Informatie(on)veilig gedrag van medewerkers

Mensen maken fouten, ook ten aanzien van de informatieveiligheid. Om deze fouten aan te kunnen pakken is inzicht in menselijk gedrag nodig. Dit vraagt om een praktisch en wetenschappelijk gefundeerd gedragsverklarend model. Die modellen zijn gangbaar in de informatiebeveiligingswereld, maar hebben zo hun beperkingen. Daarom presenteren we hier een alternatief.

Mensen maken fouten en veroorzaken daarmee incidenten, ook met betrekking tot digitale data. In een organisatie hebben medewerkers zowel een negatieve als een positieve invloed op de informatieveiligheid, doordat zij enerzijds fouten kunnen maken en anderzijds oplossingen kunnen bedenken en uitvoeren die risico's voorkomen of beperken. Het is nuttig om vooral de negatieve impact te beperken door het aantal en de ernst van fouten te verminderen. Daarvoor is inzicht nodig in het gedrag van medewerkers en de mechanismes die leiden tot fouten. Het is weliswaar onmogelijk om bij medewerkers fouten ten aanzien van de informatieveiligheid helemaal te voorkomen, maar het terugbrengen van het aantal incidenten door fouten is niet te veel gevraagd. Inzicht in gedrag en gemaakte fouten kan ook aantonen dat veel fouten van medewerkers eigenlijk voortkomen uit organisatorische problemen. Zo maakt bijvoorbeeld een onervaren medewerker zonder goede begeleiding fouten die voorkomen hadden kunnen worden door wel goede begeleiding te geven.

Modellen

In de afgelopen decennia zijn heel wat modellen voorgesteld om menselijk gedrag te verklaren, of zijn oude modellen afgestoft. Enkele bekende modellen die in de informatiebeveiligingswereld worden gebruikt zijn Theory of Planned Behaviour (TPB), Protection Motivation Theory (PMT), Knowledge-Attitude-Behaviour (KAB), Capability Opportunity Motivation - Behaviour (COM-B) en Theory of Situation Awareness (TSA). De grootste gemene deler van deze modellen is dat ze nogal hoog over gaan en/of zich maar op een deel van de relevante gedragsbeïnvloedende factoren richten (1). Daardoor kunnen ze een onvolledige verklaring van informatieveilig gedrag geven. Een relatief uitgebreid model is in 2000 in een whitepaper gepubliceerd (2) en opgenomen in het boek Informatiebeveiliging onder controle (3), maar dat model is voor veel mensen te veel van het goede. Er is dan ook behoefte aan een handzaam, maar wel wetenschappelijk gefundeerd gedragsverklarend model dat alle belangrijke gedragsbeïnvloedende factoren bevat.

Met een gedragsverklarende model in de hand kunnen we niet alleen fouten in informatieveilig gedrag van medewerkers verklaren, maar ook organisatiefouten

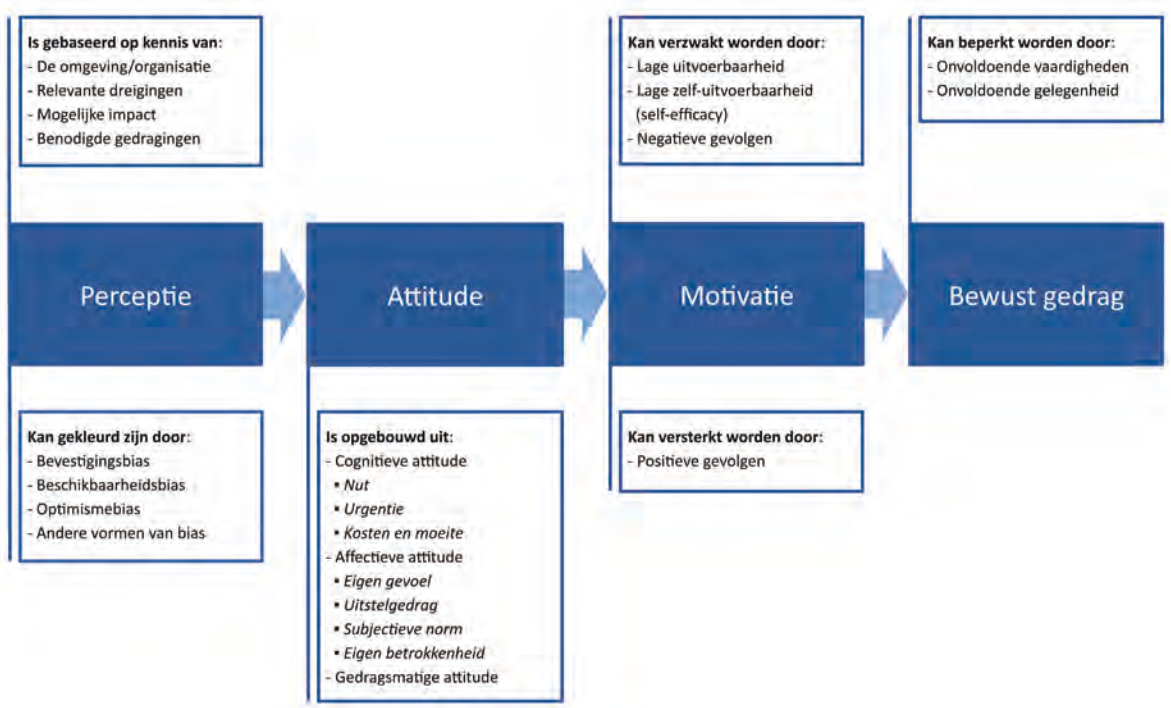
In een organisatie bestaat informatieveilig gedrag van een medewerker uit gedragingen die de betreffende medewerker onbewust of bewust uitvoert (3, 4, 5). Het onbewuste informatieveilig gedrag stoelt op automatismen en wordt bepaald door de omgeving, oftewel de organisatie. Fouten in het onbewuste gedrag moeten dan ook worden aangepakt door de organisatie zodanig aan te passen dat deze fouten niet meer worden gemaakt.
Het bewuste informatieveilig gedrag is gedrag waarvan de medewerker zich bewust is (3). Hieronder valt ook gedrag dat de medewerker uit onwetendheid, onoplettendheid, slordigheid, of nalatigheid uitvoert, waardoor de betreffende medewerker zonder opzet, oftewel per ongeluk, fouten maakt. Daarnaast kan de medewerker ook opzettelijk fouten maken, oftewel de regels overtreden. Dit kan de medewerker te goeder trouw doen, bijvoorbeeld in een uitzonderingssituatie waarin de regels niet voorzien zijn of te kwader trouw, bijvoorbeeld uit rancune. Het aanpakken van fouten in het bewuste informatieveilig gedrag is een complexe zaak. In deze paragraaf gaan we daarom in op het verklaren van het bewuste informatieveilig gedrag (1). Dit heeft betrekking op enerzijds het uitvoeren van handelingen ten aanzien van informatieveiligheid, bijvoorbeeld het afwijzen van cookies die niet nodig zijn en anderzijds het uitvoeren van informatiebeveiligingsmaatregelen, bijvoorbeeld door het gebruik van sterke wachtwoorden. Vanuit zichzelf doen veel mensen dit nog onvoldoende (6).

Gedrag

De belangrijkste voorspeller van bewust informatieveilig gedrag bij een medewerker is de motivatie, oftewel de intentie, om dit gedrag daadwerkelijk uit te voeren. Vanzelfsprekend moet de medewerker dan wel de benodigde vaardigheden bezitten. Verder mag de organisatie het informatieveilig gedrag niet te lastig of zelfs onmogelijk maken of anders gezegd, de organisatie moet de persoon wel de gelegenheid bieden om informatieveilig gedrag uit te voeren.

Een belangrijke invloedsfactor op de motivatie van de medewerker voor informatieveilig gedrag is diens perceptie (7). De perceptie is het beeld dat de medewerker in kwestie heeft van de betreffende situatie. Dit beeld steunt in belangrijke mate op kennis van de omgeving/organisatie, de relevante dreigingen, de mogelijke impact ervan en de benodigde gedragingen. Wanneer deze kennis bij medewerkers niet in voldoende mate aanwezig is, dan kunnen ze de risico's van de situatie niet goed inschatten en weten ze niet welk informatieveilig gedrag van hun wordt gevraagd.

Maar het blijft niet bij kennis alleen. De perceptie van de medewerker kan namelijk vertekend zijn door bias (8). Hiervoor zijn meerdere oorzaken, maar voor informatieveilig gedrag lijken vooral de bevestigingsbias, de beschikbaarheidsbias en de optimismebias van belang. De bevestigingsbias ontstaat doordat mensen de neiging hebben om vooral de risico's te zien die ze verwachten te zien of die aansluiten bij hun mening. De beschikbaarheidsbias ontstaat doordat mensen risico's overschatten van dreigingen waarover ze veel gehoord of gelezen hebben en ze onderschatten risico's van dreigingen die ze niet goed kennen. De optimismebias ontstaat doordat mensen hun eigen kennis en vaardigheden overschatten en de risico's ten aanzien van hunzelf en hun organisatie onderschatten.
Zelfs als de medewerker een juiste perceptie van de situatie heeft, dan betekent dat niet per se dat de medewerker ook positief staat tegenover het voor die situatie benodigde informatieveilig gedrag. De medewerker weet dan weliswaar op basis van de perceptie welk gedrag nodig is,



Figuur 1: Gedragsmodel met de factoren die van invloed zijn op het bewuste informatieveilig gedrag van medewerkers (1).

maar vindt toch dat hij of zij ervan af kan of moet wijken. In dit geval is de attitude, oftewel de houding of mening, ten aanzien van het benodigde gedrag afwijzend. De attitude is opgebouwd uit drie componenten: cognitieve attitude, affectieve attitude en gedragsmatige attitude (9). Ieder van deze componenten kan positief of negatief zijn en zo de motivatie positief of negatief beïnvloeden.

De cognitieve attitude is een rationele attitude. Het is gebaseerd op de mate waarin de medewerker enerzijds vindt dat het beoogde gedrag nuttig (effectief en proportioneel) en urgent is en anderzijds vindt dat er geen onredelijke kosten en moeite voor worden gevraagd.

De affectieve attitude is een gevoelsmatige attitude. Het is gebaseerd op een combinatie van gevoelsmatige aspecten:

1) het eigen gevoel ten aanzien van het benodigde gedrag, bijvoorbeeld de angst om gehackt te worden;
2) het uitstelgedrag, vooral als het activiteiten betreft waar de medewerker niet blij van wordt;
3) de subjectieve norm, oftewel de druk die de medewerker voelt om zich te conformeren aan wat hij of zij denkt dat anderen wenselijk vinden, met name als dit gerelateerd is aan belangrijke groepen zoals relevante peer-groepen, belangrijke personen of influencers;
4) de eigen betrokkenheid, bijvoorbeeld als de medewerker heeft geparticipeerd in het formuleren van veilige gedragingen.

De gedragsmatige attitude richt zich op het afstemmen van de eigen mening op het eigen gedrag, om de verschillen ertussen glad te strijken. In het kader van dit artikel is deze component minder van belang, omdat deze component vooral uit gedrag volgt en veel minder de oorzaak van gedrag is. Als de medewerker een goede perceptie van de situatie heeft en een positieve attitude ten aanzien van het benodigde informatieveilig gedrag, dan heeft dat een positief effect op de motivatie voor dat gedrag. Maar dan moet de medewerker wel vinden dat het betreffende gedrag uitvoerbaar is, ook door haar- of hem zelf (self-efficacy) (10).

Verder kunnen positieve gevolgen vanuit de organisatie, zoals complimenten of beloningen, de motivatie voor het

benodigde gedrag versterken. Anderzijds kunnen negatieve gevolgen vanuit de organisatie, zoals straffen, de motivatie juist verzwakken. De hierboven beschreven factoren die het bewuste informatieveilig gedrag van een medewerker beïnvloeden, zijn geresumeerd in figuur 1.

Toepassing van het model

Op basis van het hierboven beschreven model kunnen we voor een organisatie de stappen aangeven die nodig zijn om het informatieveilig gedrag van medewerkers te verbeteren. Uit het model blijkt dat de perceptie van een medewerker invloed heeft op diens attitude, die weer invloed heeft op diens motivatie, die weer invloed heeft op diens bewuste gedrag. Diezelfde logica moeten we dan ook terugzien in de aanpak van fouten in het bewuste gedrag. Dus de perceptie zo nodig aanpassen zodat de attitude optimaal afgestemd is op de situatie. Vervolgens de attitude aanpassen zodat de motivatie optimaal gebruik kan maken van de positieve insteek van de medewerker. En dat leidt dan tot het gewenste gedrag van de medewerker, mits de medewerker de benodigde vaardigheden heeft en de organisatie zodanig meewerkt dat het benodigde informatieveilig gedrag ook goed uitgevoerd kan worden.

Toch laat de praktijk zien dat er in veel organisaties wel erg makkelijk vanuit wordt gegaan dat alle geconstateerde fouten worden veroorzaakt door incapabele medewerkers, die hoognodig een bewustwordingscampagne moeten krijgen. Vaak is dit uitgangspunt onjuist en bovendien doet het geen recht aan de variatie van mensen en functies binnen de organisatie. Daarom is het goed om eerst de geconstateerde fouten in het informatieveilig gedrag van de medewerkers te analyseren en de oorzaken te achterhalen.

Uit analyse van geconstateerde gedragsfouten blijkt dat het merendeel van de gedragsfouten van medewerkers wordt veroorzaakt door organisatiefouten. De organisatiefouten kunnen het gedrag van medewerkers ongunstig beïnvloeden door in te grijpen op de factoren die van invloed zijn op het bewuste informatieveilig gedrag van medewerkers, zie figuur 1.

Veelvoorkomende voorbeelden van organisatiefouten zijn:

- Er is geen adequaat informatiebeveiligingsbeleid of dit beleid is niet goed gecommuniceerd naar of uitgelegd aan de medewerkers. Dit heeft bij de medewerkers een negatieve invloed op de kennis van relevante dreigingen, mogelijke impact en relevante gedragingen. Van de medewerkers kan dan niet worden verwacht dat ze een goed beeld hebben van wat er qua informatieveilig gedrag van hun wordt gevraagd.
- Het hoger management geeft qua informatieveilig gedrag zelf niet het goede voorbeeld. Dit heeft bij de medewerkers een negatieve invloed op de mening over de urgentie van het gevraagde gedrag. De medewerkers veronderstellen dan dat het beoogde informatieveilig gedrag ook voor hun niet noodzakelijkerwijs nodig is en laten dit achterwege.
- Informatiebeveiligingsmaatregelen zijn ondoordacht, onsamenhangend, of te belastend voor de medewerkers, bijvoorbeeld niet actueel of ingevoerd zonder rekening te houden met de eigenaardigheden van de organisatie. Dit heeft bij de medewerkers een negatieve invloed op de mening over het nut van de maatregelen. De medewerkers verzinnen dan veelal workarounds.
- Informatiebeveiligingsmaatregelen zijn onvoldoende geïntegreerd in de organisatieprocessen. Voor de medewerkers komen de inspanningen voor informatiebeveiliging dan bovenop hun 'gewone' werk. Dit heeft bij de medewerkers een negatieve invloed op de mening over de redelijkheid van de benodigde kosten en moeite. De medewerkers omzeilen dan bij voorkeur de betreffende maatregelen.

Organisatiefouten eerst aanpakken

Een prettige bijkomstigheid van het aanpakken van organisatiefouten is dat hiermee in één moeite ook de oorzaken van fouten in het onbewuste informatieveilig gedrag kunnen worden aanpakt. Dat is dus nog een reden om te beginnen met het aanpakken van de organisatiefouten.

Als ná het oplossen van de organisatiefouten uit verdere

Figuur 2: Stappen in de aanpak van fouten in informatieveilig gedrag van medewerkers.

analyse van de geconstateerde fouten blijkt dat er toch nog het een en ander schort aan het informatieveilig gedrag van bepaalde groepen medewerkers, dan kan het nodig zijn om bij die medewerkers de gevonden lacunes in perceptie, attitude en/of vaardigheden aan te pakken. Dit moet dan wel doelgericht worden opgepakt bij de medewerkers die het betreft en niet bij de andere medewerkers. Organisatiebrede maatregelen, zoals postercampagnes of verplichte multiplechoicetests, hebben in het algemeen geen noemenswaardig positief effect. Figuur 2 resumeert de stappen waarmee het informatieveilig gedrag van medewerkers verbeterd kan worden.

Conclusie

Medewerkers in organisaties maken fouten en veroorzaken zo incidenten, ook met betrekking tot al dan niet digitale data. Voor het aanpakken van deze fouten is inzicht nodig in het informatieveilig gedrag van medewerkers en daarvoor is een geschikt gedragsverklarend model nodig. De gedragsverklarende modellen die in de informatiebeveiligingswereld gangbaar zijn, hebben zo hun beperkingen. Daarom hebben we in dit artikel een alternatief model gepresenteerd, zie figuur 1.

Met dit gedragsverklarende model in de hand kunnen we niet alleen fouten in informatieveilig gedrag van medewerkers verklaren, maar ook organisatiefouten. Voor het aanpakken van fouten in het informatieveilig gedrag van medewerkers kan een stapsgewijze aanpak worden gevolgd, zie figuur 2. De aanpak begint bij het vinden en oplossen van organisatiefouten, omdat daarmee al een flink deel van de fouten in het bewuste en onbewuste informatieveilig gedrag opgelost kan worden.

Referenties

(1) Spruit, M., Oosting, D. & Kreffer, C. (2023). Factors that influence secure behaviour while using mobile digital devices. Information and Computer Security. https://doi.org/10.1108/ICS-02-2024-0035.
(2) Spruit, M. (2000). Human Error and Information Security. Whitepaper, Technische Universiteit Delft, Delft.
(3) Van Houten, P., Spruit, M., & Wolters, K. (2023). Informatiebeveiliging onder controle. Pearson.
(4) Bernstein, D. A. (2016). Psychology. Cengage Learning.
(5) Robbins, S. P., & Judge, T. A. (2019). Organizational Behavior. Pearson.
(6) Cybersecurity monitor 2021. CBS.
(7) Endsley, M.R. (1995). Toward a Theory of Situation Awareness in Dynamic Systems. Human Factors, 37(1), 32-64.
(8) Kahneman, D. (2011). Thinking, Fast and Slow. Farrar, Straus and Giroux.
(9) Ostrom, T. M. (1969). The Relationship between the Affective, Behavioral and Cognitive Components of Attitude. Journal of Experimental Social Psychology, 5(1), 12-30.
(10) Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. Psychological Review, 84(2), 191-215.