De mens als sleutel tot effectieve informatiebeveiliging

31 augustus 2021

(Publicatiedatum: 6 september 2021)

Nagenoeg alle securityprofessionals zullen het beamen: de medewerkers vormen het grootste risico op security-incidenten voor de organisatie en daarmee is risicobewustzijn met betrekking tot informatie belangrijker dan ooit. Toch is *security awareness* vaak onderbelicht en tamelijk onvolwassen, en daardoor zijn de meeste security awareness-programma's niet effectief. Sterker: de meeste securitystrategieën zijn ineffectief. Dit artikel bespreekt veelvoorkomende valkuilen en geeft inzicht in een aanpak voor veiliger (cyber)gedrag, met daarin voorbeelden van relevante controls, instrumenten, conclusies en aanbevelingen. Alles gebaseerd op praktijkervaring en onderzoek naar de ideale mensgerichte methode, gericht op één doel: (cyber)veilig gedrag.

Waarom security awareness-programma's niet effectief zijn

Securityprofessionals worden opgeleid in de wetenschap dat het draait om mens, proces en technologie. Het inzetten van de juiste instrumenten op deze drie domeinen zou ervoor moeten zorgen dat de risico's op het gebied van beschikbaarheid, vertrouwelijkheid en integriteit tot een acceptabel niveau beheerst worden. Toch zijn er maar weinig securityprogramma's echt effectief omdat er te weinig mensfocus is. De aandacht vanuit het hoger management is eindelijk groeiende. Aan ons als security-professionals de taak om goed met die aandacht om te gaan. We richten ons hier op belangrijke oorzaken van ineffectieve securityprogramma's en bieden vervolgens handreikingen om ons te verbeteren.

Budgetten worden verkeerd besteed

Budgetten voor informatiebeveiliging worden in veel gevallen verkeerd besteed. Uit onderzoek van Gartner blijkt dat van de 125 miljard dollar die jaarlijks wereldwijd besteed wordt aan informatiebeveiliging ruim 85 procent besteed wordt aan technologie, ruim 14 procent aan consultancy en minder dan 1 procent aan het trainen en opleiden van onze werknemers op het gebied van informatiebeveiliging. [GART20] Als we deze

wetenschap afzetten tegen de manier waarop cybercriminelen bedrijven aanvallen, dan kan het contrast bijna niet groter. Uit verschillende onderzoeken blijkt dat 85 tot 99 procent van alle aanvallen een vorm van menselijke interactie nodig heeft om succesvol te zijn. In de Inleiding stelden we al dat securityprofessionals zich de meeste zorgen maken om de medewerkers als oorzaak van security-incidenten. Dit betekent dat de wijze waarop diezelfde securityprofessional zijn budget besteedt op zijn minst een heroverweging verdient. Gelukkig wordt er volgens het Infosec Institute eindelijk meer budget vrijgemaakt voor securitytraining. [TOLL20]

De verkeerde doelen worden gesteld

Wanneer er wel geïnvesteerd wordt in security awareness, dan zijn de aantallen getrainde medewerkers het kompas en compliance het doel. Immers, door keer op keer aan te tonen dat medewerkers een training doorlopen, kan ik na zes maanden stellen dat de controls op het gebied van security awareness-training bewezen effectief zijn. Helaas zegt dit niets over het risico dat ik daarmee beheers, kortom de verkeerde doelstelling is gesteld. Dat de kennis overgebracht wordt zegt niets over de vraag of kennis juist is opgenomen, laat staan dat het resulteert in veilig gedrag. Uiteindelijk is gedrag het enige menselijke element dat kan bijdragen aan het verlagen van de risico's door menselijk handelen. Kennis en bewustzijn zijn niets meer dan randvoorwaarden.

Security awareness wordt gezien als bijzaak

Security awareness wordt veelal behandeld als bijzaak, ook als het onderwerp expliciet op de agenda staat. In de praktijk zien we vaak dat gehoopt wordt dat security awareness de bijvangst is van talrijke andere securityprojecten. De implementatie van een nieuwe firewall wordt breed gedeeld, nieuws over security-incidenten worden via interne nieuwsbrieven en het intranet verspreid en er wordt uitvoerig gecommuniceerd over nieuwe beleidsstukken en het belang om die aandachtig door te lezen. Steeds vaker zien we losstaande workshops en phishing-simulaties uitgevoerd worden om aandacht te krijgen voor de materie. Allemaal in de hoop dat er van al die initiatieven iets blijft plakken, waardoor de security awareness toeneemt. Daarnaast blijft het een uitdaging om security awareness-programma's goed georganiseerd te krijgen, maar de oorzaak hiervan is dan vaak dat de volledige informatiebeveiliging bij één persoon belegd is – of iemand in de organisatie doet het 'erbij'.

Er zijn meerdere uitdagingen bij security awareness, denk bijvoorbeeld aan:

1. de bestaande *control frameworks* zoals ISO, ISF, BIO die marginale aandacht bieden aan het menselijke aspect van informatiebeveiliging;
2. security awareness-campagnes die als *one size fits all* worden aangevlogen;
3. het ontbreken van echte verantwoordelijkheid voor het programma en de onderliggende projecten;

4. het ontbreken van risicodimensie aan het security awareness-programma;
5. security awareness die wordt aangevlogen als een eenmalige exercitie, maar net als alles op het gebied van informatiebeveiliging, geldt ook hier dat het gaat om een continu proces.

De vraag die nu beantwoord moet worden, is wat er anders kan en moet. We lichten dit hierna toe. We putten hierbij uit ervaring, kennis, wetenschap en misschien wel het belangrijkste gezond verstand. Aan de slag!

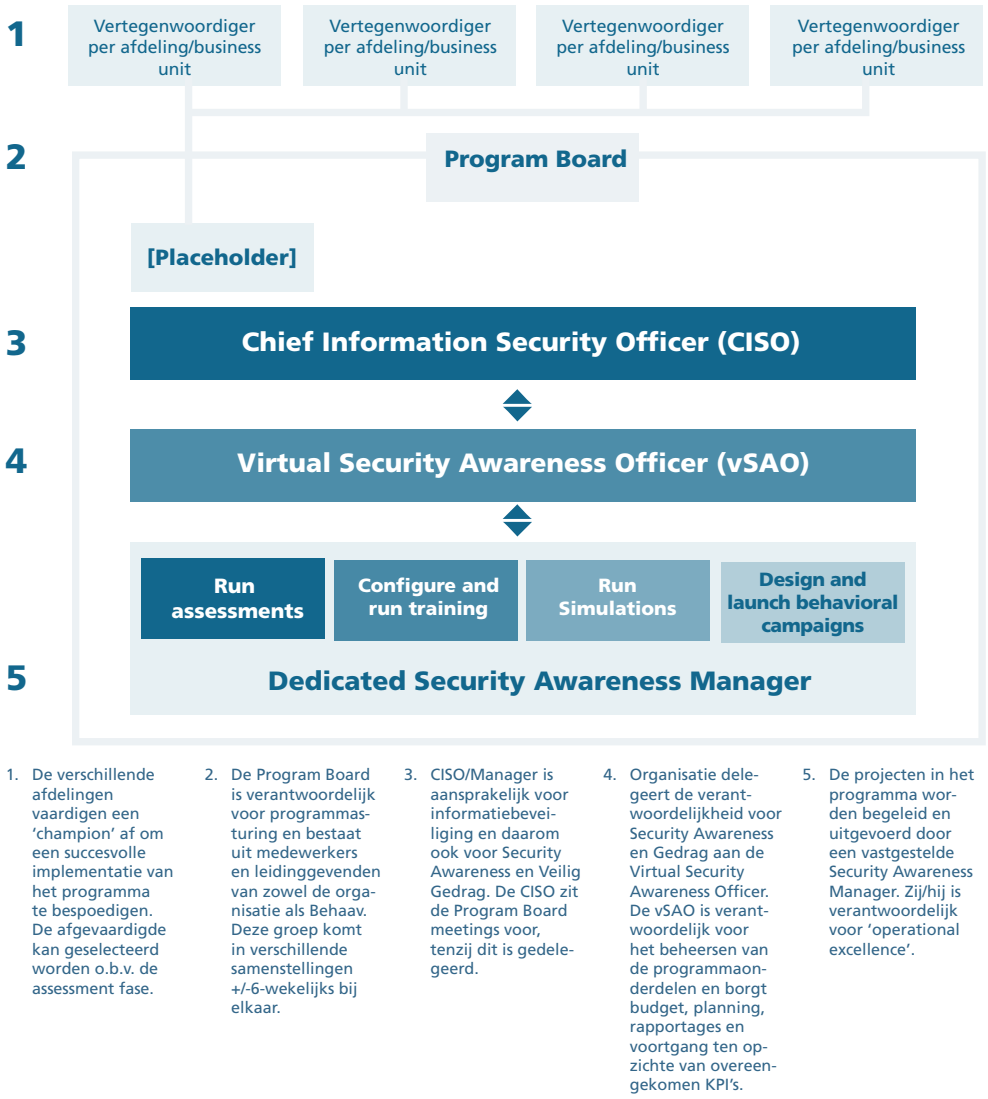
Betrek het management, organiseer en zorg voor een open dialoog

Zorg dat de mensen die eindverantwoordelijk zijn binnen de organisatie niet alleen betrokken zijn, maar blijf ze enthousiasmeren om het juiste voorbeeld te geven. Vertel ze over het belang van informatiebeveiliging voor de organisatie en over het gewicht dat het senior management kan uitdragen. Het signaal dat zij zenden of de woorden die zij spreken, wegen vaak zwaarder dan ze zelf beseffen. Als zij shortcuts op de security policy's nemen, dan kan dat het hele programma ondermijnen.

Een goede organisatie met duidelijke afspraken over taken en verantwoordelijkheden draagt niet alleen bij aan het succes van een programma, maar zeker ook aan een brede betrokkenheid bij het programma. Er komt steeds meer op het bordje van de CISO te liggen en daarom moet je ervoor zorgen dat je kan rekenen op medewerkers vanuit verschillende lagen en afdelingen. Maak dus iemand gedelegeerd verantwoordelijk voor het domein 'Security awareness en veilig gedrag'. Dit stelt je in staat zaken te delegeren. Op deze manier ben je als CISO beter in staat om:

1. het sponsorschap vanuit management te borgen;
2. de brede organisatiebetrokkenheid te borgen (de dialoog);
3. de continuïteit van het programma te borgen;
4. realistische doelstellingen per entiteit van de organisatie te stellen.

Wij stellen hiervoor een vrij pragmatisch model voor dat uit te rollen is voor organisaties van klein tot groot (zie figuur 1). Creëer een teamsamenstelling waar je blind op durft te varen, inclusief de partij aan wie je delen van het programma uitbesteedt.



Figuur 1: Governancemodel voor security awareness -en gedragsprogramma (bron: Behaav)

De verschillende taken die belegd worden, dragen afzonderlijk bij aan de realisatie van de doelen. Om inzicht te houden is van het belang om de resultaten te allen tijde meetbaar te maken tijdens het programma. Daarvoor kan een maturitymodel soelaas bieden (figuur 4, verderop in dit artikel).

Als de organisatie rondom je programma geregeld is, zorg dan als volgt continu voor een open dialoog:

1. Praat met medewerkers over waarom ze werken zoals ze werken. Soms zijn er geheel verklaarbare redenen waarom men securityprocedures niet volgt. Leer van deze gesprekken, om de securityboodschap nog effectiever vorm te geven. Bijvoorbeeld: multifactorauthenticatie (MFA), gecombineerd met complexe, sterke wachtwoorden is niet altijd mogelijk op legacy-systemen. Het sorteert dus geen effect om voor de groep mensen die daarop werken campagnes voor MFA of wachtwoordgebruik te

organiseren.

2. Ga in gesprek met de mensen die weten hoe er gewerkt wordt op de desbetreffende afdelingen. Luister naar hun belangen en vertel ze over het belang van security en veilig gedrag in hun processen. Dat zijn de gesprekken waarin je elkaar gaat vinden en het succes van de campagnes kan vergroten. Maak duidelijk dat je niet iets wil bedenken wat het werken onmogelijk maakt, en draag dit in je campagnes uit. Laat ook blijken dat je hun business begrijpt.

Formuleer de doelstelling nooit alleen

Dit onderwerp snijdt een universeel concept aan. Stephen Covey verwoordt het perfect in zijn boek *7 habits of highly effective people: Always start with the end in mind.* [COVE99] Hoe logisch dit ook is, keer op keer zien we in de praktijk dat men projecten start zonder dat de doelstellingen duidelijk zijn. Soms zijn ze vrij te interpreteren of zijn ze überhaupt niet gesteld. Zorg ervoor dat het doel in overleg met het management gesteld wordt om zeker te zijn dat de securitydoelen dienend zijn aan de organisatiedoelstellingen.

Als we ons beperken tot de doelstelling voor informatiebeveiliging, en in het bijzonder security awareness als (sub)doelstelling, dan is het belangrijk dat de (sub)doelstelling hiërarchisch geplaatst wordt (zie figuur 2). Onthoud daarbij dat kortetermijndoelstellingen mogen afwijken van langetermijndoelstellingen. Het gaat erom dat wanneer de doelstelling voor security awareness expliciet gemaakt wordt in het totale programma voor informatiebeveiliging, het als vanzelf meebeweegt in het programma doordat het zijn eigen waardes krijgt.

Figuur 2: Concept positionering doelstelling voor security awareness en gedrag

Hoewel security awareness met betrekking tot informatierisico's nuttig is, mag het in geen geval de doelstelling van awarenessprogramma's zijn. De doelstellingen moeten dieper liggen dan slechts het overbrengen van kennis. Op de korte termijn is het prima om de focus op security awareness te houden, dit bewustzijn beschouwen wij als de randvoorwaarde voor veilig gedrag. Het ultieme doel van bewustzijnsprogramma's moet liggen op het beheersbaar maken van het risico van menselijk handelen. Daarbij is het niet kennis of bewustzijn dat een directe impact op risico heeft, alleen gedrag heeft invloed op de risico's.

Volgens het Centrum voor Filantropie en Maatschappij van de Universiteit van Stanford is er een ruime hoeveelheid onderzoek dat aantoont dat mensen die alleen meer informatie krijgen, zelden hun overtuigingen of gedrag veranderen. Ook wijst onderzoek volgens het Centrum 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 stellen van veilig gedrag als doel heeft een enorme impact op het security awareness-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 in termen van kwantiteit nu juist de impact van het programma op het menselijk handelen in termen van risico's. Met andere woorden, in plaats van het meten van deelname, scores en voltooiing van het curriculum, kan nu de impact van het programma op risico gemeten worden. Indicatoren kunnen zijn:

1. gerapporteerde incidenten;
2. door mensen veroorzaakte informatiebeveiligingsincidenten;
3. deelnameratio van de afdeling Informatiebeveiliging in sleutelprojecten;
4. percentage (juist) geclassificeerde documenten;
5. verlaging van kosten applicatieontwikkeling.

Naast een zinvoller inzicht in de effectiviteit van het security awareness-programma, is de waarde van het programma voor de organisatie op deze manier duidelijker aan te tonen. Voor het aantonen van de progressie ten opzichte van de gestelde doelen is het aan te raden om daar een meetmethode voor te hanteren die perspectief biedt naar toekomstige doelen. Dit kan echter niet zonder vertrekpunt te bepalen (IST) dat als basis gaat dienen voor het plan om de gestelde doelen te halen (SOLL).

Bepaal het vertrekpunt op kennis, gedrag en risico

De assessments op kennis, gedrag, securitycultuur en risico's vormen gezamenlijk de analyse ofwel assessmentfase. Omdat het doel van het programma veilig gedrag is, moet deze analyse zich richten op het identificeren van risicovol gedrag, wie het vertoont, waarom het bestaat, 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 dient wetenschappelijk onderbouwd te 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, zoals de 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.

De resultaten van de initiële risicoanalyse vormen de baseline. Op basis van 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.

Omdat email phishing op dit moment de meest gebruikte aanvalsmethode is, zouden phishingsimulaties een vast onderdeel moeten zijn van de risicoanalyse. Onderzoek van Knowbe4 onder 17.000 bedrijven en meer dan 9,5 miljoen phishingsimulaties [KNOW21] wijst uit dat het juiste gebruik van een geautomatiseerd phishing -en simulatieplatform gemiddeld resulteert in een verlaging van 87 procent van het aantal clicks op kwaadaardige links. Dergelijke simulaties dienen ook een continu terugkerend onderdeel te zijn van het programma. Immers, de uitkomsten van simulaties geven een weergave van het gedrag in praktijksituaties.

Blijf relevant voor alle doelgroepen

Door medewerkers te analyseren op kennis, houding, gedrag en type werkzaamheden vergroot je de relevantie van het programma per individu of groep. De uitkomsten van de analysefase worden gebruikt voor besluitvorming over het trainingscurriculum. Omdat we dit op basis van feitelijke data uit de organisatie doen, stelt de analyse de organisatie in staat om relevante training en simulaties te doen door medewerkers op te groeperen op basis van:

1. kennis
2. risico's
3. een mix kennis en risico
4. afdeling, geografie en/of samengestelde projectteams

Zo 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.

Ter illustratie nemen we de groep Sales. Uit onze ervaringen blijkt dat salesmensen van nature bereid zijn om meer risico's te nemen en dat ze lager scoren op de verschillende kennistesten. Dit zegt overigens niet altijd dat ze het niet weten, dit kan ook ingegeven worden door een gebrek aan aandacht die aan een vragenlijst wordt besteed. Daarnaast is het een groep die veel meer tijd buiten de kantooromgeving doorbrengt, waardoor een verhoogd risico bestaat op het gebruik van onveilige draadloze netwerken. Een training op het gebied van veilig remote werken, gekoppeld aan een simulatie met zogenaamde *rogue hotspots* zou wel eens een positief effect kunnen hebben op het gedrag van deze groep medewerkers.

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:

1. **Gamification (niet te verwarren met games)**. Hierbij gaat het om het subtiel stimuleren van betrokkenheid door feedback in de grafische interface. Bijvoorbeeld het bereiken van 'expertstatus'.
2. **Tijd.** Hou rekening met de beschikbare tijd voor training per medewerker. Het moet in te passen zijn in het dagelijkse takenpakket.
3. **Hoeveelheid.** Korte, gerichte trainingen regelmatig herhalen werkt beter dan twee maal per jaar een lange training.
4. **Portabiliteit van content.** Het kunnen volgen van het curriculum op elk apparaat, overal ter wereld.
5. **Afstemmen van de inhoud met persoonlijke doelen.** Het overbrengen van kennis die ook voor persoonlijke doeleinden gebruikt kan worden.

6. **Didactiek.** Het aanpassen van de leerstof, bijvoorbeeld qua toon, aan de doelgroep zodat zij beter leren. Amerikaanse didactiek werkt bijvoorbeeld niet per se voor Nederlanders.
7. **Beoordelingen.** Het beschikbaar hebben van een proces van het verwerken van feedback van de doelgroep, zodat de content steeds meer op maat gemaakt kan worden.

Simulatie als ultiem instrument om gedrag in de praktijk te toetsen

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 voor het opdoen van nieuwe inzichten in het gedrag van medewerkers in de praktijk. We zien organisaties daarin ook groeien door scherp te zijn op de effectiviteit van de verschillende activiteiten die worden ondernomen.

Wat veel gebeurt bij organisaties is dat de resultaten van een phishing-simulatie netjes worden gerapporteerd, met daarbij een set aan aanbevelingen. Wat we zelden zien is dat de resultaten vanuit simulaties direct worden opgevoerd in het trainingsprogramma, terwijl dit een cruciaal onderdeel is. Ook voor security awareness geldt: wat zijn mijn 'lessons learned' ook in geval van simulaties?

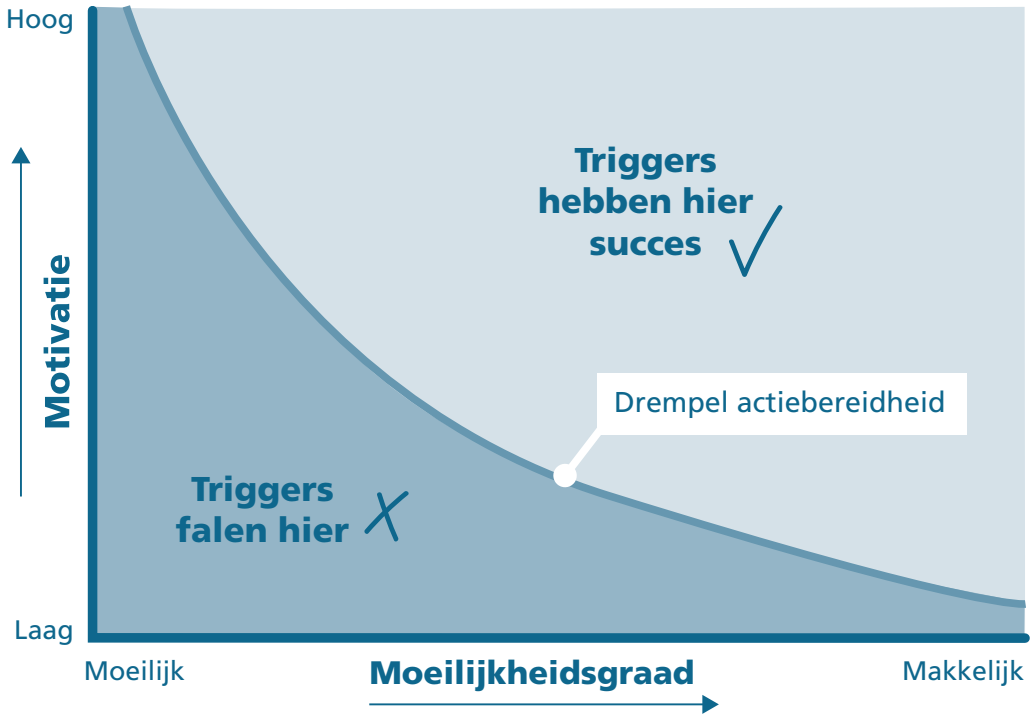
Naast email phishing zijn social engineering, usb- en telefonische phishing-simulaties ook het overwegen waard. Het stelt de medewerker bloot aan meerdere scenario's, waardoor het risicobewustzijn verder stijgt. Het levert ook een diversificatie van de dataset op, waardoor betere conclusies getrokken kunnen worden met betrekking tot de effectiviteit van het programma.

Bestaat er in security awareness-programma's iets als restrisico?

De vraag stellen is hem beantwoorden, zo logisch is het. Toch krijgt het geen aandacht, blijkt in de praktijk. Na het uitvoeren van een assessment, de inzet van educatiemiddelen en simulaties zal er mogelijkerwijs ongewenst gedrag blijven bestaan. Hiermee bedoelen we dat gedrag, dat rechtstreeks een niet te accepteren risico voor de organisatie met zich meebrengt.

Dit restrisico kan effectief worden aangepakt door gedragsveranderingscampagnes uit te voeren. Een gedragsveranderingscampagne duurt gemiddeld tussen de zes en acht 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 eerste factor is de diversiteit van het campagneteam, die zorgt voor de verscheidenheid van perspectieven die nodig is om een succesvolle campagne te ontwerpen. De tweede factor zijn de data, die 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. Deze drie gedragselementen zijn volgens gedragswetenschapper BJ Fogg van het Behavioral Science Institute van Stanford University, cruciaal om gedragsverandering te bewerkstelligen (zie figuur 3). [FOGG20]



Figuur 3: B=MAT (Behaviour = Motivation, Ability and Trigger) [FOGG20]

Ter illustratie hebben we twee voorbeelden beschreven: een voorbeeld uit onderzoek en een voorbeeld uit de eigen praktijk.

Uit onderzoek [KRUL09]: in openbare toiletten hebben urinoirs vaak 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

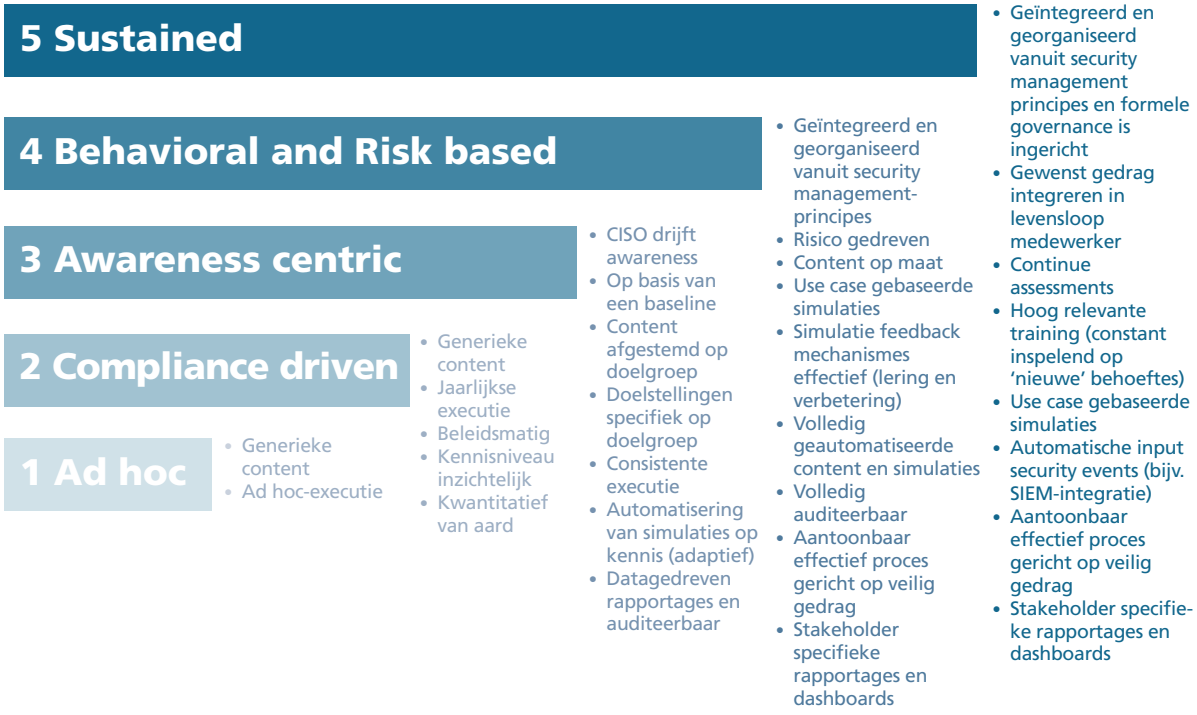
bijdragen aan de organisatie.

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

Houd continu voet aan de bal

Tot slot is het van belang dat je continu inzicht blijft verschaffen in de gerealiseerde voortgang en de status ten opzichte van de doelen in termen van tijd, budget en risico's. Programma's hebben budgetten en het is daarom van belang er zeker van te zijn dat geld juist wordt besteed en dat er koers gehouden wordt op de gestelde doelen. Maak zaken daarom zichtbaar en meetbaar en voorkom een mislukt programma. Er bestaan modellen om volwassenheid in awareness te meten, maar die schieten in onze ogen te kort, omdat uiteindelijk gedrag het doel moet zijn. Hiervoor is het 'Behavioral Security Maturity-model' ontwikkeld (zie figuur 4), dat geïnspireerd is op het SANS Security awareness maturity model.

Daarbij dient direct vermeld te worden dat een hoog volwassenheidsniveau niet per se iets zegt over hoe veilig de organisatie daadwerkelijk is. Het zegt wel iets over de mate van weerbaarheid van de organisatie en het vermogen om processen, procedures en controles na te leven, ofwel veilig gedrag in de praktijk te brengen.



Figuur 4: Behavioral Security Maturity Model, inclusief high level 'control-objectives' (model van Behaav)

Zoals met alle security controls die je inregelt, is het van belang je af te vragen bij welke typen controls en tot op welk niveau jouw organisatie het meest gebaat is. Een risicoanalyse vooraf geeft daar antwoord op. Ga nooit af op aannames en baseer je op feiten. Ook wanneer dit artikel veronderstelt dat meer dan 90 procent van de aanvallen de mens nodig heeft om succesvol te zijn, moet je voor jouw organisatie bepalen of datzelfde van toepassing is.

Het meten op deze controls doen we op basis van effectiviteit. We stellen dat een control minimaal zo'n zes maanden in werking moet zijn om aantoonbare effectiviteit te kunnen bewijzen.

Geef het resultaat een duurzaam karakter

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.

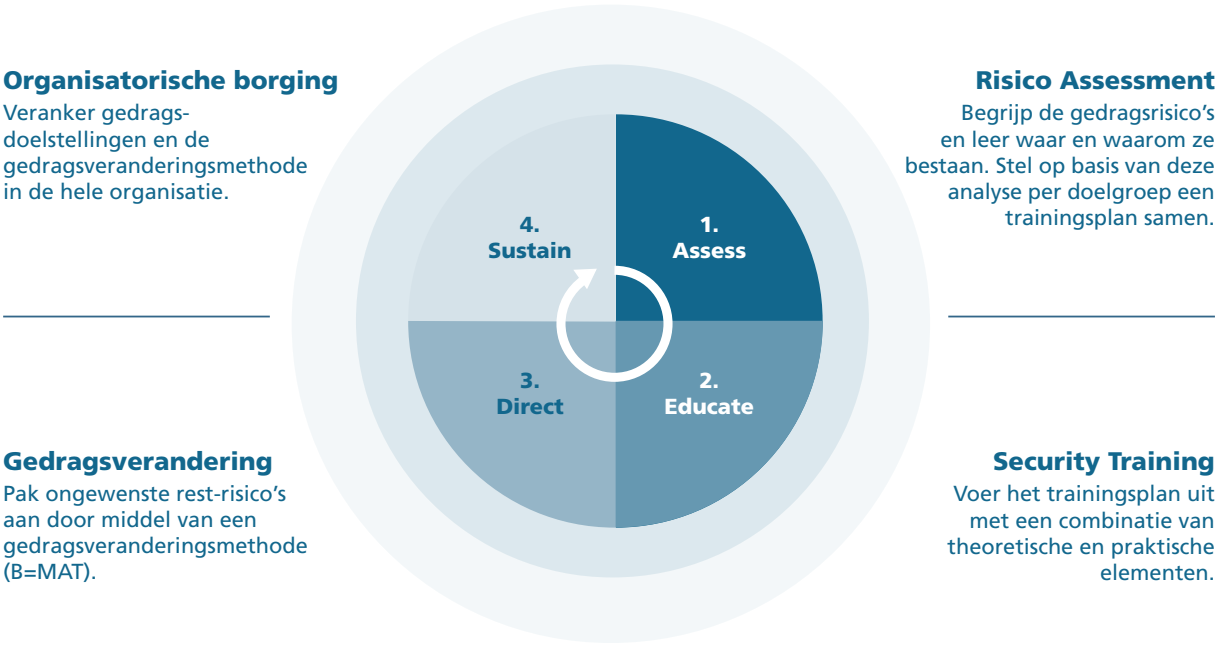
HR zou in samenspraak met andere bedrijfsonderdelen gedragsdoelen kunnen integreren in functiebeschrijvingen, zodat het een criterium wordt voor promoties, bonussen of toewijzing van speciale opdrachten. Daarnaast is het heel verstandig om bijvoorbeeld het volgen van securitytrainingen, aangeboden door de organisatie, die dienend zijn aan de rol van de medewerkers, een vast onderdeel te maken van het pakket van taken en verantwoordelijkheden.

Het ultieme doel is om gedrag gedurende de levensloop van medewerkers zodanig te beïnvloeden, dat veilig gedrag de norm wordt. De mens is daarmee de sleutel tot echt effectieve informatiebeveiliging.

Tot slot: de creatie van veilig gedrag is een continu proces

We hebben in deze publicatie verschillende onderdelen beschreven die security awareness-programma's succesvoller kunnen maken, door de focus te verleggen naar gedrag met een gedegen methode daaronder. Security awareness en gedragsprogramma's vergen continue aandacht en verdienen daarom een methode die ingericht is als continu proces gericht op gedragsverbetering. De belangrijkste aspecten worden hieronder kort samengevat:

1. **Betrek en enthousiasmeer management en directie:** Lead by example en walk the talk zijn veel gebruikte voornemens in managementkringen, aan onder anderen de CISO de taak om ze eraan te houden
2. **Hou een open dialoog en blijf relevant:** De medewerkers maken het verschil tussen een veilige of onveilige organisatie. Win ze voor je programma door in te spelen op hun behoeftes en kernwaarden.
3. **Organiseer en structureer:** De organisatie rondom je programma is cruciaal. Je kunt het niet alleen, en door te delegeren vergroot je niet alleen je bereik, maar krijg je ook meerdere perspectieven. Daarnaast geeft het structuur doordat verantwoordelijkheden breder gedragen worden.
4. **Stel duidelijke doelen:** Stel een doel en hou daaraan vast. Maar zorg vooral dat het doel afgestemd is met de beleidsbepalers van de organisatie. Informatiebeveiliging is belangrijk, maar staat altijd in dienst van de kerndoelstelling van de organisatie.
5. **Creëer bewustzijn:** Breng kennis over en maak medewerkers bewust van de noodzaak om veilig gedrag toe te passen in hun werkprocessen. Zorg dat ze de risico's leren zien en begrijpen. Dit vergt maatwerk op het gebied van kennis, risico, afdeling en gedrag. Daar moet het programma op voorbereid zijn.
6. **Train en simuleer:** Alleen door te trainen en te simuleren kun je testen of de kennis in de praktijk gebracht wordt. Dit is de fase waarin gedrag getoetst wordt, het enige element in het menselijk handelen dat bij kan dragen aan risicobeheersing.
7. **Wees scherp op restrisico's:** Gedrag is aangeleerd en is soms ontstaan in jaren en jaren voorafgaand aan het programma voor security awareness en gedrag. Niet al het onveilige gedrag is dus direct weg. De gedragsaspecten die onacceptabel zijn voor de organisatie neem je weg met specifieke campagnes gericht op die risicovolle gedragingen
8. **Meten is weten: Cliché?** Wellicht, maar niet weg te denken uit het programma. Immers, als het doel wordt gesteld op gedragsverandering om risico's te reduceren, dan dienen we daar op elke gewenst moment inzicht in te kunnen geven.
9. **Duurzaamheid:** Uiteindelijk moet nieuw verworven veilig gedrag als norm gelden. Betrek HR en directie bij het ontwerpen van logische functiebeschrijvingen, taken en KPI's op dit vlak.
10. **Een continu karakter:** Veel, zo niet alle security-initiatieven volgen een bepaalde managementcyclus op basis van bijvoorbeeld de PDCA. Kies een methode die daarop gebouwd is om security awareness en gedrag als continu proces aan te pakken (zie voorbeeld figuur 5).



Figuur 5: De Resilient Workforce-methode van Behaav gericht op veilig gedrag

Literatuur

[COVE99] Stephen Covey, *The 7 Habits of Highly Effective People; Powerful lessons in personal change, Simon & Schuster US*, 1999.

[FOGG20] B.J. Fogg, *Fogg Behavior Mode*l: https://behaviormodel.org/, 2020, geraadpleegd op 9 augustus 2021.

[GART20] Gartner, *Gartner Forecasts Worldwide Security and Risk Management Spending Growth to Slow but Remain Positive in 2020*, Gartner Press Release, Sydney, Australia, 17 juni 2020: https://www.gartner.com/en/newsroom/press-releases/2020-06-17-gartner-forecasts-worldwide-security-and-risk-managem#:~:text=Worldwide%20spending%20on%20information%20security,2020%20(see%20Table%201), geraadpleegd op 9 augustus 2021.

[KNOW21] *Report: 2021 Phishing By Industry Benchmarking*, KnowBe4, 2021: https://info.knowbe4.com/phishing-by-industry-benchmarking-report, geraadpleegd op 9 augustus 2021.

[KRUL09] Robert Krulwich, *There's A Fly In My Urinal*, WBUR, 19 december 2009: https://www.wbur.org/npr/121310977/story.php, geraadpleegd op 9 augustus 2021.

[TOLL20], Rodika Tollefson: *Cybersecurity spending grows*, Infosec: https://resources.infosecinstitute.com/topic/cybersecurity-budgeting-and-spending-trends/, geraadpleegd op 9 augustus 2021.

R. (Rudy) Spinola CISSP en CISM | Mede-eigenaar bij *Behaav*

Rudy Spinola heeft tweeëntwintig jaar ervaring in informatiebeveiliging. Hij was onder meer werkzaam als manager en consultant, en was vaak het gezicht van informatiebeveiliging naar klanten. Hij werkte voor snelgroeiende startups en 's werelds grootste multinationals op het snijvlak van business en security. Vanuit zijn overtuiging dat de mens de sleutel is naar effectieve informatiebeveiliging, werkte Rudy samen met Melvin Broersma vanaf 2018 aan de ontwikkeling van een methode voor het verbeteren van bewustzijn en gedrag. Dat werd de Resilient Workforce Method. Om organisaties te helpen de methode toe te passen, richtten zij in 2019 samen Behaav op met als adagium: People improve security.

M. (Melvin) Broersma CISSP, CISM en OSSINT | Mede-eigenaar bij *Behaav*

Melvin Broersma is een van de oprichters en eigenaren van Behaav en heeft inmiddels ruim vijftien jaar ervaring in informatiebeveiliging, waarvan de laatste vijf jaar als ondernemer. Hij helpt bedrijven van klein tot groot bij een effectieve opzet en executie van informatiebeveiliging. De menselijke focus op begrip, betrokkenheid en executie van informatiebeveiliging in de hele organisatie is in zijn ogen fundamenteel. In 2018 schreef hij het boek 'Cyber Security in 60 minuten' om managers en bestuurders snel en in eenvoudige taal te informeren over ons soms complexe vakgebied.