

Awareness-Campagne

Dienstbeschrijving Versie 1.1

Introductie

Het creëren van bewustzijn met betrekking tot informatiebeveiliging is vaak een lastige, moeizame aangelegenheid. Veelal ontgaat nut en noodzaak de medewerkers geheel – niet alleen de 'gewone' medewerkers, maar doorgaans ook het management – of is de gevestigde cultuur er niet naar. Ook kan informatiebeveiliging kampen met een slecht imago (is alleen maar lastig, alleen maar extra regeltjes) of heeft men het idee dat het 'ut pakkie an' is van anderen in de organisatie – zoals de IT-afdeling - en niets met de eigen functie (en verantwoordelijkheid!) te maken heeft.

Het gedrag van medewerkers wordt onder andere bepaald door de kennis die men bezit, de mening die men heeft, maar ook door de eigen afkomst en persoonlijkheid. Daarnaast spelen externe factoren een rol. Het gedrag laat zich niet zomaar sturen, maar toch is de houding ten aanzien van informatiebeveiliging en het bewustzijn hieromtrent – en daarmee het collectief handelen – goed te beïnvloeden. Hiervoor is een juiste benadering noodzakelijk: maak het doorgaans als saai ervaren onderwerp leuk(er) en bespreekbaar. En net zoals bij reclame komt een positief gevoel mede door herhaling tot stand.

LBVD beschikt over een uitgebreid arsenaal aan middelen om het bewustzijn te prikkelen en te stimuleren. Op uiteenlopende wijze helpt LBVD met het ontwikkelen van betere, gevoeliger zintuigen en de juiste *mindset* bij medewerkers. Voor een hogere effectiviteit van genomen maatregelen. LBVD heeft hiervoor speciale awareness-acties ontwikkeld, welke kunnen worden ingezet in een op maat samengestelde awareness-campagne.

Doel

Het doel van de awareness-campagne is het creëren van bewustzijn bij een geselecteerde doelgroep: bewustzijn m.b.t. de nut en noodzaak van het zorgvuldig omgaan met, en het beveiligen van informatie. De specifieke doelgroepen kunnen bijvoorbeeld de 'normale' medewerkers zijn, maar ook specifiek het management, call-centre medewerkers of de systeem- en netwerkbeheerders.

Campagne

Een awareness-campagne is een project met een kop en een staart. LBVD hanteert de volgende fasering:

1. Intake
2. Nul-meting
3. Uitvoering awareness-acties
4. Rapportage, evaluatie en afronding

Intake

Tijdens de intake wordt met opdrachtgever de gehele uitvoering tot in de puntjes doorgesproken en afgestemd. Gemaakte afspraken worden vastgelegd. Ook het specifieke doel van de awareness-campagne wordt gedurende de voorbereidingsfase nogmaals met de Opdrachtgever besproken en scherp gesteld, om 1) de individuele awareness-acties beter te kunnen richten en 2) na de uitvoering van de verschillende acties terug te kunnen kijken, om vast te stellen of specifieke doelstellingen zijn gehaald.

Nul-meting

Awareness is lastig te meten. Om echter tot een beter afgestemde en daarmee de meest effectieve invulling te komen, is het wenselijk de uitvoering vooraf te laten gaan door elektronische en/of face-to-face awareness-enquêtes. Dit geeft aan het begin van het traject een goed inzicht in het bewustzijn van de doelgroep en vormt daarmee tevens een nul-meting. In de verschillende acties die gaan volgen worden de uitkomsten gebruikt, om accenten te (ver)leggen of bepaalde zaken meer aandacht te geven. De vragenlijsten voor de enquêtes komen in samenwerking met opdrachtgever tot stand. De uitkomsten van de enquêtes worden meegenomen in het evaluatierapport en vormen tevens een vertrekpunt, waartegen bereikte verbetering op een later tijdstip kan worden afgezet.

Uitvoering awareness-acties

Een awareness-campagne is op maat samen te stellen, waarbij kan worden gekozen uit een groot aantal, in karakter uiteenlopende awareness-acties uit diverse categorieën. Los van elkaar kunnen de individuele acties specifiek bedoeld zijn om te prikkelen, om kennis over te dragen, enzovoorts. De volgende tabel geeft een overzicht van mogelijke awareness-acties met hun specifieke uitwerking:

Categorie	Awareness-actie
Prikkelen	MysteryGuest Telefonische MysteryGuest Hackaanval buiten-naar-binnen of van binnen-naar-binnen Nep-virus Phishing e-mail Wachtwoorderval
Uitdagen	Security Quiz Appelflappen-race (ontmasker de MysteryGuest) Koffie-teaser
Informereren en enthousiasmeren	Demo-hack Ronde-tafelsessies Workshops (diverse doelgroepen) Communicatie-uitingen (posters, flyers, intranet, etc.) Give-aways Themabijeenkomsten Enquête

De bijlage bevat een korte toelichting per awareness-actie, gesorteerd naar uitwerking.

Rapportage, evaluatie en afronding

LBVD rondt de awareness-campagne af met een helder evaluatierapport, een evaluatiegesprek en een Verklaring van Oplevering en Acceptatie (VOA).

Rapportage

In het evaluatierapport komt tenminste het volgende aan bod:

1. De resultaten van de nul-meting;
2. Hoe de verschillende onderdelen zijn verlopen;
3. Welke leermomenten er zijn geweest voor de deelnemers;
4. Hoe er is gepresteerd en gereageerd bij de verschillende onderdelen door de deelnemers;
5. Feedback van de deelnemers;
6. Opmerkelijke observaties en bevindingen;
7. Conclusies en aanbevelingen.

Eindgesprek en VOA

In een eindgesprek met de opdrachtgever wordt het verloop van de awareness-campagne besproken en geëvalueerd. De meest markante bevindingen komen aan bod en het evaluatierapport wordt nader toegelicht. Tijdens het gesprek is volop ruimte voor vragen, extra toelichting en eventueel aanvullend advies. Opdrachtgever stelt de doelgroep voor het eindgesprek samen.

Na afloop van het eindgesprek vraagt LBVD de Opdrachtgever een Verklaring van Oplevering en Acceptatie van de bewerkstelligde resultaten (VOA) af te geven. Opdrachtgever kan hierbij aangeven of alle gegevens na afloop van de campagne dienen te worden vernietigd. Na ondertekening van de VOA is de voltooiing van de opdracht een feit.

Bijlage – Toelichting Awareness-acties

Categorie Prikkelen

MysteryGuest

Een specialist van LBVD tracht zich toegang te verschaffen tot het kantoor van Opdrachtgever en een bepaalde missie te volbrengen. Dit kan zijn het verkrijgen van toegang tot verboden ruimtes, maar ook het ontfutselen van allerlei informatie met een vertrouwelijk karakter, al dan niet met gebruik van social engineering. Het prikkelende effect zit 'm in het bekendmaken van de resultaten tijdens een later te houden, bedrijfsbrede bijeenkomst, met het tonen van bewijsmateriaal, zoals foto's, vertrouwelijke documenten, etceteras. Ook is een opzet mogelijk waarbij het doel is om te kijken hoe medewerkers handelen bij (te) opvallend gedrag. Houdt men de MysteryGuest staande en schakelt men de bewaking in?

Telefonische MysteryGuest

Wie heb ik daar aan de telefoon? Bepaalde informatie mag niet via de telefoon worden prijsgegeven. En zeker niet aan een volslagen vreemde. De telefonische MysteryGuest probeert via social engineering de medewerkers toch vertrouwelijke informatie te ontfutselen. Lukt dat? Waar gaat men de fout in? Ook hier doet een presentatie van de resultaten, bedrijfsbreed of aan een afdeling, de ogen openen.

Hack-aanval

Een hack-specialist van LBVD probeert van buitenaf of op het interne netwerk in te breken en toegang te verkrijgen tot belangrijke systemen. De resultaten worden in een interactieve workshop met systeem- en netwerkbeheerders besproken, waarbij volop gelegenheid is voor verdere toelichting, vragen en advies.

Nep-virus

Op diverse werkplekken wordt een nep-virus geïnstalleerd. En dan afwachten hoe gebruikers reageren. Ontdekken ze dat er iets mis is? Zo ja, wat is dan de reactie? Houden ze zich aan het beleid of proberen ze het op een andere manier op te lossen?

Phishing e-mail

Hoe reageren medewerkers op e-mails die erop gericht zijn vertrouwelijke informatie te ontfutselen? Hebben ze het door of geven ze bijvoorbeeld hun wachtwoord of andere geheime informatie zomaar prijs? Via listige e-mails van LBVD komt de opdrachtgever er achter.

Wachtwoorderval

Geven medewerkers makkelijk hun wachtwoord af? Via slinkse wegen en trucs proberen de specialisten van LBVD in een kort tijdsbestek zoveel mogelijk wachtwoorden te weet te komen. Vaak is maar één wachtwoord genoeg en is dus ieder bemachtigd wachtwoord er één te veel.

Categorie Uitdagen

Security Quiz

De Security Quiz is een prijsvraag waarbij een beloning plaatsvindt voor het geven van de goede antwoorden. Diverse vormen zijn mogelijk zoals deelname individueel of in teams, schriftelijk of elektronisch, met of zonder herhaling, etceteras. Een mogelijkheid is bijvoorbeeld om in de kantine de vragenlijsten op tafel te zetten, om bij de lunch discussies te ontlocken.

De Appelflappen-race

De appelflappen-race is een variant van de MysteryGuest-actie. Ze is er in deze vorm op gericht om ontdekt en aangesproken te worden. Iedereen die de MysteryGuest durft te vragen wie hij/zij is en wat hij/zij komt doen krijgt direct iets lekkers voor bij de koffie of thee!

Koffie-teaser

De mens is nieuwsgierig. De koffie-teaser maakt hiervan dankbaar gebruik. Bij de koffie-automaat (of een andere plek waar medewerkers zich dagelijks minimaal een keer ophouden) komen de resultaten van een gehouden werkplek-inspectie versluierd te hangen, met een beloning voor degene die er achter komt wat het cryptische diagram te betekenen heeft. Door dit te herhalen en geleidelijk meer informatie te verstrekken ontdekt men de relatie met clean desk, clear screen en andere zaken waar tijdens de inspectieronde op wordt gelet. En komt men er achter hoe het met de eigen werkplek is gesteld ...

Categorie Informeren en enthousiasmeren

Demo-hack

Hoe gemakkelijk is het om op een computer in te breken? Hoe gemakkelijk is het om op *jouw* computer in te breken? Met een in scène gezette demo-hack laat LBVD dit zien. Zo gemakkelijk dus ... ! Dan toch maar zorgvuldiger met zaken omgaan?

Veilig WWW

Een modulair, reeds 10 jaar bestaand zelfsturend programma waarin medewerkers en managers van één afdeling met elkaar discussieren over nut & noodzaak van informatiebeveiliging. Dat is Veilig WWW. Acht modules met elk een psychologie proefschrift als onderliggende theorie, die er samen voor zorgen dat er begrip ontstaat. En vanuit dat begrip weten. En willen. Zo is de naam van dit product ontstaan: Veilig Weten, Willen, Worden!

Rondetafelgesprek

Hebben we een (beveiligings)probleem? Zo ja, wat kunnen we er aan doen? Hoe gaan we het doen? Via begeleidde rondetafelgesprekken kunnen problemen worden getackeld en kan ervoor worden gezorgd dat de neuzen dezelfde kant op wijzen.

Workshops en training

In tegenstelling tot het volgen van een cursus met veel leeswerk of het aanhoren van een docent, is de bedoeling van workshops en trainingen om medewerkers bij de hand te nemen en flink te laten stoeien met materie. Begeleidt door een ervaren deskundige. Laat management met elkaar in de clinch gaan over controversiële stellingen, laat beheerders vertellen hoe zij denken de IT-omgeving veiliger, zo niet

het veiligst te maken, en doop call-centre- of helpdeskmedewerkers in een 'social engineering-bad'. Met juiste invulling nemen de deelnemers niet alleen kennis van informatiebeveiliging, maar ervaren zij het ook intensief.

Communicatie-uitingen (posters, flyers, etceteras)

Informatiebeveiliging moet aan de medewerkers worden verkocht. Ze zullen er zelf niet snel om vragen. De communicatie die hier voor nodig is, is vergelijkbaar met het maken van reclame. Het AIDA(S) principe – Attention, Interest, Desire, Action en Satisfaction – in combinatie met herhaling leent zich dan ook goed. Hang bijvoorbeeld prikkelende posters op op verschillende plaatsen waar medewerkers (liefst gezamenlijk) tijd doorbrengen, zoals bij de koffieautomaat, in de lift en/of in de kantine. Leg beveiligings-placemats in de kantine, enzovoorts. Mogelijkheden te over om het onderwerp onder de aandacht te brengen.

Give-aways

Mensen zijn dol op gadgets. Een goed gekozen give-away krijgt een plek op de werkplek en herinnert de medewerkers dagelijks aan informatiebeveiliging.

Themabijeenkomsten

Informatiebeveiliging is iets van de hele organisatie, van onder tot boven, van afdeling x tot y. Het is goed dit tot uiting te laten komen in themabijeenkomsten met alle medewerkers. Het is belangrijk de bijeenkomsten aantrekkelijk en levendig te maken, bijvoorbeeld door de resultaten of uitkomsten van voorafgaande awareness-acties bekend te maken – zoals prijswinnaars, de scores van verschillende afdelingen, hilarische zaken, etceteras - of een act op te nemen. LBVD kan zorgdragen voor een goede, complete aankleding, bijvoorbeeld met een demo-hack of door het inschakelen van een zakkenroller of acteurs.

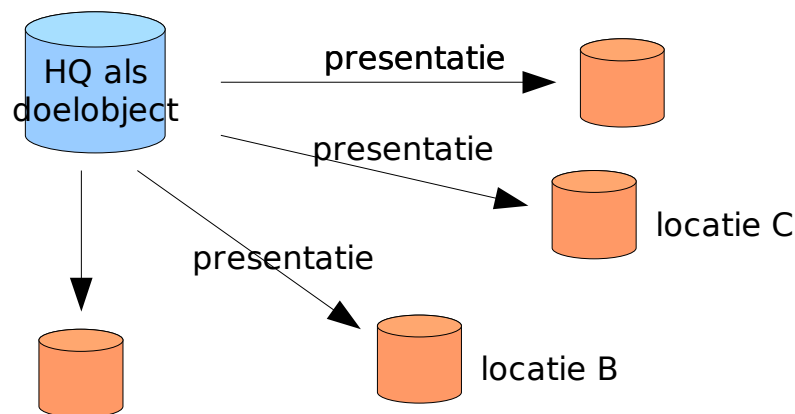
Online IB Peiling en Face-to-Face gesprekken

'Hallo, mag ik u wat vragen over informatiebeveiliging?'. Naast het verkrijgen van inzicht kan het stellen van gerichte vragen bewust een verborgen agenda krijgen. Door het stellen van gerichte vragen moet de geïnterviewde nadenken over een aantal zaken waar hij/zij niet dagelijks bij stilstaat, maar waarvan het wel wenselijk is dat hij/zij er een keer goed over nadent. Zeker het management zal proberen de vragen goed te beantwoorden en dus eerst grondig nadenken alvorens antwoord te geven. Zulk een enquête kan zowel face-to-face als elektronisch worden afgenomen, waarbij face-to-face bewerkelijker is, maar tegelijk het voordeel heeft dat directe terugkoppeling en discussie mogelijk is (twee-weg i.p.v. één richting).

Bijlage – Informatie-Beveiligings-Week

Speciaal voor ondernemingen en organisaties die groter en/of geografisch verdeeld zijn (500+ medewerkers) is de Informatie-Beveiligings-Week (IBW) ontwikkeld.

Een IBW (niet noodzakelijk in één week onder te brengen) is feitelijk een opeenvolging van awareness-acties gedurende een langere periode, bij afzonderlijke afdelingen of op aparte locaties.



Een IBW maakt gebruik van de typisch Nederlandse eigenschap humor te zien in de vergissing van 'een ander'. Tegelijk is IBW op zichzelf een continu herhalingsmodel.

Uitvoering

Net als bij elke gewone awareness campagne worden doelen vastgesteld, een campagneplan opgezet, en diverse awareness-acties voorbereid. De acties worden vervolgens in een opeenvolgende periode bij één bepaalde doelafdeling of doellocatie uitgevoerd. Een plenaire presentatie ter plaatse van de bevindingen sluit het deel af.

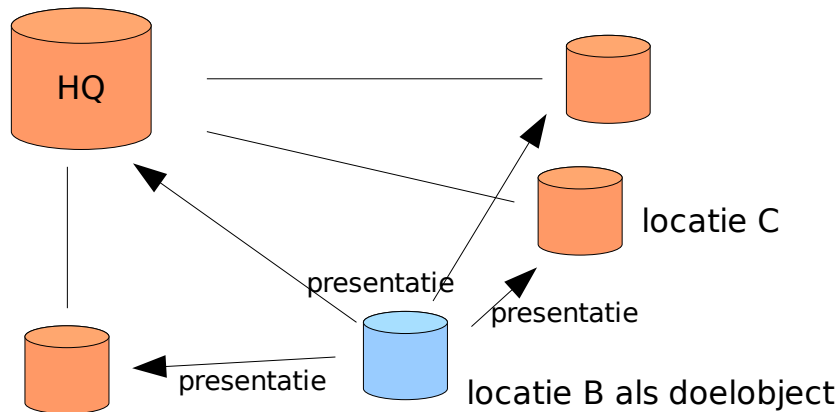
De bevindingen worden echter tevens (deels) gecommuniceerd aan de overige afdelingen of locaties. De communicatie kan op velerlei manieren geschieden. Effect van deze handelwijze is dat de andere locaties kennis nemen van (gesimuleerde) incidenten van naaste collega's – in feite gelijkgestemden (dit kan mij ook gebeuren).

Hier gebeuren twee dingen: men vormt zich een mening, en zet deze af tegen de gangbare norm. De mening kan slechts worden gevormd bij afdoende kennis (dit lokt wellicht vervolgactie uit als vragen stellen, kennisvergaring, etc.). Afzetten tegen de eigen (of *corporate*) norm heeft vaak tot gevolg dat er hilarisch wordt gereageerd. Dit zijn vaak reacties die in groepsverband worden beleefd. En is dat niet net wat je wilt bereiken? Informatiebeveiliging tot een groepsgevoel maken?

Deze hilariteit is deel van het succes! Een keer goed lachen om de 'domheid' van een ander(e afdeling) blijft in de praktijk veel langer hangen dan de stok achter de deur van De Baas of de regelgeving¹.

¹ Neem het voorval 'Joost Tonino'! Dat is inmiddels meer dan 2 jaar geleden, maar men herinnert zich de situatie meestal nog precies. En ook waarom het niet kon. Er is veel over gesproken en

Na verloop van tijd wordt dezelfde set acties bij een andere afdeling of doellocatie herhaald. Met hetzelfde gevolg in presentatie: alle afdelingen of locaties krijgen wederom (een deel van) de resultaten te zien. Op die manier is gedurende een langere periode met relatief weinig middelen een goed voor te bereiden awareness campagne tot een succes te maken.



De organisatie zal merken dat de volwassenheid aangaande informatiebeveiliging toeneemt. De boodschap komt helder over. Het begrip groeit, er wordt minder lacherig over gedaan. Het 'Not My Problem' wordt – veel meer 'Niet **Alleen** Mijn Probleem'.

Hiermede is de basis gelegd voor acceptatie en naleving van de huisregels. En de opvolging ervan. Er ontstaat een meer open cultuur, waarin mensen elkaar wél durven aanspreken op gedrag.

Het draagvlak dat hiermede is gecreëerd kan enerzijds worden gebruikt voor opvolging van de huidige regels, maar is in de praktijk ook prettig bij het invoeren van nieuwe maatregelen: doordat men weet waar het om gaat.

LBVD helpt!

LBVD beschikt over de kennis, ervaring en middelen om penetratietesten in uiteenlopende vormen te verzorgen.

Meer weten? Neem contact op met Hans Labruyère voor de tariefstelling en bijzondere mogelijkheden. E-mail info@lbvd.nl, tel. 015-2682533.

indertijd heeft iedereen zich vast afgevraagd of en hoe dit soort dingen in de eigen organisatie zijn geregeld ...