Auteur: Bas Schiltmans is Chief Technology Officer (CTO) van KCM Group. Hij is van huis uit bedrijfskundige en heeft enkele decennia ervaring in vele functies binnen ICT-omgevingen. Bas Schiltmans is bereikbaar onder: welcome@kcmgroup.eu.

Medewerkersbewustzijn is meer dan een training

Veel organisaties steken een groot deel van hun inspanningen om veiliger te werken in zaken als techniek en formele organisatie. Belangrijk, maar al deze inspanningen zijn echter van beperkte waarde als medewerkers niet in staat zijn op een veilige manier om te gaan met (ICT-)hulpmiddelen die ze daarin ondersteunen.

Een veilige manier zou bijvoorbeeld kunnen zijn: vergaande technische anti-phishingmaatregelen met sluitende formele procedures hoe je moet handelen wanneer je zo'n phishing e-mail ontvangt. Als er toch een mail door het technisch net slipt en bij een medewerker terechtkomt die niet weet hoe hiermee om te gaan, is er een grote kans op een veiligheidsincident.
Er ligt dus een grote uitdaging voor organisaties om ervoor te zorgen dat medewerkers qua kennis en gedrag opgewassen zijn tegen de bedreigingen die op ze afkomen op het gebied van veilig werken met gegevens. Veel organisaties doen nog helemaal niets aan medewerkersbewustzijn, andere organisaties grijpen voor het initieel op peil brengen van het bewustzijn instinctief vaak naar trainingsmiddelen als e-learning. Een eenmalige training met een toets die bewijst dat mensen weten wat ze moeten doen. Soms worden deze trainingen en toetsen periodiek herhaald om de kennis beter te laten beklijven, maar dit gebeurt dan meestal niet heel vaak en met relatief lange tussenpozen.
Wanneer je het 10-20-70 model (1) toepast, wordt duidelijk dat alleen formeel leren niet de benodigde langetermijneffecten zal hebben om kennis en gedrag continu te verbeteren. Tenminste 70% van het leren vindt volgens dit model immers plaats buiten formele leeromgevingen. Slechts 10% in de formele leeromgeving, dus e-learning.

De vergeetcurve van Ebbinghaus (2) maakt ook duidelijk dat eenmalig trainen met eventuele periodieke herhaling met wat langere tussenpozen niet voldoende is om praktisch kennis en gedrag van medewerkers structureel te verbeteren. Mensen vergeten dingen die ze in dit soort formele training geleerd hebben heel erg snel. Een keer per kwartaal herhalen en toetsen is dus eigenlijk veel te weinig, als je dit beschouwt.
Wanneer dan ook nog de implicaties van de zaken die door neurowetenschapper Erik Schoppen zijn aangedragen in zijn publicatie in iB-Magazine uit 2019 (3), blijkt nog duidelijker dat alleen formeel trainen echt onvoldoende is. Uit zijn betoog volgt onder andere dat gedragsverandering continue aandacht en herhaling vereisen. Mensen reageren met het primaire deel van hun hersenen – het zgn. reptielenbrein – op veiligheidsdreigingen en vragen om informatie. Het aanpassen van dit primaire gedrag is bijzonder lastig. Wat we leren in het rationele deel van ons brein passen we maar moeilijk toe in situaties waarin het primaire deel klakkeloos reageert. Om gedrag te veranderen is continue aandacht en oefening nodig. Dit benadrukt hoe belangrijk het is om meer te doen dan een 'standaard' training. Idealiter zouden we ervoor moeten zorgen dat primaire reacties veranderen. Op zijn minst willen we een situatie creëren waarin herkenning optreedt van situaties waarin de primaire reacties tot verkeerde resultaten leiden. We willen dan een bewustwordingsmoment creëren bij de medewerker om de ratio aan te kunnen spreken. Dit is een intensief proces waarin het in elk geval heel belangrijk is om met zo groot mogelijke regelmaat het onderwerp onder de aandacht van de medewerker te brengen en zo mogelijk te oefenen. Al met al een onmogelijke opgave om de zogenaamde human firewall van je organisatie op peil te brengen en te houden met alleen af en toe eens trainen.

Bewustzijnsverbetering

Wat zou je als organisatie kunnen doen om bewustzijn, kennis en gedrag te vergroten op het gebied van veilig werken met gegevens? Relevante kennis beschikbaar stellen aan je medewerkers is belangrijk. E-learning is en blijft hierbij een heel belangrijk startpunt maar voor echte bewustzijnsverbetering is meer nodig.

Hierbij een aantal uitgangspunten:

- De kennis moet begrijpelijk zijn. Soms wordt de fout gemaakt strikt formele procedures en instructies uit bijvoorbeeld een ISMS zonder filter aan medewerkers van alle niveaus in de organisatie te geven. Dit is een veel te hoge drempel voor velen. Denk aan het vertalen van relevante zaken in jip-en-janneketaal zodat elke medewerker deze makkelijk tot zich kan nemen.

- De kennis moet hapklaar zijn. Wanneer kennis alleen te volgen is in de vorm van een langdurige e-learning of langdradig document, zal dit voor veel medewerkers een te hoge drempel zijn. Ze zullen deze kennis wellicht initieel nog wel tot zich nemen, maar in hun dagelijkse werkpraktijk kunnen ze er weinig mee, omdat ze de informatie vaak snel nodig hebben. Denk hier aan korte beschrijvingen, tips-and-tricks; liever niet langer dan een paar schermen om te lezen.

- De kennis moet zo compleet mogelijk en actueel zijn. Wanneer kennis niet compleet en actueel wordt gehouden zullen mensen snel interesse verliezen en het nut er niet meer van inzien.

- De kennis moet eenvoudig te vinden zijn. Een centrale plek; goede zoekmogelijkheden liggen voor de hand. Nog veel beter is het om de kennis te koppelen aan zaken die medewerkers in hun werk tegenkomen. Denk bijvoorbeeld aan het koppelen van instructieteksten en reminders binnen 'normale' werkinstructies, checklists of zelfs in het scherm van bepaalde applicaties waarmee mensen werken.

Zoals vanuit het 10-20-70 model blijkt, leert men het meeste tijdens het toepassen in het werk. Naast het beschikbaar stellen van kennis is het belangrijk ervoor te zorgen dat mensen snel en eenvoudig contact kunnen krijgen met ondersteuning wanneer zij zaken niet (tijdig) zelf kunnen vinden, zaken aantreffen die niet specifiek beschreven staan of twijfelen. Een open bedrijfscultuur waardoor mensen zich niet bezwaard voelen hulp in te schakelen en een laagdrempelige manier van contact vinden en maken is hierbij van groot belang. Zorg dus voor informatie over de beschikbare communicatiemogelijkheden op de plaatsen waar mensen deze nodig hebben. Een telefoonnummer verstopt op het intranet is niet voldoende!

Uiteraard is alleen kennis beschikbaar stellen niet voldoende. Mensen moeten getriggerd worden om de kennis te consumeren. Het liefst zo vaak mogelijk. Dit kan door kennis op te nemen op logische plaatsen in werkprocessen zoals hierboven beschreven, maar er is meer mogelijk:

- Regelmatige simulaties helpen om gedrag te conditioneren zodat mensen (zonder te veel gevaar) geconfronteerd worden met de gevolgen van hun acties. Phishingsimulaties en telefoongesprekken waarin social hacking wordt gesimuleerd zijn goede voorbeelden. Let op, met name de tweede genoemde optie kan een relatief dure vorm van bewustzijnsverhoging zijn.
- Games waarin bewustzijn wordt getest kunnen een goede en leuke manier zijn om mensen duidelijk te maken welke zaken ze nog niet goed genoeg weten of doen. Een competitief element kan sommige mensen enorm stimuleren om meer te willen weten of het beter te doen. Belangrijk is wel dat in deze games dan ook terugkoppeling is naar de eerder besproken kennis.
- Zeer regelmatig toetsen. Door bijvoorbeeld elke week op een gemakkelijke manier één vraag stellen. Als hierbij ook wordt uitgelegd wat het goede antwoord zou zijn geweest als iemand een fout antwoord kiest en een gemakkelijke verwijzing wordt gegeven naar bijbehorende kennis, wordt dit nog effectiever.

Een belangrijk aspect bij bovenstaande manieren om mensen te activeren is de tijd die het hen kost. Voor de meeste organisaties is veilig werken met gegevens belangrijk, maar zeker niet de core business. Men is in de praktijk vaak huiverig om hier veel aan te doen met het idee dat dit te veel 'productietijd' van medewerkers opslokt. Het is daarom heel belangrijk om weloverwogen keuzes te maken uit de verschillende manieren om mensen bij het onderwerp te blijven betrekken. Effect versus kosten en tijdsbeslag is daarbij dan een belangrijke factor. Het kostenplaatje zou voor veel – met name kleinere –organisaties sowieso een beperkende factor kunnen zijn om medewerkersbewustzijn zo veelomvattend op te pakken, ondanks het belang. Daarom moet zoveel mogelijk naar standaardisatie worden gezocht. Als elke organisatie het wiel opnieuw gaat uitvinden zal dit onvermijdelijk leiden tot suboptimale oplossingen en onnodige kosten. Zorg dus voor:

- Een bestaande bron van kennis uit de markt die ook actueel wordt gehouden. De meeste kennis die hier benodigd is, is voor vrijwel elke organisatie hetzelfde. Een kleiner deel is organisatie-specifiek. Deze kun je dan toevoegen. Dit scheelt uiteraard enorm in het opbouwen en onderhouden van alle benodigde kennis.

- Standaard technische hulpmiddelen om je te helpen met het continue triggeren van je medewerkers zonder dat dit telkens veel tijd kost om te organiseren.

- Een geïntegreerde set van hulpmiddelen zodat de gegevens die je hieruit wilt registreren om je organisatie te sturen en je acties aantoonbaar te maken voor stakeholders als directie, klanten, auditors en worst case de Autoriteit persoonsgegevens, centraal en met minimale moeite te produceren zijn. Naast het verbeteren van kennis en gedrag van je medewerkers is dit aantoonbaar doen immers bijna net zo belangrijk.

Door bovenstaande te implementeren is het mogelijk medewerkersbewustzijn over veilig werken met gegevens naar een hoger plan te tillen in je organisatie. Duidelijk is ook dat hiermee veel meer bereikt wordt dan met alleen die eerste training. En dat binnen rede voor tijdsbeslag van medewerkers en kosten.

Referenties

(1) https://702010institute.com/702010-model/
(2) https://en.wikipedia.org/wiki/Hermann_Ebbinghaus
(3) Artikel Keynote speech Erik Schoppen en interview in iB-Magazine 3 2019