Cyber
Weerbaarheidscentrum
Greenport

Cyberbewustwording: stappenplan opzetten van een cyberbewust-wordingscampagne

Cyberbewustwording

De meeste cyberincidenten ontstaan door menselijke fouten. Cybercriminelen maken slim gebruik van naïviteit en gemakzucht die de gemiddelde mens niet vreemd is. Bewustzijn van cyberrisico's is dus heel belangrijk voor het voorkomen van incidenten.
Verkeerd omgaan met inloggegevens en wachtwoorden, het gebruik maken van gratis online en mogelijk onveilige Cloud-diensten, het onbedoeld verspreiden van gevoelige informatie via privémail of het printen van gevoelige documenten op onbeheerde printers. Het klinkt onschuldig, maar deze voorbeelden kunnen leiden tot serieuze cyberincidenten. Het is daarom belangrijk dat informatiebeveiliging onderdeel wordt van de dagelijkse routine.

Campagne opzetten voor cyberbewustwording

Hoe werk je structureel aan de cyberbewustwording van je organisatie? Met een cyberbewustwordingscampagne, zie verder in dit document.

Adviezen voor het creëren van cyberbewustwording
Hieronder een aantal adviezen en aandachtspunten voor het creëren van cyberbewustwording binnen je organisatie.

- **What's in it for me?**

Het veranderen van gewoontes is niet zo makkelijk. Het vraagt om een positieve basishouding ten opzichte van het onderwerp informatieveiligheid. Het is belangrijk om concreet te maken wat de positieve effecten zijn van de nieuwe gewoonte. Kort gezegd, 'what's in it for me?'.

- **Prikkel continu de alertheid voor cybersecurity**

Informatieveiligheid is een uitdaging die continue alertheid en aandacht vraagt. Dat komt mede door de snelle technologische ontwikkelingen. Als de schade al is aangericht, is het te laat. Het is belangrijk om constante alertheid te prikkelen. Ook een campagnematige aanpak, werkt. Zie ons stappenplan voor het opzetten van een bewustwordingscampagne.

- **Vergroot kennis en maak mensen bewust van cybercrime**

Hoe kun je de alertheid van bestuurders, managers en medewerkers op gebied van informatieveiligheid vergroten en ervoor zorgen dat zij ook veilig handelen? In eerste instantie zal dit gedaan moeten worden door het vergroten van de kennis van collega's over de mogelijke risico's, waarbij de ene gewoonte (geen alert veiligheidsbewustzijn) vervangen dient te worden door de andere (alertheid). Als je bijvoorbeeld nooit iets met veiligheid hebt hoeven doen in je werk, is het van belang dat je een informatieveilige omgeving creëert. Dit doe je door reële situaties te schetsen die dicht bij de mens staan. Dit kan door middel van een doorlopende bewustwordingscampagne met als doel het bewustzijn van collega's te vergroten en hun gewoontes te veranderen.

- **Wacht niet totdat het te laat is**

Kortom, kies een aanpak die er op gericht is om (alle) collega's bewust te maken van, en alert te houden op de risico's die zij lopen; wat zijn de risico's en wat kun je en moet je zelf doen om die te beperken? Mobiliseer het management, want betrokken management zal zorgen voor een gedragen bewustwordingscampagne. Daarnaast is het uiteraard belangrijk om de kennis en de bijbehorende gewoontes te toetsen, zodat de maatregelen - indien gewenst per afdeling of onderwerp - hierop kunnen worden bijgesteld. Dus, wacht niet tot het te laat is en maak van de zwakste schakel - de mens -, je sterkste wapen.

Hoe maak je je medewerkers bewust van de risico's van digitaal werken? In dit stappenplan leggen we je uit hoe je een bewustwordingscampagne opzet.

1. Mobiliseer stakeholders binnen je organisatie

Een kritische succesfactor voor een bewustwordingscampagne binnen je organisatie is het mobiliseren van stakeholders. Het management is hierin een van de belangrijkste stakeholders. Het management zorgt immers voor budget, tijd en middelen voor de campagne. Daarnaast vervult het management een voorbeeldfunctie voor de organisatie. Wanneer zij achter de campagne staan, zal de acceptatie binnen de organisatie voorspoediger verlopen.

2. Breng de informatiebeveiligingsrisico's van je organisatie in kaart

Een belangrijke eerste stap is het in kaart brengen van de informatiebeveiligingsrisico's binnen je organisatie. De keuze om risico's te negeren, onderschatten of te elimineren kan helpen bij het maken van keuzes binnen de bewustwordingscampagne. Uit de risico's vloeit logischerwijze een onderwerpenlijst waar de campagne op gebaseerd kan worden.

Tip: Organiseer een enquête

Risico's kunnen in kaart gebracht worden door ICT-specialisten. Maar je kunt ook de rest van de organisatie erbij betrekken, met bijvoorbeeld een enquête. Met behulp van een enquête kan je toetsen hoe je medewerkers omgaan met informatie. De uitkomsten hiervan kun je inzetten voor de agendavorming van de campagne. Op deze manier blijft het geen 'ICT-feestje' en wordt je hele bedrijf bij de campagne betrokken. Een enquête kan ook als een vertrekpunt van je campagne fungeren, als nulmeting. Jaarlijks kan er zo getoetst worden of je campagne effectief is.

3. Kies de juiste doelgroep voor je bewustwordingscampagne

Om je medewerkers doeltreffend te bereiken, is het verstandig om onderscheid in verschillende doelgroepen te maken. Deze doelgroepen hebben ieder een eigen aanpak nodig om het gewenste effect te bewerkstelligen. Binnen je organisatie kan je bijvoorbeeld denken aan doelgroepen als:

- Management (denk aan: CEO fraude)
- Secretaresses (denk aan: social engineering)
- HR (denk aan: instroom en uitstroom van medewerkers)
- Ontwikkelaars (denk aan: security by design/default)

4. Kies het gewenste effect van je bewustwordingscampagne

Per doelgroep is het verstandig om een bepaald gewenst effect te definiëren. Wat is het doel dat je wilt bereiken? Wil je kennis bijbrengen? Wil je de houding van je medewerkers ten opzichte van bepaalde thema's veranderen of wil je hun gedrag veranderen?

Een van de klassieke communicatiemodellen om een doelgroep te mobiliseren is het zogenaamde model kennis-houding-gedrag. In dit model herkennen we een lineaire hiërarchie, bestaande uit 3 elkaar volgende fases: kennis, houding, gedrag. In de eerste fase probeert men via communicatie mensen eerst te informeren. Als ze voldoende kennis bezitten, is daarmee de basis gelegd voor de verandering van de houding in de gewenste richting. En als mensen een positieve attitude hebben, zullen ze geneigd zijn het gewenste gedrag aan te nemen.

Kennis: wat weet de doelgroep over het nieuwe gedrag?

- Informatie verschaffen
- Kennistekorten wegwerken

- Weerleggen van onjuiste kennis

Houding: welke gevoelens heeft de doelgroep ten opzichte van dit gedrag?

- Positieve gevoelens versterken
- Negatieve gevoelens afzwakken
- Gewenst gedrag sterker positioneren
- Belang van voordelen gewichtiger maken

Gedrag: wat is de actiebereidheid van de doelgroep?

- Ervaringen laten opdoen
- Belemmeringen wegwerken
- Ondersteuning door de omgeving

Het gewenste effect dat je met je campagne wilt bewerkstelligen, gaat hand in hand met welk middel je inzet.

5. Kies het juiste middel om je bewustwordingscampagne uit te voeren

Mensen leren verschillend en onthouden dingen beter als ze een onderwerp op verschillende manieren krijgen aangeboden. Zo werkt het hoofd van de mens immers. Belangrijk dus om tijdens een bewustwordingscampagne goed na te denken welke middelen je voor welke doelgroep inzet. Er zijn namelijk diverse middelen die ingezet kunnen worden, denk aan: media (intranet, blogs), evenementen, workshops, activiteiten, fysieke middelen (posters, flyers), phishingtest, enquêtes, e-learning, serious gaming en trainingen.
Elke doelgroep spreekt een andere 'taal'. Het is heel belangrijk je middelen en boodschap hierop af te stemmen om deze groepen op een effectieve manier te bereiken.

6: Kies de juiste boodschap voor je bewustwordingscampagne

Om onze gewoontes te veranderen, moet het ons ook iets opleveren. We moeten de positieve impact van informatieveiligheid voelen en zien. Om dit te bewerkstelligen is het dus belangrijk dat je het dicht bij de doelgroep brengt en concreet en persoonlijk maakt. Anders blijft het voor velen een 'ver van mijn bed show' en blijft het makkelijk af te schuiven als een ICT-feestje.
Het is daarom belangrijk dat je weet welke 'taal' elke doelgroep spreekt, welke belangen er spelen, welke behoeften er zijn. Om hier achter te komen is het wellicht een idee om met ambassadeurs te gaan werken. Zo kan elke doelgroep een bewustwordingscampagne-ambassadeur hebben om inzicht in de doelgroep te geven en als koppelstuk tussen ICT en de business te fungeren.

Middelenmatrix

Om bovenstaande overzichtelijk weer te geven kan gebruik gemaakt worden van een middelenmatrix. Dit is een combinatie van alle media, evenementen, activiteiten, die ingezet kunnen worden om communicatiedoelen van een campagne te bereiken.

Doelgroep	Gewenste effect	Boodschap	Middel

Dit document is gebaseerd op het document 'Stappenplan Opzetten van een cyberbewustwordingscampagne' en 'Cyberbewustwording' van het Digital Trust Center. De originele documenten zijn te vinden via https://www.digitaltrustcenter.nl/stappenplan-cyberbewustwordingscampagne en https://www.digitaltrustcenter.nl/informatie-advies/cyberbewustwording