Het alternatief is dan om een op enquêtes gebaseerde methode te hanteren. Dit stelt zelfs grotere organisaties in staat om snel een *volledige* analyse van de kennis, het bewustzijn en gedrag van mensen ten opzichte van informatierisico uit te voeren. De gekozen methode moet uiteraard wetenschappelijk onderbouwd zijn, zodat de vatbaarheid voor cyberaanvallen betrouwbaar kan worden vastgesteld.

Aanvullend kunnen vervolgens traditionele risicoanalyse-elementen worden gebruikt om meer context te geven aan de uitkomsten van de analyse. We hebben het dan over het uitvoeren van deskresearch (bijv. analyse van security incidenten in het verleden, het opnemen van

sector- of zelfs bedrijfsspecifieke dreigingsanalyses) en het houden van interviews met sleutelfiguren in de organisatie.

Kennis

De resultaten van de initiële risicoanalyse vormen de baseline. Op basis deze baseline kunnen meetbare doelen gesteld worden voor het gewenste kennis- en bewustzijnsniveau, en het gedrag van de doelgroep. Deze meetpunten geven het programmamanagement een krachtig stuurmiddel en de security officer een mechanisme om gedurende de levensloop de waarde van het programma naar het management te communiceren.

De uitkomsten van de risicoanalyse kunnen ook gebruikt worden om op data gebaseerde beslissingen te nemen ten opzichte van het curriculum. Bij voorbeeld, door medewerkers op basis van hun kennis te groeperen, wordt het programmamanagement in staat gesteld om juist díe onderwerpen te belichten die aansluiten op de doelgroep, en ze aan te bieden op het juiste niveau.
Hetzelfde kan gedaan worden op basis van ongewenst gedrag wat in de analyse is gemeten: Specifieke modules kunnen geselecteerd worden die dat gedrag addresseren. Op die manier wordt de training relevant gemaakt voor de doelgroep en zullen zij situaties herkennen en actief een oplossing geboden krijgen.

Om het curriculum nog relevanter te maken, is het belangrijk na te denken over hoe de modules worden aangeleverd aan de doelgroep. Daarbij spelen de onderstaande factoren een rol. We zullen daar in een volgend artikel meer aandacht aan geven.

- Gamification (niet te verwarren met games) – Hierbij gaat het om het subtiel stimuleren van betrokkenheid door feedback in de grafische interface. Bij voorbeeld het bereiken van “Expert” status.
- Portabiliteit van content – het kunnen volgen van het curriculum op elk apparaat, overal ter wereld.
- Afstemmen van de inhoud met persoonlijke doelen – het overbrengen van kennis die ook voor persoonlijke doeleinden gebruikt kan worden.
- Didactiek – het aanpassen van de leerstof (bijv. toon) aan de doelgroep zodat zij beter leren. Amerikaanse didactiek werkt bij voorbeeld niet persé voor Nederlanders.
- Beoordelingen – het beschikbaar hebben van een process van het verwerken van feedback van de doelgroep, zodat de content steeds meer op maat gemaakt kan worden.

Simuleren

Zoals eerder aangegeven, zal kennis het bewustzijn verhogen, maar is de impact op het gedrag van mensen minimaal. Een eerste stap naar het transformeren van kennis en bewustzijn in gedragsverandering kan genomen worden door het uitvoeren van simulaties. Dit geeft de doelgroep de kans om het geleerde toe te passen in een veilige omgeving en, bij voldoende herhaling, hun vaardigheden te verbeteren. Daarnaast zijn simulaties een uitstekende bron van data met betrekking tot het het opdoen van nieuwe inzichten naar het gedrag van medewerkers in de praktijk (al dan niet ten opzichte van de baseline).

Omdat email phishing op dit moment de meestgebruikte aanvalsmethode is, zouden phishing simulaties een vast onderdeel moeten zijn van elk bewustzijnsprogramma. Sterker nog, onderzoek wijst uit dat het juiste gebruik van een geautomatiseerd phishingsimulatieplatform, gemiddeld resulteert in een verlaging van 89% van het aantal clicks op kwaadaardige links.

Naast email phishing zijn social engineering, USB en telefonische phishingsimulaties ook het overwegen waard. Het stelt de medewerker bloot aan een bredere set van situaties, waardoor het risicobewustzijn verder stijgt, en levert een diversificatie van de dataset op waardoor wederom betere conclusies getrokken kunnen worden met betrekking tot de inhoud van het programma.

Sturen

Toch zal er na het uitvoeren van het curriculum en simulaties ongewenst gedrag blijven bestaan. Indien nodig, kan dit rest-risico effectief worden aangepakt door gedragsveranderingscampagnes uit te voeren. Een gedragsveranderingscampagne duurt gemiddeld tussen de 6 en 8 weken; wordt op maat ontworpen; gebruikt diverse middelen om het doel te bereiken; en is gericht op één ongewenste gedraging die een significant risico inhoudt voor de (activiteiten van de) organisatie.

Het succes van dit soort campagnes kent drie belangrijke factoren. De diversiteit van het campagneteam zorgt voor de verscheidenheid van perspectieven die nodig zijn om een succesvolle campagne te ontwerpen, terwijl de data component het programmamanagement – wederom – in staat stelt bij te sturen waar nodig. De derde factor heeft betrekking op de focus van het programma op de elementen van gedrag: motivatie, moeilijkheidsgraad en trigger.

Ter illustratie: In openbare toiletten hebben de meeste urinoirs een slim geplaatste sticker van een vlieg. Volgens de wetenschap hebben mannen een diepgewortelde behoefte om doelen te raken en kunnen zij de drang niet weerstaan om er daarom op te richten. Dit voorbeeld laat zien hoe motivatie (bevrediging), moeilijkheidsgraad (plaatsing) en trigger (doel) samenwerken om gewenst gedrag te bewerkstelligen en het verlagen van risico kan bijdragen aan de organisatie.

Toen Schiphol Airport de vlieg introduceerde, nam de gemorste hoeveelheid urine af met 80% volgens manager Aad Keiboom, wat zich laat vertalen naar een significante kostenreductie op onderhoud.

Duurzaamheid

Nadat het bewustzijns- en gedragsprogramma aan volwassenheid heeft gewonnen, is het belangrijk de aanpak te verankeren in de organisatie. Hiertoe kunnen relevante gedragsdoelstellingen worden opgenomen in strategische functies van de organisatie.

Bij voorbeeld: HR zou in samenspraak met andere bedrijfsonderdelen gedragsdoelen kunnen integreren in functiebeschrijvingen, zodat het een criterium wordt voor promoties, bonussen of toewijzing van speciale opdrachten.

Het ultieme doel is om gedrag gedurende de levensloop van medewerkers zodanig te beinvloeden, dat veilig gedrag de norm wordt.

De in dit document beschreven aanpak werd ontworpen door Behaav en wordt aangeduid met **Resilient Workforce Method**. Vragen? Stuur een email naar communications@behaav.com.