Auteur: Inge Wetzer is sociaal psycholoog cybersecurity & compliance. Zij werkt bij Secura, waar zij zich druk maakt over het menselijk gedrag in (cyber)security, en hoe dat te verbeteren. Inge is bereikbaar via inge@secura.com.

Veilig gedrag in informatiebeveiliging: leren, motiveren, faciliteren

Deel 3 van drieluik 'Onderzoek naar de human factor in informatiebeveiliging'

Dit drieluik beschrijft onderzoek naar de menselijke factor in informatiebeveiliging. De eerste twee artikelen uit deze reeks lieten zien hoe het gesteld is met het huidige kennisniveau en gedrag ten aanzien van 15 verschillende onderwerpen in informatiebeveiliging. Deze data toonden aan dat voor een aanzienlijk deel van onveilig gedrag in informatiebeveiliging, kennis wel aanwezig is. Het laatste artikel in deze reeks gaat in op handvatten om juist die gedragingen te veranderen; waar mensen al wel weten wat ze zouden moeten doen, maar nog niet doen.

Cyberdreigingen zijn actueler dan ooit. Dat de menselijke factor een wezenlijk onderdeel van de weerbaarheid uitmaakt, is inmiddels ook bekend. Organisaties zien ook steeds meer het belang in van daadwerkelijke gedragsverandering, dus niet stoppen bij het zenden van kennis maar kijken naar alle factoren die gedrag beïnvloeden. Wat nog lastig blijft is, hoe te komen tot die daadwerkelijke gedragsverandering.

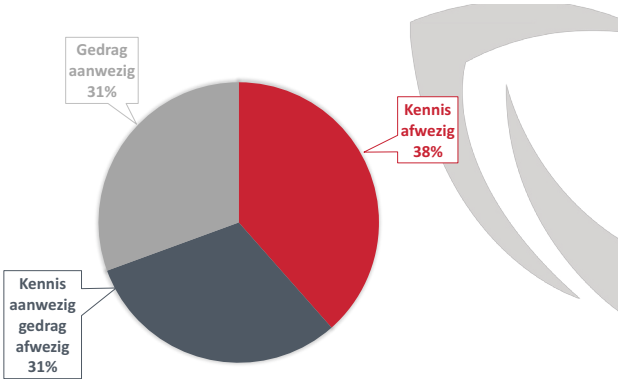
De menselijke factor in informatiebeveiliging

Gedrag in informatiebeveiliging. Een uitdaging voor iedere (C)ISO. Want opstellen van een passend beleid is één ding, maar zorgen dat iedereen zich daar ook aan houdt, een tweede. In het dagelijks leven zien we voortdurend situaties waarin mensen wel wéten wat ze eigenlijk zouden moeten doen, maar zich er toch niet aan houden. Denk aan het niet insmeren om wat sneller bruin te worden, het negeren van het thuiswerkadvies of het appen op de fiets. Deze kloof tussen kennis en gedrag kan worden verklaard door het feit dat gedrag het resultaat is van meerdere factoren, niet alleen kennis. In dit artikel wordt beschreven welke factoren dat zijn en hoe dit kan helpen bij het bereiken van gewenste gedragsverandering.

Het onderzoek tot nu toe

In de eerste twee artikelen van dit drieluik werd onderzoek beschreven naar het huidige kennisniveau, onder 1155 respondenten van 20 organisaties (1), (2). Het onderzoek betrof 15 onderwerpen met betrekking tot informatieveiligheid, waarvoor zowel kennis als gedrag werd gemeten. De resultaten lieten zien dat gemiddeld genomen over 15 onderwerpen, in 38% van de gevallen kennis de ontbrekende factor is. Met andere woorden: voor iets meer dan een derde van de gevallen heeft het wel degelijk zin om mensen kennis aan te bieden! Het is alleen wel zaak te weten voor wélke onderwerpen dat is, zodat deze kennis gericht kan worden aangeboden. Dit werd uitgebreid beschreven in het eerste artikel van dit drieluik (1).

Daarnaast lieten de resulaten zien dat in 31% van de gevallen, het juiste gedrag al wordt vertoond (2). Deze onderwerpen behoeven dus de minste aandacht, want hier gaat het immers al goed. Maar dan blijft er nog 31% van de gevallen over, waarbij de kennis wel aanwezig is, maar het gedrag niet. Voor deze gevallen heeft het uiteraard geen zin om verder in te zetten op kennisverhogende activiteiten, omdat men voor deze onderwerpen wel hoog scoorde op kennis. Voor deze onderwerpen is dus sprake van de kennis-gedragskloof. Kennis zenden kan in deze gevallen zelfs weerstand oproepen, omdat mensen hier niets meer van leren en juist andere redenen hebben om zich toch anders te gedragen. Om deze kloof te overbruggen, zal dus verder gekeken moeten worden; welke andere aspecten beïnvloeden het menselijk gedrag nog meer? En hoe kunnen we daarop ingrijpen als we gedrag willen veranderen?



Figuur 1 - Kennis en gedrag in cybersecurity gemiddeld over 15 onderwerpen.

De psychologie over gedrag

Als we kijken naar een basale theorie van gedrag uit de psychologie, zien we dat gedrag wordt bepaald door drie factoren (3). Allereerst is gedrag afhankelijk van iemands capaciteit: is iemand wel in staat om het te doen, weet iemand wat er verwacht wordt en beschikt hij/zij over de vaardigheden? Hieronder valt dus het stukje bewustwording waar de meeste campagnes in het verleden op gebaseerd waren. Naast kennis wordt gedrag echter ook bepaald door iemands motivatie: Wil iemand het wel doen, vindt deze persoon het wel belangrijk genoeg? De derde factor die gedrag bepaalt is gelegenheid: Wordt iemand wel in staat gesteld om het te doen en krijgt deze persoon wel de kans om het te doen? Voor de onderwerpen waarbij kennis wel aanwezig is maar gedrag niet, zal voor gedragsverandering dus ingezet moeten worden op deze twee factoren: motivatie en gelegenheid.

Motivatie

Zoals hierboven beschreven, is het niet alleen belangrijk of iemand een regel kent en weet wat er verwacht wordt. Minstens zo belangrijk is het willen! Deze motivatie voor bepaald gedrag kan volgens de psychologie in verschillende typen worden onderverdeeld:

Intrinsieke motivatie

Intrinsiek gemotiveerd zijn betekent dat je als individu handelt vanuit je eigen wil/verlangen. De motivatie komt vanuit iemand zelf. Met andere woorden: je doet iets omdat je het zelf graag wil.

Extrinsieke motivatie

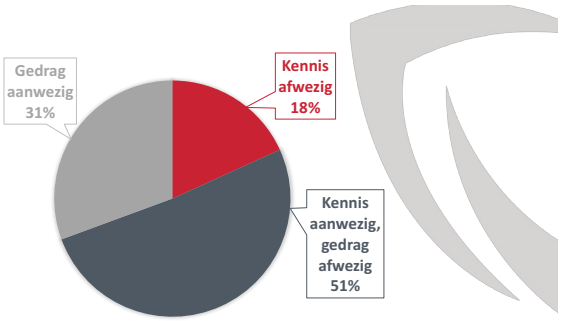
De motivatie die wordt ingegeven door een extern doel dat iemand kan bereiken met informatieveiligheid. Bijvoorbeeld: het ontvangen van een 'beloning' (bv. waardering) of het vermijden van straf.

Zelfeffectiviteit (Self-efficacy)

Het vertrouwen in je eigen bekwaamheid om met succes een bepaalde taak te volbrengen. Met andere woorden; het vertrouwen dat je kunt wat er van je gevraagd wordt. Dit is dus het geloof in eigen kunnen (4).

Motivatie het probleem? Motiveren de oplossing!

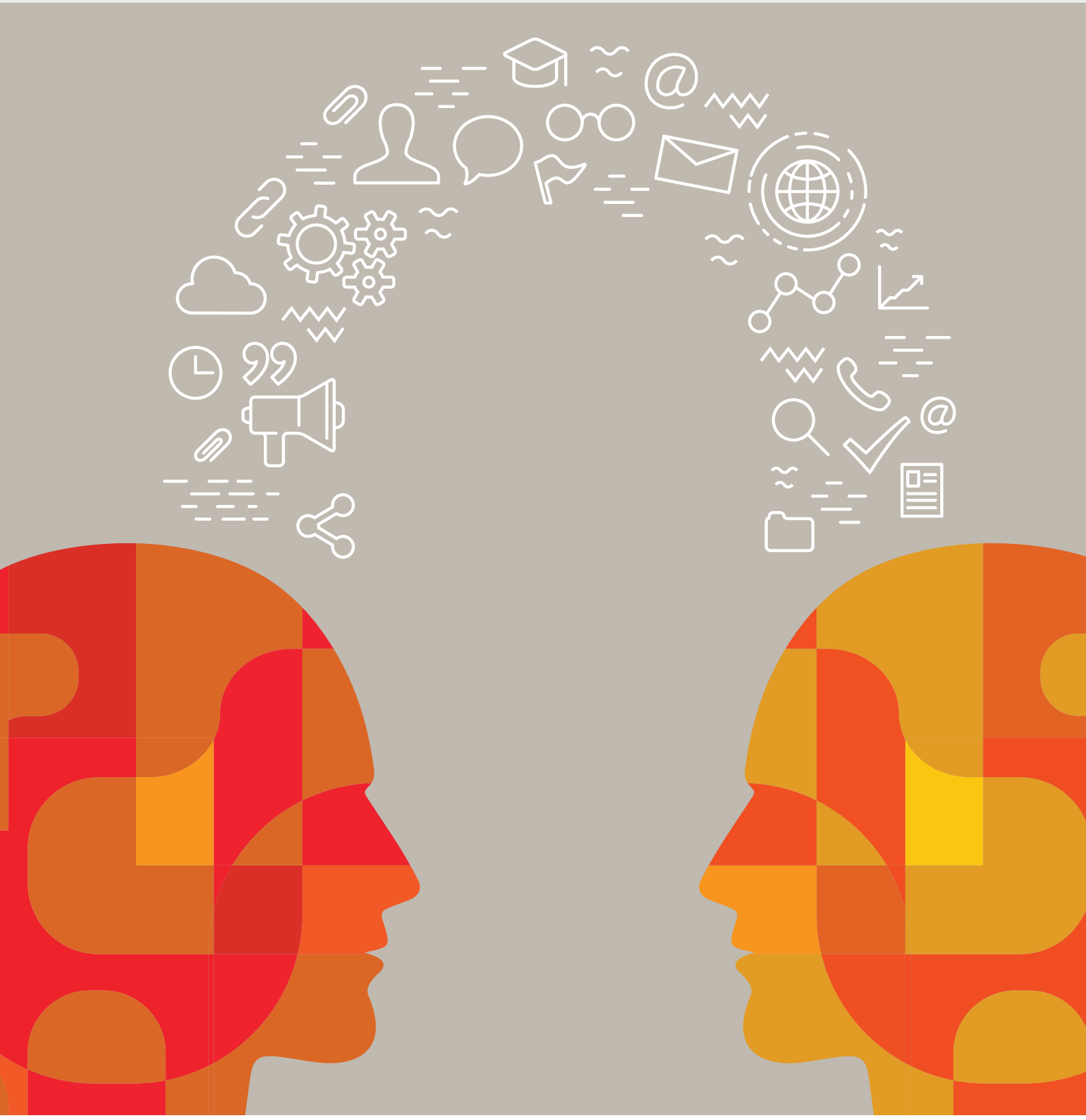
Op het moment dat blijkt dat kennis niet ontbreekt maar gedrag wel, is het interessant om een stap verder te kijken: Vindt men het wel belangrijk genoeg? Ziet men het risico? Als voorbeeld kijken we naar het onderwerp 'sterk wachtwoord'. De data in Figuur 2 laten zien dat maar liefst 82% van de respondenten in de kennistest kan aanwijzen welke van vier wachtwoorden het sterkste is. Als vervolgens gevraagd wordt of zij zelf ook een sterk wachtwoord gebruiken, geeft slechts 31% aan dat te doen. Dus 51% van de respondenten weet wel wat een sterk wachtwoord is, maar gebruikt het zelf niet. Wat is hier aan de hand?



Figuur 2 - Sterk wachtwoord.

Waarschijnlijk motivatie! Of nou ja, een gebrek daaraan dus. Voor sommige organisaties voeren wij aanvullend een reeks interviews uit. In deze interviews is ruimte om dieper in te gaan op de barrières die medewerkers ervaren waardoor ze bepaald gedrag niet vertonen. Wanneer het over 'niet willen' gaat, kunnen daar veel redenen aan ten grondslag liggen. Uit interviews met medewerkers in verschillende organisaties, bleek dat mensen zich vaak laten weerhouden een sterk wachtwoord te kiezen omdat ze het lastig vinden om dat te onthouden. Hoe krijgen we deze mensen dan toch zover dat zij deze barrière kunnen overwinnen? Door ze uit te leggen hoe je een wachtwoord kunt maken dat sterk is maar dat je óók nog kunt onthouden! Of door ze uit te leggen hoe je hiervoor gebruik kunt maken van een wachtwoordmanager. Het inspelen op de reden om niet te willen, motiveert mensen om het ander gedrag te gaan vertonen.

Een ander voorbeeld: wij hielpen een organisatie waar nooit informatiebeveiligingsincidenten gemeld werden. Nooit…. Gewoon geen dus. Heel even zou je kunnen denken dat dat een goed teken is, maar wie iets verder doordenkt, begrijpt dat het waarschijnlijk betekent dat er wel incidenten zijn, maar dat deze niet gemeld worden. Uit de kennistest bleek echter dat veruit het grootste deel van de medewerkers wel wist wat er gemeld diende te worden en waar. Capaciteit op orde dus en het herhalen van de regels niet zinvol meer. Toen we vervolgens met diepte-interviews ingingen op de barrières voor mensen om toch



die stap naar het melden te maken, bleek dat zij niet meer meldden omdat men in het verleden meerdere malen had gemeld, maar daar nooit iets over terug had gehoord. Hierdoor had men de conclusie getrokken dat incidenten niet werden opgepakt en dat melden dus eigenlijk voor niets was. De oplossing in dit geval is dus: motiveren door het laten weten dat meldingen wel degelijk opgepakt worden! Een persoonlijke feedbackmail op een melding in combinatie met een maandelijks overzichtsmail van alle meldingen, wat daarmee gedaan was én wat er door deze meldingen voorkomen was, was voor deze organisatie de sleutel naar gedragsverandering.

Gelegenheid

Naast motivatie is er nog een derde variabele die een sterke invloed op gedrag heeft: gelegenheid. Want wat nou als iemand wel wéét dat hij alleen in zijn eigen account mag werken (capaciteit) en dat ook wel wíl (motivatie), maar dat niet kán omdat hij niet de juiste autorisaties heeft om bij de systemen te kunnen waar hij bij zou moeten kunnen? Gelegenheid kan worden onderverdeeld in context en cultuur.

Context

Bij het bepalen van gedrag, speelt context een belangrijke rol. Immers, de omgeving moet wel toelaten dat mensen kunnen doen wat er van hen verwacht wordt. We kunnen bijvoorbeeld niet verwachten dat mensen documenten met gevoelige informatie veilig weggooien als er geen mogelijkheden voor zijn zoals een shredder. Of dat ze gevoelige informatie niet per mail delen terwijl er geen veilig alternatief is. Vaker dan misschien gedacht wordt, ontbreekt het nog aan dit soort praktische zaken. Wanneer er sprake is van een hoog kennisniveau maar weinig gedrag, is het daarom van belang om zorgvuldig na te gaan of de context voldoende ondersteunend is. Door de medewerkers zelf te vragen! Onze ervaring leert dat security professionals vaak aannemen dat bepaalde zaken voldoende zijn ingeregeld, maar dat ze in de praktijk uiteindelijk niet blijken te werken.

Cultuur

Naast context wordt gelegenheid bepaald door de cultuur in een organisatie. Cultuur speelt een niet te onderschatten rol in wat wel en niet van mensen verwacht kan worden. Zo kan het op papier wel duidelijk zijn dat iedereen wordt geacht elkaar aan te spreken op bijvoorbeeld het niet vergrendelen van een computerscherm of het niet dragen van een pas, maar als de organisatie geen aanspreekcultuur heeft, is elkaar aanspreken wellicht helemaal (nog) niet geaccepteerd en durft niemand zich eraan te branden. Dus wanneer het gaat om het overbruggen van de kennis-gedragskloof, zal ook naar het cultuuraspect gekeken moeten worden: laat de cultuur van de organisatie wel toe dat mensen doen wat van hen gevraagd wordt?

Gelegenheid het probleem? Faciliteren de oplossing!

Wanneer er sprake is van een kloof tussen kennis en gedrag, kan dit dus het gevolg zijn van een gebrek aan gelegenheid. Met andere woorden: mensen vertonen het gedrag niet omdat ze daar de kans niet (voldoende) voor krijgen. Als er in dit soort gevallen wordt ingezet op het communiceren van de regels, kan dit leiden tot frustratie en weerstand. Mensen wéten immers heus wel wat er van hen verwacht wordt, maar ze zijn niet in de gelegenheid om te handelen. Bijvoorbeeld wanneer het systeem om bezoekers aan te melden niet goed werkt, je niet de juiste authorisaties hebt om je werk goed te kunnen doen, of de cultuur niet toestaat dat je anderen zomaar aanspreekt. In deze gevallen heeft het veel meer zin om in te zetten op faciliteren: zorg dat procedureel en technisch goed ingeregeld is dat mensen kunnen doen wat er van hen verwacht wordt en dat de cultuur dit toestaat. Dat is uiteraard makkelijker gezegd dan gedaan, zeker wanneer er cultuurverandering nodig is. Maar het begint allemaal met het besef waar de focus op gelegd moet worden.

Door te begrijpen aan welke knop gedraaid moet worden om gedragsverandering te bewerkstelligen, wordt al een enorme stap voorwaarts gezet. Hierdoor wordt niet langer geïnvesteerd in intiatieven die niet de oplossing zijn en kan juist worden gezocht naar manieren die wel bij de actuele behoefte aansluiten. Efficiënter en effectiever

Referenties

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

(2) Wetzer, I. M. (2022). De kloof tussen awareness en gedrag. Informatie Beveiliging, 1,14-17.

(3) MacInnis, D. J., Moorman, C., & Jaworski, B. J. (1991). Enhancing and Measuring Consumers' Motivation, Opportunity, and Ability to Process Brand Information from Ads. Journal of Marketing, 55, 32-53.

(4) Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. Psychological Review, 84, 191-215.