Authors: 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.

Het begint met bewustwording

Hoe ver zijn we daar inmiddels mee?

Deel 1 van drieluik 'Onderzoek naar de human factor in informatiebeveiliging'

Tijd voor een nieuw drieluik over cyberveilig gedrag. Omdat de aanvallen op de menskant in cybersecurity steeds geavanceerder worden, is het belangrijk om ook continu te blijven streven naar vernieuwende manieren om mensen weerbaar te maken. Dit drieluik beschrijft de resultaten van nieuw onderzoek naar de menskant van informatiebeveiliging. In dit eerste deel wordt aandacht besteed aan het huidige kennisniveau: Wat wéten mensen tegenwoordig wel en niet over cybersecurity?

De resultaten van het in de lead aangehaalde onderzoek, geven waardevolle inzichten in wat je kunt doen om het gedrag van medewerkers veiliger te maken. Nog vaak wordt er standaard gegrepen naar pogingen om regels te communiceren, zoals e-learnings, informatieve posters of awarenesstrainingen. Dit is echter alleen zinvol als ook echt blijkt dat die kennis ook daadwerkelijk ontbreekt. Is dat nog wel het geval?

Niet weten of niet doen?

Je wéét dat je niet mag appen in de auto, maar betekent dat ook dat je het nooit doet? Je wéét dat je genoeg moet bewegen en op tijd naar bed moet (zonder schermpje), maar doe je dat altijd? In ons dagelijks leven zien we overal voorbeelden van gedrag dat niet strookt met regels die we kennen, of met wat we weten dat goed voor ons is. Dat mensen zich niet volgens de regels gedragen lijkt een geaccepteerd feit; er is niemand die vreemd opkijkt als een voetganger snel even oversteekt terwijl het licht nog op rood staat maar er verder geen verkeer aankomt. Anderhalf jaar lang zagen we onze minister-president worstelen met het meekrijgen van de bevolking om de opgelegde regels na te leven; via aanspreken op verantwoordelijkheid, motiveren door te zeggen dat we er bijna zijn, streng worden als het niet goed ging. Uit alles mag duidelijk zijn dat menselijk gedrag zich niet makkelijk laat sturen.

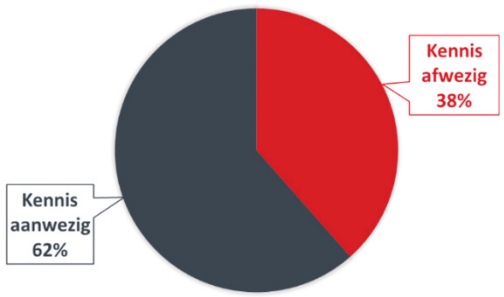
In de wereld van informatiebeveiliging lijkt dit besef maar langzaam door te dringen. Heel lang is ingezet op het communiceren van de regels. Communicatiecampagnes, trainingen en e-learnings werden ingezet om medewerkers te leren wat er van ze verwacht wordt. Voor het stuk daarna was nauwelijks aandacht. Maar zoals bij alle bovenstaande voorbeelden, is het weten van de regel geen garantie voor het bijbehorend gedrag. Wéten mensen het niet, dan moeten we het ze leren. Maar als ze het wél weten en ze doen het niet, dan volstaan communicatiecampagnes en leerinitiatieven niet meer, dan moeten we aan de slag met andere acties.

Hoeveel wéten mensen eigenlijk over informatiebeveiliging?

Om inzicht te krijgen in het kennisniveau ten aanzien van informatiebeveiliging, hebben wij data van onze nulmeting van twintig organisaties in de zorgsector gecombineerd. Daarmee kwamen we op een totaal van 1155 respondenten. De meting bestond uit een online vragenlijst die was opgesplitst in verschillende delen. Voor dit artikel richten wij ons op het kennisgedeelte van de studie. Om kennis te meten, zijn door cybersecurity experts vijftien onderwerpen geselecteerd, gebaseerd op ISO, NIST en NEN-richtlijnen. Voor elk van deze onderwerpen is vervolgens een (meerkeuze-)kennisvraag ontwikkeld die door experts vanuit verschillende vakgebieden is getoetst.

Allereerst het overall resultaat. Wanneer we kijken naar het gemiddelde over de vijftien onderzochte onderwerpen, zien we dat in 38% van de gevallen, mensen het verkeerde antwoord hebben gegeven op de kennisvraag. In 62% van de gevallen wist men wel het juiste antwoord. Kennis ontbreekt dus gemiddeld in iets meer dan één derde van de gevallen.

De bovengenoemde 38% is een gemiddelde. Opvallend was een grote spreiding tussen verschillende onderwerpen: voor sommige onderwerpen is het kennisniveau aanzienlijk hoger dan op andere onderwerpen. Dit varieert zelfs van 15% van de respondenten die het goede antwoord wist tot 96%. Interessante materie om verder in te duiken, omdat hieruit blijkt dat er onderwerpen zijn waarover we mensen dus vooral niet meer hoeven 'lastig te vallen' met communicatie omdat blijkt dat ze het echt wel weten. Tevens geeft het inzicht in waar de kennishiaten nog wél zitten. Dit stelt ons in staat om mensen dus veel gerichter te voorzien van díe kennis die nu nog ontbreekt, en ook alleen maar van díe kennis.



Figuur 1 - Kennis gemiddeld over 15 onderwerpen.

Wat weet men al wel?

De resultaten in tabel 1 laten zien dat voor vijf onderwerpen het kennisniveau boven de 80% ligt. Met andere woorden: voor vijf onderwerpen kunnen we stellen dat men het over het algemeen wel weet. Voor deze onderwerpen heeft het herhalen van de regels dus niet veel toegevoegde waarde. Het betreft de onderwerpen clean desk, het vergrendelen van je computer bij het weglopen, het aanspreken van een onbekende zonder (bezoekers)pas, het gebruiken van een sterk wachtwoord en het gebruiken van veilige of goedgekeurde tools voor videoconferencing.

Onderwerp	Kennisniveau
Clean desk	96%
Computer vergrendelen	88%
Onbekende aanspreken	82%
Sterk wachtwoord	82%
Videoconferencing	80%

Figuur 2 - Tabel 1.

Opvallend is dat de meeste van deze onderwerpen gemeen hebben dat ze gaan over zaken die tegenwoordig algemene kennis betreffen. Mensen hoeven niet per se bij de onderzochte organisaties te werken om te weten wanneer zij hun computer moeten vergrendelen. Sterker nog, deze vijf onderwerpen zijn inmiddels zo bekend dat de kans groot is dat bij een straatinterview, mensen ook de goede antwoorden geven. Dit komt omdat we gelukkig steeds wijzer worden op het gebied van cybersecurity! Waar tien jaar geleden mensen nog geld overmaakten naar een zogenaamde Nigeriaanse prins om aanspraak te maken op een erfenis, is het bewustzijn over de dreigingen de afgelopen jaren sterk toegenomen. Dat zien we duidelijk terug in deze cijfers. Belangrijke bevindingen want zo weten we waar we onze kennisinspanningen níet meer op hoeven te richten!

Wat weet men nog niet?

Ondanks het toenemende cyberbewustzijn, zien we dat er ook nog onderwerpen zijn waar de respondenten veel lager scoorden op aanwezige kennis. Voor deze onderwerpen is het dus van belang om mensen wél meer te leren en instrueren, zodat hun kennisniveau stijgt. Specifiek gaat dit over het herkennen of een URL naar de correcte of veilige website verwijst en over het herkennen van phishing.

Onderwerp	Kennisniveau
Herkennen URL	15%
Herkennen phishing	23%

Figuur 3 - Tabel 2.

Opvallend is dat beide onderwerpen waar de respondenten laag op scoorden, praktisch toegepaste onderwerpen zijn met een technische component. Op basis van deze data kan gesteld worden dat dit het gebied is waar mensen nog het meest behoefte hebben aan instructie. Aan de slag dus, laten we de mensen dit gaan leren. Belangrijk hierbij is wel te begrijpen dat leren en instrueren op veel verschillende manieren kan. De meest simpele vorm van leren bestaat uit het communiceren van de regels. Dit kan kort zijn, bijvoorbeeld middels een poster met een paar regels, of uitvoeriger in bijvoorbeeld een uitgebreide instructie. Maar naast het communiceren van regels, zijn er meer vormen van leren.
Een belangrijke leervorm in dit kader is trainen: Het aanleren en oefenen van nieuw gedrag. Waar communiceren stopt bij het zenden van de regels, gaat trainen verder doordat het nieuwe gedrag meer wordt ingeslepen. Door iets meer te doen en door feedback te krijgen, worden mensen beter. Vergelijkbaar aan trainen van een bepaalde sport. Juist deze praktische onderwerpen als het goed kunnen 'lezen' van een URL en het herkennen van phishing, lenen zich uitstekend voor training. Leer mensen eerst de basis door ze de nodige kennis te geven

en laat hen daarna aan de hand van voorbeelden oefenen om deze kennis toe te passen.

En de overige onderwerpen?

Hierboven hebben we toegelicht welke onderwerpen zeer hoog en zeer laag scoren op kennisniveau. Voor de overige zeven onderwerpen uit onze meting is een gemiddelde score te zien; tussen de 45% en de 71% van de respondenten gaven het goede antwoord. Het betreft hier de onderwerpen: het melden van incidenten, het delen van informatie per e-mail, het gebruiken van een uniek wachtwoord voor je werkaccount, het kennen van je handelingsperspectief nadat je informatie naar de verkeerde persoon hebt gestuurd, het gebruik van tweefactor authenticatie, het veilig opslaan van gegevens en het delen van vertrouwelijke bestanden.

Onderwerp	Kennisniveau
Incidenten melden	45%
Informatie delen per mail	55%
Uniek wachtwoord	56%
Handelen na datalek	60%
Tweefactorauthenticatie	60%
Veilig opslaan gegevens	66%
Delen vertrouwelijke bestanden	71%

Figuur 4 - Tabel 3.

Is er een overeenkomst te zien tussen deze onderwerpen? Jazeker: het betreft hier onderwerpen die merendeels te maken hebben met het beleid van een organisatie: Dat bepaalt immers welke incidenten gemeld moeten worden en waar, welke informatie wel en niet per mail gedeeld mag worden, welke andere opties voor veilig delen er zijn, wat de regels zijn voor tweefactor authenticatie enzovoorts. We zien hier dat in de onderzochte organisaties wel degelijk aandacht is geweest voor het verhogen van bewustwording op deze beleidsonderwerpen.
Deze data laten zien dat mensen dus best wat kennis hebben van deze beleidsonderwerpen, maar dat deze kennis nog niet heel hoog is. Om het juiste gedrag te kunnen vertonen, is het wel belangrijk dat men goed weet wat er verwacht wordt. Dat pleit ervoor dat ook deze onderwerpen nog wat aandacht mogen krijgen op het kennisvlak, zij het minder dan de operationele onderwerpen die we hierboven beschreven.

Wat kan ik met deze data?

De resultaten die in dit artikel beschreven worden, geven inzicht in het huidige kennisniveau op vijftien verschillende onderwerpen in informatiebeveiliging. Daarmee geven deze data richting aan de stappen die genomen kunnen worden om medewerkers verder cyberweerbaar te maken. Zo maakt het duidelijk welke onderwerpen nu nog kennisaanbod behoeven. Ook maakt het duidelijk op welke onderwerpen de kennisinitiatieven zich juist minder hoeven te richten.
Een kanttekening bij deze data is dat ze verzameld zijn bij twintig organisaties in de zorgsector. Uiteraard geven deze resultaten geen uitsluitsel dat het beeld bij organisaties in andere sectoren, of zelfs bij andere organisaties binnen de zorg, precies gelijk is. Om voor een specifieke organisatie aan de slag te gaan, is het dus interessant om te starten met een dergelijke meting. Dit voorkomt namelijk dat medewerkers lastig worden gevallen met e-learnings over zaken die zij al lang weten, wat zelfs tot weerstand kan leiden. Tevens zorgt het ervoor dat er wel gericht kennis kan worden aangeboden specifiek op díe gebieden waar kennis nog mist. Dat is dus veel efficiënter.

Betekent weten ook doen?

De resultaten van dit onderzoek geven dus een duidelijk beeld van het huidige kennisniveau op het gebied van informatiebeveiliging, uitgesplitst naar verschillende onderwerpen. Van hieruit is duidelijk welke onderwerpen nog aandacht behoeven op het vlak van kennisverhoging. Maar hoe zit het met de mensen die deze dingen al wél wisten? Dóen zij ook het juiste? Dus voor die onderwerpen waar het kennisniveau boven de 80% is? Zijn we daar dan klaar, zien we dat ook terug in gedrag? Het tweede deel van dit drieluik beschrijft onderzoek naar de kloof tussen kennis en gedrag in informatiebeveiliging: betekent weten ook dat mensen het doen, of zitten daar nog andere factoren tussen?