Auteurs: Rosanne Pouw, Product Manager Awareness & Training bij SURF rosanne.pouw@surf.nl. Marijke Stokkel, senior manager team Cybersecurity en verantwoordelijk voor de propositie security & privacy awareness marijke.stokkel@bdo.nl. Susanne van 't Hoff-de Goede, criminoloog en sr onderzoeker bij het Centre of Expertise Cyber Security, Haagse Hogeschool m.s.vanthoff-degoede@hhs.nl. Maaike van der Wal, criminoloog en junior onderzoeker bij het Centre of Expertise Cyber Security, Haagse Hogeschool m.l.vanderwal@hhs.nl.

Van twijfel naar enthousiasme

Innovatie in het meten van awareness en daadwerkelijk veilig gedrag

'Is het een idee om de awarenessmeting dit jaar anders aan te pakken?' Deze vraag groeide uit tot een unieke samenwerking tussen drie verschillende organisaties: SURF, BDO en de Haagse Hogeschool. Ondanks weerstand en complicaties maakten we een innovatieve gedragsmeting, onderdeel van de awarenessmeting bij onderwijs- en onderzoeksinstellingen. Een inspanning die naast het meten van kennis, ondersteuning en motivatie inzicht geeft in de voorspelling van daadwerkelijk cyberveilig en privacybewust gedrag.

SURF en BDO begonnen in 2021 met het meten van awareness bij onderwijs- en onderzoeksinstellingen. De meting is gebaseerd op het COM-B model voor gedragsverandering. Kort samengevat: hoe mensen zich gedragen wordt bepaald door wat zij weten en kunnen (bekwaamheid), willen (motivatie) en of zij gefaciliteerd worden (gelegenheid).

De deelname was op vrijwillige basis en voor maximaal 30 instellingen. De metingen bestonden uit onlinevragenlijsten voor medewerkers aangevuld met interviews. Deze rapportages werden vervolgens geanalyseerd om tot een sectorrapportage te komen. Met deze resultaten konden onderwijsinstellingen richting geven aan awarenessactiviteiten en het belang van awareness ondersteunen.

Toen Marijke Stokkel (BDO) in 2022 een presentatie gaf over deze meting, ontdekte ze dat er een nog een spreker op het programma stond die over het COM-B model zou spreken. Susanne van 't Hoff-de Goede (de Haagse Hogeschool) had gedragsmetingen ontwikkeld die ze afzette tegen het COM-B model. De link werd snel gelegd: de gedragsmeting combineren met de SURF-awarenessmeting zou voor beide partijen waardevolle inzichten kunnen opleveren.

Sterk wachtwoord

Hoe ging de gedragsmeting in zijn werk?

- Aan de deelnemers van de SURF-awarenessmeting werd bij aanvang gevraagd om een account aan te maken, inclusief een wachtwoord. Zonder account was het niet mogelijk om de meting te voltooien.
- Vervolgens werd aan de hand van 20 indicatoren gemeten hoe sterk het wachtwoord was (het wachtwoord zelf werd niet opgeslagen in de onderzoekstool). Voorbeelden van indicatoren zijn het aantal karakters, aantal cijfers, hoofdletters, speciale karakters en het aantal brute force pogingen nodig om het wachtwoord te kraken.
- Aan de hand van deze indicatoren werd een score (0-4) vastgesteld. Wachtwoorden met score 3 of 4 worden als 'sterk' bestempeld.

Delen van persoonsgegevens

Hoe ging de gedragsmeting in zijn werk?

- Aan het eind van de vragenlijst van de SURF-awarenessmeting kregen de respondenten het verzoek om een aantal persoonsgegevens in te vullen.
- Het betrof zeven soorten persoonsgegevens:
- Naam
- Adres
- Postcode
- Plaats
- Telefoonnummer
- Geboortedatum
- Medewerker nummer

Vervolgens werd gekeken of, en zo ja hoeveel, gegevens de respondenten deelden. Respondenten die helemaal geen persoonsgegevens deelden, kregen het stempel 'niet ongewenst delen persoonsgegevens'.

Start van de samenwerking

Toch waren er wat bedenkingen vanuit SURF. Deze aanpak zou de meting complex maken en mogelijk vertragingen opleveren. En wat als de instellingen hierdoor helemaal zouden afzien van de meting? Voor productmanager Rosanne Pouw (SURF) was dit de eerste keer dat ze de meting zou coördineren. Met enige twijfel en na een gesprek met Marijke en Susanne besloot ze toch mee te doen. SURF is een partij die graag innovatieve ideeën uitvoert en samenwerkt.

Het plan was om samen met de awarenessmeting daadwerkelijke ook het onlinegedrag te meten, en wel in de volgende (gefingeerde) situaties:

1) het aanmaken van een veilig wachtwoord en
2) het delen van persoonlijke informatie.

Het doel van de meting was om de relatie tussen daadwerkelijk gedrag en awareness te onderzoeken op basis van COM-B.

Weerstand

Dit plan werd met gemengde gevoelens ontvangen door de deelnemende instellingen. Sommige zagen dit als een mooie kans, terwijl andere zich zorgen maakten. Er ontstond onrust omdat dit plan de vertrouwensband tussen de security- en privacy-professionals en de rest van de organisatie kon schaden; medewerkers zouden 'genept' worden met zo'n gedragsmeting, vergelijkbaar met een phishingtest. Medewerkers zouden mogelijk sneller afhaken als zij een (fictief) account moesten aanmaken, met als gevolg een lagere response. Besloten werd dat de gedragsmeting optioneel zou zijn. Instellingen konden ook kiezen voor de awarenessmeting met vragenlijsten zoals zij die de voorgaande jaren hadden uitgevoerd.

Daarnaast stelden we een handleiding op om met negatieve reacties van medewerkers om te kunnen gaan (beloon opmerkzaamheid, wees transparant, vraag om geheimhouding tijdens de looptijd). En schreven we begeleidende teksten om instellingen te helpen het management te overtuigen om met de meting mee te doen. Van de 29 deelnemende instellingen kozen er uiteindelijk 20 om ook aan de gedragsmeting mee te doen.

Parallel meten

Nu het besluit genomen was, konden we aan de slag. De gedragsmeting gebruikte een andere testomgeving en het klaarzetten van die omgeving bracht nieuwe vragen met zich mee. Welke URL gebruiken we en hoe betrouwbaar oogt de URL voor medewerkers? Is deze omgeving zowel in het Nederlands als in het Engels beschikbaar? En voldoet deze omgeving aan de strenge securityeisen van SURF?

Gelukkig kon de technisch beheerpartij deze vragen oplossen. De meting startte half mei en liep tot begin juni. Tijdens de meting kregen instellingen elke twee weken een update van het aantal respondenten. Instellingen kozen zelf hoe zij de meting onder de aandacht brachten, bijvoorbeeld via intranet of door medewerkers een e-mail te sturen met het verzoek aan de meting mee te doen.
Tijdens de meting pakten SURF, BDO en De Haagse Hogeschool elk een andere rol. SURF deed vooral de communicatie en beantwoordde de vragen. BDO voerde de awarenessmeting uit en stelde instellingsrapporten op en de Haagse Hogeschool voerde de gedragsmeting uit.

Onderzoekers en consultants

Na afloop van de meting was het tijd om de data te onderzoeken. Het samenvoegen van de verschillende datasets bleek een praktische uitdaging. Vervolgens was de vraag hoe we het verband tussen het COM-B en de gedragsmeting helder konden neerzetten. Bij het duiden van de resultaten bleek dat onderzoekers de neiging hebben heel voorzichtig te zijn in hun uitspraken, terwijl consultants juist concrete adviezen willen meegeven. Dat leidde tot interessante gesprekken. Bovendien wilde SURF graag dat de sectorrapportage ook gebruikt kan worden om het management van instellingen te wijzen op het belang van awareness. Dat alles onder hoge tijdsdruk, want de instellingen ontvingen hun instellingsrapportage vlak voor de zomervakantie.
Er volgden meerdere meetings waarbij we elk onze punten inbrachten en van daaruit uiteindelijk tot een compromis kwamen. Zoals het besluit om de resultaten van de gedragsmeting in de sectorrapportage verder uit te diepen omdat het lastig was om per instelling correlaties te leggen vanwege het lage aantal respondenten.
Naast de metingen per instelling werd er ook een sectorrapport opgesteld. Hierin werden niet alleen de resultaten van de SURF-instellingen meegenomen, maar ook die van 41 MBO-instellingen. Dit jaar voerde MBO Digitaal namelijk dezelfde awarenessmeting uit.

Resultaten gedragsmeting

Wat komt er naar voren uit de gedragsmeting? Onveilig online-gedrag blijkt veelvuldig voor te komen onder medewerkers. Zo koos slechts 61% van de medewerkers een sterk wachtwoord en koos 18% van de medewerkers een wachtwoord dat al gelekt was. Ook deelde 25% van de medewerkers persoonlijke gegevens, zoals naam (21%) en geboortedatum (11%). Uit de analyse blijkt dat de componenten bekwaamheid en motivatie een zeer beperkt positief verband hebben met daadwerkelijk veilig gedrag. Het component gelegenheid laat een zeer beperkt negatief verband zien met het delen van persoonlijke gegevens. Deze factoren verklaren echter slechts is 1-2% van het gedrag. Dat betekent dat 98-99% van de variantie tussen medewerkers in het informatieveilige gedrag wordt verklaard door andere factoren die niet zijn meegenomen in dit onderzoek.

Wat is het effect van de gedragsmeting op response? Omdat er bij de start van het traject twijfels waren, hebben we ook

Onderzoekers hebben de neiging voorzichtig te zijn in hun uitspraken, terwijl consultants juist concrete adviezen willen meegeven

gekeken of het vermoeden dat mensen zouden afhaken bij de gedragsmeting juist was. Door de responsepercentages te vergelijken tussen de groep zonder gedragsmeting en de groep met gedragsmeting zagen we dat het responsepercentage in beide groepen vergelijkbaar is.

Ook wilden we weten of er veel vragen en reacties van medewerkers waren. Dit bleek mee te vallen: er werden wel vragen gesteld, maar de voorgestelde route om dit gedrag te belonen, transparant te zijn en om geheimhouding te vragen, haalde de scherpste randjes ervan af. We zijn de instellingen die het aandurfden om de gedragsmeting uit te voeren hiervoor dankbaar en zijn tevreden dat de negatieve reacties meevielen.

Terugblik

Het was de eerste keer dat deze meting uitgevoerd werd met input vanuit SURF, BDO en De Haagse Hogeschool. De samenwerking verliep soepel en we konden snel schakelen. Bijvoorbeeld voor het maken van aanpassingen in vragen of het uitwerken van het proces. Desondanks hadden we elk ook onze eigen unieke expertise en blik op het onderzoek. Dat leverde interessante discussies op, bijvoorbeeld over het advies dat we mee konden geven aan instellingen. Tijdens het opstellen van de rapportage brachten we elkaar op nieuwe ideeën om de resultaten duidelijker weer te geven. We hebben die multidisciplinaire aanpak als verrijkend ervaren omdat het onze blik verruimd heeft.

Ondanks de verschillende belangen en achtergronden hebben we door communicatie en compromissen een manier gevonden om de gedragsmeting succesvol uit te voeren. We zijn tevreden over het proces. De resultaten wijzen er op dat het daadwerkelijk gedrag complexer is dan binnen het COM-B model kan worden aangegeven, extra onderzoek in welke factoren een rol spelen zal hier nieuwe inzichten in geven.
Het is nog te vroeg om een uitspraak te doen of deze samenwerking een vervolg krijgt. SURF is in elk geval van plan om ook in 2024 een awarenessmeting uit te laten voeren. We reviewen met de deelnemers van de gedragsmeting hoe zij dit proces ervaren hebben en hoe zij de extra gegevens in de rapportages kunnen inzetten. Voor ons was deze samenwerking in elk geval een groot succes.

Belangrijkste conclusies sectorrapportage

1. Over de hele linie zijn de resultaten beter dan vorig jaar, maar deze zijn nog niet voldoende;
2. Er is een zeer beperkt verband tussen 'COM-B' en daadwerkelijk informatieveilig gedrag;
3. Informatieveilig werken lijkt een individuele aangelegenheid: een sterke security cultuur ontbreekt.

De rapportage kun je hier terugvinden:
https://sec.surf.nl/awareness-meting-sector-rapportage/
Of hier: https://edu.nl/jgnhn

Auteur: Vincent van Dijk, eigenaar van Security Scientist. Hij is bereikbaar via: vincent@securityscientist.net.