Het gaat niet alleen om kennis van cybersecurity, ook om gedrag

Als psycholoog in de wereld van cybersecurity is en blijft Inge Wetzer een beetje een vreemde eend in de bijt. Het vakgebied van cybersecurity bestaat grotendeels uit IT'ers, informatiebeveiligingsspecialisten en techneuten. Maar het is tegenwoordig juist vaak via de mens dat een bedrijf wordt aangevallen. Hoe wapen je je daartegen? Inge Wetzer deed er onderzoek naar.

Door Rosalie de Groot en Cindy van der Helm
Fotografie Patricia van Dun

Inge Wetzer is gepromoveerd in de sociale psychologie. Na 10 jaar onderzoek naar gedragsbeïnvloeding bij TNO is zij sinds 2015 gespecialiseerd in cybersecurity. Ze werkt momenteel bij Secura als sociaal psycholoog cybersecurity & compliance in het team dat zich richt op de 'menskant' van informatiebeveiliging.

Vijftien jaar geleden waren de aanvallen nog een stuk minder geavanceerd dan nu. Destijds bestond de grootste cyber-aanval op de mens nog uit slecht geformuleerde e-mails over een erfenis van een Nigeriaanse prins. Daar konden de IT'ers en cybersecurityspecialisten ons prima tegen wapenen en al gauw trapte haast niemand daar nog in. Tegenwoordig zijn de mensgerichte aanvalstechnieken van cybercriminelen echter een stuk vernuftiger. We zijn op het punt beland dat waarschuwen met e-mailtjes en posters niet meer volstaat. Geavanceerdere aanvallen vragen om geavanceerdere verdediging. Voer voor psychologen! Want zorg er maar eens voor dat mensen niet meer in deze aanvallen trappen…

Verschil tussen weten en doen

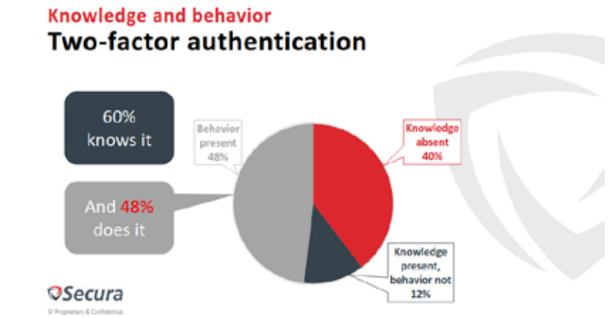
Om mensen te weten tegen het feit dat cybercrime op de loer ligt, wordt vaak informatie gezonden over de do's en don'ts. En natuurlijk is het super belangrijk dat mensen weten wat ze moeten doen. Er zit alleen een verschil tussen wéten wat je zou moeten doen en dat daadwerkelijk doen.

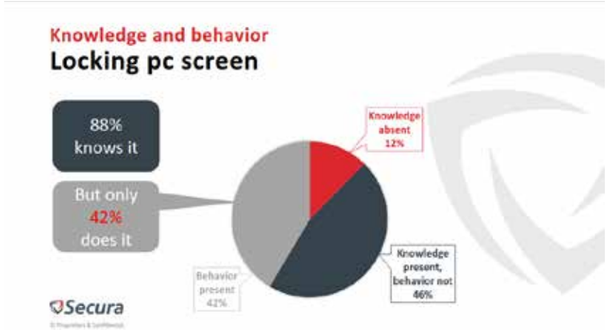
"Eigenlijk bestaat mijn baan eruit om mensen te bewegen tot daadwerkelijk veilig gedrag. Dat gaat verder dan communiceren. Soms moeten mensen juist gemotiveerd worden, of moeten technische zaken eenvoudiger gemaakt worden voordat men over een drempel heen kan stappen. Ook bestaat mijn baan er regelmatig uit om in normale woorden de techniek uit te leggen. Als ik iets niet snap dan vraag ik aan de techneuten om het mij uit te leggen. Pas als ik het goed begrijp kan ik het 'vertalen' naar anderen. En dat is waar het in de techniek vaak misgaat. Mensen snappen niet waarom ze iets moeten doen of juist laten wanneer een techneut aangeeft dat cybercrime op de loer ligt."

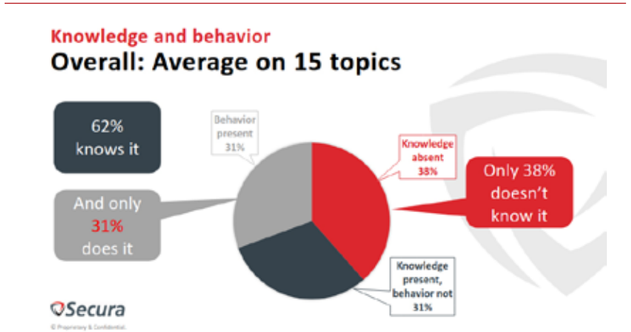
Laten we even bij het begin beginnen. Wie is Inge Wetzer en waarom is zij een vreemde eend in de bijt? Inge is afgestudeerd in de economische psychologie. Daarna is zij gepromoveerd in de sociale psychologie en is vervolgens verdergegaan in psychologisch onderzoek, onder andere bij TNO, waarbij ze zich richtte op defensie en veiligheid. Zij deed steeds menskundig onderzoek in veiligheid gerelateerde vraagstukken. Dat kan zover gaan als "kan je mensen bij brand beter met auditieve of visuele signalen naar buiten sturen? Kan een politie of een ME bij boze hooligans beter een waterkanon in het zicht of om de hoek plaatsen?" Zij richtte zich dus steeds op het gedragskundige aspect van veiligheidsissues.

Aanvallen werden vernuftiger

Rond 2015 werden de cyberissues steeds groter. Vooral aan de menkant. Heel lang waren het alleen de slecht geformuleerde e-mails van 'de Nigeriaanse prins'. Daarbij konden IT-ers nog wel zorgen dat mensen er niet intrapten, maar de aanvallen werden vanaf 2015 steeds vernuftiger. Er was dus steeds betere bescherming nodig. Je merkte dat IT-ers het toen niet meer voor elkaar kregen om mensen weerbaar te maken. Toen ben ik me er als psycholoog mee gaan bemoeien. Ik was werkelijk de eerste psycholoog in Nederland die dat op zich nam en ja, ik was best wel een pionier. Eigenlijk bleek dat een hele goeie zet, omdat er best veel behoefte is aan informatie over de manier waarop je het gedrag van mensen kan veranderen. Dat is een groot verschil met wat er standaard gebeurt. Als niet-gedragskundigen proberen mensen weerbaar te maken tegen cyberdreigingen, dan beperken die initiatieven zich eigenlijk voornamelijk tot het communiceren van de regels: "Zorg nou dat je updates draait. Lock nou je computer. Klik niet op linkjes." En als men meer z'n best doet wordt die boodschap eigenlijk alleen vaker, ludieker of op meer plekken herhaald. Dus dan gaan ze posters maken, of ze gaan de informatie in een nieuwsbrief zetten. Vanuit de psychologie kan ik echter kijken naar de gedragsverandering die je wil zien. Hoe komt het nou dat mensen iets niet doen, ook al wordt het van ze gevraagd? Soms doen mensen niet wat je wil omdat ze de regels niet kennen, maar vaak zijn er andere oorzaken voor afwijkend gedrag."







Inge Wetzer is de eerste psycholoog die onderzoek heeft gedaan naar de kloof tussen de kennis en het gedrag van mensen op het gebied van cybersecurity. Deze afbeeldingen tonen enkele uitkomsten uit haar onderzoek.

Zijn mensen gemotiveerd?

Psychologie is de wetenschap van gedrag. Psychologie laat zien dat de oorzaak vaak meer is dan alleen maar gebrek aan kennis. Belangrijk naast kennis is motivatie. Vinden mensen iets wel belangrijk? Je kan iets wel weten, maar je moet het ook belangrijk vinden en het willen doen. Dat zag je ook wel tijdens de pandemie. De regels van het afstand houden, het thuisblijven en weinig in contact komen met andere mensen werden ook vaak niet opgevolgd. En dat was heus niet omdat de regels niet bekend waren. Dat zie je dus eigenlijk terug in elk gedrag. Naast iets weten moet je iets ook willen. Ik richt me dus vanuit de psychologie op hoe we kunnen zorgen dat mensen met betrekking tot cybercrime ook het goede gaan doen. Daar ontwikkel ik programma's voor en dat doe ik vanuit organisaties die hun medewerkers willen helpen om geen slachtoffer te worden van een menselijke fout. Dat ze te maken krijgen met ransomware, omdat een

Er is een kloof tussen weten en doen

medewerker op een fout linkje klikt of iets dergelijks. Of dat ze in de krant komen, omdat een medewerker vertrouwelijke informatie laat slingeren. Bedrijven zien steeds vaker in dat het belangrijk is om daar aandacht aan te besteden. Want hacks via mensen zijn gevaarlijk.

Gevaar komt van twee kanten

Het kan aan twee kanten misgaan. Aan de ene kant kan het per ongeluk gaan. Dat kan zijn door slordigheid of nalatigheid. Je vergeet wel eens wat en we zijn ook maar mensen. Je klikt per ongeluk op een linkje of vergeet een belangrijk document mee te nemen uit de trein.
Aan de andere kant is er de cybercriminaliteit die zich steeds meer echt op mensen richt. De techniek is inmiddels steeds beter dichtgetimmerd. Maar als je daarentegen probeert iemand te bellen, om een wachtwoord vraagt en hij geeft het gewoon, dan kost dat weinig moeite. Waarom zou je dan al die moeite doen om te hacken? En om daar minder vatbaar voor te worden schakelen bedrijven Inge's team in. Zij zetten in op de menselijke kant en niet op de techniek.

Om haar bevindingen te onderbouwen heeft Inge onderzoek gedaan. Met de uitkomsten kunnen opdrachtgevers bovendien de kloof tussen kennis en gedrag binnen hun eigen organisatie identificeren en starten met de aanpak om die kloof te verkleinen. Net als in de beginjaren, toen Inge als psychologe pionierde in het cybersecurity wereldje, heeft zij nu als eerste onderzoek gedaan naar de kloof tussen de kennis en het gedrag van mensen op het gebied van cybersecurity.

Onderzoek met nulmeting

"Wat ik altijd heb verteld is gebaseerd op theorie. Het was 'gevoel', maar nu is mijn aanpak ook echt bewezen." Voor elke klant doet zij een nulmeting zodat zij over grote groepen mensen uitspraken kan doen. Al die nulmetingen doet zij op precies dezelfde manier, zodat zij alle data met elkaar kan vergelijken. "Ik heb data van bijna 1200 mensen en heb kennistesten gedaan met allerlei vragen over cyber. Bijvoorbeeld: "wanneer moet je je computer locken?". Ik vraag ook niet zomaar of mensen weten hoe ze een sterk wachtwoord maken. Nee, ik zet vier wachtwoorden op een rij en vraag welke het sterkst is. Daarnaast heb ik gevraagd wat mensen daadwerkelijk doen."

Belangrijk naast kennis is motivatie

Het is méér dan alleen awareness

Op die manier heeft Inge onderzoek gedaan naar circa 15 cybersecurity gerelateerde onderwerpen. Een van die onderwerpen is dus het locken van een computer. Uit het onderzoek is gebleken dat 88% van de mensen weet wanneer ze hun computer moeten vergrendelen. "Dan zou je denken, dan ben je klaar, want mensen weten het. Qua awareness zit het dus wel goed. Maar gebleken is dat slechts 42% dit ook op het goede moment doet. En 46% vergrendelt de computer zelfs helemaal niet. Qua awareness zit het dus wel goed, maar in termen van gedrag zijn we nog niet eens op de helft. Hieruit blijkt maar eens temeer dat we ons niet meer op bewustwording moeten richten. We moeten die extra stap zetten: naar het gedrag.

Ik merk dat mensen geneigd zijn om gedrag van medewerkers te veranderen door het positief te maken, bijvoorbeeld door beloningen te geven of een spelelement toe te voegen, terwijl het maar de vraag is of dat mensen beïnvloedt. Je weet immers niet waarom mensen het niet doen. Als mensen iets echt niet belangrijk vinden, is de oplossing soms gewoon afdwingen, bijvoorbeeld met twee-factor authenticatie."

Afdwingen kan effectiever zijn

"Iets wat ik echt vaak zie is dat veel bedrijven het structureel heel lastig hebben met medewerkers die hun personeelsbadge gewoonweg niet zichtbaar dragen terwijl dat wel van ze verlangd wordt. Mensen gebruiken hem alleen om binnen te komen en gooien de pasjes vervolgens overal neer, terwijl de organisatie graag wil zien wie er thuishoort op de werkvloer. Die passen zijn ook iets wat ik zelf veel gebruik als ik een test doe om te proberen ergens binnen te dringen. Als ik dat probeer is mijn eerste zet ook om te proberen een pasje weg te grissen. Of mensen hebben geen pas om, en dan val ik helemaal niet op. Als je gaat vragen, dan weten heel veel mensen wel dat het de bedoeling is dat je zo'n pas draagt, maar ze vinden het gewoon niet belangrijk. De motivatie ontbreekt. Als je dat gaat afdwingen, door bijvoorbeeld tussendeuren te plaatsen die op die pas open gaan of als je je pas nodig hebt voor koffie, dan gaat iedereen die pas dragen. Daar kan geen e-learning tegen op. Je gaat die pas dragen als het moet. Je kan mensen wel vragen of ze weten dat die pas verplicht is, maar dat gaat het gedrag niet veranderen. Er zijn ook bedrijven waarbij rokers alleen die pas dragen vanwege de rookingang. Aan de pas zie je dus wie er rookt en wie niet. Als mensen echt een reden hebben om die pas te dragen dan gaan ze dat wel doen. Soms is afdwingen veel efficiënter en effectiever dan mensen proberen te motiveren voor iets wat ze toch niet belangrijk vinden. Want laten we wel wezen, security komt er voor werknemers vaak maar bij. Mensen hebben een andere baan en aan dit, dat altijd zichtbaar dragen van een pas, moet je ook nog maar even denken. Ik ben dan ook van mening dat we het niet te veel van motivatie af moeten laten hangen. Hoeveel motivatie kan je verwachten van mensen die iets heel anders doen?"

Duidelijke regel, toch geen gehoor

"Ook het maken van updates is zo'n mooi voorbeeld. Dat is een duidelijke regel, en toch draaien mensen vaak geen updates. Als ik doorvraag waarom het zo belangrijk is om updates meteen uit te voeren en dat vervolgens uitleg aan werknemers, dan verandert de hele houding. Als er een update klaar staat is het blijkbaar bekend dat er een zwak punt in de software of applicatie zit. Door die update beschikbaar te stellen en aan te kondigen dat er een update is, maak je het ook wereldkundig dat er een kwetsbaarheid is. Alle hackers op de wereld weten bij een update dat er een kwetsbaarheid is. Hackers hebben dus vanaf het moment dat die update beschikbaar is de kans om van die kwetsbaarheid gebruik te maken. Bottom line: je moet de hackers voor zijn. Als mensen dat weten zijn ze veel eerder geneigd om te updaten. Hier is het waarom dus wel heel belangrijk.

Er zijn echter veel manieren om mensen te bewegen. Je weet alleen van tevoren nooit welke manier werkt. De crux is echt uitzoeken wat mensen tegenhoudt om iets te doen. Dat is iedere keer anders.
Het verhaal dat ik vanaf het allereerste begin afsteek blijft dus hetzelfde: richt je op veilig gedrag als einddoel en kijk wat mensen er nu nog van weerhoudt om het te doen, alleen de invulling verandert per scenario. Want dit is wat ik doe en dit is wat werkt."

Goede tip voor organisaties? Niet denken dat je weet wat er speelt. Ik spreek vaak directies die zeggen 'oh dat is gewoon gemakzucht. Mensen zijn te lui', maar als ik dan met medewerkers ga praten hoor ik andere dingen. Denk niet dat je exact weet wat er speelt op de werkvloer, ga echt open het gesprek in. Dat is heel belangrijk."

Eyeopeners

Het onderzoek levert meerdere eyeopeners op. "Over 15 onderwerpen zien we dat inmiddels gemiddeld 62% van de kennis algemeen bekend is. Mensen groeien mee met de ontwikkelingen. Eigenlijk zie je hier dat er over 1/3 van de onderwerpen nog kennis gezonden moet worden. Voor 2/3 van de onderwerpen niet meer. Als ze al budget vrijmaken voor cyber security, stoppen veel organisaties alles in e-learnings en kennis sessies. Dat kan handig zijn, maar over sommige dingen is alles al bekend. Ik doe altijd eerst onderzoek naar wat mensen al weten. Dan weet je welke e-learnings nodig zijn en welke niet zodat je niet iedereen hoeft te vermoeien met kennis die ze al in huis hebben en je je budget veel efficiënter kan gebruiken.
Over 38% van de informatie moet dus nog kennis worden verspreid. Bij 31% is het gedrag goed. Voor het andere deel moeten andere oplossingen bedacht worden. Soms moet je dan mensen motiveren door uit te leggen wat het risico is, door voorbeeldgedrag van het management te stimuleren of door het gedrag af te dwingen. Ik denk dat je daar een hoop mee kan bereiken.

Inge Wetzers baan bestaat eruit om mensen te bewegen tot daadwerkelijk veilig gedrag.
(fotograaf Melvin Tas)

Zorg ervoor dat je beter beveiligd bent dan de buren

En weet je, ik kom vast ook een keer aan de beurt. Ik ga vroeg of laat ook op een linkje klikken. We zijn allemaal mensen en iedereen heeft weleens haast. Alle basis dingen moet je verzorgen. De makkelijke dingen kan je wel voorkomen, maar als ze het echt op je voorzien hebben dan pakken ze je wel. Je kan nu eenmaal niet waterdicht zijn. Maar je kan wel zorgen dat je beter beveiligd bent dan de buren." <