Position Paper:

# Nederlands Cyber Security Lab Labsessie #2

*''Beyond awareness: Maar hoe!?''*


Rutger Leukfeldt *(Directeur Centre of Expertise Cyber Security - Haagse Hogeschool)*
Bernold Nieuwesteeg *(Directeur Centre for the Law and Economics of Cyber Security - Erasmus Universiteit Rotterdam)*
Inge van der Beijl *(Director behaviour & training – Northwave)*
Inge Wetzer *(Sociaal psycholoog cybersecurity & compliance – Secura)*
Jelle Wieringa *(Security Awareness Advocate – KnowBe4)*
Melle Van den Berg *(Security consultant - Rapid Circle)*
Petra Oldengarm *(Directeur Cyberveilig Nederland)*
Rory O'Connor *(Chief Information Security Officer - Erasmus Universiteit Rotterdam)*
Sophie van der Zee *(Assistant professor at the Erasmus School of Economics- Erasmus Universiteit)*



NOVEMBER 2021

# Achtergrond

Cybersecurity is meer dan alleen het nemen van technische maatregelen. En alhoewel gebruikers ten onrechte vaak alleen worden aangemerkt als 'de zwakke schakel' binnen die cybersecurity, moet een deel van de maatregelen zich toch echt wel richten op deze groep. Gebruikers gedragen zich immers soms bewust of onbewust onveilig:

- ze klikken op hyperlinks als ze dat niet moeten doen;
- reageren op een phishingmail;
- gebruiken zwakke wachtwoorden;
- hergebruiken wachtwoorden;
- melden incidenten niet;
- geven (te) veel gegevens prijs van zichzelf op social media;
- maken niet consequent back-ups van hun data.

Sinds jaar en dag lijken organisaties 'awareness' te zien als de sleutel om van gebruikers iets minder de zwakke schakel te maken. De gedachte daarachter is kortgezegd dat gebruikers zich 'beter' gaan gedragen als we ze voeden met informatie over dreigingen, goed en fout gedrag en het cybersecurity-beleid.

Het is inmiddels echter wel duidelijk dat een beleid dat alleen gericht is op 'awareness' niet gaat zorgen voor het gewenste effect. Onderzoek toont bijvoorbeeld aan dat anti-phishingcampagnes, waar nepphishingmails worden verstuurd, niet heel lang beklijven.  Cybersecuritybedrijven geven dan ook steeds vaker aan dat het niet alleen gaat om het verhogen van kennis en bewustwording, maar ook om andere aspecten die gedrag lijken te beïnvloeden. Recent wetenschappelijk experimenteel onderzoek laat zelfs zien dat het hebben van meer kennis kan leiden tot onveiliger gedrag: gebruikers die (een beetje) meer weten, gedragen zich nog onveiliger.  Mogelijk komt dat doordat die groep zichzelf overschat en daardoor ten onrechte grotere risico's durft te nemen.

We moeten dus verder komen dan alleen awareness. Het lab observeert dat er twee grote vraagstukken spelen.

1. **Wat moeten we dan verder nog doen?** Het is duidelijk dat er geen simpele oplossing is voor het bevorderen van veilig cybergedrag. Toch is het goed om nieuwe oplossingsrichtingen te onderzoeken die richting geven aan het verbeteren van cyberveilig gedrag.

2. **Hoe zorgen we ervoor dat organisaties daadwerkelijk verder gaan dan alleen het creëren van meer awareness?** Individuele organisaties hebben lang niet altijd de kennis en kunde om dit zelf te doen. Moet de overheid dit stimuleren? Zo ja, hoe dan? Kan het aan de markt zelf (lees: cybersecurity bedrijven) overgelaten worden? Wat kunnen we leren over het stimuleren van effectieve gedragsinterventies binnen andere vakgebieden?

1. Van 't Hoff-de Goede, S., E.R. Leukfeldt, R. van der Kleij & S. Van de Weijer (2021) The online behaviour and victimization study: the development of a research instrument for measuring and explaining actual online behavior and online victimization. p21-42. In: Weulen Kranenbarg, M. & E.R. Leukfeldt (eds) Cybercrime in Context: the Human Factor in Victimization, Offending, and Policing. Springer.Van 't Hoff-de Goede, S., R. van der Kleij, S. van de Weijer & E.R. Leukfeldt (2019) Hoe veilig gedragen wij ons online? Een studie naar de samenhang tussen kennis, gelegenheid, motivatie en online gedrag van Nederlanders. Den Haag: De Haagse Hogeschool.

# **Onze positie: investeer structureel** in gedragsonderzoek en samenwerking tussen bedrijfsleven en wetenschap.

**Zowel cybersecuritybedrijven als wetenschappers geven aan dat het hard nodig is om de volgende stap te zetten in het voorkomen van slachtofferschap en/of de impact van cyberaanvallen.** Het is dan ook duidelijk dat we af moeten van het haast alleen symbolische 'creëren van meer awareness' naar interventies die daadwerkelijk veilig online gedrag van eindgebruikers stimuleren.

**In de dagelijkse praktijk blijkt dat alleen het creëren van awareness en het afvinken van compliance lijstjes niet zorgt voor het gewenste gedrag.** Verder is het voor gebruikers steeds lastiger om online te onderscheiden wat echt en wat nep is, komen er tal van dreigingen op eindgebruikers af (van phishing tot malware tot CEO-fraude), verandert het dreigingsbeeld steeds en is het ingewikkeld om te kunnen overzien wat mensen zelf kunnen doen om veilig te zijn online. Sommige oplossingen zijn wellicht wel veilig, maar in de praktijk niet werkbaar. In combinatie met de niet directe link tussen actie en gevolg – slachtofferschap kan zich immers soms veel later openbaren – is het voor eindgebruikers nu lastig, zo niet onmogelijk, om in te schatten wat ze zelf kunnen doen en wat wel en niet werkt.

Er zijn tal van oplossingen voor onveilig gedrag van medewerkers te bedenken. Van technische oplossingen die ervoor moeten zorgen dat medewerkers geen onveilige acties kunnen uitvoeren of systemen zo in te richten dat een menselijke fout niet meteen voor een grote impact zorgt, tot psychologische oplossingen zoals gewenst gedrag proberen te nudgen.

# Onze observaties

**Het lab ziet één overkoepelend thema dat relevant is bij alle mogelijke interventies: fundamentele inzichten in hoe eindgebruikers zich daadwerkelijk gedragen en hoe zij reageren op interventies onder verschillende omstandigheden.**

Inzicht in daadwerkelijk gedrag is van essentieel belang. Veel van de huidige kennis is gebaseerd op zelf-gerapporteerd gedrag. Onderzoekers of cybersecuritybedrijven vragen eindgebruikers om aan te geven wat zij wel of niet weten en wel of niet doen. Zelf-gerapporteerd gedrag is echter niet gelijk aan daadwerkelijk gedrag. Daarbij is het van belang om te onderkennen dat alleen inzicht in de kennis van medewerkers niet voldoende is. Gedrag wordt gestuurd door meerdere factoren. Daarom moeten ook factoren als motivatie en gelegenheid worden meegenomen. Welke randvoorwaarden zorgen er bijvoorbeeld voor dat geïnformeerde en gemotiveerde medewerkers daadwerkelijk veilig gedrag vertonen?

**Een tweede observatie van het lab is dat de kennisbehoefte een gedeeld doel is van bedrijfsleven en wetenschap.**

Cybersecuritybedrijven worstelen met het gedragsaspect binnen cybersecurity. In de praktijk blijkt het lastig te zijn om gedegen onderzoek uit te voeren onder klanten: er is geen tijd, geen medewerking of te weinig expertise. Wetenschappers hebben een ander probleem: gedragswetenschappelijk onderzoek naar cybersecurity staat nog in de kinderschoenen. Er is nog geen onderzoekstraditie op dit veld die decennialang teruggaat. Pas sinds een jaar of tien vindt er mondjesmaat onderzoek plaats binnen dit vakgebied. En waar veel psychologisch onderzoek wordt uitgevoerd op studenten, is dat voor onderzoek naar digitaal veilig gedrag minder toepasselijk omdat de bevindingen niet representatief zijn voor medewerkers of kwetsbare groepen zoals ouderen. Samenwerking met het bedrijfsleven is dus ook voor wetenschappers cruciaal.

Om te komen tot fundamentele kennis over gedrag moeten bedrijfsleven en wetenschappers dus samenwerken.

*''Om te komen tot fundamentele kennis over gedrag moeten bedrijfsleven en wetenschappers dus samenwerken.''*

# Call to action

Het lab ziet de volgende oplossingsrichting: investeer structureel in het opbouwen van fundamentele kennis over veilig online gedrag en stimuleer daarbij nadrukkelijk de samenwerking tussen bedrijfsleven en wetenschap.

1. Investeer structureel in het ontwikkelen van een visie én fundamenteel en praktijkgericht onderzoek naar de gedragscomponent binnen cybersecurity. Gedrag is complex. Gedrag binnen cybersecurity is mogelijk nog complexer. Om te verworden tot een volwassen onderzoeksveld is een langetermijnvisie nodig op het structureel opbouwen van kennis over gedrag binnen cybersecurity. Zonder fundamentele kennis komen we niet verder, omdat we dan niet weten hoe eindgebruikers reageren op interventies om hun gedrag rondom cybersecurity te verbeteren. Een voorbeeld: Technische en organisatorische oplossingen kunnen nooit effectief zijn zonder kennis over hoe gebruikers daarop reageren.
2. Stimuleer samenwerking tussen bedrijven en wetenschappers. Cybersecuritybedrijven hebben samen toegang tot een enorme hoeveelheid aan kennis over daadwerkelijk gedrag. Onafhankelijk onderzoek kan zorgen voor een evidence base waardoor interventies ontwikkeld en getoetst kunnen worden die daadwerkelijk effectief zijn. Logisch dat er een grote behoefte aan fundamentele kennis van dat gedrag, blijkt uit onze labsessie. Gebruik wetenschappelijk onderzoek (‘in het lab’) als de basis om dat vervolgens uit te zetten in minder ideale omstandigheden: de praktijk binnen cybersecuritybedrijven. Evalueer vervolgens die praktijkinterventies, om ook daar weer van te leren.
3. Creëer randvoorwaarden voor het delen van data. Bijvoorbeeld het delen van (indien gewenst geanonimiseerde) incidenten die afgehandeld zijn of data betreffende awareness-programma’s van bedrijven.

## Over het Nederlands Cyber Security Lab (NCSL)

Nederland heeft behoefte aan maatschappelijke oplossingen voor optimale cybersecurity buiten de bestaande kaders. Door wetenschappers en bedrijfsleven bijeen te brengen combineert het NCSL wetenschappelijke inzichten met best practices vanuit het bedrijfsleven. De overheid is klankbord. Het Lab bestaat uit een bureau dat labsessies organiseert. Het bureau selecteert thema’s en genodigden per labsessie. Tijdens de labsessie faciliteert het bureau het creatieve proces. Na de labsessie wordt een position paper met een kernachtige weergave van de oplossingen openbaar gemaakt en verspreid.