Audittrail
information security | privacy | quality | grc

BIC Building Blocks Bewustzijn

AANDACHT VOOR HOUDING EN GEDRAG

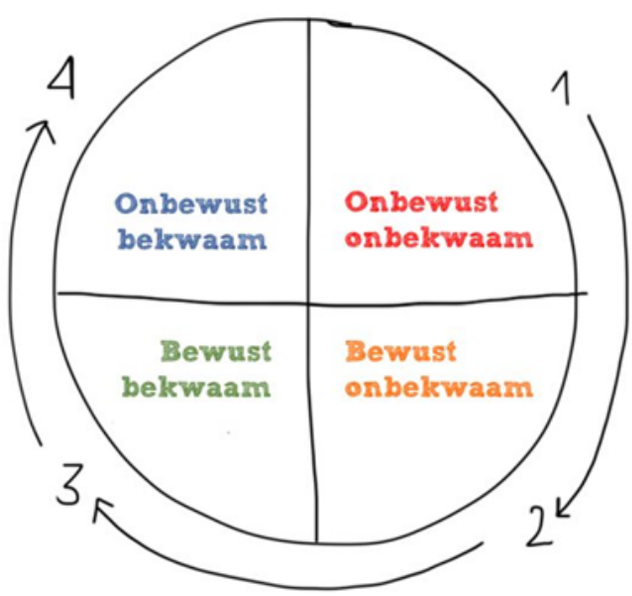
Informatiebeveiliging gaat niet alleen over het implementeren van (technische) maatregelen, risicoanalyses of het formuleren van informatiebeveiligingsbeleid. Aandacht voor houding en gedrag van medewerkers is even belangrijk. Misschien is het zelfs wel belangrijker. Informatieveilig werken is een werkwoord, iets wat je doet. Niet in het laatste half uurtje van de dag, maar de hele dag door. Informatiebeveiliging is geen losse silo in de organisatie maar een manier van werken. Het implementeren van informatiebeveiliging is daarmee ook een verandertraject dat invloed heeft op de hele organisatie.

Het bewerkstelligen van gedragsverandering binnen een organisatie is geen simpel proces. Het vereist een goede communicatiestrategie, kennis van medewerkers en hoe zij het beste leren. Er bestaat geen vaste aanpak voor het bewust maken van het belang van veilig omgaan met informatie en welke rol medewerkers hierin spelen. Dit zal altijd maatwerk zijn.

Er zijn allerlei producten op de markt die bijdragen aan het verhogen van de awareness van medewerkers: van escaperooms tot bordspellen en van phishingtesten tot e-learnings. Maar op welke basis kiest u producten en hoe komt u tot een juiste mix? In deze whitepaper gaan we dieper in op bewustzijn van medewerkers.

Leerfasen van Maslow

Bewustzijn start met bewust worden. Iedereen begint Onbewust Onbekwaam. In deze fase weet men niet wat een goede manier van werken is, en wordt er ook niet juist (informatieveilig) gehandeld. Vaak beseffen mensen dit pas als ze geïnformeerd worden over het onderwerp en komen er reacties als: “Daar ben ik niet van”, of “in welke tijd verwacht je dan dat ik dit allemaal moet doen?” Laat je hierdoor als security officer niet afschrikken. Vaak hebben mensen wel een zeker beeld of vooroordeel over informatiebeveiliging, maar wat het nu precies is of welk effect het heeft op werk, dat is niet helder. De veronderstelling is vaak dat het meer werk op gaat leveren of werk belemmert. Tijd dus om te informeren en mensen langs de fase Bewust Onbekwaam (mensen weten nu wat het onderwerp inhoud en weten ook dat dit nog niet overeen komt met de manier waarop ze werken) naar Bewust Bekwaam (informatieveilig werken) te leiden.



FASES VAN AWARENESS

Bij bewustwordingstrajecten binnen organisaties onderscheiden we over het algemeen vier fases.

Initiële fase

Vaak start een traject als onderdeel van bijvoorbeeld een project, of wanneer een nieuw informatiebeveiligingsbeleid wordt ingezet. Het gaat dan om een traject in campagnevorm waarbij de gehele organisatie wordt meegenomen: een seminar, postercampagne, folders in koffiekamers. De campagne kenmerkt zich door een tijdelijk karakter en vaak wordt er geen onderscheid gemaakt in doelgroepen: de gehele organisatie wordt op eenzelfde manier aangesproken. Het heeft als doel mensen bewust te maken van basis van informatiebeveiliging en algemene maatregelen: kantoorhygiëne als het afsluiten van schermen en het gebruik van afgesloten papierbakken bijvoorbeeld. Maar wat nu als er medewerkers net ziek blijken in de campagneweek, of op vakantie, of ze komen een maand later pas in dienst?

Herhaalfase

Bezemklasjes, nieuwe medewerkerstrajecten, herhalingse-mails. Het zijn allemaal kenmerken van een herhaalfase. Juist voor de mensen die de campagne niet hebben meegemaakt. In de herhaalfase wordt dezelfde informatie gecommuniceerd als in de initiële fase maar dan in kleine klasjes, of aan individuen. Het doel is hetzelfde, de boodschap ook, de middelen soms iets anders.

Continue fase

De kracht van de herhaling is iedereen duidelijk, en dat ongebruikte kennis steeds dieper wegzakt ook. Het is dan ook van belang om kennis te blijven delen om het basisbewustzijn dat is verkregen in de initiële fase te behouden. Dit kan op verschillende manieren. Denk aan een e-learning die medewerkers periodiek maken, of een awareness communicatieplan met de doorlooptijd van een jaar, waarbij op gezette tijden informatie de organisatie in wordt gestuurd. Let wel, dat waar het eerst voldoende was om de organisatie in zijn geheel aan te spreken, specifieker communiceren nu steeds belangrijker wordt om mensen aan te blijven spreken. Denk bijvoorbeeld aan casustrainingen voor afdelingen, of gebruik gericht voorbeelden die een bepaalde doelgroep aanspreken. Om mensen aan te kunnen spreken op hun verantwoordelijkheden moet de communicatie ook dicht bij hun dagelijkse werkdag liggen.

Testfase

Na het doorlopen van de eerste drie fases heeft u als security officer veel en duidelijk gecommuniceerd. Hoog tijd om eens testen wat mensen van uw boodschap hebben opgestoken. Er zijn verschillende manieren om te testen. Denk bijvoorbeeld aan een phishingtest. Dit is een type Social Engineering waarbij een (gecontroleerde) phishing e-mail wordt uitgestuurd naar de gehele organisatie. Ondertussen wordt gemonitord of uw medewerkers op de mail klikken en/ of inloggen. Er zijn nog vele andere vormen van social engineering testen: van bellen tot een bezoek van een mystery guest of het phishen via sms. Denk ook eens aan het laten testen van een (incidenten)procedure of een uitwijkscenario door dit te simuleren. Het testen van medewerkers geef niet alleen een goede indicatie hoe effectief de eerdere bewustwordingsmaatregelen zijn geweest, maar werken vaak ook als een extra bewustwordingsmoment.

Audittrail
information security | privacy | quality | grc

ONDERHOUD VAN BEWUSTZIJN

De verdiepingsslag maken

De meeste organisaties kiezen er voor een algemene, organisatiebrede awareness campagne uit te rollen met gebruik van elementen zoals flyers, posters en een algemene e-learning module. Zolang dit regelmatig wordt herhaald is dit natuurlijk een prima uitgangspunt. Echter merken we dat wanneer bedrijven willen groeien in hun mate van informatieveilig werken en de organisatie naar het volwassenheidsniveau willen brengen, een verdiepingsslag nodig is. Onderdeel van de continue fase is het aanbrengen van een tweede laag in de communicatie. Specifieke materie voor bepaalde teams of incidentsimulaties voor bepaalde teams kunnen hieraan bijdragen. Ook kunnen er op maat gemaakte trainingen worden ontwikkeld om teams meer specifieke kennis bij te brengen. Wanneer organisaties echt de verdieping willen opzoeken merken we dat naast verdieping, ook afwisseling en frequentie een rol spelen. Door bijvoorbeeld meerdere 'praktische' tests af te wisselen met online educatieve elementen (denk aan e-learning modules, trainingsvideos, of referentiecasussen) krijgt awareness een continue karakter. Door toevoeging van andere motiverende elementen zoals het verzamelen van punten of certificaten krijgt ook de motivatie van werknemers een extra stimulans.

Terugkijkend op de vier leerfases van Maslow bereiken we zo gestaag het onbewust bekwaam handelen. Dit is een ideale situatie waarin medewerkers automatisch gewenst gedrag vertonen, zonder dat dit de manier van werken beïnvloed of extra moeite kost.

Het doel is de sleutel

Welk medium u ook kiest om uw boodschap over te brengen, het is vooral van belang om vooraf het te behalen doel helder voor ogen te hebben. Wat moet de communicatie uiteindelijk opleveren? Bedenk ook dat communicatie een vak op zich is, de meeste organisaties hebben een communicatieafdeling. Laat u als security officer ook vooral adviseren over de inzet van middelen! Vaak zijn er al veel lessons learned in de organisatie te vinden over wat wel en niet werkt op het gebied van interne communicatie.

Audittrail
information security | privacy | quality | grc

Contactgegevens
Audittrail
Sisalbaan 5a
2352 AE Leiderdorp

KantNoord
Winschoterdiep 50
9723 AB Groningen

071 - 747 71 71
BBB@audittrail.nl

Audittrail
information security | privacy | quality | grc