Veilig cybergedrag: niet ver

Net als voor fysieke beveiligingsmaatregelen geldt voor cyberveiligheid dat de techniek nog zo goed op orde kan zijn, als mensen klikken op links in phishing mails of gebruik maken van openbare WiFi-netwerken kan gevoelige data worden gelekt of kunnen computers worden besmet met ransomware. Bedrijven en organisaties proberen dit te voorkomen door het aanbieden van cyber awareness programma's aan medewerkers. In de praktijk zijn deze niet altijd effectief, onder meer omdat vaak bepaald gedrag wordt verboden in plaats van te zoeken naar alternatieven waarmee medewerkers hun doelen op een cyberveilige manier kunnen bereiken. Veilig cybergedrag komt echter niet neer op veranderen, maar op faciliteren.

Het is een bekend probleem: mensen doen niet altijd wat goed voor ze is. Veel mensen weten dat ze 250 gram groente per dag moeten eten, maar slechts 2 procent haalt dat (*1). Mensen kennen de richtlijnen, ze kennen de gezondheidsvoordelen en groente is makkelijk te vinden en betaalbaar. Waarom lukt het dan maar zo weinig van ons de 250 gram te halen? Omdat dit stuk over veilig cybergedrag gaat, gaan we niet verder in op eetgewoontes, maar één ding is zeker: het eten van groente heeft weinig te maken met awareness.

Hetzelfde geldt voor veilig cybergedrag. Mensen zijn steeds beter op de hoogte van de risico's die op de loer liggen: criminelen die je IT-systemen willen infecteren en je gegevens stelen. Technologie om je tegen deze dreigingen te beschermen wordt steeds beter. Toch zorgt onveilig menselijk gedrag regelmatig voor incidenten bij zowel organisaties als particulieren, met irritatie, chaos en schade als resultaat. Er wordt geschat dat mogelijk tot wel 95 procent van alle cyberincidenten te wijten is aan menselijk handelen (*2). Cyberincidenten zijn daarmee veel meer een menselijk probleem dan een technisch probleem (*3 en *4).

Veel bedrijven wapenen zich tegen deze menselijke risico's door hun personeel via awareness programma's en trainingen bewust te maken van cyberrisico's en hoe daarmee om te gaan. Google maar op 'cyber awareness programma' als je twijfelt over hoe populair awareness is. Helaas laat de werkelijkheid zien dat hoe noodzakelijk awareness ook is - en dat is het zeer zeker - het in veel gevallen niet voldoende is om het gewenste effect teweeg te brengen (*5).

Theorie Voordat we het hebben over een alternatieve manier om cyberveilig gedrag te stimuleren is een beetje theorie op z'n plek. In het kort zijn er drie verschillende manieren waarop gedrag tot stand komt. Ten eerste: automatisch gedrag dat het grootste deel van wat wij dagelijks doen voor zijn rekening neemt. Denk bijvoorbeeld aan het hard op de rem trappen als je voorligger dat ook doet: puur stimulus-respons. In de cyber wereld klik je in een moment van onoplettendheid automatisch op een phishing link: link, klik, klaar!

Ten tweede: gewoontegedrag, oftewel dingen die we vaak doen en waarover we slechts een beetje hoeven na te denken. Bijvoorbeeld het kiezen van de route die je 's ochtends naar je werk neemt: makkelijk maar net niet automatisch. Je checkt misschien de verkeersinformatie voordat je vertrekt, maar in principe neem je altijd dezelfde route ondanks dat een andere route wellicht korter of sneller zou zijn. In cyber kun je denken aan het gebruik van WiFi in de trein om op weg naar huis de laatste loodjes van het werk nog even af te handelen: niet veilig, wel een gewoonte.

Ten slotte kennen we weloverwogen gedrag, waarbij we echt moeten nadenken over iets dat we niet vaak tegenkomen. Bijvoorbeeld het afsluiten van een hypotheek. Welke vormen heb je met welke voordelen? Wat is het beste voor mij? Kan ik beter een adviseur in de arm nemen? In cyber kun je denken aan het als leek de veiligheid inrichten van je thuisnetwerk. Hier gelden dezelfde vragen als bij het afsluiten van een hypotheek. Wellicht ook met dezelfde onzekerheid over de antwoorden. Het probleem met weloverwogen gedrag is dat mensen er meestal weinig zin in hebben: het kost veel mentale energie en tenzij de motivatie en noodzaak groot genoeg zijn, zijn we eerder geneigd om ons er niet voor in te spannen. Dit is geen kwestie van luiheid, maar van beperkte mentale middelen die we gericht en geprioriteerd moeten inzetten.

Mismatch Een aannemelijke reden waarom awareness niet altijd even effectief is om cybergedrag te verande-

anderen maar faciliteren!

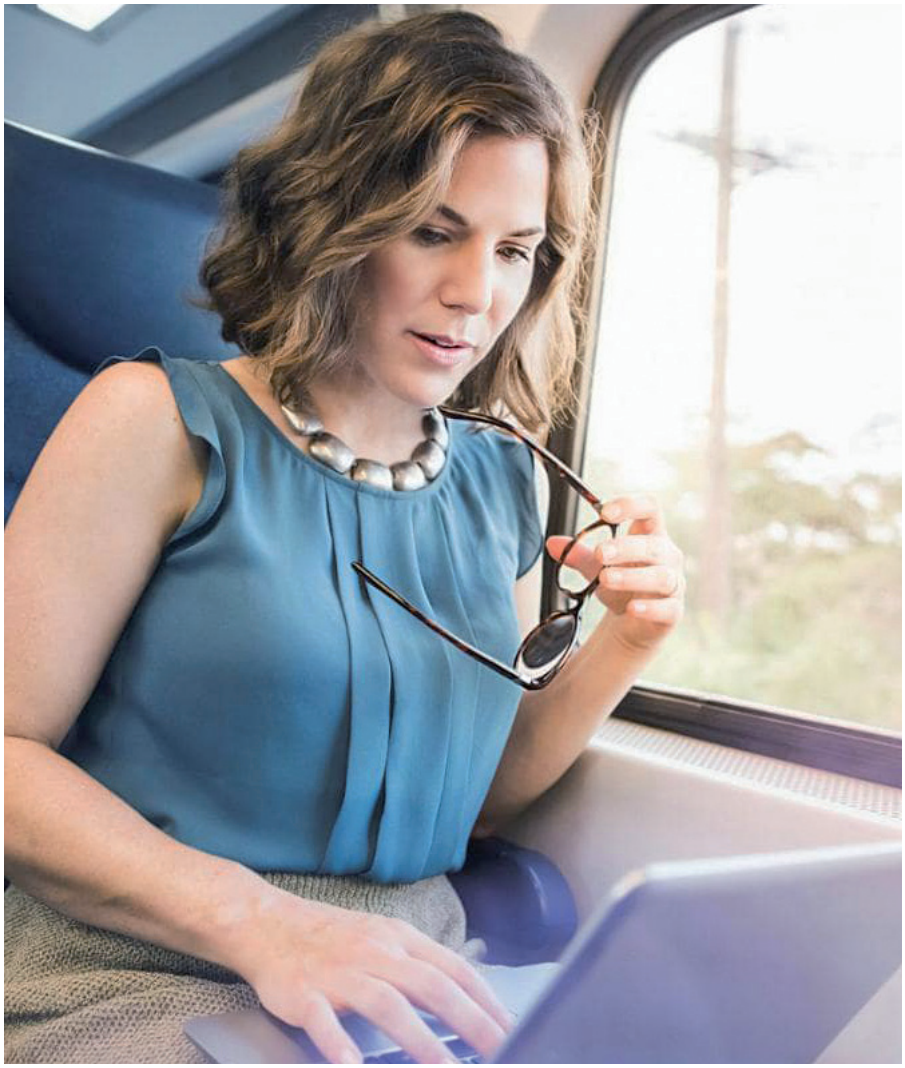
Probeer gedrag helemaal niet te veranderen. Ga in plaats daarvan na waarom mensen onveilig gedrag vertonen - zoek naar hun onderliggende doelen - en probeer die doelen op een cyberveilige manier te faciliteren.

ren, is dat het een beroep doet op een weloverwogen denkproces om automatisch of gewoontegedrag te veranderen. Er is een inherente mismatch tussen het niveau waarop het probleem zich afspeelt en het niveau waarop de oplossing wordt gezocht. Trainingen die veilig gedrag laten herhalen zijn wel beter, maar kunnen vaak nog steeds niet op tegen ingeslepen of aangeleerde gewoontes of gedrag dat niet onder onze bewuste controle staat. Zoals de CTO van IBM Resilient het zo doeltreffend zei: '…je kunt gebruikers niet trainen om niet op links te klikken nadat je hen de afgelopen twee decennia hebt geleerd dat links er zijn om op geklikt te worden.' (*6)

Een andere belangrijke reden waarom awareness waarschijnlijk slechts matig werkt is dat awareness bedoeld is om gedrag te veranderen of verbieden, dat mensen simpelweg graag willen doen. Anders gezegd: het belemmert mensen in het behalen van hun directe doelen. Zoals we vaak zien, moeten lange termijn, abstracte belangen (cyberveiligheid) het meestal afleggen tegen onmiddellijke concrete beloningen (met spoed dat ene mailtje sturen). Even terug naar het voorbeeld van werken in de trein waar mensen dringende e-mails willen afhandelen. De beslissing de openbare WiFi in de trein wel of niet te gebruiken zal niet makkelijk worden beïnvloed door mensen enkel bewust te maken van de risico's. Het nastreven van hun doel 'dringende e-mails afhandelen' zal nog altijd zwaarder blijven wegen als er geen voor de hand liggend alternatief is.

Effectief Nu even vanuit een ander perspectief: laten we kijken naar waarom mensen WiFi in de trein gebruiken. Is er sprake van een deadline die gehaald moet worden? Het gaat dus waarschijnlijk helemaal niet om de WiFi zelf, maar om het gebruik van de WiFi als middel om een ander doel te verwezenlijken: op tijd dat belangrijke rapport opsturen. Als je mensen het makkelijk kunt maken hun doel te halen op een cyberveilige manier, heb je het probleem van de openbare WiFi opgelost. Laat bijvoorbeeld je medewerkers hun mobieltjes als hotspot gebruiken. Een bijkomend voordeel is dat een mobieltje meestal ook een stuk sneller is dan WiFi in de trein!

Wil je niet dat je personeel in het openbaar werkt wegens het risico op zogenaamd shoulder surfing? Verbied het niet! Kijk eerst naar waarom mensen in openbare ruimtes werken. Het is meestal niet omdat ze indruk willen ▸



maken op omstanders, maar eerder omdat ze hun tijd nuttig willen gebruiken. Faciliteer dit door ze privacyfilters te geven voor hun beeldschermen. Zo kan je personeel hun tijd effectief gebruiken op een cyberveilige manier. Zo zijn er zo veel manieren om cyberrisico's te lijf te gaan die mensen ontlasten in plaats van belasten.

Phishing mails Nog één voorbeeld met twee kanten: klikken op links in phishing mails. Enerzijds weten we uit onderzoek (*7) dat mensen vaak klikken in een moment van onoplettendheid. Mensen weten dat het onveilig is en doen meestal hun best om niet te klikken. Soms kan het echter zijn dat ze te druk zijn met andere dingen en er per ongeluk op klikken. Het is moeilijk om een automatisch respons (klikken) te onderdrukken wanneer je weinig gelegenheid hebt om na te denken (wanneer je heel druk bent). In dergelijke gevallen zal het vergroten van awareness niet helpen; mensen zijn zich al bewust dat ze niet moeten klikken, maar een ongeluk zit in een klein hoekje. Zoek dus de oplossing bijvoorbeeld in het presenteren van mail van onbekende afzenders in platte tekst waarbij de links niet actief zijn en je het automatische van het klikken onderbreekt.
Anderzijds weten we uit hetzelfde onderzoek dat mensen soms op phishing mail links klikken omdat ze nieuwsgierig zijn. Dit is een ander probleem dan per ongeluk klikken, en vraagt dus om een andere oplossing. Omdat het hier om een bewuste beslissing gaat om te zien wat achter de link schuilt, kunnen awareness, nieuwe handvatten en training mogelijk wél effectief ingezet worden. Train mensen met de muis over de link heen te gaan en naar de URL te kijken. Is het bonafide of verdacht? Leer ze de URL handmatig in de browser in te typen in plaats van op de link te klikken. Hoe dan ook, geef ze een veilige manier om hun nieuwsgierigheid te bevredigen in plaats van het gedrag te verbieden.

Handig In het kort: probeer gedrag helemaal niet te veranderen. Ga in plaats daarvan na waarom mensen onveilig gedrag vertonen - zoek naar hun onderliggende doelen - en probeer die doelen op een cyberveilige manier te faciliteren. Neem hierin mee het niveau waarop het gedrag zich afspeelt: automatisch, gewoontematig of weloverwogen. Wanneer veilige alternatieven net zo makkelijk en handig zijn als de onveilige, begin je pas echt cyberveilig gedrag te stimuleren.

■ Dr. Heather Young, Dr. Remco Wijn, Drs. Richelle van Rijk
TNO Soesterberg, Afdeling Human Behaviour and Organisational Innovation

***1) https://www.rtlnieuws.nl/gezondheid/we-eten-veel-te-weinig-groente-maar-hebben-dat-niet-door**
***2) IBM (2015). IBM Cyber Intelligence Index; analysis of cyber attack and incident data from IBM's worldwide security services operations.**
***3) https://www.bcg.com/publications/2018/cybersecurity-human-problem-masquerading-technical-problem.aspx**
***4) Wijn, R., van den Berg, H., Wetzer, I., Broekman, C. (2016). Supertargets: Verkenning naar voorspellende en verklarende factoren voor slachtofferschap van cybercriminaliteit. TNO Rapport nr. 2015 R11499. TNO Soesterberg.**
***5) http://www.nextgov.com/cybersecurity/2014/10/do-we-really-need-more-cyber-awareness/95981/**
***6) https://www.schneier.com/blog/archives/2016/10/security_design.html**
***7) Van Vliet, T., Broekman, C., van Hemert, D., Prins, S., Rijk, R., Wijn, R., Young, H., Brusselers, M., Coetsier, D., Hueting, T., Jol, S., Langefeld, A., & Verburgh, T. (2017). Human Factors in Cybersecurity: Een conceptueel raamwerk en empirische toepassingen. TNO Rapport nr. 2017 R11574. TNO Soesterberg.**