Auteur: Inge Wetzer is werkzaam bij Secura als social psychologist cybersecurity & compliance. Zij is gepromoveerd in de sociale psychologie en is bereikbaar via e-mail: inge@secura.com

De psychologie over een effectief mensprogramma in cybersecurity

Baat het niet dan schaadt het wel

Deel 1 van tweeluik

Cybersecurityprogramma's focussen steeds meer op gedrag, maar zonder doordachte aanpak werkt dit vaak averechts. Veelgemaakte fouten zijn: teveel aandacht voor wat al goed gaat, focus op verkeerde gedragsfactoren zoals kennis of motivatie, en mismatches met het kennisniveau. Dit leidt tot frustratie, weerstand en onveilig gedrag, ondanks goede intenties. Door eerst te meten wat medewerkers weten en de echte knelpunten te identificeren, kunnen organisaties gerichte interventies inzetten en duurzame gedragsverandering bereiken zonder weerstand.

Je opent je inbox en ziet weer een nieuwe cybersecuritytraining verschijnen. Het is al de derde dit jaar en je hebt de vorige pas net afgerond. Wederom krijg je te horen hoe belangrijk sterke wachtwoorden zijn en dat je alert moet blijven op phishingmails. Je weet het allemaal wel inmiddels. Bij de koffieautomaat hangt weer zo'n poster: "Vergrendel je scherm als je wegloopt!" En dan zijn er nog de gele kaarten: de zoveelste waarschuwing, de zoveelste reminder—het begint zijn effect te verliezen. Sterker nog, het begint langzaam weerstand op te roepen.

De afgelopen jaren is er binnen organisaties steeds meer aandacht gekomen voor de menselijke factor in cybersecurity. Waar cybersecurity voorheen voornamelijk werd gezien als een technische kwestie, gericht op firewalls, antivirussoftware en encryptie, beseffen steeds meer bedrijven dat het gedrag van medewerkers minstens zo belangrijk is om cyberdreigingen tegen te gaan. Cyberaanvallen worden steeds geraffineerder, maar tegelijkertijd blijkt uit onderzoek dat een groot deel van de beveiligingsincidenten nog steeds voortkomt uit menselijk handelen: onbewuste fouten, slordigheden of simpelweg het niet volgen van protocollen.

Dit inzicht heeft ertoe geleid dat organisaties massaal zijn gaan inzetten op het vergroten van cybersecurity-awareness onder hun personeel. Via trainingen, e-learnings, posters en workshops worden medewerkers bewust gemaakt van de risico's en verantwoordelijkheden. Denk aan waarschuwingen over phishingmails, het gebruik van sterke wachtwoorden en het belang van het vergrendelen van je computerscherm als je wegloopt. Deze focus op bewustwording – of awareness – is een belangrijke eerste stap in het erkennen van de rol van de mens in cybersecurity.

Meer aandacht voor gedrag

De afgelopen jaren heeft een belangrijke verschuiving plaatsgevonden: veel organisaties hebben ingezien dat het niet enkel draait om bewustwording, maar juist om gedragsverandering. De psychologie leert ons dat gedrag wordt bepaald door meer dan alleen bewustzijn. Naast bewustzijn spelen motivatie (wil iemand het wel?) en gelegenheid (wordt iemand in staat gesteld om het te doen?) een cruciale rol. Weten wat veilig gedrag is, betekent niet automatisch dat iemand het ook vertoont. Mensen moeten zowel kennis hebben als gemotiveerd zijn én de mogelijkheid hebben om het gedrag daadwerkelijk te vertonen.

Deze inzichten komen voort uit onderzoek naar de menselijke kant van cybersecurity. Daarbij werd duidelijk dat gedrag slechts deels afhankelijk is van kennis. Zonder aandacht voor motivatie en gelegenheid blijft gedragsverandering uit ((1), (2), (3), (4)).

Veel organisaties hebben inmiddels begrepen dat het niet genoeg is dat medewerkers weten wat veilig gedrag is; ze moeten dit gedrag ook daadwerkelijk vertonen. Dit heeft geleid tot een toenemende focus op gedragsveranderingsprogramma's: posters ophangen in kantoren, medewerkers aanmoedigen elkaar aan te spreken op onveilig gedrag en het uitdelen van gele kaarten bij overtredingen.

Het idee achter deze programma's is goed: medewerkers actief betrekken bij cybersecurity en hen helpen om cyberveilig gedrag te omarmen. Maar hier schuilt ook een risico. In veel gevallen worden deze gedragsprogramma's ingevoerd zonder dat er grondig wordt onderzocht hoe medewerkers ze ervaren. De druk om snel iets te doen—om iets uit te rollen—kan ertoe leiden dat organisaties maar wat proberen, in de hoop dat er iets blijft hangen. In plaats van medewerkers te helpen hun gedrag structureel te veranderen, kunnen slecht doordachte gedragsprogramma's juist negatieve effecten hebben.

De risico's van ongefundeerde initiatieven

Een overdaad aan losse interventies – van herhaalde trainingssessies en postercampagnes tot het uitdelen van gele kaarten – kan ertoe leiden dat medewerkers vermoeid raken en afhaken. In plaats van cyberveiligheid als iets positiefs en belangrijks te zien, ontstaat er irritatie of zelfs cynisme. Wanneer gedragsprogramma's niet goed aansluiten bij de werkpraktijk of de motivatie van medewerkers, kunnen ze meer kwaad dan goed doen. Dit betekent dat organisaties zorgvuldig moeten nadenken over hun aanpak van gedragsverandering.

De sleutel ligt in een doordachte, op maat gemaakte benadering, die niet alleen kijkt naar kennis en bewustwording, maar ook naar de motivatie, gelegenheid en ondersteuning die nodig zijn om gedragsverandering daadwerkelijk te laten plaatsvinden. Dit artikel beschrijft hoe gedragsprogramma's effectief kunnen worden ingezet om medewerkers te ondersteunen, zonder hen te overspoelen met ondoordachte campagnes die uiteindelijk tot weerstand leiden.

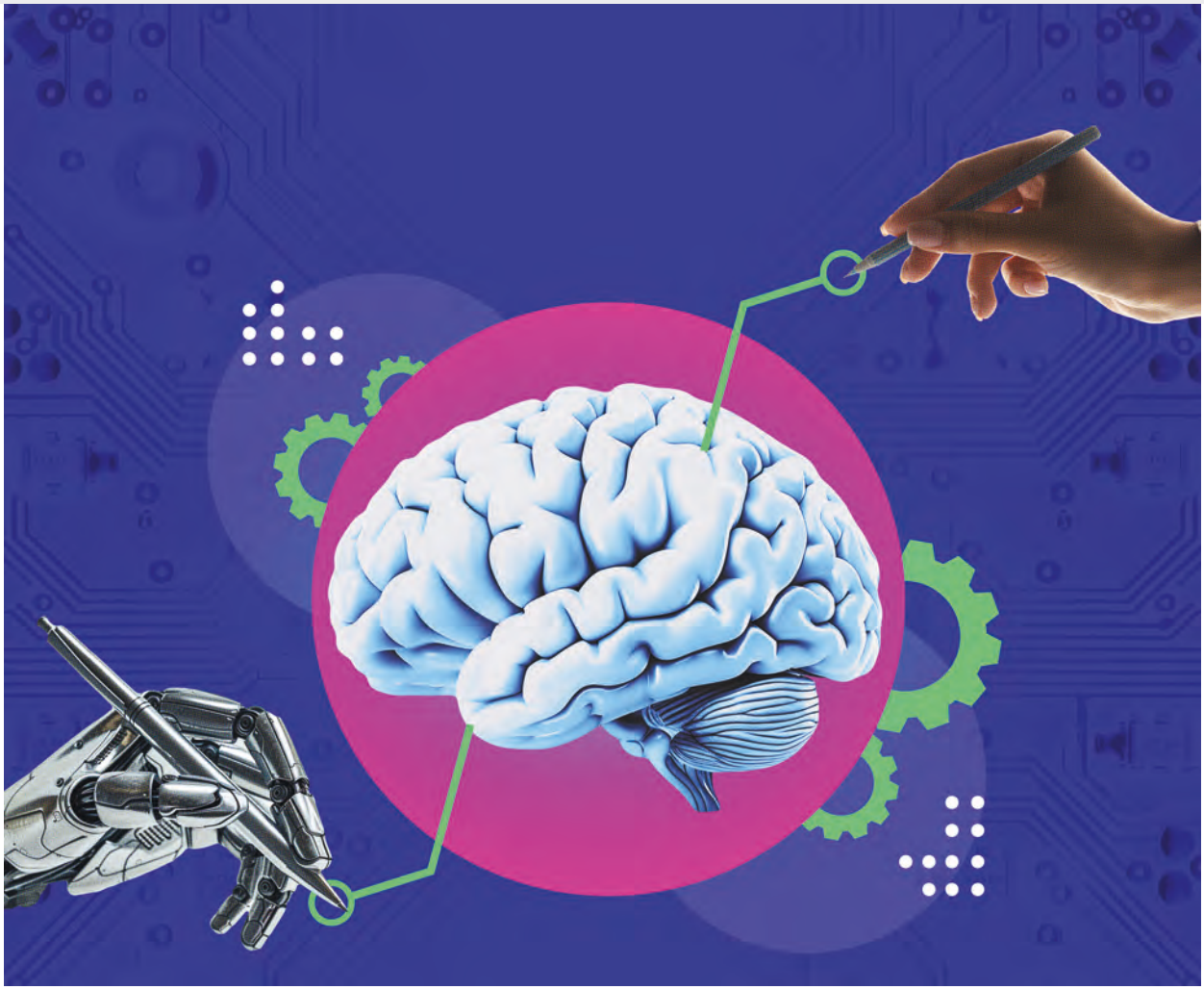
De meest gemaakte fouten in gedragsprogramma's

Wanneer een gedragsprogramma blijft hameren op onderwerpen die medewerkers al beheersen, kan dit snel leiden tot frustratie en weerstand. Mensen worden moe van het steeds opnieuw horen van dezelfde boodschap, zeker als ze al weten wat er van hen verwacht wordt. Dit kan resulteren in wat we security fatigue noemen: een toestand waarin medewerkers verzadigd raken door herhaling en hun motivatie om nog mee te doen afneemt. Ze haken af, niet omdat ze de risico's niet serieus nemen, maar omdat ze het gevoel krijgen dat de programma's weinig toevoegen. Dit maakt het lastig om hen later nog te bereiken met nieuwe, mogelijk wél relevante informatie.

De oplossing begint met inzicht. Voordat je een gedragsprogramma uitrolt, moet je eerst vaststellen welke onderwerpen al goed gaan en waar nog werk aan de winkel is. Dit betekent niet zomaar aannemen of gokken, maar echt meten. Alleen door te weten wat medewerkers al goed doen en waar de knelpunten liggen, kun je een programma opzetten dat zich richt op wat er écht toe doet. Zo voorkom je dat medewerkers verzanden in herhaling en frustratie, en zorg je ervoor dat hun aandacht gericht blijft op de onderwerpen die daadwerkelijk verbetering nodig hebben.

Aandacht voor de verkeerde factor van gedrag

Een tweede veelgemaakte fout in gedragsprogramma's is dat de focus ligt op de verkeerde factor van gedrag. Vaak wordt kennis eindeloos herhaald, terwijl het echte probleem in de gelegenheid zit. Medewerkers weten wel wat ze moeten doen en



willen het ook wel, maar worden belemmerd door praktische obstakels. Dit leidt tot frustratie: als je steeds hoort wat je al weet, zonder dat de juiste omstandigheden worden gecreëerd om het gedrag daadwerkelijk te vertonen, voelt dat als zinloze herhaling. Hierdoor ontstaan workarounds: medewerkers zoeken manieren om hun werk toch gedaan te krijgen, vaak op manieren die de veiligheid ondermijnen. Zolang de barrières in de gelegenheid niet worden weggenomen, blijft het gewenste gedrag uit en groeit de weerstand tegen verdere interventies.

Het kan natuurlijk ook andersom: dat er júist aandacht voor kennis nodig is, maar dat de nadruk ligt op het verhogen van motivatie. Medewerkers willen wel veilig handelen, maar weten niet precies hoe. Neem bijvoorbeeld het kiezen van een sterk wachtwoord: wat in 2025 nog als veilig wordt beschouwd, verandert snel. Als deze kennis niet up-to-date is, heeft het weinig zin om medewerkers te blijven motiveren zonder hen de juiste informatie te geven. Dit leidt niet alleen tot verwarring, maar ook tot onveilig gedrag, simpelweg omdat mensen niet weten wat van hen wordt verwacht. Het resultaat is dat, ondanks alle inspanningen om motivatie te verhogen, het gedrag niet verandert omdat de basiskennis ontbreekt.

Om effectief gedrag te veranderen, moet je per onderwerp helder krijgen welke factor ontbreekt: kennis, motivatie of gelegenheid. Dit betekent dat je niet zomaar kunt aannemen wat het probleem is, maar dit daadwerkelijk moet meten. Als het bijvoorbeeld gaat om veilig wachtwoordgebruik, moet je weten of medewerkers niet begrijpen wat een sterk wachtwoord is, of dat ze het wel weten, maar niet gemotiveerd zijn om het toe te passen, of dat ze worden belemmerd door praktische obstakels zoals ingewikkelde procedures. Pas als je precies weet waar het knelt, kun je gericht ingrijpen. Zo voorkom je dat je blijft hameren op kennis terwijl de barrières in de faciliteiten liggen, of dat je motivatie probeert te verhogen terwijl mensen simpelweg niet weten wat ze moeten doen. Alleen met een gerichte aanpak kun je echte gedragsverandering realiseren.

Effectieve gedragsprogramma's in cybersecurity vragen om meer dan alleen goede bedoelingen

Aandacht op het verkeerde kennisniveau

Een derde veelgemaakte fout in gedragsprogramma's is dat de inhoud niet is afgestemd op het juiste kennisniveau van de medewerkers. Soms zijn de e-learnings of trainingen te simpel, waardoor mensen het gevoel krijgen niet serieus genomen te worden. Dit kan leiden tot irritatie en demotivatie, omdat ze het idee krijgen dat hun kennis wordt onderschat of dat er niet genoeg moeite wordt gedaan om de inhoud op maat aan te bieden, terwijl er wel tijd wordt gevraagd om een training te volgen bovenop een toch al vol takenpakket. Aan de andere kant kunnen de programma's ook te complex zijn, waardoor medewerkers overweldigd raken. Dit kan resulteren in een gevoel van machteloosheid of learned helplessness, waarbij ze denken dat ze het toch niet kunnen begrijpen of toepassen. In beide gevallen raken medewerkers gedemotiveerd en neemt hun betrokkenheid af, wat de effectiviteit van het programma ondermijnt.

Om dit te voorkomen, is het essentieel om eerst het juiste kennisniveau van de medewerkers te meten voordat je een training of e-learning aanbiedt. Door te weten waar je medewerkers staan, kun je de inhoud van het programma beter afstemmen op hun behoeften. Dit betekent dat je voorkomt dat trainingen te eenvoudig zijn voor mensen die al veel weten, en niet te complex voor degenen die nog basiskennis nodig hebben. Een goed afgestemd programma zorgt ervoor dat iedereen zich serieus genomen voelt en op het juiste niveau wordt uitgedaagd. Zo blijven medewerkers betrokken en voorkom je dat ze afhaken door frustratie of overweldiging.

Belangrijke lessen

Effectieve gedragsprogramma's in cybersecurity vragen om meer dan alleen goede bedoelingen. Ze vereisen een zorgvuldige aanpak waarbij organisaties niet alleen inzicht krijgen in de huidige kennis en het gedrag van hun medewerkers, maar ook begrijpen welke factoren echte verandering tegenhouden. Door te meten en te richten op wat werkelijk nodig is of dat nu kennis, motivatie of gelegenheid betreft—kunnen organisaties programma's ontwikkelen die niet alleen effectief zijn, maar ook weerstand en frustratie voorkomen. Het doel is niet alleen om medewerkers bewuster te maken, maar hen ook daadwerkelijk in staat te stellen en te motiveren om veilig gedrag te vertonen, waardoor de organisatie als geheel sterker en veiliger wordt.
In deel 2 van dit tweeluik zullen cijfers gepresenteerd worden van een grote benchmarkstudie. Deze resultaten laten zien waar organisaties gemiddeld genomen staan: welke onderwerpen blijven achter in gedrag en waar ontbreekt het aan kennis, motivatie of gelegenheid? Door de resultaten van een grote steekproef over verschillende organisaties te analyseren, krijgen we inzicht in de startpunten (gemiddeld gezien) van een effectief programma. Want inmiddels weten we: als gedragsprogramma's slecht worden ontworpen, kunnen de gevolgen ernstig zijn. Medewerkers kunnen gefrustreerd raken door herhaling van overbodige informatie, wat leidt tot demotivatie en cynisme. Onjuiste focus op kennis of motivatie kan ervoor zorgen dat belangrijke praktische barrières niet worden weggenomen, waardoor medewerkers workarounds gaan zoeken die de veiligheid ondermijnen. In het ergste geval ontstaat er een gevoel van machteloosheid, waarbij medewerkers afhaken en zelfs bewust onveilig gedrag vertonen. Dit benadrukt hoe cruciaal het is om zorgvuldig te meten en de juiste interventies in te zetten. Want wat betreft 'awareness' in cybersecurity geldt: baat het niet, dan schaadt het wel.

Referenties

(1) Wetzer, I. M. (2017a). Voorbij awareness; grip op cyberveilig gedrag. InformatieBeveiliging, 17 (IB.3), 24-26.

(2) Wetzer, I. M. (2017b). Cyberveilig gedrag: Meer dan alleen het locken van je beeldscherm. InformatieBeveiliging, 17 (IB.6), 4-7.

(3) Wetzer, I. M. (2018). Cyberveilig gedrag: Waarom dóen we het nou niet? InformatieBeveiliging, 18 (IB.1), 12-15.

(4) Wetzer, I. M. (2021). Het begint met bewustwording. Hoe ver zijn we daar inmiddels mee? Informatie Beveiliging, 6, 26-29.