Digitale weerbaarheid van burgers

Lezing voor Fryske Akademy

21-11-2023

Sander Ebbers
(Promovendus Onderzoeksgroep Cybersafety)

THORBECKE ACADEMIE

NHL STENDEN

Voorwoord en leeswijzer

Op 21 november heb ik een lezing mogen verzorgen voor de Fryske Akademy. De lezing gaat over digitale weerbaarheid van burgers, vanuit een integraal perspectief. Deze lezing is uitgeschreven en te lezen in onderhavig document.

Voor wat context stel ik mijzelf graag eerst voor, daarnaast licht ik ook toe wat mijn achtergrond is qua expertise. Ik ben Sander Ebbers, 34 jaar, man van Joanne en vader van Samuel en Elena. Ik ben in Groningen opgeleid als arbeids- en organisatiepsycholoog. Na mijn studie ben ik aan de slag gegaan als adviseur in de cybersecurity. In deze rol heb ik mij beziggehouden met het opzetten van uitvoeren van trainingsprogramma's voor het bedrijfsleven, gericht op digitaal veilig gedrag. Na mijn werk als adviseur ben ik eind 2019 aan de slag gegaan als docent en onderzoeker bij NHL Stenden. Hierbij ben ik verbonden aan de onderzoeksgroep Cybersafety. Deze onderzoeksgroep houdt zich bezig met bestuurlijke, juridische en menselijke aspecten van digitale veiligheid. Binnen de onderzoeksgroep richt ik mij op projecten die met bewustwording en gedrag te maken hebben. Specifiek ligt mijn focus op meldgedrag in organisaties: wat maakt dat medewerkers wel of niet een digitaal incident melden en hoe kunnen we dit stimuleren.

Over meldgedrag gaan we het in deze lezing niet hebben. Ik wil het namelijk niet hebben over de context van organisaties, maar over de context van burgers, de maatschappelijke context. In deze lezing neem ik de toehoorder mee in de wereld van digitale veiligheid, en probeer ik dit thema uit de techniek te halen en meer menselijk te maken.

Deze lezing bevat een viertal secties:

- Sectie 1 gaat over online criminaliteit: Wat is het, wat is de psychologie achter slachtofferschap en wat zijn beschermende maatregelen.
- Sectie 2 gaat over veiligheid en verantwoordelijkheid. In hoeverre zijn wij verantwoordelijk voor onze eigen veiligheid? En in hoeverre zijn er maatschappelijke vangnetten aanwezig en nodig?
- In sectie 3 schets ik een toekomstperspectief. Deels vanuit mijn eigen ervaring en deels vanuit maatschappelijke trends. Ik zal hier ook kort ingaan op in hoeverre digitale veiligheid aandacht krijgt in de verkiezingsprogramma's, daar de verkiezingen op 22 november zijn (geweest).
- Ik rond in sectie 4 af met een aantal dilemma's rondom digitale veiligheid. Dilemma's waar ik graag met jullie over nadenk na de pauze. Ik heb deze lezing uitgeschreven en zal deze na afloop delen met de organisatie.

Veel leesplezier!

Sander Ebbers, Groningen, 23 november 2023

Sander.ebbers@nhlstenden.com

Contents

1. Online criminaliteit en maatregelen

1.1 Introductie

Mevrouw Rijpstra gaat achter haar tablet zitten en opent haar e-mailprogramma. In alle drukte van de dag wil ze nog even haar mail checken, ze verwacht namelijk een mailtje van PostNL met een track en trace code. Wanneer het mailprogramma eindelijk is geopend ziet ze een mail van PostNL: ah, mevrouw Rijpstra klikt op de link zodat ze weet hoe laat haar pakketje morgen wordt bezorgd! Wanneer ze op de link klikt moet ze nog een keer haar e-mailadres en wachtwoord invoeren... Vreemd, maar goed, dat zal vast een extra beveiliging zijn. Nadat ze dit gedaan heeft krijgt ze een lege, blanco, website te zien. Dat lijkt wel een foutmelding. Hé vervelend, net nu een storing op de website van PostNL. Ik probeer het later wel nog een keer...

Dit is een voorbeeld van iemand die slachtoffer is geworden van phishing.

Zal ze zich op dit moment een slachtoffer voelen?

Waarschijnlijk niet.

De cybercriminelen hebben haar e-mailadres en haar wachtwoord verkregen. Waar mevrouw Rijpstra dacht dat het ging om een extra beveiliging, bleek het te gaan om een phishingwebsite. De cybercriminelen kunnen deze gegevens gebruiken om in te loggen op het e-mailadres van mevrouw Rijpstra, om zich voor te doen als haar, om nog meer gegevens van haar te verzamelen.

Wellicht gebruikt mevrouw Rijpstra hetzelfde wachtwoord op meerdere plekken en verkrijgen te criminelen niet alleen toegang tot haar e-mailadres, maar ook tot haar privédocumenten, vliegtickets (met paspoortnummer), creditcardgegevens, stukken van de notaris et cetera. Alvorens ik inga op de psychologie van dit incident, eerst een korte uitleg over online criminaliteit.

1.2 Online criminaliteit

Je zult merken dat ik in deze lezing spreek van online criminaliteit, en niet over cybercrime. Dat heeft te maken met een definitiekwestie. In mijn onderzoeksveld onderscheiden we cybercrime en gedigitaliseerde criminaliteit. Beide vallen onder de brede noemer 'online criminaliteit'.
Cybercrime gaat over alle strafbare feiten die worden gepleegd via een ICT middel én die gericht zijn op een ICT middel. Gedigitaliseerde criminaliteit gaat over strafbare feiten waarbij gebruik gemaakt wordt van een ICT middel. Je zou kunnen zeggen dat cybercrime alleen kan bestaan dóór het internet, waarbij gedigitaliseerde criminaliteit oude wijn in nieuwe zakken is. Voorbeelden van cybercrime zijn phishing en hacken. Phishing hebben we zojuist besproken, dat gaat om het vissen naar gegevens om deze later te gebruiken. Hacken wil zeggen dat er daadwerkelijk ongewenst wordt binnengedrongen in je telefoon, computer of tablet. Voorbeelden van gedigitaliseerde criminaliteit zijn bijvoorbeeld online aankoopfraude, online identiteitsfraude en online stalking. Allemaal strafbare delicten die ook al bestonden zonder de digitale mogelijkheden. Voor u als burger maakt dit onderscheid wellicht niet uit, maar voor de aanpak door politie en voor de uitvoering van onderzoek maakt dit wel uit. Voor het vervolg van de lezing zal ik voor het gemak verder spreken van online criminaliteit.

De laatste cijfers van het CBS[1] laten zien dat in 2022 2,2 miljoen Nederlanders slachtoffer zijn geworden van online criminaliteit. Dat is 15% van alle Nederlanders van 15 jaar of ouder. 20% van de Nederlanders deed hier aangifte van. De meest gemelde vorm van online criminaliteit is online oplichting en fraude, 8% geeft aan hiermee in aanraking te zijn gekomen. Op twee en drie staan hacken en online bedreiging intimidatie, met respectievelijk 5% en 4%. Wanneer we inzoomen op de Friese context zien we soortgelijke cijfers[2]: 16% van de Friezen zijn slachtoffer geworden van een vorm van online criminaliteit. Dit percentage neemt, net zoals het landelijke percentage, langzaam toe en is bijna verdubbeld in 10 jaar tijd. Ook in Friesland komt daarbij online oplichting en fraude het meeste voor. Er is gelukkig steeds meer aandacht voor de emotionele impact van slachtofferschap. Volgens mij rapporteert het CBS dit jaar voor het eerst over de emotionele impact van slachtofferschap van online criminaliteit. 37% van de respondenten geeft aan dat zij minder vertrouwen hebben in mensen na hun slachtofferschap, 30% voelt zicht minder veilig. Depressieve klachten, slaapproblemen en angst worden ook door 7 á 8 % van de slachtoffers genoemd. Met name online bedreiging en intimidatie blijken flinke impact te hebben.

Het 'cyberwoord' van 2022 was 'cyberschaamte'[3]. Ongeveer 60% van de respondenten in een onderzoek van I & O research gaf aan zich te schamen nadat ze op een malafide link in een mail hadden geklikt. Wanneer je ergens slachtoffer van wordt kun je simpel gezegd op twee manieren reageren: je wordt boos óf je schaamt je. Wanneer je boos wordt stel je eigenlijk dat oorzaak buiten jezelf om ligt. Je bent wellicht boos op de cybercrimineel. Schaamte daarentegen impliceert dat jij schuldig bent, dat jij het had kunnen voorkomen. Ik wil in de volgende sectie toelichten hoe we wellicht mogen concluderen dat we te streng zijn voor onszelf.

1.3 Psychologie en digitale weerbaarheid

Even terug naar het eerder genoemde voorbeeld. Wellicht herkent Mevrouw Rijpstra negen van de tien keer wel een dubieuze e-mail, maar kwam deze mail precies op het juiste moment. Dit voorbeeld laat zien dat een ongeluk in een klein hoekje zit. Het beschermen van jezelf tegen online criminaliteit gaat dus niet alleen om het daadwerkelijk herkennen wat malafide of bonafide is. De invloed van psychologische factoren is evenredig belangrijk. Denk daarbij aan factoren als digitaal zelfvertrouwen, tijdsdruk en risicoperceptie. Ik zal deze drie factoren kort toelichten.

1. Allereerst digitaal zelfvertrouwen: wanneer je kennis hebt van zaken betekent dit niet direct dat je deze kennis ook effectief inzet. Er moet ook het zelfvertrouwen aanwezig zijn dat je de kennis ook daadwerkelijk durft en kan inzetten. In het Engels is het woord hier vaak *self efficacy*: heb ik het gevoel dat de vaardigheid/kennis kan inzetten.
2. Als tweede, tijdsdruk: wanneer wij onder druk staan beïnvloedt dit ons beoordelingsvermogen. Ons hersenen gaan dan vaker over op de 'efficiënte' modus, dat wil zeggen: we kijken vooral naar punten van herkenning. In het

[1] https://www.cbs.nl/en-gb/news/2023/19/2-2-million-cybercrime-victims-in-2022
[2] https://www.planbureaufryslan.nl/monitoren/veiligheid/
[3] https://ecp.nl/cyberschaamte-is-het-cybersecuritywoord-van-het-jaar-2022/

genoemde geval van mevrouw Rijpstra bijvoorbeeld: 'je verwacht een mail met een track &trace', deze herkenning 'vertroebeld' de gedachte om de mail op meer punten te checken op malafide kenmerken.

3. Als derde, risicoperceptie: hoe wij risico's inschatten verschilt van persoon tot persoon. Ook al weet je hoe je je moet beschermen is nog steeds vraag of en wanneer dit nodig is. Zie je een cybercrimineel achter elke mail? Of denk je dat je geen interessant doelwit bent? De waarheid ligt in de praktijk ergens in het midden.

Ik had ook nog andere psychologische factoren kunnen benoemen. Wat ik met bovenstaande punten vooral wil verduidelijken is 'weten wat je moet doen om jezelf digitaal te beschermen' een deel, en wellicht zelfs maar een klein deel is van digitale weerbaarheid. De praktijk en ook onderzoeken laten zien dat niemand 100% in staat is om online criminaliteit te herkennen. Daarom spreek ik in deze lezing in sommige gevallen over digitale weerbaarheid en niet over digitale veiligheid of digitale beveiliging. Digitale veiligheid suggereert namelijk dat het bovenal gaat om tegenhouden en niet zozeer om wat je moet doen wanneer slachtofferschap zich voordoet. Digitale weerbaarheid daarentegen gaat over het tegenhouden, de impact verlagen én over veerkrachtig herstellen wanneer slachtofferschap zich voordoet.

Naast dat ik wil spreken van digitale weerbaarheid wil het later in deze lezing ook hebben over verantwoordelijkheid. Een deel van deze lezing gaat over wat je als individu kan doen, maar het is ook belangrijk om te benadrukken dat er meer vangnetten nodig zijn. Juist door het hebben van inzicht in psychologische factoren die ons gedrag beïnvloeden. Denk hierbij aan wetgeving of maatschappelijke initiatieven om de digitale weerbaarheid te verhogen. Hierover later meer. Ik wil het nu eerst hebben over een aantal maatregelen, of praktische tips, waarmee je de kans op en impact van slachtofferschap kunt verlagen. Per maatregel wil ik tevens benoemen welke uitdagingen er zijn om de maatregel correct door te voeren.

1.4 Wat kun je doen om slachtofferschap te voorkomen?

De eerste maatregel die ik wil benoemen gaat over het gebruik van wachtwoorden. Wanneer we spreken over wachtwoorden is een belangrijke samenvatting: langer is beter. Een langer wachtwoord betekent namelijk dat een cybercrimineel langer bezig is met het kraken van het wachtwoord. Een manier om eenvoudiger langer wachtwoorden te maken is door gebruik te maken van wachtwoordzinnen[4]. Een voorbeeld hiervan is: *Fryske_Akademie_is_veilig_echt_waar.* Voor een extra goede beveiliging raad ik daarnaast aan om waar mogelijk gebruik te maken van 'inloggen in twee stappen'. Soms heet dit 'tweestapsverificatie' of in het Engels *twofactor-authentication*. Dit betekent dat je na het invoeren van je wachtwoord op je mobiel een sms-ontvangt, een code in moet voeren of bijvoorbeeld je vingerafdruk gebruikt om in te loggen. Dit is erg lastig te kraken voor cybercriminelen, want ze hebben dan niet alleen je wachtwoord nodig, maar ook

[4] https://www.digitaltrustcenter.nl/tips-voor-het-bedenken-van-een-sterk-wachtwoord

daadwerkelijk je telefoon of tablet. Met name de grote platforms zoals Google[5], Microsoft[6] en Facebook[7] bieden deze mogelijk standaard aan. Ik raad om bij de instellingen van deze platforms te checken hoe je dit kunt instellen. Zie daarvoor ook de voetnoten in de uitgeschreven lezing. De eerste uitdaging bij de wachtwoordmaatregel is dat ons geheugen beperkt is. Idealiter gebruik je namelijk voor ieder programma een ander wachtwoord, maar dat is wellicht lastig te onthouden. Een manier om dit te ondervangen is door een online of fysieke wachtwoordkluis te hebben. Een andere uitdaging is dat, ook al bedenk je nog zo'n goed wachtwoord, deze soms alsnog op straat komt te liggen doordat bijvoorbeeld een website gehackt is. Een oplossing die sommige website al bieden is het zogenoemde 'wachtwoordloos' inloggen. Dan krijg je bijvoorbeeld een eenmalige link in de mail waarmee je kunt inloggen. Daar kleven overigens ook weer wat nadelen aan. Het is dus nog zoeken naar de beste oplossingen. Voor nu wil ik in ieder geval herhalen: een langer wachtwoord is beter.

De tweede maatregel die ik wil benoemen gaat over het online delen van vertrouwelijke gegevens. Simpel gezegd: wat je niet deelt kan ook niet tegen je worden gebruikt. Scenario's die cybercriminelen creëren voor bijvoorbeeld phishing zijn gemaakt door gebruik te maken van informatie die over je te vinden is op het internet. Wat zou er gebeuren wanneer je een briefje op de voordeur plakt waarop staat *ik ben op vakantie naar Mallorca en weer terug op 15 augustus?* Hetzelfde doen we wel met enige regelmatig op onze sociale media. Mijn tip: doe dat niet. In aanvulling hierop kun je ook je sociale media zoveel mogelijk afschermen en regelmatig controleren met wie je verbonden bent of wie je volgers zijn. De uitdaging bij deze maatregel is dat je niet altijd grip hebt over wat over jezelf online te vinden is. Het internet vergeet niet. Zelf Google ik soms op mijn eigen naam om te kijken wat er online te vinden is. Wanneer het onwenselijk is wat je vindt is het altijd mogelijk om een verwijderverzoek in te dienen bij bijvoorbeeld Google.

De laatste maatregel die ik wil benoemen heeft te maken met het gebruiken van standaard veilige instellingen. We maken steeds meer gebruik van apparaten die 'aan het internet hangen'. Deze zogenoemde slimme apparatuur is wellicht slim, maar niet erg veilig. Veel producten staan standaard onveilig ingesteld. Met bijvoorbeeld privacy-onvriendelijke instellingen of zwakke wachtwoorden. Hetzelfde geldt overigens voor de privacy-instellingen op social media en andere online platforms. Ook hierbij is het aan te raden om regelmatig te controleren of te laten controleren wat de instellingen zijn. De uitdaging is dat het bijna niet te doen is om alles te controleren. Je wilt ervan uit kunnen gaan dat wat je gebruikt of wat je koopt digitaal veilig is. Ik wil het hierover hebben in de volgende sectie.

Naast deze drie genoemde maatregelen kan ik nog meer maatregelen benoemen. Ik laat het voor nu bij deze drie. Dit doe ik omdat deze drie maatregelcategorieën mijns inziens het meest tastbaar en uitvoerbaar zijn. Wellicht dat we bij de discussie nog ruimte hebben om een aantal andere maatregelen te bespreken.

---

[5] https://support.google.com/accounts/answer/185839?hl=nl&co=GENIE.Platform%3DDesktop
[6] https://support.microsoft.com/nl-nl/account-billing/verificatie-in-twee-stappen-gebruiken-met-uw-microsoft-account-c7910146-672f-01e9-50a0-93b4585e7eb4
[7] https://nl-nl.facebook.com/help/148233965247823

2. Veiligheid en verantwoordelijkheid

Ik heb in de eerste sectie van de lezing gesproken over wat online criminaliteit is, welke invloed psychologische factoren kunnen hebben op ons gedrag en welke maatregelen je kunt nemen om jezelf te beschermen tegen online criminaliteit. In dit tweede deel ik wil ingaan op de vraag: wie is verantwoordelijk voor onze online veiligheid? In hoeverre wij ons online veilig kunnen gedragen afhangt van ons eigen gedrag, in hoeverre de techniek dit gedrag faciliteert en in hoeverre overheid en bedrijfsleven voorzorgsmaatregelen en vangnetten organiseert. We hebben de focus in het eerste deel voornamelijk gelegd op ons eigen online gedrag. Ik wil nu ingaan op hoe techniek veilig gedrag kan faciliteren.

2.1 Techniek en veilig gedrag

Het samenspel tussen mens en techniek wordt weleens een socio-technisch systeem genoemd. Dit impliceert dat veiligheid en onveiligheid een gevolg zijn van een balans of onbalans in dit systeem. Wanneer wij bijvoorbeeld zeer gemotiveerd zijn om veiligheidsmaatregelen te nemen maar de techniek is zeer-gebruiksonvriendelijk zorgt dit voor onveiligheid. Of wanneer de techniek er wel is en gebruiksvriendelijk werkt, maar wij denken dat het niet nodig is om de maatregel te nemen, ook dan is er onveiligheid. Veiligheid ontstaat dus wanneer onze eigen houding, kennis, gedrag in balans zijn met de kwaliteiten en mogelijkheden van de techniek. Hier gaat het regelmatig mis. Bij het ontwikkelen van technische maatregelen voor onze digitale veiligheid wordt te weinig rekening gehouden met de gebruiksvriendelijkheid van de maatregel. Ik denk dat wij allemaal wel de voorbeelden kennen dat we wellicht graag een nieuwe virusscanner wilden gebruiken, of een wachtwoordkluis wilden aanschaffen, maar dat we door de bomen het bos niet meer zagen of, wanneer we het programma eenmaal hadden aangeschaft, het zo complex was om te gebruiken dat we de onveiligheid maar accepteerden. Hoe dit vanuit de technische, cybersecurity-kant, vaak wordt geïnterpreteerd is: "de mens is de zwakste schakel. Wij maken goede producten, maar de mens, de burger wil er geen gebruik van maken". Terwijl wij, de burgers, wellicht welwillend zijn, maar gewoon vinden dat het product of de dienst ongebruiksvriendelijk is.

Voor een deel van mijn tijd geef ik les aan studenten op NHL Stenden, specifiek in de minor Digitale Weerbaarheid. De studenten in deze minor hebben zeer verschillende achtergronden. Er zitten Veiligheidskunde studenten tussen, ICT-studenten, Rechten-studenten, zelfs pedagogiek-studenten. Een bonte mix. Wat vooral opvalt is dat ICT-studenten op een geheel andere manier kijken naar de techniek en de relatie tussen mens en techniek. Ik kan mij een voorval herinneren waarbij aan een groep van vier ICT-studenten het volgende werd gevraagd: ontwikkel een product of aanpak die ervoor zorgt dat meer burgers gebruik gaan maken van VPN. Voor de goede orde: VPN is een beveiligingsmaatregel die ervoor zorgt dat je internetverbinding beschermt wordt. De oplossing van de studenten was als volgt: zij maakten een presentatie van 30 minuten waarin ze gedetailleerd uitlegden hoe een VPN technisch werkt, met woorden als 'protocollen', 'servers', en 'ip-adressen. Een volledige focus op de techniek. Ze waren voorbijgegaan aan het feit dat het installeren van een VPN en het gebruiken van een VPN als complex en gebruiksonvriendelijk wordt ervaren. De burgers hadden behoefte aan praktische hulp en handvatten en niet aan een technische uitleg over 'hoe' VPN werkt. Achteraf moesten de studenten er overigens zelf om lachen. Ze benoemden dat ze beter

interviews hadden kunnen doen met een aantal burgers om bijvoorbeeld VPN gebruiksvriendelijker te maken met een praktische handleiding.

Met dit voorbeeld wil ik laten zien dat kennis van menselijk gedrag nodig is bij het ontwikkelen van technische maatregelen. Waarom zouden we een maatregel nemen die te complex en technisch is? Gelukkig is er een groeiend onderzoeksveld naar zogenoemde 'human-centred cybersecurity'. Binnen dit onderzoeksveld spreken we niet van de mens als zwakste schakel en ook niet zozeer van de mens als sterkste schakel. Het gaat in dit veld over hoe we de juiste balans kunnen vinden tussen techniek en menselijk gedrag, waarbij beide een bepaalde verantwoordelijkheid dragen. Ik kijk hoopvol uit naar de resultaten die dit zal opleveren voor ons digitale veiligheid.

2.2 Voorzorgsmaatregelen en vangnetten overheid en bedrijfsleven

In de veiligheidskunde wordt gesteld dat wanneer bij gewoontegedrag een ongeluk in een klein hoekje zit de oplossing voor een veilige omgeving allereerst gezocht moet worden in het creëren van een veilig ontwerp. Wanneer we het hebben over digitale weerbaarheid moeten wij onderkennen dat de digitale omgeving waarin we ons gedrag moeten vertonen veel hiaten kent. Zoals eerder aangegeven zijn veel slimme producten die wij gebruiken nog erg onveilig en privacy-onvriendelijk. Veel apparatuur en programma's die wij gebruiken vallen al snel om wanneer wij een keer op een verkeerd linkje klikken. Daarnaast zijn de organisaties waar wij diensten van afnemen ook verre van weerbaar. Organisaties waar wij onze vertrouwelijke gegevens hebben opgeslagen worden regelmatig slachtoffer van online criminaliteit of er ontstaat door eigen toedoen een groot datalek.

Het is niet zozeer dat ons gedrag of het gedrag van bedrijven inherent is veranderd in de online wereld. De impact in de digitale wereld is alleen groter. Wanneer iemand je woonadres weet en je huissleutel kopieert heb bovenal jijzelf daar last van. In de online wereld betekent levert dit echter vaak een keten van problemen op. Wanneer een cybercrimineel jouw e-mailadres en wachtwoord heeft wordt jouw e-mailadres gebruikt voor phishingmails of andere vormen van online fraude. En wanneer bij bedrijven online data lekt gaat het gelijk om grote hoeveelheden, in plaats van een aantal ordners met informatie. De impact van incidenten is groter geworden. Daarom is er gelukkig steeds meer aandacht voor voorzorgsmaatregelen om slachtofferschap van online criminaliteit bij de overheid en het bedrijfsleven te voorkomen. Daarnaast is er ook steeds meer aandacht hoe bedrijven jouw, de burger, kunnen beschermen tegen datalekken en online criminaliteit. Ik wil hiervan een aantal voorbeelden uitlichten.

Het eerste beschermingsvoorbeeld heeft te maken met standaarden en normenkaders. Van organisaties wordt steeds vaker gevraagd dat zij voldoen aan standaarden of normenkaders. Denk hierbij aan een set regels, procedures en beleidsstukken die laten zien dat de organisatie grip heeft op digitale dreigingen en risico's. Soms doen organisaties dit omdat het wettelijk vereist is, denk aan bedrijven die onderdeel uitmaken van onze vitale infrastructuur of bedrijven in de bankensector. Soms omdat ze veel persoonsgegevens verwerken en daarom ons verscherpt toezicht staan van de Autoriteit Persoonsgegevens. In enkele gevallen nemen organisaties maatregelen omdat het veilig omgaan met onze data inherent onderdeel is van hun organisatie, denk aan data-centers en IT-bedrijven.

Het tweede beschermingsvoorbeeld dat ik wil benoemen is dat de laatste jaren steeds meer organisaties oefenen met cyber-incidenten. Zo bestaat er sinds een aantal jaren de overheidsbrede cyberoefening en nodigen steeds meer bedrijven goedwillende hackers uit om hun ICT-systemen te testen. Zie het als een digitale brandoefening. Want zoals ik al aangaf: niet alle incidenten zijn te voorkomen. In een cyberoefening leren bedrijven hoe ze een incident kunnen erkennen, hoe ze impact zo laag mogelijk kunnen houden en hoe ze om moeten gaan met communicatie richting burgers. Een goede ontwikkeling hierin is daarnaast dat de uitkomsten van dergelijke oefeningen publiek worden gedeeld, zodat meer organisaties hiervan kunnen leren.

Een belangrijk derde beschermingsvoorbeeld dat ik wil benoemen is het feit dat er steeds meer, met name Europese, wet- en regelgeving is om een veilige digitale omgeving te creëren. Veel online dreigingen spelen op Europees: de aanpak van de macht van techbedrijven, de aanpak van cybercrime, het beschermen van onze online privacy. Vraagstukken die nu allemaal allereerst op EU-niveay worden aangepakt. Zo is er de welbekende AVG om onze online privacy te beschermen, zijn er wetten die vereisen dat bedrijven veiligheidsmaatregelen nemen en incidenten melden. Daarnaast is er een recente EU-richtlijn die ervoor zorgt dat onze slimme apparaten veiliger gaan worden, de radioapparatuurrichtlijn[8]. Deze richtlijn voor slimme apparaten vereist dat producten die worden verkocht op de Europese markt niet alleen fysiek veilig, maar ook digitaal veilig zijn en gaat gelden vanaf 2024. Een mooie ontwikkeling om de verantwoordelijkheid voor digitale veiligheid meer bij de organisaties neer te leggen. Net zoals je wilt vertrouwen op een goed slot op je voordeur, moet je ook kunnen vertrouwen op je slimme en veilige speaker, oven of lampen.

[8] https://www.secura.com/nl/blog/iot-producten-basis-veiligheidseisen

3. Toekomstperspectief

Voordat ik inga op een aantal dilemma's die ik graag met jullie wil bespreken na de pauze wil ik allereerst een toekomstperspectief schetsen. Hierbij wil ik ingaan op drie thema's: meer aandacht voor slachtofferschap, meer samenwerking tussen techniek en psychologie en verschuiving verantwoordelijkheid. Omdat de verkiezingen op 22 november zijn wil ik ook kort ingaan op hoe de politieke partijen denken over onze digitale veiligheid.

3.1 Drie perspectieven

Ten eerste: De trend die maatschappelijk is ingeslagen is dat er meer aandacht is voor de zachte kanten van slachtofferschap van online criminaliteit. Er wordt onderkent dat bepaalde vormen van online criminaliteit evenredig veel psychologische impact kunnen hebben als traditionele criminaliteit. Dit is een goede ontwikkeling. Mijn hoop is dat wij allemaal meer open durven te zijn over slachtofferschap, geen schaamte ervaren en ook slachtofferschap melden bij de politie. Slachtofferschap van online criminaliteit wordt namelijk slechts in 20% van de gevallen gemeld bij de politie. Redenen om niet te melden zijn bijvoorbeeld de aanname dat de politie er niets aan kan doen. De praktijk is echter dat politie steeds meer expertise ontwikkeld om goed om te gaan met online criminaliteit. Hoe meer meldingen er binnenkomen hoe meer prioriteit het thema krijgt.

Als tweede wil ik benadrukken dat de praktijk laat zien dat er meer samenwerking nodig is tussen techniek en psychologie. Hoe ik dit voor me zie is dat IT-bedrijven die maatregelen aanbieden voor onze digitale veiligheid meer naar de burgers toe gaan. En daarbij burgers aan de hand meenemen om maatregelen te implementeren. Dit kan bijvoorbeeld op scholen, bibliotheken en andere openbare plekken. Daarnaast is het nodig dat opleidingen voor digitale veiligheid meer met elkaar samenwerken om tot gezamenlijke digitaal-veilige oplossingen te komen. Uiteraard hoop ik dat ik hier vanuit mijn werkgever aan kan bijdragen, door studenten van NHL Stenden te verbinden. Ook op de hogeschool is het namelijk zo dat de technische opleidingen op een andere plek zitten dan de 'zachte' opleidingen. Digitale veiligheid vraagt om een integrale aanpak.

Als derde wil ik aangeven dat de trend moeten worden doorgezet dat er steeds meer wet- en regelgeving ontstaat om een veilige digitale omgeving te creëren, waarbij de verantwoordelijkheid minder bij de burgers ligt en meer bij de bedrijven. Waar we uiteraard voor moeten waken is dat dit doorslaat in regelzucht. Zo wordt er steeds strenger gehandhaafd op online bedreigingen en online haat[9], maar het is niet transparant waarom het ene bericht wordt verwijderd, terwijl het andere bericht mag blijven staan. Online handhaving is daarmee in een kwetsbare balans of onbalans met de vrijheid van meningsuiting.

3.1 Digitale veiligheid in de verkiezingsprogramma's

Zoals aangegeven wou ik nog kort ingaan op wat de verkiezingsprogramma's zeggen over digitale veiligheid. Wat het geval is dat er op dit moment te weinig geld en aandacht is voor onze digitale veiligheid. Op overheidsniveau is expertise over het thema versnipperd en het is onduidelijk wie over het thema gaat. Wat opvalt is dat in de huidige verkiezingsprogramma's duidelijker en concreter wordt geschreven over digitale

[9] https://ecer.minbuza.nl/-/digitale-dienstenverordening-dsa-definitief-vastgesteld

veiligheid[10]. Er wordt geschreven over allerlei technische en procedurele maatregelen om onze digitale veiligheid beter te beschermen. Zo heeft Groenlinks/PVDA het vooral over inperken van de macht van de grote techbedrijven, spreekt NSC over het updaten van verouderde overheidssystemen en de beveiliging hiervan en heeft de VVD veel aandacht voor een cyberkeurmerk voor het MKB. D66 wil in nationaal datalekregister om meer openheid te geven over datalekken en Volt wil meer ruimte geven aan ethisch hackers, de goede hackers die onze systemen veilig houden. Het CDA legt de focus op striktere privacy en beveiligingsmaatregelen voor overheidssystemen en de Partij voor de Dieren legt de nadruk op digitale geletterdheid en bewustwording bij burgers. Samenvattend: we zijn gegaan van vaag naar concreet. Een goede ontwikkeling. Wanneer je op 22 november stemt komt het erop neer dat iedere stem zorgt voor meer focus op digitale weerbaarheid.

[10] https://bernold.substack.com/p/wat-vertellen-de-verkiezingsprogrammas

4. Dilemma's en afronding

4.1 Dilemma's

Voordat ik ga afronden wil ik een aantal dilemma's bij jullie neerleggen. Dilemma's die we hopelijk met elkaar kunnen bespreken bij de koffie of na de pauze.
Het eerste dilemma heeft te maken met de psychologische factoren die invloed hebben op slachtofferschap van cybercrime. Een manier om de invloed van psychologische factoren in te perken is daar allerlei beveiligingsmechanismes in te bouwen die de gebruiksvriendelijkheid van digitaal werken veelal verlaagd. Denk daarbij aan extra wachtwoordlagen met bijvoorbeeld vingerafdruk of irisscan. Wat kunnen anderzijds ook besluiten om te accepteren dat slachtofferschap gewoon kan voorkomen. We accepteren simpelweg het risico. Het eerste dilemma luidt:

- *Hoe balanceer je tussen gebruikersgemak en digitale veiligheid wanneer je wordt geconfronteerd met de keuze om een meer robuust beveiligingsproces te gebruiken, waardoor het voor burgers moeilijker wordt om toegang te krijgen tot hun accounts, maar tegelijkertijd de kans op toegang door cybercriminelen aanzienlijk vermindert?*

Het tweede dilemma heeft te maken met de vraag: wie is er verantwoordelijk voor onze digitale veiligheid? Ik heb een aantal voordelen genoemd van het feit dat er meer verantwoordelijkheid bij bedrijven wordt neergelegd. Tegelijkertijd neemt dit vaak met zich mee dat deze bedrijven veel gegevens willen verzamelen van het gebruik van het apparaat, om zo de veiligheid te waarborgen. Veelal zijn dit privacygevoelige gegevens, zoals locatie en het IP-adres (je digitale woonadres). Het tweede dilemma luidt:

- *In hoeverre rechtvaardig je het verzamelen van privacygevoelige gegevens door slimme apparaten om hun functionaliteit en veiligheid te verbeteren, wetende dat deze gegevens mogelijk kunnen worden gebruikt voor profilering (of reclame), zelfs als het doel is om de burger te beschermen tegen potentiële veiligheidsrisico's?*

Het derde dilemma is meer politiek van aard, op 22 november de verkiezingen zijn geweest. Een aantal partijen pleit voor een minister van Digitale Zaken. Een reden hiervoor is dat beleid rondom digitale zaken veelal versnipperd is over meer ministeries. Tegenstanders van een door een dergelijk ministerie stellen juist dat het goed is dat op alle ministeries aandacht is voor de impact van digitalisering en dat een specifiek ministerie niet nodig is. De focus zal volgens tegenstanders vooral moet liggen op het verhogen van digitale kennis in de tweede kamer en het voortzetten van de commissie digitale zaken (die al dus al bestaat). Het derde dilemma luidt:

- *Het oprichten van een afzonderlijk ministerie van Digitale Zaken biedt de mogelijkheid om de toenemende digitalisering te reguleren en te bevorderen, waardoor expertise op dit gebied wordt geconcentreerd. Echter, dit brengt het risico met zich mee dat er een versnippering ontstaat in de beleidsvorming, aangezien digitale aspecten ook verweven zijn met diverse andere beleidsterreinen, waardoor een gecoördineerde en integrale benadering bemoeilijkt kan worden.*

Deze dilemma's heb ik op een aantal powerpointslides gezet en afgedrukt. Naast de dilemma's ben ik uiteraard ook benieuwd naar de vragen die leven onder jullie na de pauze.

4.2 Afronding

Dan wil ik nu deze lezing graag afronden. We hebben het gehad over online criminaliteit, digitale weerbaarheid en de balans de veiligheid en verantwoordelijkheid. Daarnaast heb ik een kort toekomstschets gegeven, met daaruit voortvloeiend een aantal dilemma's.

Zoals jullie merken heb ik in deze lezing niet specifiek gefocust op uitdagingen die spelen in de Friese context. Dat heeft ermee te maken dat veel van de dreigingen en de aanpak van deze dreigingen universeel zijn en grenzenoverstijgend. Ik wil wel een aantal voorbeelden noemen waarmee we in Friesland vooroplopen in het digitaal weerbaarder maken van de maatschappij. De gemeente Leeuwarden is bijvoorbeeld de eerste gemeente geweest die een grootschalige cyber-oefening heeft uitgevoerd, een voorbeeld voor veel gemeenten. We hebben met de MKB Cyber Campus een uitstekend aanspreekpunt voor MKB-ers die aan de slag willen met digitale veiligheid. En wij hebben met de onderzoeksgroep cybersafety één van de drie onderzoeksgroepen in Nederland die op een integrale en menselijke wijze kijken naar digitale veiligheid.

Digitale veiligheid en digitale weerbaarheid vragen om een menselijke blik op digitalisering. Terwijl op dit moment meer de techniek overheerst. Het ontwerpen van een digitale veilige toekomst is een samenspel tussen techniek, menselijk gedrag en de context waarbinnen dit samenspel samenkomt: onze maatschappij. Ik ben hoopvol over de weg die we als maatschappij zijn ingeslagen, waarmee we meer grip krijgen op digitale ontwikkelingen.

5. Waardevolle bronnen voor meer digitale weerbaarheid

- Digitale Weerbaarheid voor senioren: boek met uitleg en achtergronden om digitale weerbaarheid te verhogen:
    - https://www.bibliotheek.nl/catalogus/titel.433473444.html/digitale-weerbaarheid-voor-senioren/
- Fraude Helpdesk: meldpunt voor online fraude/valse e-mails/tips voor herkennen
    - https://www.fraudehelpdesk.nl/
- Maakt Het Ze Niet Te Makkelijk: overheidswebsites met tips
    - https://www.maakhetzeniettemakkelijk.nl/senioren-en-veiligheid
- Seniorweb: praktische tips en ondersteuning
    - https://www.seniorweb.nl/onderwerp/veilig-internetten
- Veilig Bankieren: Voorlichtingsplatform van banken over fraude en veiligheid
    - https://www.veiligbankieren.nl/
- Veilig Internetten: praktische tips en ondersteuning
    - https://veiliginternetten.nl/

THORBECKE
ACADEMIE

NHL STENDEN