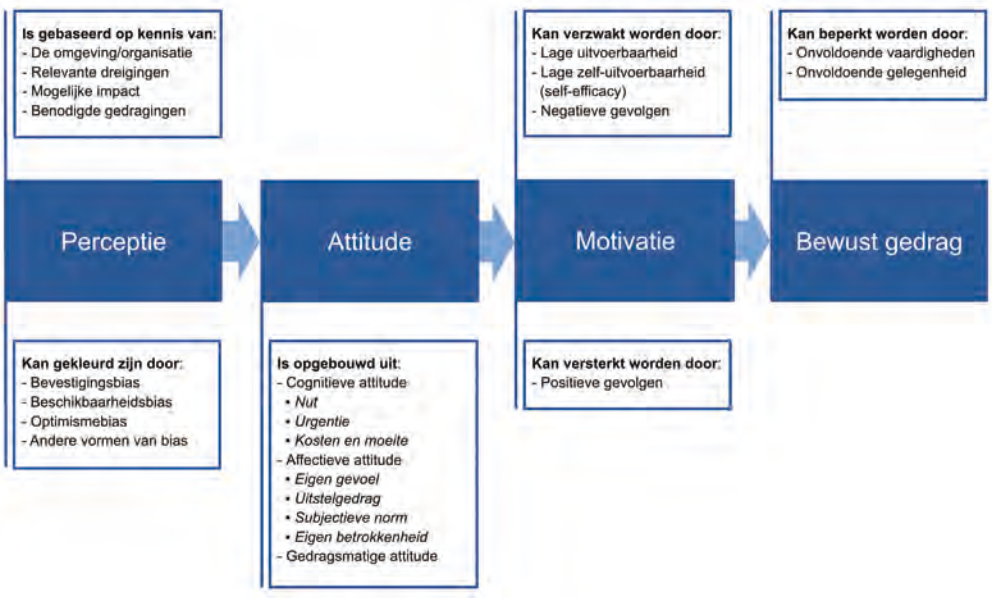
Auteurs: Marcel Spruit is Lector Cybersecurity aan het Kenniscentrum Cybersecurity van de Haagse Hogeschool in Den Haag. Hij is te bereiken op m.e.m.spruit@hhs.nl. Céline Kreffer was ten tijde van het onderzoek, waarop deze publicatie is gebaseerd, Onderzoeker Cybersecurity aan het Kenniscentrum Cybersecurity van de Haagse Hogeschool. Inmiddels is zij Analist Bestuurlijke Informatie bij het Ministerie van Justitie en Veiligheid in Den Haag.

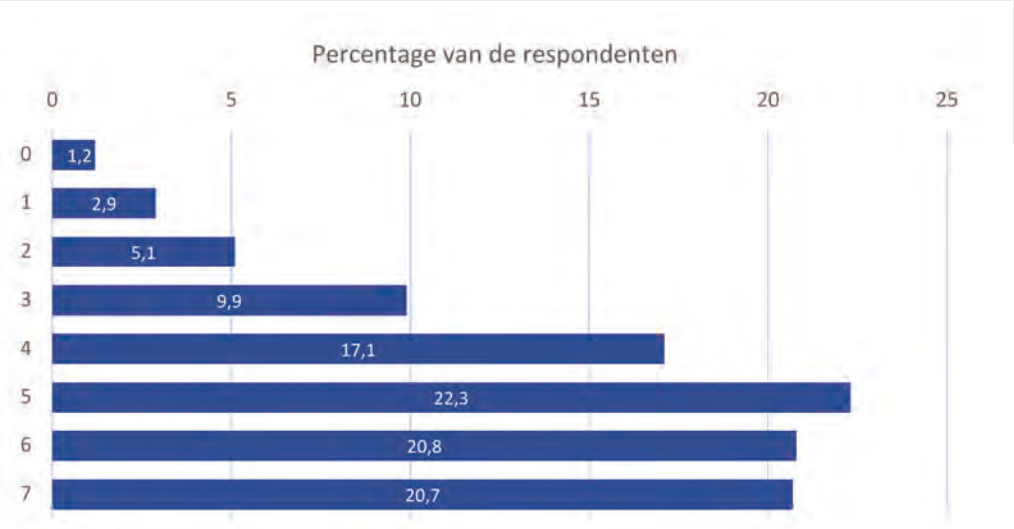
Veldonderzoek naar (on)veilig gedrag

Het is waardevol om een praktisch en wetenschappelijk onderbouwd model te hebben om menselijk gedrag – en de fouten daarin – te verklaren. Maar zo'n model bevat veel factoren. Welke daarvan zijn relevant voor veilig gebruik van mobiele digitale media, zoals smartphones en laptops? In dit artikel bespreken we de belangrijkste factoren en hoe we hier in de praktijk mee om kunnen gaan.

In de informatiebeveiliging wordt de mens beschouwd als zwakke factor. Dit is niet geheel onterecht, want mensen maken fouten, veel fouten. Sommige mensen maken meer fouten dan anderen. Fouten worden echter lang niet altijd veroorzaakt door degenen die in de fout gaan, want ook de omgeving, bijvoorbeeld de organisatie waar iemand werkzaam is, kan fouten in de hand werken of de impact ervan verergeren. In ons vorige artikel (1) hebben we een wetenschappelijk gefundeerd gedragsmodel gepresenteerd, zie figuur 1. En bovendien hebben we laten zien dat dit model gebruikt kan worden voor het stapsgewijs aanpakken van fouten in informatieveilig gedrag van medewerkers in een organisatie.



Figuur 1: Gedragsmodel met factoren (2).



Figuur 2: De uitvoering van O tot 7 veilige gedragingen.

Het model bevat nogal wat factoren en deelfactoren die het gedrag van iemand kunnen beïnvloeden. Dat doet de vraag rijzen of in de praktijk al die factoren wel van belang zijn of dat we slechts met één of een paar factoren rekening hoeven te houden.

Aanpak

Om bovenstaande vraag te kunnen beantwoorden, hebben we een veldonderzoek gedaan op basis van een breed uitgezette enquête over veilig gedrag met persoonlijke, mobiele, digitale media, zoals smartphones en laptops (2). Een aantal factoren uit figuur 1 zijn in dat geval dan niet van belang, zoals lage uitvoerbaarheid en onvoldoende gelegenheid.

Aangezien vragenlijsten in gangbare enquêtes niet de duidelijke antwoorden zouden opleveren die we wilden hebben, hebben we voor onze enquête een nieuw type vragenlijst opgesteld waarin we zowel naar het gedrag van de respondent in het afgelopen jaar vroegen, als naar de verklaring die de respondent daar zelf voor geeft. Voor het gedrag hebben we, op basis van relevantie en geschiktheid voor ons onderzoek, gekozen voor de volgende gedragingen:

1. verschillende wachtwoorden gebruiken;
2. beveiligingssoftware installeren;
3. VPN gebruiken;
4. privacy-instellingen voor software checken en zo nodig aanpassen;
5. toegang tot gevoelige gegevens op sociale media beperken;
6. onnodige cookies weigeren of aanpassen en
7. de locatiedienst uitzetten als deze niet nodig is.

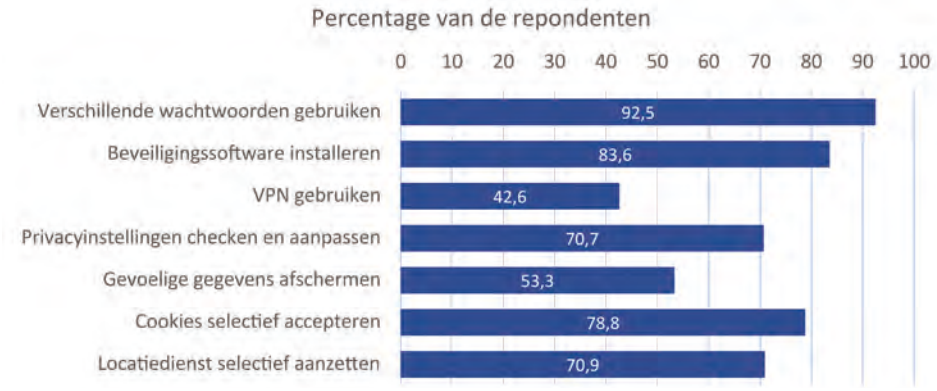
Uit vooronderzoek met respondenten waarvan het gedrag bij de onderzoekers bekend was, bleek dat respondenten hun eigen gedrag van het afgelopen jaar goed kunnen reproduceren, als dit gedrag gekoppeld is aan voor hun goed herkenbare beslissingen of activiteiten. Ook bleek dat de respondenten in een anoniem onderzoek in het algemeen eerlijk zijn over hun gedrag. We gaan er dan ook vanuit dat de antwoorden van de respondenten overeenkomen met hun feitelijke gedrag. Bovendien werd aan de respondenten gevraagd naar de verklaring die ze zelf geven voor hun gedrag. Uit het vooronderzoek bleek dat het voor respondenten moeilijk is om de psychologie achter hun eigen gedrag te verklaren. Daarom hebben we een lijst met herkenbare beweringen opgesteld waaruit de respondenten per gedraging de voor hun best passende beweringen konden kiezen. Dat bleek goed te werken. Op basis van de gemaakte keuzes konden de onderzoekers vervolgens bepalen welke gedragsbeïnvloedende factoren aan zet waren geweest. De enquête is anoniem uitgezet bij Nederlanders van twintig jaar en ouder. De respons kwam van 1.000 mensen, die samen een goede afspiegeling vormden van de Nederlandse samenleving van twintigplus (3).

Bevindingen

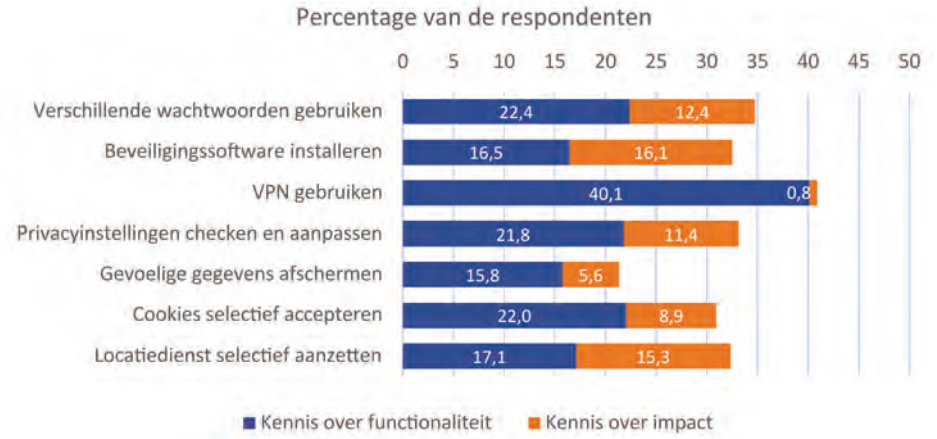
De resultaten van de enquête laten zien dat ongeveer 80% van de respondenten niet alle bevraagde veilige gedragingen uitvoeren, zie figuur 2. Ongeveer één procent van de respondenten gaf zelfs aan dat ze geen enkele hiervan uitvoerde.

De populariteit van de bevraagde veilige gedragingen verschilt aanzienlijk, zie figuur 3. Met name het gebruik van een VPN en het afschermen van gevoelige gegevens op sociale media komen er bekaaid vanaf. In figuur 4 zien we voor welk percentage van de respondenten het gemis aan de benodigde kennis de oorzaak was om een gegeven gedraging niet te doen. Hierbij maken we per gedraging onderscheid tussen twee deelfactoren, namelijk het niet weten wat de gedraging behelst (functionaliteit) en het missen van inzicht in de potentiële impact van het al dan niet doen van de gedraging. In de figuur zien we dat beide deelfactoren de oorzaak kunnen zijn van het niet uitvoeren van veilige gedragingen.

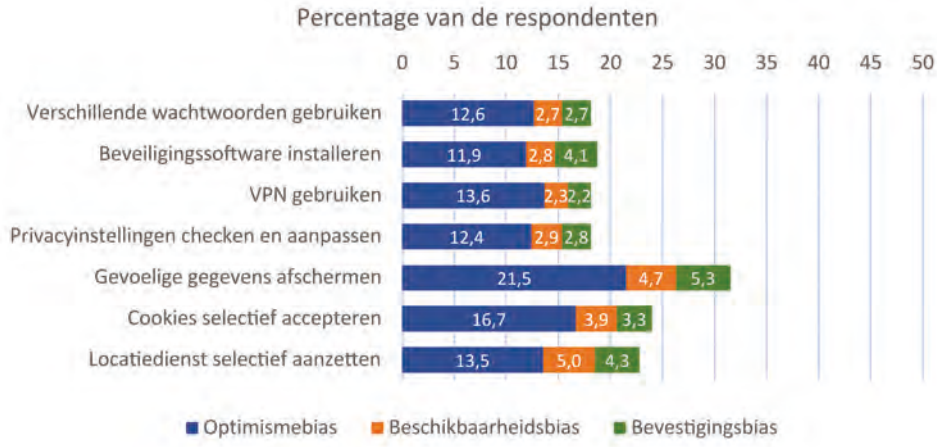
Degenen die een bepaalde gedraging en de impact ervan wel kennen, kunnen toch een door bias vertekende perceptie hebben. We maken per veilige gedraging onderscheid in optimisme-, beschikbaar-



Figuur 3: De uitvoering van veilig gedrag.



Figuur 4: Ontbreken van kennis als oorzaak voor nalaten veilig gedrag.

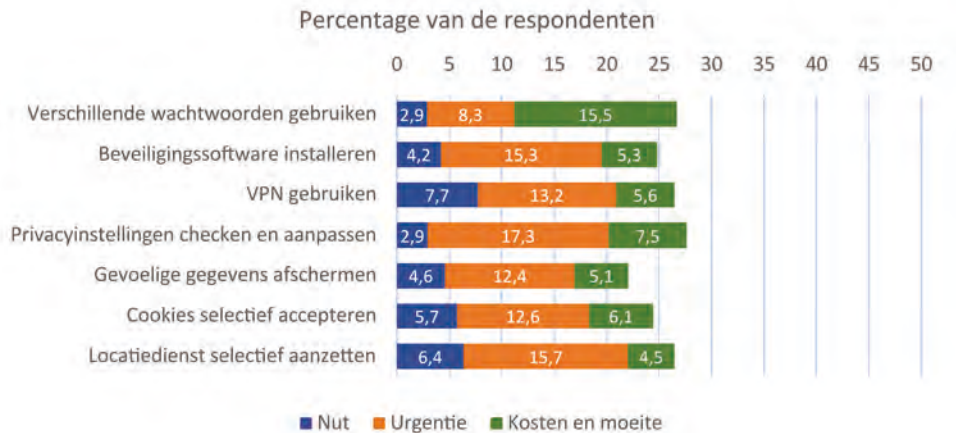


Figuur 5: Bias als oorzaak voor uitblijven veilig gedrag.

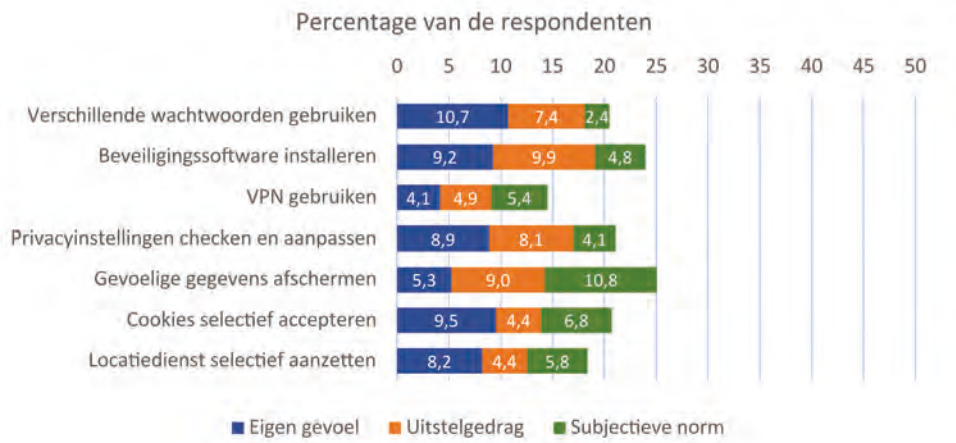
heids- en bevestigingsbias. In figuur 5 zien we alle drie vormen van bias, welke een oorzaak kunnen zijn - vooral optimismebias - voor het niet uitvoeren van veilige gedragingen. Als de perceptie in orde is, dan kan de attitude de oorzaak zijn van het niet uitvoeren van veilige gedragingen. Ten eerste de cognitieve attitude die een aantal rationele deelfactoren omvat, te weten; de mening over het nut van: de gedragingen, het gevoel van urgentie voor het uitvoeren van de gedragingen alsook de kosten en moeite die gemoeid zijn met het uitvoeren van de gedragingen. In figuur 6 zien we dat al deze deelfactoren een oorzaak kunnen zijn van het niet uitvoeren van veilige gedragingen.

Ten tweede de affectieve attitude die een aantal gevoelsmatige deelfactoren omvat, te weten: het eigen gevoel (onderbuikgevoel), het uitstelgedrag en de subjectieve norm. In figuur 7 zien we dat alle drie de deelfactoren een oorzaak kunnen zijn voor het niet uitvoeren van veilige gedragingen.

Als we de gegevens uit de figuren 4 tot en met 7 met elkaar combineren, zie figuur 8, dan zien we dat er onderlinge verschillen zijn tussen de invloed die de verschillende factoren uitoefenen op de bevraagde gedragingen. Het gemis van relatief vaak de



Figuur 6: Cognitieve attitude als oorzaak van nalaten van veilig gedrag.



Figuur 7: Affectieve attitude als oorzaak van nalaten van veilig gedrag.

oorzaak van het niet uitvoeren van gedragingen. Dit speelt met name bij het niet gebruiken van VPN. Uit figuur 4 kunnen we opmaken dat het daarbij vooral gaat over functionaliteitskennis. Bij het niet goed beschermen van gevoelige gegevens op sociale media speelt met name bias een rol. Uit figuur 5 kunnen we opmaken dat het vooral de optimismebias betreft. Het meest opvallende in figuur 8 is echter dat geen van de factoren onbelangrijk blijkt te zijn. Alle factoren spelen in de praktijk een rol van betekenis. In de figuren 4 tot en met 7 zien we dat dit ook geldt voor de deelfactoren.

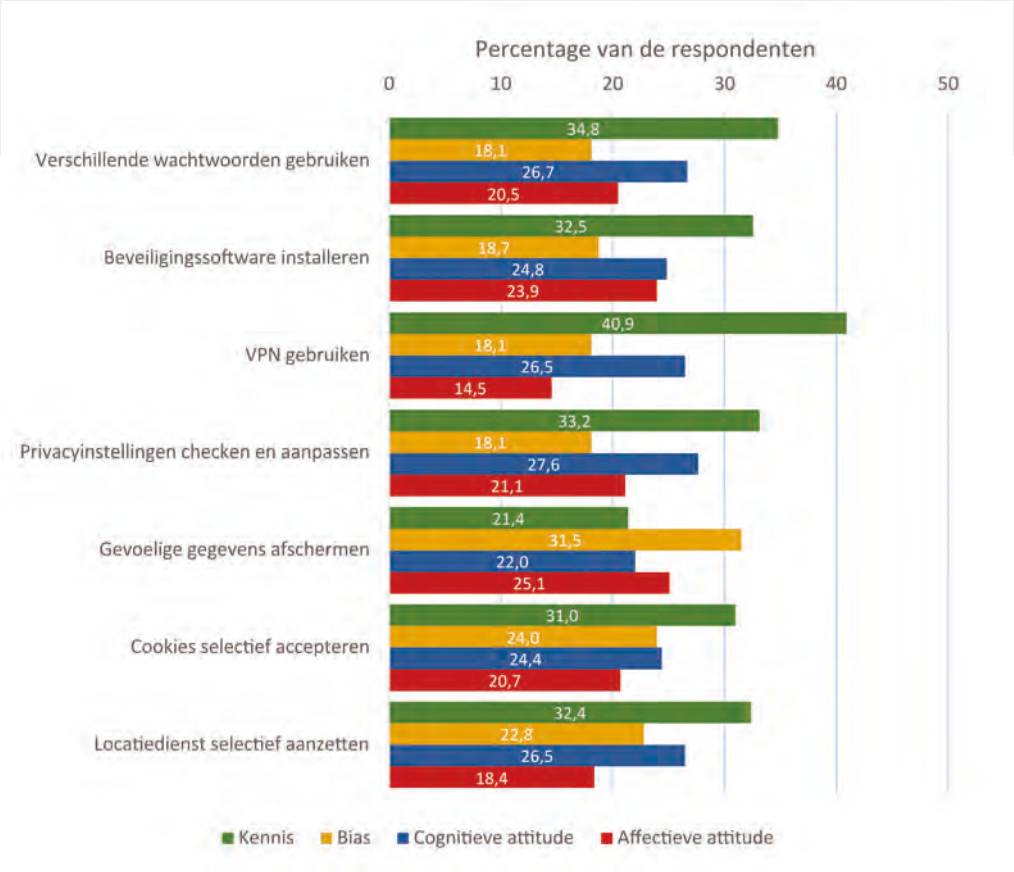
Implicaties voor organisaties

In de vorige paragraaf hebben we gezien dat alle bevraagde gedragsbeïnvloedende factoren een duidelijke invloed op veilig gedrag kunnen hebben. Aangezien iedere factor voor het verbeteren ervan om een specifieke aanpak vraagt, zijn er meerdere verschillende aanpakken nodig. Zo kan bijvoorbeeld iemands kennis worden verbeterd door de betreffende persoon een cursus te laten volgen. Bias kan bijvoorbeeld worden aangepakt door de betreffende persoon een simulatie of spel te laten doen, waardoor de persoon een beter beeld krijgt van de werkomgeving en de daarin relevante risico's en benodigde gedragingen (4). De cognitieve attitude, oftewel de mening die iemand heeft over het nut en de urgentie van het benodigde gedrag en de kosten en de moeite die daarvoor nodig zijn, kan bijvoorbeeld worden verbeterd door de informatiebeveiligingsmaatregelen in de organisatie goed in te richten en het daarvoor benodigde gedrag te integreren in de dagelijkse werkprocessen (5). De affectieve attitude, oftewel iemands eigen gevoel, uitstelgedrag, subjectieve norm en eigen betrokkenheid, kunnen bijvoorbeeld worden verbeterd door peers in te schakelen en medewerkers te betrekken bij informatiebeveiligingszaken (6,7). Hieronder is per gedragsbeïnvloedende factor aangegeven welke aanpakken daarbij passen (4,5,6,7). De opsomming beoogt niet volledig te zijn, maar geeft voor iedere factor één of meer geschikte aanpakken voor verbetering. De (deel)factoren die in cursief zijn weergegeven, zijn niet in de enquête meegenomen, omdat ze niet relevant zijn voor de veilige omgang met persoonlijke mobiele digitale media. Maar binnen een organisatie zijn ze wel relevant.

Gedragsbeïnvloedende factoren en bijpassende verbeteringen (4,5,6,7).

Kennis

- Functionaliteit:
  - Laat de medewerkers die het betreft één of meer relevante



Figuur 8: De relatieve invloed van de factoren op al of niet veilig gedrag.

cursussen volgen en toets of de benodigde kennis er daarna wel is.

- Impact:
  - Voorzie de medewerkers van relevante informatie met betrekking tot de informatiebeveiliging. Voor een manager kunnen dat bijvoorbeeld test-, audit- en incidentrapportages zijn.
  - Laat interne of externe autoriteiten de medewerkers uitleggen wat de impact van bedreigingen kan zijn. Voor een uitvoerend medewerker kan diens manager dit oppakken. Voor een strategisch manager kan dit de CISO, de auditor, of de toezichthouder dit oppakken.

Bias

- Bevestigings¬-, beschikbaar¬heids-, of optimismebias:
  - Geef de medewerkers die het betreft inzicht in hun bias zodat ze deze kunnen bijstellen. Hiervoor kunnen ze daarvoor bedoelde simulaties of spellen doen, waarin ze leren om hun werkomgeving en de daarin relevante risico's en het benodigde gedrag beter in te schatten.

Cognitieve attitude

- Nut:
  - Implementeer de beveiligingsmaatregelen zodanig dat ze effectief en logisch zijn voor alle medewerkers die ermee te maken hebben.
- Urgentie:
  - Laat managers en ervaren collega's de medewerkers uitleggen welke maatregelen waarom en wanneer nodig zijn en wat er kan gebeuren als de maatregelen niet of niet goed worden uitgevoerd. Om dat te staven, dienen de managers en ervaren collega's zelf het goede voorbeeld te geven.
- Kosten en moeite:
  - Integreer het voor informatiebeveiliging benodigde gedrag in de 'gewone' werkprocessen zodat het uitvoeren van beveiligings¬maatregelen een natuurlijk onderdeel van het 'gewone' werk is.
  - Implementeer de beveiligingsmaatregelen zodanig dat daarvoor geen onnodig lastig of tijdrovend gedrag nodig is.

Affectieve attitude

- Eigen gevoel, Uitstelgedrag:
  - Verlaag drempels voor het uitvoeren van de benodigde beveiligingsmaatregelen en richt de maatregelen in als 'hapklare brokken'.
  - Werk in teams waarin een sfeer ontstaat van 'we doen dit samen'.
  - Pas (zachte) dwang toe om de medewerkers die het betreft te stimuleren de benodigde maatregelen direct uit te voeren.
  - Beloon goed gedrag.
- Subjectieve norm:
- Schakel gewaardeerde collega's ('peers') van de medewerkers die het betreft in voor het geven van het goede voorbeeld en het stimuleren dat de betreffende medewerkers de benodigde beveiligingsmaatregelen ook goed uitvoeren.
- Eigen betrokkenheid:

- betrek de medewerkers bij het selecteren, uitwerken en evalueren van de benodigde beveiligingsmaatregelen. Doordat de maatregelen dan meer 'eigen' zijn, worden ze beter nageleefd.

Lage uitvoerbaarheid

- Implementeer de beveiligingsmaatregelen zo dat het uitvoeren ervan goed te doen is voor alle medewerkers die ermee te maken hebben.

Lage zelf-uitvoerbaarheid

- In het algemeen veroorzaakt deze factor met betrekking tot de beveiligingsmaatregelen op de werkvloer weinig problemen. Mocht dat toch het geval zijn, overweeg dan om de medewerkers die het betreft coaching te geven, waardoor ze het zelfvertrouwen op kunnen bouwen dat ze zelf de benodigde maatregelen uit kunnen voeren.

Positieve en negatieve gevolgen

- Implementeer de beveiligingsmaatregelen zodanig dat het uitvoeren ervan niet leidt tot represailles; en dat het niet - of niet goed - uitvoeren van de beveiligingsmaatregelen niet wordt beloond. Het belonen van goed gedrag kan een positieve invloed hebben.

Onvoldoende vaardigheden

- Verbeter de vaardigheden van de medewerkers die het betreft door het herhaald en onder begeleiding uitvoeren ervan in training, in simulatie of op de werkvloer.

Onvoldoende gelegenheid

- Implementeer de beveiligingsmaatregelen zodanig dat voor de medewerkers geen hindernissen worden opgeworpen om ze uit te voeren.

De genoemde gedragsbeïnvloedende factoren zijn persoonsgebonden en kunnen in een organisatie dan ook voor verschillende medewerkers in verschillende mate een probleem zijn. Daarom zal eerst vastgesteld moeten worden welke gedragsbeïnvloedende factoren bij welke medewerkers een probleem veroorzaken (1). Als bij een bepaalde medewerker is geconstateerd dat één of meer factoren een probleem zijn, dan kunnen die factoren voor die medewerker, met daarbij passende aanpak, gericht worden verbeterd. Sommige aanpakken worden op medewerkerniveau ingevuld, zoals het laten volgen van een cursus. Andere worden groepsgewijs opgepakt, zoals het inschakelen van peers. En soms aanpak voor de organisatie of een onderdeel ervan, zoals het goed inrichten van informatiebeveiligingsmaatregelen. Als bij een bepaalde medewerker meerdere factoren niet op orde zijn, dan geldt voor de aanpak ervan een bepaalde volgorde (1). Eerst dient bij de medewerker de kennis op orde te worden gebracht, want als de medewerker de benodigde gedragingen niet kan plaatsen of de relevantie er niet van inziet, dan komt het veilige gedrag er ook niet. Als de kennis op orde is, dan kunnen respectievelijk de bij de betreffende medewerker geconstateerde bias- en attitudeproblemen worden aangepakt. Organisatiefouten met betrekking tot de informatiebeveiliging, zoals een ongelukkige keuze van de beveiligingsmaatregelen of het niet betrekken van medewerkers bij de informatiebeveiliging, zouden al in een eerder stadium aangepakt en opgelost moeten zijn (1,5).

Conclusie

Op basis van het gedragsverklarend model dat we in ons vorige artikel hebben beschreven (1), hebben we gemeten welke gedragsbeïnvloedende factoren een rol spelen bij het niet uitvoeren van het benodigde, veilige gedrag. We hebben het onderzoek gericht op het veilig omgaan met mobiele digitale media, zoals smartphones en laptops.
Uit het onderzoek blijkt dat geen van de meegenomen gedragsbeïnvloedende factoren en deelfactoren onbelangrijk is. Alle factoren en deelfactoren spelen in de praktijk een rol van betekenis. Bij het ontwerpen van verbeteringsaanpakken voor veilig gedrag zal hier terdege rekening mee moeten worden gehouden. De in ons onderzoek opgestelde vragenlijst, of een variant daarvan, kan gebruikt worden om te bepalen welke gedragsbeïnvloedende factoren bij welke medewerkers niet op orde zijn. Op basis daarvan kunnen dan daarop toegespitste verbeteringsaanpakken worden ingezet bij de betreffende medewerkers, groepen, of organisatieonderdelen.

Referenties

(1) Spruit, M. & Kreffer, C. (2024). Informatie(on)veilig gedrag van medewerkers. IB Magazine, 5, 8-13.

(2) Spruit, M., Oosting, D. & Kreffer, C. (2024). Factors that influence secure behaviour while using mobile digital devices. Information and Computer Security. Https://marcelspruit.nl/papers/Spruit_Oosting_Kreffer_-_Cybersec_Awareness_-_IACS_2024.pdf

(3) CBS (2024). StatLine - Nederland in cijfers. Https://opendata.cbs.nl/statline/#/CBS/nl/

(4) Korteling, J.E., Gerritsma, J.Y.J., & Toet, A. (2021). Retention and Transfer of Cognitive Bias Mitigation Interventions: A Systematic Literature Study. Frontiers in Psychology, 12:629354.

(5) Spruit, M. (2010). Informatiebeveiliging en bewustzijn. De IT-Auditor, 1, 24-27.

(6) Pramaesti, A.V. et al. (2022). Reducing Laziness in Learning: A Review. The 15th University Research Colloqium 2022 Universitas Muhammadiyah Gombong.

(7) Felkey, A.J., Dziadula, E., & Chiang, E.P (2023). Microcommitments: Mitigating procrastination with more than a nudge. Southern Economic Journal, 90 (2), 497-509.