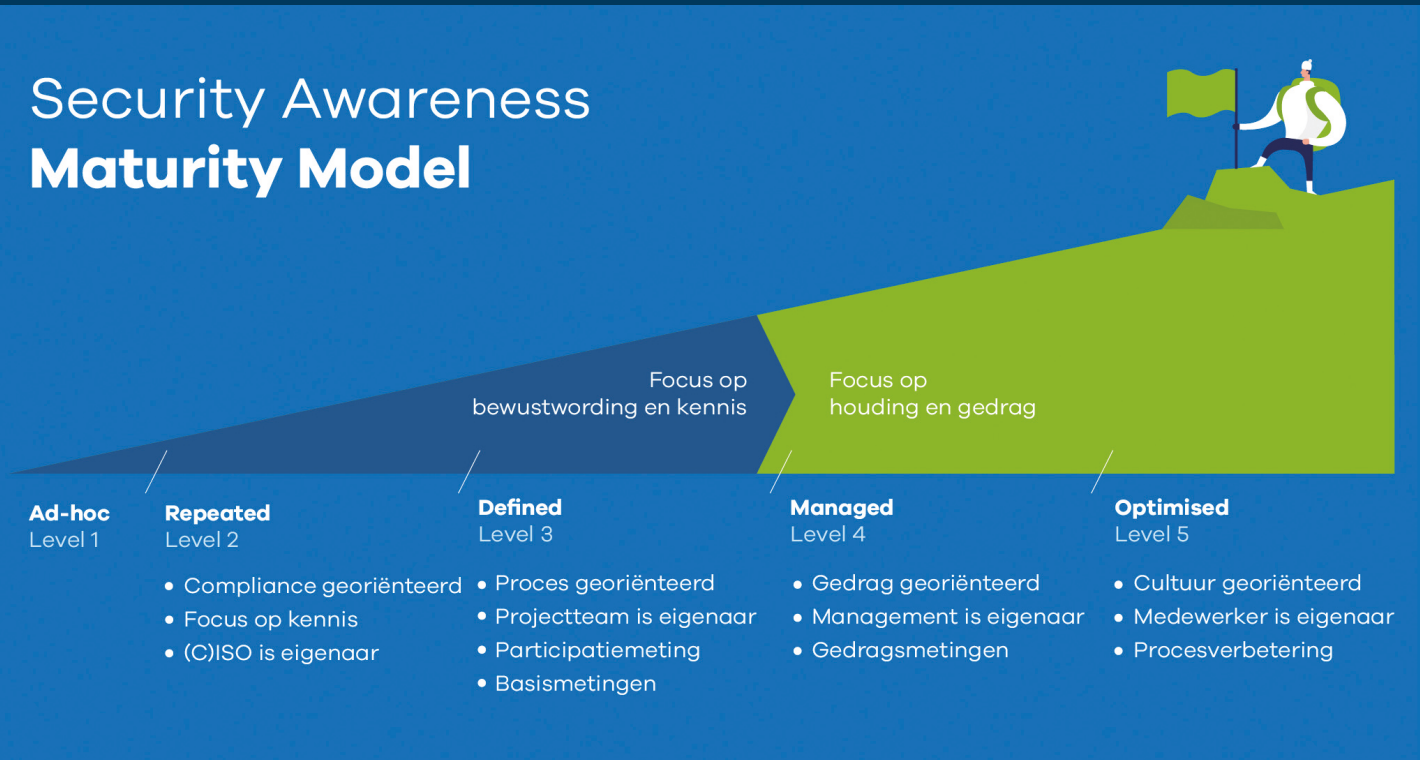
Auteur: Wilbert Pijnenburg CISA CISSP is commercial director bij Infosequre en sinds 1996 werkzaam in de informatiebeveiliging. Sinds 2007 heeft hij een volledige focus op security awareness. In de afgelopen 15 jaar heeft Wilbert tientallen nationale en internationale organisaties geholpen bij de inrichting van hun awareness programma's. Wilbert is bereikbaar via wilbert.pijnenburg@infosequre.com.

Security Awareness Volwassenheidsmodel

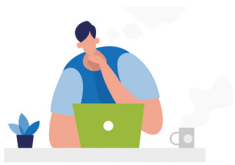
Verleg de focus van bewustwording en kennis naar houding en gedrag



Afbeelding 1 - Infosequre-security-awareness-CMM model.

Iedere security expert weet dat goede informatiebeveiliging een combinatie is van mens, organisatie en techniek. Bewustwording en training van medewerkers is een standaard onderdeel van ieder beveiligingsprogramma. Een security framework zonder awareness bestaat niet. De laatste jaren hoor je steeds vaker dat security awareness gaat om gedragsverandering in plaats van bewustwording. Gedragsverandering en het creëren van een duurzame beveiligingscultuur is de Big Hairy Audacious Goal (1), maar dat betekent niet dat iedere organisatie meteen aan gedragsverandering moet of kan werken.

Het ontwikkelen van een beveiligingscultuur is een lange reis en iedere reis begint bij de eerste stap. Iedere beginnende karateka wil ooit in zijn leven de zwarte band halen, maar weet ook dat het begint met de gele band. En zo is het met security awareness ook. Je hoeft het einddoel niet onmiddellijk te bereiken, je kunt er stapsgewijs naartoe groeien. Om je te helpen bij het ontwikkelen van je bewustwordingsprogramma, je inzicht te geven in je huidige situatie en je een vooruitzicht te geven op je potentiële volgende stap, ontwikkelden we een security awareness volwassenheidsmodel.



Level 1: Ad-hoc level: "We moeten iets doen aan security"

In dit level is er nog niet echt sprake van een bewustwordingsprogramma. Het volwassenheidsniveau van de organisatie is dusdanig laag dat informatiebeveiliging vooral bestaat uit technische maatregelen met hier en daar wat procedures. Onder het motto 'we moeten iets doen', wordt er ad-hoc over security gecommuniceerd, meestal als reactie op een incident in de markt. Het initiatief ligt volledig bij de security verantwoordelijke of IT-manager. Het management is niet betrokken.

Level 2: Repeated – creëren van bewustwording en kennis

Er wordt met enige regelmaat aandacht besteed aan security awareness. We spreken voor het eerst over een bewustwordingsprogramma. De insteek is veelal 'compliance' georiënteerd, bijvoorbeeld omdat een toezichthouder zegt dat er iets aan security awareness moet worden gedaan of het in een security framework staat beschreven. De security verantwoordelijke of IT-manager is zowel eigenaar, bedenker als uitvoerder van het programma. De focus ligt volledig op het creëren van bewustwording en het bijbrengen van kennis. Er is weinig budget voor de uitvoering aanwezig. Management is niet betrokken en management commitment is onduidelijk. Er wordt weinig tot niets gemeten. Misschien wordt er een ad-hoc phishingtest uitgevoerd. De incidenten registratie is technisch van aard en er wordt geen root-cause naar menselijk gedrag uitgevoerd. Zit jouw organisatie in dit niveau? Je bent niet de enige. In Nederland zit 60% tot 70% van de organisaties ergens tussen niveau 2 en 3. Met de volgende stappen breng je jouw security awareness programma naar een hoger niveau.

Level 3: Defined – security awareness als proces

Het is niet voor niets dat dit level 'defined' heet. Het is het eerste niveau waar je kunt spreken van enige volwassenheid en waar security awareness als proces is ingericht. De focus ligt nog steeds voornamelijk op het creëren van bewustwording en kennis, maar de activiteiten worden nu gepland en geregeld uitgevoerd. Als onderdeel van de procesinrichting is een on-boarding programma opgenomen. Nieuwe medewerkers worden bij aanname geïnformeerd over de geldende richtlijnen. Langzamerhand verschuift de individuele aanpak van een security verantwoordelijke naar een meer multidisciplinair team. Om de activiteiten uit te kunnen

voeren is een basisbudget aanwezig. Management commitment is beperkt en nog niet echt betrokken bij de uitvoer. Het team is volledig verantwoordelijk en voert alles zelf uit. De onderwerpen worden op basis van eigen inzicht gekozen. De incidentenregistratie is technisch van aard en wordt niet op basis van de menselijke factor in kaart gebracht. Er vinden voor het eerst metingen plaats, maar deze zijn vaak participatie georiënteerd. Zo af en toe wordt een praktijktest uitgevoerd.

Level 4: Managed – focus naar houding en gedrag

In dit level vindt de omslag plaats. Bij level 3 maakten we nog een belangrijke stap om security awareness als proces in te richten. De focus lag op bewustwording en kennis. In dit level maken we de overstap naar de focus op houding en gedrag.

Op managementniveau zijn er fundamentele wijzigingen. De verantwoordelijkheid voor security awareness is verschoven van het uitvoerende team naar het management. Management commitment is duidelijk aanwezig en betrokken. Het management spoort medewerkers aan deel te nemen aan de awareness programma's, besteedt aandacht aan informatiebeveiliging in het werkoverleg en vertoont voorbeeldgedrag. Door het toegenomen managementsupport is er meer budget beschikbaar en medewerkers mogen tijd besteden aan de diverse activiteiten. Het multidisciplinaire projectteam heeft een faciliterende en ondersteunende rol gekregen.

Er worden SMART gedragsdoelstellingen gedefinieerd om aan gedragsverandering te kunnen werken. De incidentenregistratie is niet meer puur technisch van aard. Incidenten veroorzaakt door menselijk gedrag worden herkenbaar gelabeld en er vindt een root-cause analyse plaats op de incidenten. Op veel voorkomende en terugkerende incidenten vindt 'problem management' plaats en er worden acties bedacht om terugkerende incidenten in de toekomst te voorkomen. De onderwerpen van het programma worden bepaald op basis van de incidentenanalyse, risico's en gerenommeerde marktrapporten. Om de effectiviteit te bepalen worden regelmatig metingen uitgevoerd die het gedrag beoordelen.

Level 5: Optimised – the holy grail

Zie dit level als de holy grail van security awareness. De ideale wereld waar veel over gesproken en geschreven wordt, maar waar maar weinig bedrijven aan voldoen. Het is ook de reden waarom dit model is uitgewerkt. Je hoeft niet meteen te voldoen aan alle eigenschappen die bij dit hoogste level horen. Dit level is de stip aan de horizon. Bepaal je huidige niveau, kijk naar de volgende stap en bepaal je groeipotentieel. In de ideale wereld draait het niet om het opleggen van gedrag maar is veilig werken een second nature van de medewerker. Hier bereiken we een securitycultuur. Management is natuurlijk van de partij, maar de medewerker staat centraal. Zij worden betrokken bij de analyse. Samen bepalen zij waar de behoefte ligt. Net als bij level 4 worden er SMART gedragsdoelstellingen gedefinieerd, maar om de medewerker optimaal te ondersteunen wordt er ook gekeken naar de omgeving. Kunnen we obstakels weghalen en hoe kunnen we veilig werken ondersteunen? Security policies en IT-middelen worden beoordeeld op werkbaarheid en de fysieke omgeving wordt aangepast als dit veilig werken vereenvoudigt. Tooling wordt toegevoegd om veilig werken makkelijker te maken. Gedrag en effectiviteit worden met regelmaat gemeten. Op basis van de incidenten en risico's die herleidbaar zijn naar menselijk gedrag, marktrapporten en de metingen, worden regulier verbeteringen aangebracht en aanpassingen doorgevoerd.

Op naar de volgende stap

Het succes van een security awareness programma wordt voor een groot deel bepaald door de inrichting van het proces. Daarna moeten de verschillende initiatieven van dusdanige kwaliteit zijn dat ze invloed hebben op het gedrag van de medewerker. Het volwassenheidsmodel gaat vooral in op het proces. Het geeft inzicht in je huidige situatie en toont de volgende stap. Het behoedt je voor onrealistische doelen. Door dit inzicht wordt het voor iedere organisatie mogelijk om aan security awareness te werken. Of je nu een bank of de bakker om de hoek bent. Wat is jouw volgende stap?

Referentie

(1) Jim Collins & Jerry Porras. Built to last: Successful Habits of Visionary Companies, Random House, 2005.