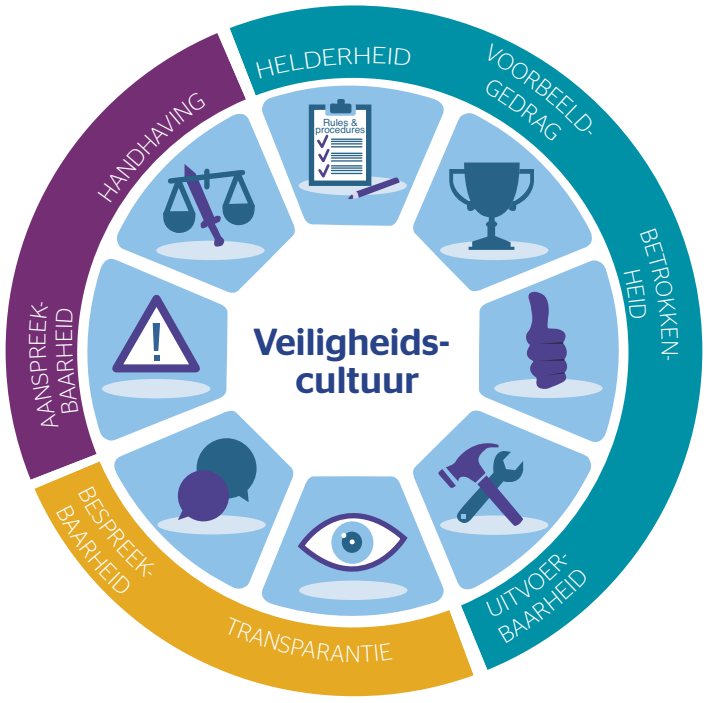
Serious gaming: het nieuwe opleiden?

‘Serious games’ zijn in opkomst als het gaat om het trainen en opleiden van medewerkers. De Cybercheck-security-awareness-game van KPMG en G4S is hiervan een goed voorbeeld. Doel is om medewerkers vertrouwd te maken met de verschijningsvormen van cybercriminaliteit en een cultuur te creëren waardoor organisaties in staat zijn efficiënt dit soort aanvallen te pareren.

tekst Matthieu Paques



Door middel van verschillende interventies en activiteiten kan de (veiligheids)cultuur op elk van acht gedragsdrijvers gemeten en versterkt worden.

U heeft ongetwijfeld een veelvoud aan artikelen gelezen waarin staat dat de mens traditioneel de zwakste schakel van de informatiebeveiliging is. Niet voor niets is de mens het favoriete en belangrijkste doelwit van cybercriminelen geworden. Mensen klikken nu eenmaal op verkeerde links, openen besmette bestanden of geven inloggegevens gemakkelijk aan derden.

Vele organisaties onderkennen dit en zetten meer en meer in op bewustwordingscampagnes gericht op eindgebruikers. Niet alleen voor de eigen medewerkers, maar zeker ook voor klanten en burgers. Vaak via voorlichtingscampagnes, aangevuld met allerlei e-learning-toepassingen. Maar deze traditionele methoden blijken in de praktijk een beperkte effectiviteit te hebben. Zo beperkten veel e-learnings zich tot het realiseren van bewustwording, zonder ook een structurele gedragsverandering na te streven.

ZWAKSTE SCHAKEL

Maar er is ook goed nieuws. De zwakste schakel (de mens) kan uw sterkste wapen tegen cybercriminaliteit worden. *Serious games* zijn een bewezen effectief antwoord op een aantal van deze beperkingen van traditionele e-learning-programma’s en zijn dan ook sterk in opkomst. Specialisten van KPMG en G4S hebben een security-awareness-game ontwikkeld waarin zeer uiteenlopende verschijningsvormen van bedreigingen uit het digitale en fysieke domein samenkomen. Doel is om medewerkers vertrouwd te maken met de verschijningsvormen van cybercriminaliteit en een cultuur te creëren waardoor organisaties in staat zijn efficiënt te reageren op dit soort aanvallen.

IN DE GAME KOMEN VERSCHILLENDE SCENARIO'S AAN BOD

VERGROTEN EFFECTIVITEIT

Om de aangeleerde kennis en vaardigheden ten aanzien van de omgang met vertrouwelijke informatie ook in de praktijk te laten brengen, is een structurele gedragsverandering nodig bij medewerkers. Immers, wanneer een medewerker het gewenste gedrag kan vertonen, maar dat niet *wil, durft*, of *niet belangrijk vindt*, blijft het gewenste effect uit. Denk bijvoorbeeld aan de situatie van de medewerker die bang is voor negatieve consequenties (*handhaving*), het niet durven aanspreken van leidinggevenden op risicovol gedrag (*aanspreekbaarheid*), medewerkers die zich niet verantwoordelijk voelen voor informatiebeveiliging (*betrokkenheid*) of onvoldoende tijd, middelen of procedures hebben om beveiligingsincidenten te melden (*uitvoerbaarheid*).

De basis voor de gedragsverandering is het creëren van een (veiligheids)cultuur, bijvoorbeeld gebaseerd op het zogeheten gedragsdrijversmodel. Dit is een wetenschappelijk gevalideerd model dat inzicht geeft in acht gedragsdrijvers die van invloed zijn op gewenst gedrag binnen organisaties. Door middel van verschillende interventies en activiteiten kan de (veiligheids) cultuur op elk van acht gedragsdrijvers gemeten en versterkt worden (zie de afbeelding op de pagina hiernaast).

Traditionele (awareness)programma's bevatten veelal een beperkt aantal trainingsmomenten (bijvoorbeeld een e-learning waarin medewerkers in één blok twee uur achter elkaar van kennis worden voorzien) zonder dat de content gedoseerd over een langere periode kan worden aangeboden en herhaald. Daarmee wordt beoogd om meer helderheid te bieden, maar wanneer de content weinig gedoseerd en uitdagend is, is de *betrokkenheid* laag.

SECURITY-AWARENESS-TRAINING

Een belangrijk verschil tussen een security-awarenesstraining en veel andere trainingen is dat bij de eerstgenoemde training medewerkers soms bewust misleid worden om onveilig gedrag te vertonen om op die manier te leren van de fouten. Denk bijvoorbeeld aan een (onaangekondigde) phishing-simulatie waarin de medewerker verleid wordt om inloggegevens te verstrekken of een mystery guest-oefening waarbij een onbekende 'ongeautoriseerd' het pand betreedt en probeert vertrouwelijke gegevens te ontvreemden. Oefeningen als deze stellen een medewerker in staat het gewenste gedrag tijdens het reguliere werk (anoniem) te oefenen waarmee het onderdeel wordt van (geautomatiseerd) gedrag.

Een van de nieuwe en effectieve leermethodes die wij hanteren voor het nastreven van de gewenste gedragsverandering, is een *serious game*. Juist een awarenessgame is bij uitstek geschikt om tussen reguliere werkzaamheden door met actuele en op de praktijk gebaseerde scenario's te oefenen. Ook leent een *serious game* – in tegensteling tot e-learning of informerende filmpjes – er zich goed voor om eerder genoemde gedragsdrijvers toe te passen.

ERVARINGEN

De Cybercheck-security-awareness-game is ontworpen op basis van onze brede ervaring met cultuur en gedrag in relatie tot cybersecurity. De game biedt een aantal meetbare voordelen in vergelijking met een traditionele e-learning:

- Klassieke e-learnings worden vaak als saai, tijdrovend en weinig uitdagend gezien. Het spelelement in de *serious game* versterkt de beleving en de overdracht van de informatie. Denk aan competities tegen collega's (bijvoorbeeld door zogenaamde 'leaderboards' met de tien beste spelers) maken medewerkers gemotiveerd om te spelen. De *betrokkenheid* gaat daarmee omhoog en door competitie wordt zichtbaar hoe bewust collega's bezig zijn (*transparantie*). Door het competitie-element zijn de game en de thema's die daarin aan de orde komen onderwerp van gesprek (*bespreekbaarheid*).
- De game kan door deze te spelen op mobiele telefoon of tablet flexibel worden gespeeld in verloren minuten onafhankelijk van tijd en plaats.
- Waar een e-learning vaak werkt met een standaard vragenlijst is de game zo opgebouwd dat een cursist automatisch op een hoger level komt als hij beter scoort. Zo blijft de game uitdagend.
- Door interactief met risicovolle situaties bezig te zijn, blijft de kennis beter hangen.
- Medewerkers kunnen zich maximaal 20 minuten goed concentreren. Doordat de game op meerde-

→

DE GAME RICHT ZICH OP DAADWERKELIJKE GEDRAGSVERANDERING

Screenshot uit de game Cybercheck.

→ re momenten in kleine tijdsblokken kan worden gespeeld, is dit veel effectiever dan eenmalig een uur lang kennis tot zich te nemen.

- In plaats van alleen maar mensen bewuster te maken van cybercrime, richt de game zich op daadwerkelijke gedragsverandering. Dit betekent dat deelnemers aan de game in real-life scenario's geconfronteerd worden met zeer uiteenlopende verschijningsvormen van cybercriminaliteit en leren deze te herkennen en hier adequaat op te reageren.
- Waar een e-learning snel veroudert, biedt een online platform casussen waarin actuele trends en ontwikkelingen uit de praktijk worden verwerkt.

In de game komen verschillende scenario's aan bod waarin telkens een leerdoel wordt getraind. De cursist is de hoofdpersoon in elk scenario. Er is bijvoorbeeld een scenario waarbij de cursist in de trein zit. Hij is dan zijn e-mail aan het beantwoorden, krijgt een verdacht telefoontje of raakt in gesprek met een collega. Voorbeelden van de leerdoelen die in dit scenario aan de orde kunnen komen, zijn het omgaan met verdachte telefoontjes, vertrouwelijke informatie, phishing-mails, draadloze netwerken (in de trein) en 'shoulder surfing'.

MODULES

De game is in de basis bedoeld voor alle medewerkers die omgaan met of toegang hebben tot vertrouwelijke bedrijfsgegevens. Dit zijn niet alleen kantoormedewerkers, maar mogelijk ook medewerkers in het veld. Naast generieke modules die voor alle medewerkers bedoeld zijn, volgen er binnenkort specifieke modules voor onder andere bestuurders, HR- en ICT-medewerkers. Ook worden er sector- en klantspecifieke maatwerkmodules ontwikkeld.

KPMG is onder andere een adviesbureau op het gebied van cybersecurity. Naast een groot team aan cyberspecialisten zijn namens KPMG gedragsdeskundigen en onderwijskundigen betrokken bij de ontwikkeling van de game Cybercheck. Dat de menselijke factor van essentieel belang is in de verdediging van het digitale domein, geldt ook voor de fysieke beveiligingswereld, het domein van beveiligingsbedrijf G4S. Een organisatie kan een zeer geavanceerd beveiligingssysteem installeren en enorm veel beveiligers inzetten, maar wanneer medewerkers niet bewust handelen, hebben deze maar beperkt effect. De veiligheid van het digitale en fysieke domein zijn daarmee onlosmakelijk met elkaar verbonden. Met samenwerking op dit vlak zijn KPMG en G4S in staat de fysieke en digitale beveiliging in een *serious game* nader tot elkaar brengen.

MIX VAN MAATREGELEN

Natuurlijk is ook een *serious game* geen allesomvattende oplossing. Wat ons betreft is een goed awareness-programma een samenhangende mix van maatregelen. Voorbeelden daarvan zijn workshops, awareness-spelshows, phishing-simulaties, profiling, boardroomsessies, penetratietesten, crisismanagementsimulaties en mystery guest-acties. Een *serious game* als Cybercheck kan daar een belangrijke bijdrage aan leveren. ■

Matthieu Paques is senior manager bij KPMG Cyber