Het is tegenwoordig al lang niet meer de vraag óf je als organisatie slachtoffer wordt van incidenten op cybersecurity-vlak, maar vooral 'wanneer'. Honderd procent veilig bestaat natuurlijk niet, want ook 'cybercrime' is inmiddels de hobbyfase voorbij. Elke organisatie doet er daarom wijs aan om te bouwen aan een sterke informatieveilige omgeving. Zowel op het vlak van techniek als op het vlak van de mens.

tekst Marlies Schamper

Van zwakste schakel naar sterkste wapen

Slim omgaan met informatieveiligheid

Informatieveiligheid staat pas echt in haar kracht als alertheid de achterliggende techniek kan versterken. Het is om die reden belangrijk dat elke collega binnen een organisatie doordacht en vooral slim leert omgaan met informatieveiligheid. De hamvraag is natuurlijk, hoe krijg je zo'n onderwerp in de dagelijkse routine van een organisatie als veiligheid niet echt tot de kern van je organisatiecultuur behoort?

DAGELIJKSE LEVEN

Digitale technologie is onderdeel van ons dagelijks leven geworden. Hiermee is het onderscheid tussen werk en privé verdwenen. Bovendien zijn we ongemerkt op alle vlakken sterk afhankelijk geworden van deze digitale informatievoorziening. Denk aan het Internet of Things, waarbij innovatieve functionaliteiten en andere nieuwe diensten via je telefoon, smartwatch, televisie, koelkast of auto elkaar in rap tempo opvolgen. Opmerkelijk en wellicht het gevolg van deze snelle ontwikkelingen, is het feit dat er in eerste instantie weinig oog lijkt voor privacybescherming en informatievei-

‘Bewustwording op informatieveiligheids-vlak is een continuproces’

ligheid. Zo berichten de media bijna wekelijks over incidenten op informatieveiligheidsvlak. Of het nu gaat om het lekken van persoonsgegevens, identiteitsfraude, cyberaanvallen, digitale fraude, cyberspionage, phishing, digitaal pesten… de media staan er bol van.

In het merendeel van de gevallen blijkt de mens de zwakste schakel te zijn. En cybercriminelen maken slim gebruik van deze naïviteit en gemakzucht die de gemiddelde mens niet vreemd is. Het 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 zijn maar een paar voorbeelden waar diezelfde gemiddelde mens zich af en toe met zekerheid schuldig aan zal maken. Het feit dat we bovendien steeds meer tijd-, plaats- en apparaatonafhankelijk werken, helpt hier zeker niet bij. Lang verhaal kort, bij deze vrijheden horen helaas ook nieuwe verantwoordelijkheden. En de eerste stap is niet anders dan in andere bewustwordingstrajecten (herinnert u zich de introductie van de verplichte autogordels nog in de jaren 70?): bewustwording van de échte risico’s, hoe ver af ze ook lijken. Kortom, ook cybersecurity start bij bewustwording; What’s in IT for me?

MENSEN ZIJN GEWOONTEDIEREN

Het veranderen van onze gewoontes is helaas niet zo makkelijk als het lijkt. Als mens gedijen we namelijk goed bij gewoontes, dat geeft ons de ruimte om te focussen op zaken die er echt toe doen. De oplossing is dus eigenlijk simpeler dan we vaak denken. Gewoontes moet je niet proberen te stoppen, dat gaat je niet lukken. Gewoontes moet je simpelweg vervangen door nieuwe gewoontes. Want het goede nieuws; gewoontes zijn allemaal ooit een keer aangeleerd.

NAAR ONBEWUST BEKWAAM

Het veranderen van oude gewoontes in nieuwe vraagt in dit geval natuurlijk om een positieve grondhouding ten opzichte van het onderwerp informatieveiligheid, óf om gevoelde spanning als het gaat om de negatieve effecten ervan op jezelf als mens. Het is dan ook belangrijk om concreet te maken wat de positieve effecten zijn van de nieuwe gewoonte. Kort gezegd, ‘what’s in it for me?’. 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 mens 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.

BURNING PLATFORM

Uw organisatie kan natuurlijk ook wachten tot het fout gaat. Dat helpt in ieder geval als het gaat om alertheid verhogen. Denk maar terug aan de DigiNotar Hack in 2011. DigiNotar verzorgde de PKI overheid-certificaten voor grote delen van de Nederlandse overheid. Er was al geruime tijd bekend dat hier veiligheidsissues speelden. Toch moest het tot een crisis komen om veel overheidsorganisaties in acute staat van paraatheid te brengen en stappen te laten zetten op informatieveiligheidsvlak. Als je korte termijn actie nodig hebt, kunnen negatieve emoties dus zeker helpen. Uiteraard gaat het bij informatieveiligheid, mede door de snelle technologische ontwikkelingen, om een uitdaging die continue alertheid en aandacht vraagt, en niet pas nadat de schade al is aangericht. Dit type verandertrajecten vraagt niet om snelle acties, maar om het prikkelen van constante alertheid. Om een campagnematige aanpak, dicht op de huid van ons als mens. Een gewaarschuwd mens telt immers voor twee. Maar uiteraard kunt u er ook voor kiezen deze handschoen niet op te pakken en te wachten tot er zich een incident voordoet, dan weet u in ieder geval zeker dat een paar kortetermijnacties gerealiseerd gaan worden. Maar besef wel dat een incident kan leiden tot materiële en immateriële schade voor uw organisatie. Reputatieschade is de meest voorkomende vorm van schade, maar ook de vorm die het meest eenvoudig te voorkomen is. De kans op een crisis is groter en dichterbij dan u vermoedt. Dus waarom wachten tot het te laat is?

JE STERKSTE WAPEN

Maar hoe kunt u de alertheid van bestuurders, managers en medewerkers op informatieveiligheidsvlak 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. Het vergroten van de bewustwording ten aanzien van de risico's en mogelijke maatregelen kan vervolgens helpen om in besluitvormingstrajecten de aspecten voor informatieveiligheid zorgvuldiger af te wegen.

Bewustwording op informatieveiligheidsvlak is een continuproces, gericht op het opbouwen en ondersteunen van een beveiligingspositieve omgeving. Continu, omdat aan de ene kant het gevaar evolueert en aan de andere kant omdat (consequente en consistente) herhaling van de boodschap het leereffect vergroot en het onderwerp vooraan in het hoofd houdt. Tevens leren mensen verschillend en onthouden zij 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 meerdere middelen in te zetten.

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? 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, uw sterkste wapen. ■

Marlies Schamper is specialist in verander- en bewustzijnstrajecten en het domein Informatieveiligheid bij soul:made