Auteurs: Dr. Rick van der Kleij is senior onderzoeker bij TNO en de Haagse Hogeschool en is bereikbaar via rick.vanderkleij@tno.nl. Tineke Hof is senior onderzoeker bij TNO en is bereikbaar via tineke.hof@tno.nl.

'Het is niet mijn verantwoordelijkheid'

Over de excuses die mensen gebruiken om het niet naleven van informatiebeveiligingsregels voor zichzelf te rechtvaardigen

Herkenbaar? Je ontvangt een Engelstalige e-mail en om de inhoud iets sneller te begrijpen kopieer je de tekst en plak je deze in Google Translate. Op basis van de Nederlandse vertaling die direct in jouw scherm verschijnt, kun je makkelijker een antwoord naar de afzender formuleren. Maar wist je dat veel bedrijven een protocol hebben opgesteld waarin staat dat het gebruik van deze vertaalwebsite verboden is?

Uit internationaal onderzoek is bekend dat mensen die zich niet volgens de regels gedragen hun ongewenste gedrag goedpraten (1). Mensen weten vaak wel dat ze zich op een bepaalde manier behoren te gedragen, maar gebruiken excuses, ofwel neutralisatietechnieken, om het gewenste gedrag niet te hoeven vertonen. Met andere woorden: ze redeneren het onprettige gevoel dat het overtreden van regels met zich meebrengt weg. Ze denken bijvoorbeeld: 'het is niet mijn verantwoordelijkheid', 'het kan geen kwaad', 'ik heb geen andere keuze' of 'vergeleken met wat anderen doen, valt dit wel mee'.

In dit artikel bespreken we een recent TNO-onderzoek waarbij we de vraag stellen: is het mogelijk om regelopvolging op het gebied van informatiebeveiliging te vergroten door het uitschakelen van neutralisatietechnieken door een gedragsinterventie? Recente andere onderzoeken laten namelijk zien dat training of communicatie kan leiden tot een vermindering van het gebruik van neutralisatietechnieken door medewerkers en tot een sterkere intentie om veilig gedrag te vertonen (2), (3).

Cyberveilig gedrag

Eerder onderzoek uit 2020 van TNO naar cyberveilig gedrag laat zien dat bewustzijn in de vorm van kennis weliswaar een belangrijke voorspeller is van gedrag, maar dat medewerkers ook gemotiveerd moeten zijn en de gelegenheid moeten krijgen om het gewenste gedrag te vertonen (4). Alleen weten dat (en hoe) je als medewerker iets wel of niet behoort te doen is niet genoeg. Denk bijvoorbeeld aan het vergrendelen van je computer of documenten alleen op een veilige wijze delen. Soms ontbreekt de motivatie om gewenst gedrag te vertonen. In andere gevallen kan de motivatie zelfs negatief zijn, bijvoorbeeld als het opvolgen van informatiebeveiligingsregels medewerkers (gevoelsmatig of daadwerkelijk) belemmert in het effectief uitvoeren van hun werk. Dit is terug te zien in de verklaringen die medewerkers geven voor hun ongewenste gedrag: ze passen neutralisatietechnieken toe om hun gedrag te rechtvaardigen. Denk hierbij aan argumenten als het kost teveel tijd, het is te moeilijk, niemand heeft er last van, of het kan toch geen kwaad. De mate waarin medewerkers gebruik maken van neutralisatietechnieken lijkt daarmee een belangrijke indicator voor het niet opvolgen van regels op het gebied van informatiebeveiliging (1), (5), (6).

Onderzoek naar regelopvolging

In ons recente onderzoek nemen we de regelopvolging rondom twee vormen van cyberveilig gedrag onder de loep bij financiële instellingen: (1) het melden van verdachte e-mails en (2) het gebruik van alleen door de organisatie toegestane applicaties en diensten. Een eerste stap in het onderzoek was het bepalen of

Onderdeel	Meetvragen [antwoordschaal]
Excuses	**Ik vind dat ik verdachte e-mails niet hoef te melden …**
Ontkenning schade of nadeel	als niemand er nadeel van ondervindt; als de organisatie er geen schade van ondervindt; als er geen schade optreedt
Ontkenning van verantwoordelijkheid	als ik niet precies weet wat het beleid daarover is; als ik het beleid daarover niet begrijp; omdat anderen het waarschijnlijk al melden.
Beroep op hogere plichten	als ik een belangrijke klus voor mijn leidinggevende aan het doen ben; als het helpt om mijn klus af te krijgen.
Veroordeling van de veroordelaars	als het me teveel tijd kost om het op de voorgeschreven manier te doen; als het beleid daarover onredelijk is; omdat ik denk dat er niets met mijn melding wordt gedaan.
Metafoor van het kasboek	omdat ik verder uitstekend presteer op werk; omdat ik hard werk voor de bank; omdat ik me verder altijd keurig aan alle regels houd.
Verdediging van noodzaak	wanneer ik haast heb; in situaties waarin ik geen andere keuze lijk te hebben; wanneer ik te maken heb met een strakke deadline.
Claim normaal te zijn	omdat bijna niemand dat doet.

Figuur 1 - Vragenlijst naar het gebruik van excuses bij het niet melden van verdachte e-mails. Links staan categorieën van excuses. Rechts de vragen waarmee het gebruik ervan is gemeten. Om de antwoorden vast te leggen is een 5-punts Likertschaal gebruikt, die loopt van oneens (1) tot eens (5).

Protocol gebruik Google Translate
De tekst die je kopieert vanuit de ontvangen e-mail kan vertrouwelijke informatie bevatten, die met jouw handeling daardoor in een paar tellen ook bij Google bekend is. Door het gebruik van deze vertaaltool houd je je dus niet aan de bedrijfsregels. Maar zo belangrijk was de informatie uit de e-mail toch helemaal niet? En met de snelle vertaling begreep je de kern van de boodschap veel beter, waardoor je kostbare tijd bespaarde... .

medewerkers de regels opvolgen rondom deze vormen van gedrag. Vervolgens, als dit niet het geval was, onderzochten we of en welke neutralisatietechnieken zij gebruiken. Hiertoe hebben we een vragenlijst-onderzoek gedaan onder meer dan 600 medewerkers van drie financiële instellingen. Een deel van deze vragenlijst is te vinden in tabel 1. Tenslotte hebben we gekeken of een interventie voor veranderend gedrag zorgt.

Verdachte e-mails

De resultaten van dit vragenlijstonderzoek zijn positief te noemen. Bijna alle deelnemers weten dat zij verdachte e-mails (phishing-mails) moeten melden. De intentie om te melden is hoog en de meeste deelnemers geven bovendien aan dat zij verdachte e-mails ook daadwerkelijk altijd melden. Een kleine groep zegt echter verdachte e-mails niet (altijd) te melden. Volgens verwachting gebruiken deze medewerkers neutralisatietechnieken om dit gedrag voor zichzelf te rechtvaardigen.

De meest gebruikte neutralisatietechniek bij deze kleine groep die geen melding maakte is 'ontkenning van verantwoordelijkheid'. Deze medewerkers vinden dat zij geen verdachte e-mails hoeven te melden omdat 'het beleid daarover naar hun mening niet is gecommuniceerd, ze het beleid niet kennen of begrijpen, of omdat anderen het waarschijnlijk al melden'. Ook 'verdediging van noodzaak' wordt gebruikt als excuus. Vooral het hebben van haast wordt aangewend als excuus binnen deze categorie. Maar over het algemeen kunnen we concluderen dat medewerkers zich correct gedragen als zij e-mails uit onbetrouwbare bron ontvangen.

Toegestane applicaties en diensten

Soms worden applicaties en diensten gebruikt die niet door de organisatie zijn toegestaan, zoals bepaalde filesharingdiensten, presentatietools of samenwerkingstools. Dit wordt ook wel schaduw IT genoemd. Deze diensten vormen een bedreiging voor de informatiebeveiliging omdat zij kunnen leiden tot een datalek of de installatie van malware op de bedrijfssystemen. De deelnemers aan dit onderzoek maken naar eigen zeggen weinig gebruik van niet-toegestane applicaties en diensten, met uitzondering van zogenaamde productiviteitstools, zoals Slideshare, Twilio en Google translate. Ongeveer 28% van de deelnemers maakt hiervan wel eens gebruik.

De meest gebruikte excuses om het gebruik van deze tools te rechtvaardigen vallen in de categorie 'Ontkenning van schade of nadeel'. De deelnemers die gebruik maken van deze niet-toegestane tools vinden dat zij deze applicaties en diensten voor hun werk mogen gebruiken omdat de organisatie er volgens hen geen schade van ondervindt. Ook excuses binnen de categorie 'ontkenning van verantwoordelijkheid' zien we hier terug.

Vergroten regelopvolging door interventie

Nu we weten dat niet alle medewerkers de regels op het gebied van informatiebeveiliging opvolgen en neutralisatietechnieken gebruiken om dit gedrag voor zichzelf te rechtvaardigen, is de volgende vraag: kan het gebruik van excuses, en daarmee regelopvolging, beïnvloed worden door een gedragsinterventie? Op basis van veelbelovende resultaten uit internationaal onderzoek (2) hebben we besloten om op maat gemaakt anti-neutralisatie communicatiecampagnes te ontwerpen. Hiermee willen we de meest gebruikte excuses verminderen die medewerkers soms aanwenden om zich niet aan het informatiebeveiligingsbeleid te houden.

Een anti-neutralisatie communicatiecampagne wordt ingezet om het proces van goedpraten van onveilig gedrag van medewerkers zichtbaar te maken. De campagne laat hen zien dat er geen enkele situatie is waarin riskant gedrag te rechtvaardigen is. Daarnaast worden medewerkers actief opgeroepen om, wanneer excuses zich voordoen, deze te negeren en de informatiebeveiligingsregels op te volgen (voor meer informatie, zie (2)).

Communicatiecampagne

De interventie zou oorspronkelijk worden getest voor beide vormen van gedrag die centraal stonden in deze studie. Onze meting van het gedrag 'melden van verdachte e-mails' laat echter zien dat de intentie om te melden hoog is en dat dit in de praktijk al bijna altijd gebeurt. Een interventie zou hier slechts

Onderwerp: gebruik van goedgekeurde applicaties en online diensten

Van: [redacted]

Aan: [redacted]

Beste [redacted],

Zoals vermeld in onze informatiebeveiligingsvoorschriften, is het niet toegestaan om ongeautoriseerde applicaties en online diensten (zoals presentatietools, productiviteitstools, samenwerkingstools en filesharediensten) te installeren of te gebruiken voor jouw werk zonder expliciete toestemming van onze IT afdeling.

Sommige medewerkers hebben het idee dat gebruik van ongeautoriseerde applicaties en online diensten in bepaalde gevallen te verdedigen is. Dat is begrijpelijk, maar het gebruik hiervan is in geen enkel geval te accepteren. Ook niet als je denkt dat [redacted] hierdoor geen schade ondervindt of als je vindt dat het beleid hierover niet duidelijk is gecommuniceerd. Want ongemerkt en indirect kan [redacted] wel degelijk schade ondervinden, zoals derden die ongewenste toegang tot vertrouwelijke informatie krijgen.

Daarom geldt: gebruik voor jouw werk alleen door onze IT afdeling goedgekeurde applicaties en online diensten.

Je leest alle beveiligingsvoorschriften op het intranet via: [redacted]

Heb je nog vragen? Laat het me gerust weten, ik help je graag.

Met vriendelijke groeten,

[redacted]
Teamlead afdeling Security

Figuur 2 - Anti-neutralisatiecommunicatie.

beperkt nut hebben. In dit artikel zoomen we daarom in op de interventie om regelopvolging te vergroten rondom gebruik van door de organisatie toegestane applicaties en diensten. De in dit onderzoek gebruikte communicatiecampagne voor dit doel is te vinden in figuur 1.

Om de effecten van de gedragsinterventie te kunnen bepalen, is deze getest binnen een financiële instelling. 242 medewerkers zijn verdeeld over twee groepen. Medewerkers in groep 1 kregen de anti-neutralisatiecommunicatie van hun leidinggevende via de e-mail. Medewerkers in groep 2 kregen geen e-mail. Enkele weken na de interventie is het gedrag gemeten via een vragenlijst. Daarbij is ook de mogelijke afname van het gebruik van excuses ten gevolge van de gedragsinterventie meegenomen in de meting. De metingen zijn zowel vooraf als naderhand gedaan bij beide groepen.

Resultaten

Verrassend genoeg zien we geen effect van de gedragsinterventie maar wel van tijd. Bij beide groepen is een afname gemeten over de duur van het onderzoek in het zelf-gerapporteerde gebruik van niet toegestane productiviteitstools. Ook is een afname vastgesteld over de tijd in het gebruik van excuses. Deze effecten zijn voor beide groepen echter even sterk. Zowel in de groep die de gedragsinterventie heeft ontvangen als in de groep die geen interventie heeft gekregen zien we een verschuiving in de gewenste richting. Het zelf-gerapporteerde gebruik van niet toegestane productiviteitstools nam af in de tijd met 63%.

Conclusie

Dit onderzoek heeft gekeken naar de mate waarin medewerkers van financiële instellingen zich zeggen te gedragen conform gedragsregels op het gebied van informatiebeveiliging. Ook is gemeten of en welke excuses zij gebruiken om het niet naleven van regels voor zichzelf goed te praten en of het mogelijk is regelopvolging te vergroten.

De resultaten van dit onderzoek laten zien dat het merendeel van de medewerkers de gedragsregels volgens het beleid omtrent informatiebeveiliging keurig opvolgen. De groep die dat niet doet, gebruikt in de meeste gevallen productiviteitstools die niet zijn toegestaan door de organisatie. De mate waarin medewerkers zich onveilig gedragen, verschilt per type van gedrag. Als medewerkers productiviteitstools gebruiken die niet zijn toegestaan, wil dit niet automatisch zeggen dat zij zich op andere gebieden ook veilig gedragen. De resultaten van dit onderzoek laten ook zien dat medewerkers excuses gebruiken om het ongewenste gedrag voor zichzelf goed te praten. Het soort van excuses dat medewerkers gebruiken, verschilt daarbij per doelgedrag. Dit toont maar weer aan dat er geen silver bullet, een kant-en-klare oplossing, bestaat voor het tegengaan van cyberonveilig gedrag op de werkvloer, maar dat maatwerk telkens is vereist.

Om het gebruik van excuses tegen te gaan is een gedragsinterventie ingezet. Deze anti-neutralisatiecommunicatie laat echter geen eenduidig effect zien. Er treedt een daling op in het zelf-gerapporteerde ongewenste gedrag alsmede in het gebruik van excuses. Omdat de dalingen ook zijn gevonden bij een controlegroep kunnen deze niet worden toegeschreven aan de gedragsinterventie. Een mogelijke storende factor kan zijn dat de deelnemers in beide groepen zich anders zijn gaan gedragen omdat zij wisten dat zij deelnamen aan een onderzoek. Waarbij het enkele feit dat er meer aandacht is voor een bepaald proces er al voor kan zorgen dat het proces beter gaat lopen (7). Ook de vragenlijst die deelnemers voorafgaand aan het onderzoek hebben ingevuld, kan de bewustwording over het beleid hebben vergroot en de regelopvolging hebben doen laten toenemen.

Mogelijkheden vervolgonderzoek

In het verlengde van dit onderzoek zien wij meerwaarde in onderzoek naar andere manieren om regelopvolging te

vergroten door het uitschakelen van neutralisatietechnieken. Zo is er evidentie dat een op maat gemaakte training over neutralisatietechnieken het gebruik van excuses zou kunnen ontmoedigen. Hoe een training kan worden ontwikkeld voor de praktijk, of deze succesvol is in het tegengaan van excuses en leidt tot gedragsverandering, zou het onderwerp kunnen zijn van vervolgonderzoek.

Een herhaling van het huidige onderzoek maar dan voor andere gedragingen is ook denkbaar. De gedragsinterventie is getest bij een specifiek soort van gedrag: het gebruik van productiviteitstools die door de organisatie niet zijn toegestaan. Het effect van de interventie op het tegengaan van ander onveilig gedrag of juist promoten van cyberveilig gedrag in de organisatie zou tevens onderwerp voor vervolgonderzoek kunnen zijn.

Er zijn bovendien andere maatregelen denkbaar die een effect kunnen hebben op het gebruik van excuses door medewerkers, zoals aanpassen van beleid of het beschikbaar stellen van veiligheidsmaatregelen die veilige gedragskeuzes ondersteunen. Denk hierbij aan een meldknop in het mailprogramma om het melden van verdachte e-mails makkelijk te maken voor de eindgebruiker. Ook hier liggen mogelijkheden tot een verdieping van het huidige onderzoek.

Referenties

(1) Siponen, M., & Vance, A. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. MIS quarterly, 34(3), 487-502.

(2) Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. (2018). Don’t even think about it! The effects of antineutralization, informational, and normative communication on information security compliance. Journal of the Association for Information Systems, 19(8), 3.

(3) Siponen, M., Puhakainen, P., & Vance, A. (2020). Can individuals’ neutralization techniques be overcome? A field experiment on password policy. Computers & Security, 88, 101617.

(4) Van der Kleij, R., Wijn, R., & Hof, T. (2020). An application and empirical test of the Capability Opportunity Motivation-Behaviour model to data leakage prevention in financial organizations. Computers & Security, 97, 101970.

(5) Morris, R. G., & Higgins, G. E. (2009). Neutralizing potential and self-reported digital piracy: A multi-theoretical exploration among college undergraduates. Criminal Justice Review, 34(2), 173-195.

(6) Silic, M., Barlow, J. B., & Back, A. (2017). A new perspective on neutralization and deterrence: Predicting shadow IT usage. Information & management, 54(8), 1023-1037.

(7) McCarney, R., Warner, J., Iliffe, S., Van Haselen, R., Griffin, M., & Fisher, P. (2007). The Hawthorne Effect: a randomised, controlled trial. BMC medical research methodology, 7(1), 1-8.