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.

De kloof tussen awareness en gedrag

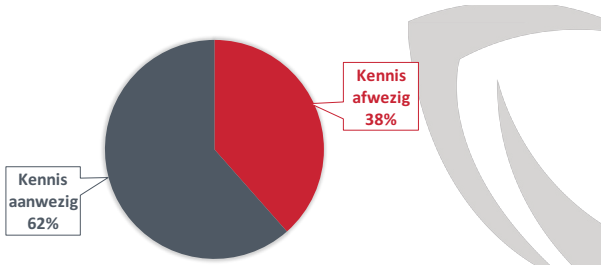
Deel 2 van drieluik: Onderzoek naar de human factor in informatiebeveiliging

Als we willen dat mensen zich cyberveilig gaan gedragen, moeten we verder kijken dan kennis en awareness. Kennis over cybersecurity leidt niet één op één tot het gewenste gedrag, wordt aangenomen, maar empirisch is dit nog maar weinig onderzocht. Hoe groot is die kloof tussen weten en doen in cybersecurity nou echt?

Dit artikel beschrijft onderzoek dat voor vijftien verschillende ISO-, NEN- en NIST-onderwerpen onderzocht hoeveel mensen nou wéten over cybersecurity en vervolgens in hoeverre zij het ook daadwerkelijk veilig handelen. Deze data maken de kloof tussen kennis en gedrag in cybersecurity inzichtelijk en geven daarmee beeld van wat er nodig is om mensen te bewegen naar het gewenste cyberveilige gedrag.

Even snel koffie halen zonder je computerscherm te vergrendelen. Je weet wel dat het eigenlijk geen goed idee is, maar de kans dat er iets misgaat is maar klein en het kost toch weer moeite om je wachtwoord opnieuw in te voeren. Een vertrouwelijk document even omgedraaid onder je toetsenbord leggen. Je weet dat je dat eigenlijk in je afgesloten kast moet opbergen, maar die heb je net dichtgedaan en de sleutel in het sleutelkastje gestopt en nu moet je rennen om je trein te halen… Traditionele awareness campagnes zijn gericht op het zenden van kennis. In de tijd dat cybersecurity nog een nieuw en onontgonnen terrein was, was dit uitermate belangrijk; om je veilig te kunnen gedragen, moet je wéten wat veilig gedrag is. De traditie van kennis zenden heeft zich voortgezet. De vraag of dit nog steeds de effectiefste manier is om gedrag te beïnvloeden, nu cybersecurity meer bekend is bij een breder publiek? Om die vraag te kunnen beantwoorden moet je weten hoe het staat met het huidige kennisniveau: hoeveel weten mensen eigenlijk over verschillende cybersecurity-onderwerpen? Deel 1 van dit drieluik beschreef de resultaten van een onderzoek naar het huidige kennisniveau, onder vijftien respondenten van twintig organisaties (Wetzer, 2021) (1).

De resultaten in figuur 1 laten zien dat wanneer we kijken naar het gemiddelde over de vijftien onderzochte onderwerpen, in 38% van de gevallen mensen niet het juiste antwoord gaven op de kennisvraag. In 62% van de gevallen wist men wel het juiste antwoord. Kennis ontbrak dus gemiddeld in iets meer dan een derde van de gevallen.



Figuur 1: Kennis gemiddeld over vijftien onderwerpen.

In termen van bewustwordingscampagnes zijn dit best mooie cijfers: in iets meer dan een derde van de gevallen ontbreekt het nog aan kennis. Voor de overige 62% hoef je niets meer te doen. Tenminste, als bewustwording je einddoel is. Bij doorvragen in organisaties blijkt echter bijna altijd dat men uiteindelijk toe wil naar veilig gedrag. Maar weten wat je moet doen is niet zomaar hetzelfde als ook daadwerkelijk veilig handelen. Dit besef wordt steeds breder gedeeld, alleen ontbraken tot nu toe de cijfers die dit konden onderbouwen en die inzicht gaven in hoe groot het verschil tussen weten en doen nou echt is in cybersecurity. Dit artikel beschrijft een onderzoek dat zich specifiek richt op het meten van de kloof tussen kennis en gedrag in cybersecurity.

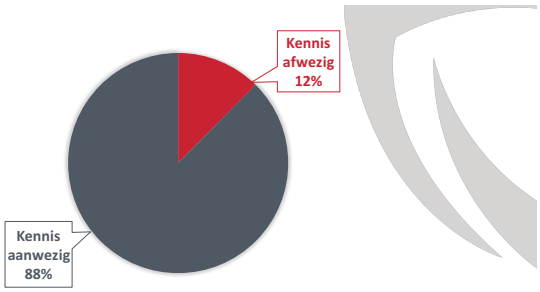
Onderzoeksmethode

Zoals in deel 1 werd beschreven, hebben we data van onze nulmeting van twintig organisaties in de zorgsector gecombineerd. Dit resulteerde in een dataset bestaande uit vijftien respondenten. De meting bestond uit een online vragenlijst met verschillende delen. Voor dit artikel richten wij ons op het kennisgedeelte en het gedragsgedeelte van de studie. Om een goed beeld te krijgen, zijn door cybersecurity-experts vijftien onderwerpen geselecteerd, gebaseerd op ISO-, NIST- en NEN-richtlijnen. Allereerst werd voor elk van deze onderwerpen een kennisvraag gesteld. Deze (meerkeuze-) kennisvraag is door experts vanuit verschillende vakgebieden (psychologen, cybersecurity-experts

en securityspecialisten uit de zorg) getoetst. Vervolgens werd voor ieder onderwerp een gedragsvraag gesteld. Hierin werd mensen gevraagd aan te geven op een schaal van 1 (nooit) tot 5 (altijd) of zij het gedrag ook daadwerkelijk vertonen.

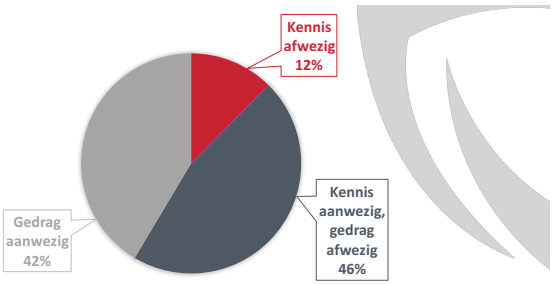
Cijfers

Om te beginnen een rechttoe rechtaan onderwerp: het vergrendelen van je computerscherm als je wegloopt bij je computer. De data uit de kennistest (figuur 2) laat zien dat 88% van de respondenten het juiste antwoord gaf op de vraag wanneer je je computerscherm dient te vergrendelen.



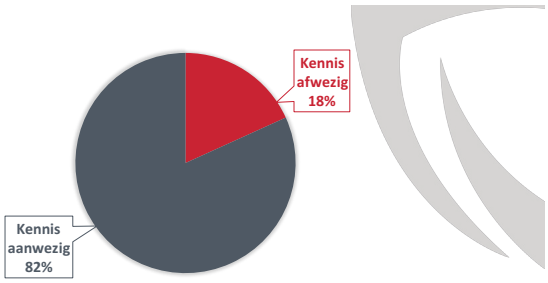
Figuur 2: Computerscherm vergrendelen: Kennis.

Op basis van deze cijfers zou je kunnen concluderen dat je bijna klaar bent. Slechts 12% weet het nog niet, geen slechte score als je ervan uitgaat dat weten betekent dat iemand het ook doet. Maar als we nu verder kijken en die groep die het weet vragen of ze het ook daadwerkelijk dóen, ontstaat er een heel ander beeld, zoals te zien is in figuur 3.



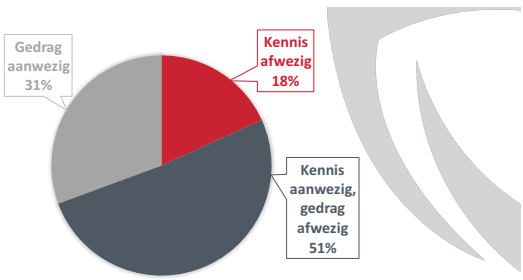
Figuur 3: Computerscherm vergrendelen: Kennis en gedrag.

Ondanks dat 88% van de respondenten in dit onderzoek dus wel degelijk wéét wanneer zij hun computerscherm horen te vergrendelen, geeft slechts 42% aan dat ook daadwerkelijk te dóen. Dat betekent dus dat meer dan de helft van diegenen die het weten, niet handelen naar deze kennis; 46% van de mensen in dit onderzoek heeft wél de kennis maar vertoont toch niet het juiste gedrag. Een kloof tussen kennis en gedrag voor dit onderwerp van 52% dus! Hoe zit dat voor andere onderwerpen? Eén van de andere onderzochte onderwerpen, is het kiezen van een sterk wachtwoord voor je werkaccount. Wanneer we mensen vroegen om uit verschillende wachtwoorden aan te geven welk wachtwoord het sterkst was, zagen we dat kennis over wachtwoordsterkte bij 82% van de respondenten aanwezig was (zie figuur 4). Hierbij is het van belang te weten dat er geen makkelijk te raden juist antwoord was, men moest echt op de hoogte zijn van wat een sterk wachtwoord definieert om het juiste antwoord te kunnen kiezen.



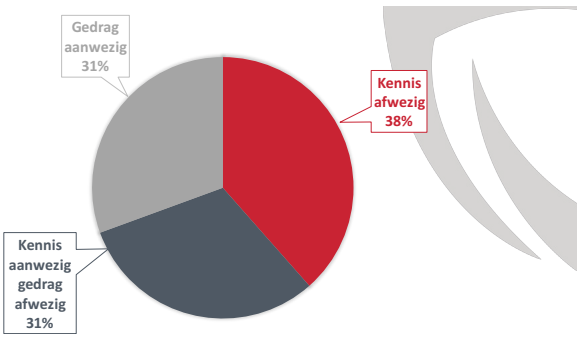
Figuur 4: Sterk wachtwoord: Kennis.

Vervolgens werd de respondenten gevraagd of zij zelf ook een sterk wachtwoord gebruiken voor hun werkaccount. De resultaten in figuur 5 laten zien dat weliswaar 82% van de respondenten wel weet wat een sterk wachtwoord is, maar dat slechts 31% van de respondenten ook daadwerkelijk een veilig wachtwoord gebruikt. Een kennis-gedragskloof van 62%.



Figuur 5: Sterk wachtwoord: Kennis en gedrag.

Bovenstaande data laat een grote kloof zien tussen kennis en gedrag in cybersecurity. Deze kloof was bij alle vijftien onderzochte onderwerpen aanwezig, maar er was wel een behoordelijke variatie in de grootte van deze kloof. Gemiddeld over vijftien onderwerpen werd het volgende beeld zichtbaar (figuur 6):



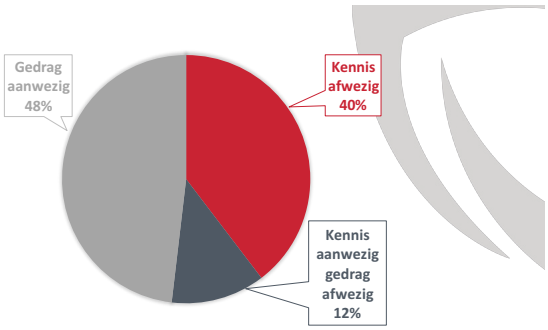
Figuur 6: Kennis en gedrag in cybersecurity gemiddeld over vijftien onderwerpen.

In 38% van de gevallen is kennis afwezig. In de overige 62% van de gevallen weet men wel het juiste antwoord op de kennisvraag (zie figuur 1). Wanneer we echter kijken naar gedrag, zien we dat van deze 62% mensen die het wéét, maar 31% aangeeft het ook daadwerkelijk te doen. Met andere woorden: over vijftien cybersecurity-onderwerpen gemiddeld, vertoont 31% van de mensen het gewenste gedrag. Als we kijken naar het percentage mensen dat wel over de noodzakelijke kennis beschikt (62%), zien we dus dat de helft (31%) van deze mensen daar ook naar handelt, en de andere helft (31%) niet. De kloof tussen kennis en gedrag in cybersecurity is dus 50%.

Veilig gedrag afdwingen

Zoals hierboven beschreven, is de kloof van 50% een gemiddelde over vijftien onderwerpen. Wanneer we meer inzoomen op specifieke onderwerpen, worden verschillende interessante patronen zichtbaar. Allereerst is er een sterk effect te zien van gedrag dat kan worden afgedwongen versus gedrag dat meer afhankelijk is van eigen keuzes. Hierboven werd de kloof tussen kennis en gedrag getoond: 52% voor het onderwerp 'computer vergrendelen' en 62% voor 'het kiezen van een sterk wachtwoord'. Beide onderwerpen betreffen gedrag waarbij de organisatie wel faciliterend kan zijn, maar veilig gedrag niet volledig kan afdwingen. Het is wel mogelijk om een computer na een korte tijd automatisch te laten vergrendelen, maar het is niet mogelijk om af te dwingen dat mensen zelf hun computer vergrendelen wanneer zij weglopen. Ook het gebruik van een sterk wachtwoord hangt nog af van de menselijke keuze. Technisch kan worden afgedwongen dat een wachtwoord een bepaald aantal karakters heeft en ook welke karakters er in ieder geval in moeten zitten, maar een wachtwoord als @msterdam01! voldoet al gauw aan deze eisen, zonder een sterk wachtwoord te zijn. Dus we kunnen mensen instrueren en feedback geven over wat een sterk wachtwoord is, maar of ze er uiteindelijk ook voor kiezen om daadwerkelijk een sterk wachtwoord te maken, is niet af te dwingen.

Er zijn ook gedragingen die wel (gedeeltelijk) af te dwingen zijn. Denk bijvoorbeeld aan het gebruik van tweefactorauthenticatie (2FA). Een organisatie kan ervoor zorgen dat mensen alleen maar in de beveiligde omgeving kunnen werken wanneer zij inloggen met een wachtwoord én een tweede factor, bijvoorbeeld een code die men ontvangt per SMS na het invoeren van het wachtwoord of een tag die gescand moet worden nadat het wachtwoord is ingevoerd. Voor de 60% van de respondenten die over de benodigde kennis beschikt voor wat betreft tweefactor-authenticatiebeleid binnen diens organisatie, bleek uit de analyse dat slechts 12% níet het bijbehorende gedrag daadwerkelijk vertoont. Dit komt neer op een kennis-gedragskloof voor 2FA van 20%. Dit is veel lager dan de gemiddelde kloof van 50%. Deze resultaten zijn in lijn met de hypothese dat de mogelijkheid om gedrag (technisch) af te dwingen een aanzienlijke invloed heeft op de kloof tussen kennis en gedrag.



Figuur 7: Tweefactorauthenticatie: Kennis en gedrag.

Wat kan ik met deze data?

De data in dit artikel geeft inzicht in de huidige status van kennis en gedrag in cybersecurity. Daarmee bieden ze handvatten voor stappen die genomen kunnen worden om cyberveiliger gedrag binnen organisaties verder te stimuleren en faciliteren. Wanneer we kijken naar het gemiddelde beeld, wordt namelijk duidelijk dat in 38% van de gevallen kennis de ontbrekende factor is. Welke onderwerpen dat voornamelijk betreft, werd in het vorige artikel van dit drieluik beschreven (Wetzer 2021) (1). Voor deze onderwerpen is de meeste winst te behalen door te beginnen met het verhogen van de kennis.

Dit artikel maakt duidelijk dat in 31% van de gevallen het juiste gedrag al wordt vertoond. Voor deze onderwerpen is dus geen verdere actie nodig. Wellicht is dit percentage in werkelijkheid nog wat lager omdat er sprake kan zijn van sociale wenselijkheid bij het invullen van het onderzoek. Wanneer mensen een rooskleuriger beeld schetsen dan de werkelijkheid, is de kennis-gedragskloof dus nog wat groter. Hoe dan ook blijft er zeker 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 kennis verhogende activiteiten, omdat hier sprake is van de kennis-gedragskloof. Sterker, ga je iemand die iets al weet maar het niet doet nog een keer uitleggen dat dit toch echt moet, dan schieten wij eigenwijze Nederlanders hoogstwaarschijnlijk in de weerstand. Om de kennis-gedragskloof te overbruggen, zal gekeken moeten worden naar de andere aspecten die gedrag beïnvloeden. Hier zal verder op worden ingegaan in het derde deel van dit drieluik.

Referentie

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