Practorale rede

Digitale Weerbaarheid

Onderwijs als motor voor
een digitaal weerbare samenleving

ROC FRIESE POORT

versterkjedigitaleweerbaarheid.nl

INLEIDING

Hoe beschermen wij onze eigen persoonsgegevens of die van bijvoorbeeld patiënten in de zorg? Normen en waarden vervagen in het digitale domein. Welke digitale normen en waarden kunnen we samen met onze studenten verkennen en uitdragen? Hoe zorgen we voor elkaar in het digitale domein? Wat mag wel en wat mag niet? Technische maatregelen bieden slechts een deel van het antwoord, het grootste aandeel zit in menselijk gedrag. Het practoraat Digitale Weerbaarheid houdt zich bezig met onderzoek en innovatie in het versterken van de digitale weerbaarheid, zowel privé als bij het beoefenen van het beroep.

Het practoraat kent twee dimensies. In de eerste dimensie staat digitale weerbaarheid als persoon en als samenleving centraal. Onderzoeken en innovaties die hierin aan bod komen zijn: een gezonde relatie met je smartphone, privacy, digitale normen en waarden en weerbaar zijn tegen digitale criminaliteit. De tweede dimensie richt zich op het duiden van de behoefte aan digitale weerbaarheid in het beroep, waarbij het practoraat start met de zorg- en welzijnsberoepen en de veiligheidsberoepen.

DE SMARTPHONE DE BAAS

Ons leven speelt zich in steeds meer online af. Er is nauwelijks meer sprake van een offline wereld. Generatie Z is een generatie waarbij internet vanzelfsprekend is en waarbij jongeren meer met leeftijdsgenoten van de andere kant van de wereld hebben, dan bijvoorbeeld met ouderen uit de buurt. We leven in een aandachtseconomie (Rushkoff,2019) waarbij bedrijven als Netflix, Google, Facebook en Twitter elkaar beconcurreren op het verkrijgen van onze aandacht en deze zo lang mogelijk proberen vast te houden. Bij jongeren wordt een FOMO (Fear of Missing Out) gecreëerd, denk maar aan Snapchat waarbij content slechts 24 uur online blijft. Is het wonderlijk dat jongeren zo gehecht zijn aan hun smartphone? Uit onderzoek van Simyo onder duizend Nederlanders blijkt dat een Nederlander gemiddeld twee uur en een kwartier per dag op zijn of haar smartphone zit. Jongeren onder de dertig zijn in die groep koploper met gemiddeld 03,21 uur per dag. In het onderwijs klinken dan ook steeds meer geluiden over het verbannen van de smartphone uit de klas. Maar past dat bij een opleiding waarbij jongeren in hun toekomstig beroep ook gebruik maken van een smartphone? Laten we in het onderwijs jongeren helpen bij het verkrijgen van een gezonde relatie met de smartphone en het kunnen sturen van de informatieprikkel die via digitale apparaten op hen afkomt. Dat het een noodzaak is, is voor iedereen duidelijk. Ook jongeren zien deze noodzaak. Uit een verkennend onderzoek van het practoraat Digitale Weerbaarheid blijkt dat 43% van de jongeren aangeeft te veel op de smartphone te zitten. Ongeveer 10% geeft zelf aan hier ook klachten van te ondervinden zoals concentratieproblemen en het slechter slapen.

#APRILOPSTIL - In april 2019 heeft ROC Friese Poort een project gedaan waarbij studenten twee weken zonder smartphone door het leven zijn gegaan. Studenten gaven aan meer aandacht voor de familie en vrienden te hebben en echte gesprekken te voeren. In april 2020 krijgt dit project een vervolg, waarbij het practoraat Digitale Weerbaarheid en het practoraat Brede Vorming onderzoek doen naar een gezonde relatie met je smartphone.

PRIVACY

In 2019 heeft de privacywet Algemene Verordening Gegevensbescherming (AVG) haar eerste verjaardag heeft gevierd. Er wordt veel over de privacywet gediscussieerd, maar één effect staat als een paal boven water. Er is meer aandacht voor privacy. En dat is nodig, want we koersen af op een maatschappij met 'Surveilance-capatalism', aldus Shoshana Zuboff (2019). Menselijk gedrag wordt vertaald naar data met gedragsgegevens. Natuurlijk onder de noemer van serviceverbetering, maar met name om zoveel mogelijk van deze gedragsgegevens te verzamelen. Hoe meer gegevens, hoe groter het dataprofiel, hoe beter kunstmatige intelligentie gedrag nu, straks en later kan voorspellen. De Franse filosoof Gaspard Koenig (2019) beschrijft dat kunstmatige intelligentie nog verder gaat. Kunstmatige intelligentie profiteert volgens hem van kennis van neurowetenschappers en gedragseconomen over hoe wij kiezen en hoe vooringenomen wij daarin zijn. Op basis van data die we zelf weggeven, kan de industrie anticiperen op ons gedrag en dit bijsturen. Volgens Koenig verlost kunstmatige intelligentie ons van de moeite om zelf te kiezen. We worden in veel alledaagse keuzes gestuurd, zonder dat we ons er echt bewust van zijn. Techgiganten verkopen informatie uit dataprofielen aan bedrijven en organisaties die hier hun voordeel mee kunnen doen. Dimitri Tokmetzis en Maurits Martijn (2016) noemen dit in het boek 'Je hebt wel iets te verbergen' ook wel 'de verborgen economie achter het internet'. Gratis bestaat niet, je betaalt altijd met je persoonsgegevens.

Tijdens de burgerschapsdagen van ROC Friese Poort Dokkum hebben studenten hun eigen digitale voetafdruk gevisualiseerd. Hierbij moesten studenten zo`n concreet mogelijk beeld vormen van de informatie die Google over hen heeft. Studenten waren geschokt over datgeen ze zagen. Ze konden bijvoorbeeld in Google Maps (timeline) zien waar ze de afgelopen jaren op ieder moment van de dag zijn geweest. Ook vonden studenten een overzicht van alle aankopen die ze de afgelopen jaren hebben gedaan. Google leest namelijk alle emails met orderbevestigingen van bijvoorbeeld kledingwinkels, fastfood ketens, of hotels en luchtvaartmaatschappijen.

In het onderwijs geef ik wel eens de opdracht om jongeren te laten googelen naar het woord 'zalm'. Daarbij laat ik ze een screenshot maken van de eerste tien zoekresultaten. Vervolgens vraag ik de jongeren om hun ouders ook te laten googelen op het woord 'zalm' en hier een screenshot van te maken. Het resultaat? Jongeren krijgen informatie over de vis zalm en ouderen krijgen voornamelijk informatie over gerechten die ze kunnen bereiden met zalm. Dit is een tastbaar voorbeeld van het gegeven dat Google zoekresultaten baseert op dataprofielen van mensen.

De digitale industrie komt op verschillende manieren aan persoonsgegevens, met de smartphone als een van de meest waardevolle bronnen. Gemiddeld hebben we zo`n twintig (gratis) apps geïnstalleerd op onze smartphone waarbij we niet of nauwelijks de voorwaarden hebben gelezen en de permissies hebben geaccepteerd. Uit onderzoek van Daniel Kahneman (2012) blijkt dat slechts 5 procent van ons gedrag te duiden is als "bewust/gepland" gedrag. En dit zien we terug in het digitale domein. We installeren klakkeloos gratis apps, geven permissies en accepteren cookies. Zonder dat we precies weten wat we accepteren of waar we toestemming voor geven.

Studenten MBO Juridisch Administratief Dienstverlener hebben tijdens de startbijeenkomst van het practoraat Digitale Weerbaarheid onderzoek gedaan naar het fenomeen dat mensen vaak klakkeloos toestemming geven, zonder dat ze daadwerkelijk de inhoud kennen. Studenten hebben deelnemers bij aanvang gevraagd een formulier te ondertekenen waar in staat dat ze bij akkoord gevraagd kunnen worden een glitterjasje te dragen. Tijdens het plenaire gedeelte van de bijeenkomst hebben studenten de resultaten gepresenteerd. Van de 90 deelnemers hebben slechts 4 niet getekend. Van de 86 deelnemers is één willekeurig persoon gevraagd het glitterjasje aan te trekken. Hierdoor was het voor de genodigden in de zaal gelijk duidelijk hoe belangrijk het is dat je goed leest voordat je van alles tekent en het glitterjasje werd desondanks met trots gedragen.

Uit onderzoek onder onze eigen studenten blijkt dat 25% zich zorgen maakt over privacy. Hierbij geven studenten aan zich zorgen te maken over foto`s, whatsapp-berichten, zoekgeschiedenis, meekijken via de webcam en wie allemaal toegang heeft tot persoonlijke gegevens. Een onderzoek van het CBS uit 2018 wijst uit dat 68% van de jongeren toegang tot persoonsgegevens via de smartphone beperkt of weigert.

DIGITALE NORMEN EN WAARDEN

Normen en waarden vervagen in de digitale wereld. Digitaal lijken we ons in een heel andere wereld te bevinden dan in de werkelijke wereld. We zijn een stuk mondiger en overzien nauwelijks wat de impact kan zijn van digitaal handelen op de werkelijke wereld van anderen.

> Zo sprak ik met een mevrouw die een dochter heeft die achttien jaar oud is. Iemand uit haar vriendenkring heeft een pornofilmpje online gezet en de naam van de dochter daarin getagd. Een personage in het filmpje leek op de dochter, maar ze was het zeker niet. Moeder en dochter hebben lang gediscussieerd over het wel of niet verwijderen van het socialmedia-account. Moeder stond erop, maar dochter wilde dat niet omdat ze daarmee zou aangeven dat zij het was in het filmpje. Het meest schrijnende vond ik dat de dochter er op een gegeven moment in ging geloven dat zij het was in het filmpje. Een grappig bedoelde tag veranderde in een nachtmerrie.

In de digitale wereld hebben we een verminderd besef van wat wel en wat niet mag. De politie (2019) heeft begin van dit jaar een campagne uitgevoerd waarbij duizenden jongeren zijn verleid tot digitale criminaliteit. Ze werden bijvoorbeeld aangespoord Instagramaccounts te hacken. Toen ze op de link klikten om de hack uit te voeren, kwamen ze terecht op de website van de politie. Van de ruim 9500 jongeren die daadwerkelijk iets illegaals van plan leken, wist ruimt één derde niet dat het strafbaar is.

DIGITALE CRIMINALITEIT

Er is een sterke verschuiving gaande van de meer traditionele criminaliteit naar digitale criminaliteit. In 2018 gaf volgens het CBS ruim 8,5 procent van de internetgebruikers aan slachtoffer te zijn geweest van digitale criminaliteit. Jongeren tussen 12 en 18 jaar zijn met 12% de een na grootste groep slachtoffers. Daarbij ging het vooral om vermogensdelicten en hacken. Uit ons eigen onderzoek onder studenten geeft 16% aan slachtoffer te zijn geweest van digitale criminaliteit.

Weerbaarheid tegen digitale criminaliteit is technisch gezien redelijk eenvoudig te versterken. De grootste uitdaging zit erin om jongeren en volwassen te prikkelen om maatregelen te nemen. Daarbij gaat het om maatregelen als; veilig omgaan met wachtwoorden, herkennen van phishing, uitvoeren van updates en veilig omgaan met identiteitsbewijzen.

Uit het onderzoek onder onze studenten blijkt dat:

- 41% unieke wachtwoorden gebruikt;
- 44% procent persoonlijke informatie in wachtwoorden gebruikt;
- 14% procent een wachtwoordkluis gebruikt;
- 21% procent het wachtwoord wel eens deelt met anderen;
- 62% procent updates direct uitvoert;
- 25 procent wel eens is gehackt.

ONDERWIJS ALS MOTOR VOOR EEN DIGITAAL WEERBARE SAMENLEVING

Jongeren in het beroepsonderwijs kunnen een wezenlijke rol spelen in het versterken van de digitale weerbaarheid van de samenleving. Veel jongeren geven aan dat ze zich zorgen maken over hun eigen privacy. Met de juiste kennis en praktische handreikingen kunnen we samen met deze jongeren de zoektocht aangaan over de rol die kunstmatige intelligentie speelt in hun leven, wat kernwaarden zijn als het gaat om privacy, welke digitale waarden en normen we willen naleven, wat een gezonde relatie met de smartphone is, hoe we sturing kunnen geven aan de die enorme digitale informatieprikkel en hoe we weerbaar worden tegen digitale criminaliteit.

Hier ligt een mooie verbinding met het practoraat Brede Vorming. Brede Vorming houdt zich bezig met persoonsvorming: studenten opleiden tot wendbare, empathische en ondernemende mensen die waardenvast kunnen en durven handelen. Het practoraat Digitale Weerbaarheid verbindt dit gedachtengoed aan de digitale wereld. Een citaat van practor Koen Vos: “Je kunt naar mijn idee pas ‘zijn’ in de online omgeving, als je iemand bent in de echte wereld.”

DIGITALE WEERBAARHEID IN HET BEROEP

Een digitaal weerbare samenleving heeft een belangrijk beroepscomponent. In ieder beroep wordt gewerkt met data en iedere medewerker heeft de plicht om hier op een ethische en veilige manier mee om te gaan. Maar wat verstaan we onder het ethisch en veilig omgaan met data? In de praktijk is dit lastig te duiden, we willen immers ook volop gebruik maken van digitale mogelijkheden en dit brengt dilemma`s met zich mee.

ZORG- EN WELZIJNSBEROEPEN

In zorg- en welzijnsorganisaties komen veel afhankelijkheidsrelaties voor en wordt veelal gewerkt met kwetsbare doelgroepen. Denk bijvoorbeeld aan de ouderenzorg waarbij (dementerende) ouderen voor digitale diensten zoals telebankieren, afhankelijk zijn van hulpverleners, kinderen of buren. Bij misbruik wordt dit vaak niet gemeld, ouderen zijn immers afhankelijk van de hulp. Of denk aan thuiszorg, waarbij gegevens worden geregistreerd op datadragers (smartphone, laptop of tablet). Bij verlies of diefstal kunnen veel gevoelige gegevens op straat komen te liggen. Ook zien we in de thuiszorg dat kinderen camerasystemen ophangen. Wat betekent dit voor de privacy? In de ziekenhuiszorg is de toegang tot gegevens via het elektronisch patiëntendossier altijd onderwerp van gesprek en een kwetsbaarheid. Uit onderzoek blijkt dat hulpverleners nog altijd veel spieken in dossiers. De verstandelijke en lichamelijke gehandicaptenzorg heeft een doelgroep die extra kwetsbaar is voor zaken als gameverslaving, cyberpesten, verspreiding van malware en loverboyproblematiek. We vinden het belangrijk om jongeren voor te bereiden op digitale dilemma`s die zich kunnen voordoen in het zorg- en welzijnsberoep.

> Aleid Wolfsen, directeur Autoriteit Persoonsgegevens: “Laatst hing een vrouw huilend aan de lijn. Ze had onmin met iemand uit de buurt, die ook in het plaatselijke ziekenhuis werkte. Tot haar grote schok confronteerde die buurtgenoot haar met haar eigen medische gegevens. Dat kan niet.”

Uit onderzoek van Autoriteit Persoonsgegevens blijkt dat de zorgsector met 31% verantwoordelijk is voor de datalekken die worden gemeld. 23% van de datalekken komt uit ziekenhuizen en 22% uit apotheken. Verpleeg- en verzorgingshuizen zijn verantwoordelijk voor 5% van de datalekken. Een voorbeeld van een datalek is een phishingaanval op een ziekenhuis. Diverse ziekenhuismedewerkers hebben op een phishingmail geklikt en vervolgens hun inlognaam en wachtwoord ingevoerd. Hackers kregen hiermee toegang tot de e-mailaccounts van de betreffende medewerkers. Via deze accounts zijn vervolgens grote hoeveelheden vergelijkbare phishingmails verstuurd. In de mailboxen van de medewerkers zijn persoonsgegevens van patiënten teruggevonden. Met bewustwording over de gevoeligheid van data en praktische handreikingen in het herkennen van dit soort risico`s kan de kans op datalekken worden geminimaliseerd. Natuurlijk zijn daarbij ook technische maatregelen nodig, zoals MFA (multifactor authentication).

VEILIGHEIDSBEROEPEN

Medewerkers uit de veiligheidsberoepen kunnen een belangrijke rol spelen in het versterken van de digitale weerbaarheid in de samenleving. Bovendien kunnen studenten een rol spelen in het versterken van de digitale weerbaarheid van de samenleving door tastbare demonstraties te geven over de wijze waarop hackers te werk gaan. Beveiligers, handhavers en politieagenten komen in hun beroep situaties tegen waarmee zij digitale criminaliteit kunnen verhinderen. Een aantal voorbeelden:

- Rondslingerende malafide usb-sticks herkennen.
- Malafide wifi-netwerken detecteren.
- Social engineers herkennen.
- Digitale sporen veilig kunnen stellen, zoals whatsapp-gesprekken.
- Identiteitsfraude voorkomen (bijvoorbeeld post /pakketjes in brievenbussen).
- Potentiële datalekken herkennen, bijvoorbeeld papieren met persoonsgegevens zoals facturen en dergelijke.
- Surveilleren in het digitale domein, bijvoorbeeld naar fraude op Marktplaats.
- Digitaal buurtonderzoek. Bijvoorbeeld via social media een beeld krijgen van betrokkenen bij een incident. Of voorspellen wat zich in de buurt zal gaan afspelen.

Omdat beveiligers, handhavers en politieagenten een bepaalde mate van autoriteit hebben kunnen zij mensen makkelijker aanspreken op gedrag. Denk bijvoorbeeld mobiele telefoons die blijven liggen en computerschermen die niet worden gelockt.

> In Nijmegen noemen twee wijkagenten zich de ‘digitale wijkagent’. Deze twee wijkagenten zijn benaderbaar via WhatsApp (want onder de leeftijd van 25 belt niemand meer). Daarnaast doen ze onderzoek naar bijvoorbeeld Marktplaatsfraude in de wijk, zoeken ze gedetailleerde informatie op over verdachten en betrekken actief inwoners via social mediaplatformen.

MBO ICT SECURITY-SPECIALISTEN

Er is een verschuiving gaande van de werkzaamheden van een mbo IT’er. Steeds meer diensten worden as-a-service in de cloud aangeboden. Studenten IT (Informatietechnologie) krijgen in toenemende mate een belangrijkere rol in cybersecurity. Vanuit hun opleiding kunnen ze al een belangrijke rol spelen in het versterken van de digitale weerbaarheid van verenigingen en kleine ondernemingen. Verenigingen en kleine ondernemingen verwerken veelal persoonsgegevens, maar hebben vaak niet de expertise of financiële middelen om hier op een veilige manier mee om te gaan. Denk bijvoorbeeld aan een ondernemer die als zzp’er makelaar is. Deze ondernemers verwerken vaak kopieën van identiteitsbewijzen, salarisstroken en andere financiële gegevens. Als klant moet je erop vertrouwen dat een ondernemer hier veilig mee omgaat. Studenten IT (Informatietechnologie) kunnen vanuit hun opleiding worden ingezet om bij deze bedrijven onderzoek te doen naar veel voorkomende digitale kwetsbaarheden en hierover te adviseren. Dit levert voor studenten bijzonder rijke leersituaties op én het is waardevol voor de ondernemer (en zijn klanten). Bovendien kunnen studenten een rol spelen in het versterken van de digitale weerbaarheid van de samenleving door tastbare demonstraties te geven over de wijze waarop hackers te werk gaan. Denk daarbij aan het demonstreren van phishing websites, kwetsbaarheden in wifinetwerken en gesprek met burgers aan te gaan over bijvoorbeeld veilig omgaan met wachtwoorden.

BIBLIOGRAFIE

CBS. (2019, Juli 17). ***1,2 miljoen slachtoffers van digitale criminaliteit.*** Opgehaald van CBS: https://www.cbs.nl/nl-nl/nieuws/2019/29/1-2-miljoen-slachtoffers-van-digitale-criminaliteit

CBS. (2019, februari 4). ***Meeste Nederlanders beschermen gegevens op smartphone.*** Opgehaald van CBS: https://www.cbs.nl/nl-nl/nieuws/2019/06/meeste-nederlanders-beschermen-gegevens-op-smartphone

Kahneman, D. (2012). ***Thinking fast en slow.*** Penguin Books.

Koenig, G. (2019, november 8). ***We moeten greep krijgen op onze eigen data.*** Opgehaald van Financieel Dagblad: https://fd.nl/futures/1323224/wij-moeten-greep-krijgen-op-onze-eigen-data

Martijn, M., & Tokmetzis, D. (2016). ***Je hebt wel iets te verbergen.*** De Correspondent.

Persoonsgegevens, A. (2019, 9 19). ***Zorgsector opnieuw koploper datalekmeldingen bij AP.*** Opgehaald van Autoriteit Persoonsgegevens: https://autoriteitpersoonsgegevens.nl/nl/nieuws/zorgsector-opnieuw-koploper-datalekmeldingen-bij-ap

Politie. (2019, februari 19). ***Jongeren een klik verwijderd van cyber crime.*** Opgehaald van Politie: https://www.politie.nl/nieuws/2019/februari/13/00-9456-jongeren-een-klik-verwijderd-van-cybercrime.html

Rushkoff, D. (2019, september 20). ***Kijk niet naar je scherm, kijk naar elkaar.*** Opgehaald van Financieel Dagblad: https://fd.nl/futures/1316492/douglas-rushkoff-kijk-niet-naar-je-scherm-kijk-naar-elkaar

Simyo. (2019). ***Word jij slimmer of juist socialer van de smartphone?*** Opgehaald van Simyo: https://www.simyo.nl/onderzoek/smartphone-gebruik/

Zuboff, S. (2019). ***The age of serveillance capitalism.*** London: Profile Books.

ROC FRIESE POORT

Werk maken van je passie

www.rocfriesepoort.nl

versterkjedigitaleweerbaarheid.nl