Exploratief onderzoek naar menselijke- en omgevingsfactoren die organisaties weerbaar maken tegen social engineeringsaanvallen

Michelle Ancher
m.ancher@hhs.nl

Docent-onderzoeker
Lectoraat Cybercrime
and Cyberreslience
The Hague University
of Applied Sciences

Waarom onderzoek naar Social engineering?

Social engineering meest voorkomende modus operandi van cybercriminelen

= Mensen overhalen om onbevoegden toegang te geven tot gevoelige informatie middels manipulatie.

Gevolgen b.v. datalekken, met reputatie- of financiële schade tot gevolg.

Focusgroep: Midden- en kleinbedrijf (mkb)

THE HAGUE
UNIVERSITY OF
APPLIED SCIENCES

Vaak focus op technische maatregelen

Dit onderzoek: maatregelen gericht op vergroten van de weerbaarheid van mensen

Onderzoeksvraag: ‘Welke menselijke- en omgevingsfactoren spelen een rol bij cyberveilig gedrag igv social engineeringsaanval?’

Cyberveilig gedrag igv social engineering = geen gevoelige gegevens of toegang tot deze gegevens prijsgeven aan onbevoegden bij manipulatie.

Subvragen:
1. Welke typen (digitale, fysieke of telefonische) social engineeringsaanvallen zijn niet geslaagd?
2. Hoe worden organisaties beschermd tegen Social Engineering-aanvallen?
3. Welke (basis)maatregelen worden genomen?

4. Spelen capability, opportunity en motivation (de COM-B-gedragsfactoren) van cyberveilig gedrag een rol bij het mislukken van aanvallen?
4.1 Is een bepaald fysiek/online design van de omgevingsontwerp gerelateerd aan cybergedrag?

5. Welke organisatiekenmerken zoals leiderschap en cultuur spelen een rol bij cyberveilig gedrag?

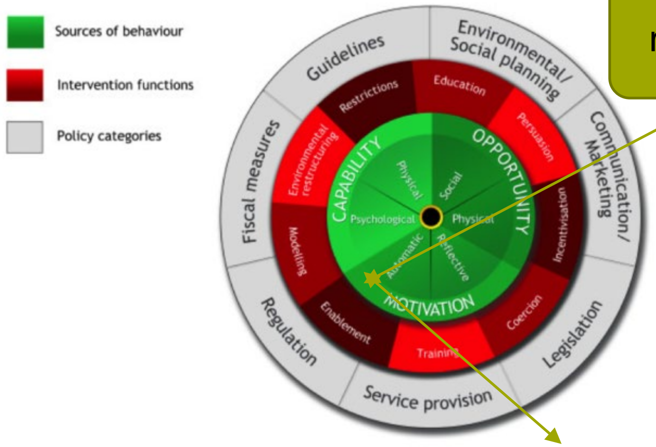
Menselijke- en omgevingsfactoren van gedrag ten aanzien van social engineering

Base: Capability Opportunity Motivation-Behaviour (COM-B) model voor gedragsverandering (Michie et al., 2011)

Theoretical Domains Framework (TDF) vragenlijst (Huijg et al., 2014)

Nadruk op Opportunity: Social influence and environmental context and resources (budget, andere afdelingen, security policy, personeel)

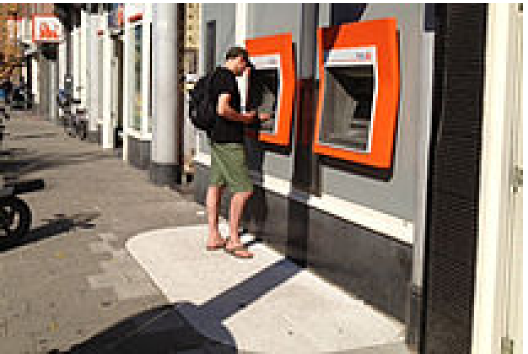
Crime Prevention Through Environmental Design (Crowe, 2014)



Safe behavior regarding social engineering

OR Following cyber rules of conduct: check sender of request, don't click automatically on a link, etc

COM-B model:
The BCW maps out which type of intervention function is likely associated COM-B component, and following this, which policy this framework you are more likely to produce effective, theory-driven interventions, grounded in evidence-based principles.



THE HAGUE UNIVERSITY OF APPLIED SCIENCES

Social engineeringsaanvallen

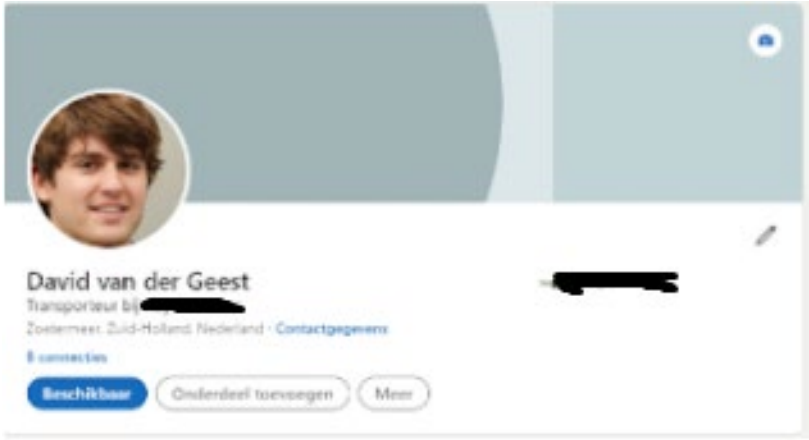
Typen social engineering

Telefonisch

Fysiek

Digitaal

- Whatsapp fraud/ email phishing
- Teams/ linkedin phishing



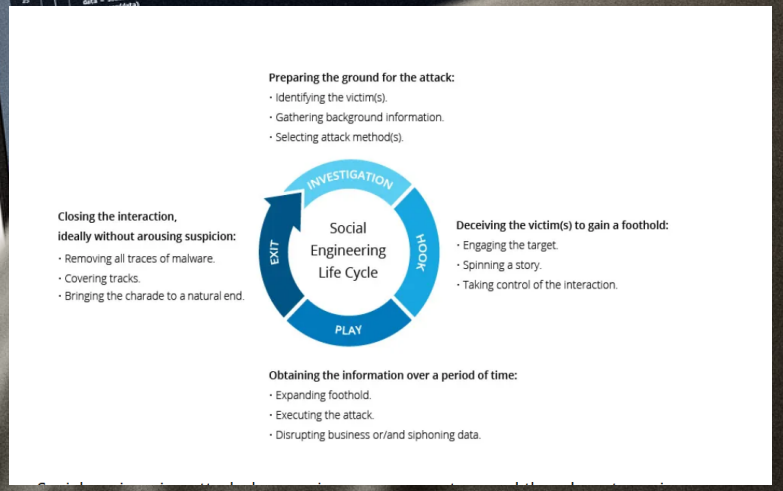
THE HAGUE UNIVERSITY OF APPLIED SCIENCES

Social engineeringsaanvallen

Gestructureerde checklist:

Type aanval
Doelobject
Uitgelokte gedrag
Type gevoelige data
Manipulatie techniek (Cialdini, 2007) bijv. autoriteit, sociale norm, schaarste)

Social engineeringcyclus



HOW: Methode

Kwalitatief verkennend onderzoek

1. Social engineeringsaanvallen (digitaal, fysiek, telefonisch) mbv checklists

Analyse social engineeringsrapporten (observaties)

2. Interview contactpersoon social engineering organisaties (11): 9 mkb's, 7 <250 medewerkers;

Publieke sector (onderwijs, zorg, overheid) en mkb (metaal, ICT, productie);

Functie: ICT-beveiligingsprofessionals (8) en directeuren (3)

Gebaseerd op: TDF-vragenlijst (Huijg et al.) en variabelen zoals organisatiekenmerken, leiderschap en beveiligingsmaatregelen.

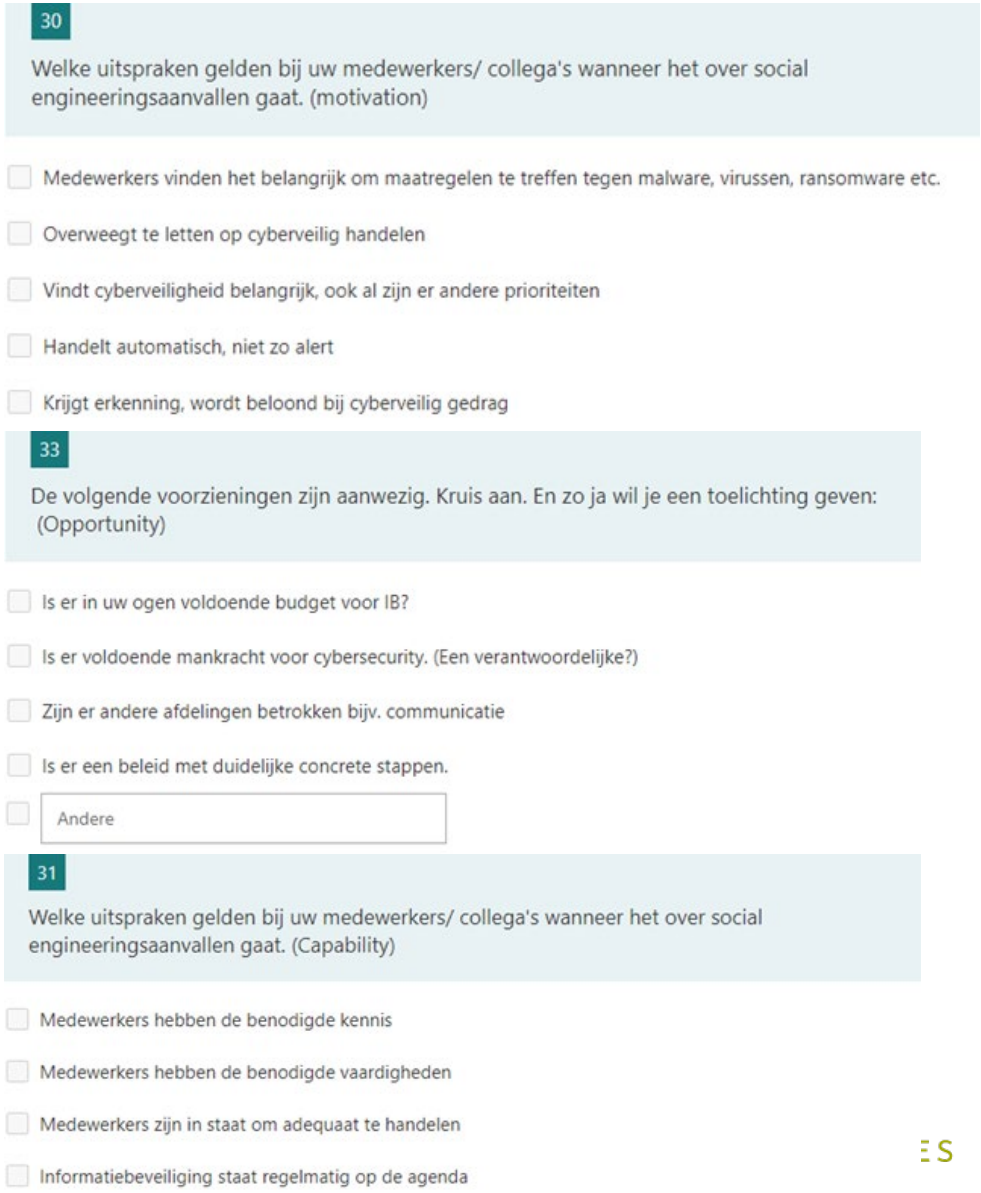
Grounded theory-analyse van interview transcripten

THE HAGUE UNIVERSITY OF APPLIED SCIENCES

Voorbeelden van interviewvragen

- Welke uitspraken gelden bij uw medewerkers/collega's wanneer het over social engineeringsaanvallen gaat (Comb)

- Hoe gaat men om met fouten? (Kan dit gezegd/aangekaart worden)
- Wat kunt u zeggen over de fysieke inrichting van de werkomgeving.
- Passen een of meerdere kenmerken bij leidinggevenden binnen uw organisatie? O Monitoren van processen, O Verantwoordelijk, O Voorbeeld functie O Authentiek leider


30

Welke uitspraken gelden bij uw medewerkers/ collega's wanneer het over social engineeringsaanvallen gaat. (motivation)

- Medewerkers vinden het belangrijk om maatregelen te treffen tegen malware, virussen, ransomware etc.
- Overweegt te letten op cyberveilig handelen
- Vindt cyberveiligheid belangrijk, ook al zijn er andere prioriteiten
- Handelt automatisch, niet zo alert
- Krijgt erkenning, wordt beloond bij cyberveilig gedrag

33

De volgende voorzieningen zijn aanwezig. Kruis aan. En zo ja wil je een toelichting geven: (Opportunity)

- Is er in uw ogen voldoende budget voor IB?
- Is er voldoende mankracht voor cybersecurity. (Een verantwoordelijke?)
- Zijn er andere afdelingen betrokken bijv. communicatie
- Is er een beleid met duidelijke concrete stappen.
- Andere

31

Welke uitspraken gelden bij uw medewerkers/ collega's wanneer het over social engineeringsaanvallen gaat. (Capability)

- Medewerkers hebben de benodigde kennis
- Medewerkers hebben de benodigde vaardigheden
- Medewerkers zijn in staat om adequaat te handelen
- Informatiebeveiliging staat regelmatig op de agenda

WHAT: Resultaten

Welke menselijke- en omgevingsfactoren spelen een rol bij het afslaan van social engineeringsaanvallen?

Organisations	Attack NOT successful	Attack successful
A		D, P
B		D, P
C	D, P	
D	T, D	P
E	T	D, P
F	T	P
G	D	T, P
H	T, P	D
I	D	
J	T, D	P
K		D

Table 1. Organisations and type of attacks that (not) succeeded
Explanation: D = Digital attack, P = Physical attack, T = Attack by telephone

- 9 van de 11 organisaties fysieke aanval (P)
- Fysieke aanvallen veel succesvoller (7 van 9) dan de andere typen
- Bijna alle T zijn gefaald (5 van 6)
- Niet geslaagde D (5 van 10) kleine ondernemingen (<50 werknemers) Sociale controle?

Resultaten

"Mensen weten het en vinden het belangrijk maar of ze zich ernaar gedragen…?"

- **Capability**: 7 van de 11 organisatie (kennis en vaardigheden) aanwezig, maar verschilt per afdeling.
- **Motivatie**: 6 op de 11 medewerkers belangrijk om maatregelen te nemen tegen malware, virussen, ransomware en overweegt aandacht te besteden aan cybersec.
- **Opportunity**:
  -Omgevingscontext & **middelen** Voldoende budget en betrokkenheid van andere afdelingen. Onvoldoende duidelijk beveiligingsbeleid en IT-personeel.
  - **Sociale invloed** + **Gesprekprotocol** geïnstalleerd over hoe om te gaan met externen: Alle gefaalde T (5) hebben een gespreksprotocol. 6 organisaties geslaagde P hebben geen protocollen voor interactie
  -**Fysiek design**

"Medewerkers pikken het sneller op dan management."

'Mijn mensen zijn chaoten, volgen geen processen. Die klikken overal snel op bijvoorbeeld.'

WHAT: Resultaten

- **Positieve kenmerken van leiders**: verantwoordelijk en bewaken van processen (6) maar gebrek aan rolmodellen in management (1); Managers zijn altijd benaderbaar/communicatiekanaal, beperkte kennis ove beveiliging.
- Open source intelligence (**OSINT**): verschillende issues gemeld (7). 3 let niet op osint (maar er is geen verband met digitale aanvallen, zijn mislukt).
- Allen awareness maatregelen zoals posters (2), bewustmakingstraining (5), mystery guest en het gebruik van beveiligingstoolkits (3) en banners in e-mail (van buitenaf).
- Aanvallen direct invloed op veilig gedrag: vaker incidentmeldingen (3) en banners in e-mails.

‘Voorbeeld gedrag is belangrijk want we zijn allemaal heel jong’.

Discussie

Creëren **cyberveilige norm**

Sociale controle belangrijke factor bij afslaan van social engineeringsaanvallen. kleine ondernemingen (<50 medewerkers).

Rolmodel en security ambassadeurs

Gespreksprotocol

Continueren observatie-onderzoek bij mkb

Design van de (werk)omgeving: zoals e-mailbanners en meldingsknop

let’s change

YOU. US. THE WORLD.

BRONNEN

- Ancher, M., Kleij, R. and Leukfeldt, E. (2019). Studenten treden in voetsporen cybercrimineel om meer inzicht te krijgen in social engineering. [online] Hbo-kennisbank.nl.
- Bandura, A. (1995). Social foundations of thought and action. Englewood Cliffs, N.J.: Prenctice Hall.
- Baarda, B. (2019). Dit is onderzoek!. Groningen/Houten: Noordhoff Uitgevers.
- Blythe, J.M. and Coventry, L. (2018). Costly but effective: Comparing the factors that influence employee anti-malware behaviours. Computers in Human Behavior, 87, pp.87–97.
- Cialdini, R.B. (2007). Influence, the psychology of persuasion. NY: Harper Collins Publishers Inc.
- Crowe, T. and Fennelly, L. (2014) Crime prevention through environmental design. 3rd ed. London, England: Elsevier Science.
- ENISA. (2018). Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity.
- Glaspie, H. (2018). Assessment of information security culture in higher education assessment of information security culture in higher education, Ucf.edu.
- Gragg, D. (2002). A Multi-Level Defense Against Social Engineering. White paper, Sans Institute.
- Huijg, J. M., Gebhart, W.A., Dusseldorp, E. et al. (2014). “Measuring determinants of implementation behavior: psychometric properties of a questionnaire based on the theoretical domains framework,” Implementation science: IS, 9(1), p. 33.
- Kirlappos, I., Parkin, S. and Sasse, M. A. (2015). “‘Shadow security’ as a tool for the learning organization,” ACM SIGCAS Computers and Society, 45(1), pp. 29–37.
- Van der Kleij, R., Wijn, R. and 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), p. 101970.
- Michie, S., van Stralen, M. M. and West, R. (2011). “The behaviour change wheel: a new method for characterising and designing behaviour change interventions,” Implementation science: IS, 6(1), p. 42.
- Notté, R., Slot, L., van 't Hoff-de Goede, S. and Leukfeldt, R. (2019). Cybersecurity in het mkb Nulmeting. The Hague University of Applied Sciences.
- Verizon.com. (2021). Data Breach Investigations Report.

THE HAGUE
UNIVERSITY OF
APPLIED SCIENCES