1 Inleiding

'Datalek bij politie, hackers bemachtigen contactgegevens alle politiemedewerkers.'

'Politiehack van 62.000 medewerkers is gevaarlijk: naam agent is handelswaar.'

'Ook onrust bij medewerkers Openbaar Ministerie om politiehack.'

Dit is slechts een greep uit verschillende krantenkoppen die in oktober 2024 verschenen rondom de zogenoemde 'politiehack'.[1,2,3] Bij het betreffende datalek,[4,5] dat eind september 2024 bekend werd gemaakt, zouden contactgegevens van bijna 65.000 politiemensen zijn buitgemaakt, en mogelijk ook van een aantal ketenpartners. Volgens inlichtingendiensten is een statelijke actor – een entiteit die een land of staat vertegenwoordigt – hiervoor verantwoordelijk. Op het moment van schrijven zijn nog niet alle details rondom het datalek bekend. Er wordt nog gewerkt aan een zogenaamde *root-cause*-analyse: een methode gericht op het identificeren (en aanpakken) van de onderliggende oorzaken van een probleem. Wel is duidelijk dat dit incident grote impact heeft.[6] Hoewel de langere termijn uitwerking hiervan ook nog niet

1 https://nos.nl/artikel/2538710-datalek-bij-politie-hackers-bemachtigen-contactgegevens-alle-politiemedewerkers.

2 https://www.ad.nl/politiek/politiehack-van-62-000-medewerkers-is-gevaarlijk-naam-agent-is-handelswaar.

3 https://nos.nl/artikel/2539487-ook-onrust-bij-medewerkers-openbaar-ministerie-om-politiehack.

4 Een datalek is een beveiligingsincident (of bijna-incident) waarin zonder autorisatie (potentieel) toegang is verkregen tot informatie. Zie https://autoriteitpersoonsgegevens.nl/themas/beveiliging/datalekken/wat-is-een-datalek.

5 Eerder in 2024 vond bij CEPOL, het Agentschap van de Europese Unie voor opleiding op het gebied van rechtshandhaving, ook al een datalek plaats. Zie https://www.cepol.europa.eu/newsroom/news/notification-data-breach-related-leed-platform.

6 https://www.politie.nl/informatie/datalek---veelgestelde-vragen.html.

precies bekend is, wordt aangenomen dat de gegevens misbruikt zullen worden om bijvoorbeeld (gerichte) phishing-aanvallen uit te voeren en identiteitsfraude te plegen.

Onmiskenbaar is de korte termijn impact. De hack heeft tot veel onrust geleid onder politiemensen. Dit heeft diverse redenen. Een belangrijke reden is dat het voor hen lastig is te doorzien welke gegevens mogelijk nog meer zijn buitgemaakt en te doorgronden welke impact zij hier persoonlijk van gaan ondervinden. Een voorbeeld hierbij is het fenomeen doxing, waarbij vertrouwelijke informatie over een persoon of organisatie, veelal via internet, publiek wordt gemaakt, met als doel mensen af te persen, te beschamen of te intimideren. Los van de vraag hoe reëel dit betreffende scenario is, zijn het wel beelden die leven.[7]

Een andere reden voor de onrust zit waarschijnlijk in de communicatie over het datalek. Dit is een ingewikkeld punt. Immers, wanneer kan wat gecommuniceerd worden – zowel intern als extern –, wanneer is de organisatie zelf voldoende op de hoogte van wat er is gebeurd en zijn daarop voldoende maatregelen getroffen? Het is een ingewikkelde zoektocht naar de juiste balans tussen veiligheid enerzijds en transparantie anderzijds, waarmee de politieorganisatie werd geconfronteerd. In de media heeft het enkele journalisten verleid tot het gebruik van sensationele krantenkoppen. 'Fout van politievrijwilliger zette deur open voor hackers: "Rusland zit achter aanval"' is hier een voorbeeld van.[8] Uit deze kop is op te maken dat hier sprake is van een reflex die in de huidige tijdsgeest niet meer relevant is. Het stellen van de schuldvraag helpt niet om een weerbare en lerende organisatie te worden. Overigens moet gezegd worden dat in de interne berichtgeving door de korpsleiding meteen afstand werd genomen van deze 'who is to blame'-benadering.

Het is van belang om de oorzaak van een incident te achterhalen, maar de schuld ligt nooit bij de medewerker wanneer de organisatie schade lijdt door diens (onbedoelde) handelingen (Spithoven et al., 2024). Het wijst er slechts op dat er een nieuw risico is ontstaan of dat

7 Het ging in de berichtgeving ook over specifieke politiefuncties, zoals politiemensen die werken bij de Mobiele Eenheid, arrestatieteams en die heimelijk werk verrichten. Dat persoonsgegevens van deze politiemensen buitgemaakt zouden zijn, werd al snel ontkracht door de minister van Veiligheid en Justitie David van Weel. Volgens hem stonden hun gegevens niet op de buitgemaakte adressenlijst. Zie https://www.ad.nl/binnenland/inlichtingendiensten-politiehack-uitgevoerd-door-ander-land~a09ea492/.

8 https://www.telegraaf.nl/nieuws/23538070/fout-van-politievrijwilliger-zette-deur-open-voor-hackers-rusland-zit-achter-aanval.

de bestaande maatregelen nog niet toereikend waren. Hoewel in een NRC-artikel enig tegengas werd geboden richting het neerleggen van de schuldvraag bij een individuele medewerker, bleef ook in dat artikel de schuldvraag centraal staan, maar dan gericht tegen 'het management'.[9] Deze reflex is begrijpelijk, maar draagt zoals gezegd niet bij aan digitale weerbaarheid. Incidenten voor de volle honderd procent voorkomen en vermijden is onmogelijk. Het is daarom belangrijker en waardevoller om de daadwerkelijke redenen inzichtelijk te maken waardoor het incident heeft kunnen plaatsvinden en deze impact kon hebben, en daar maatregelen op te nemen, om zo systemen en procedures te verbeteren.

We moeten op een andere manier naar digitale weerbaarheid kijken en de rol van de mens daarin, van *mens als probleem* naar *mens als oplossing*, en daarmee oude patronen loslaten. Dit komt verderop in mijn rede nader aan bod. Eerst wil ik de context waarin mijn lectoraat zich beweegt, neerzetten. Ik start met de veiligheidsuitdagingen waarmee we te maken hebben en krijgen (par. 1.1). Vervolgens beschrijf ik beknopt wat ik versta onder digitale weerbaarheid (par. 1.2) en ga ik daarna in op de kernthema's rondom politie en digitalisering (par. 1.3).

1.1 Digitalisering en veiligheidsuitdagingen

De samenleving digitaliseert in rap tempo.[10] Digitale processen spelen een steeds grotere rol in ons dagelijks leven, en ze worden vaak beschouwd als het 'zenuwstelsel' van onze maatschappij (NCTV, 2022; Van Dijk, 2012). Dit komt doordat de maatschappij zonder digitale technologieën niet meer goed kan functioneren. Onze toenemende afhankelijkheid van digitale processen (incl. producten, diensten en netwerken) maakt ons kwetsbaar en biedt kansen voor kwaadwillenden op allerlei niveaus om daar misbruik van te maken. Veiligheid is een basisvoorwaarde voor een samenleving die vitaal en weerbaar is, en waarin mensen naar tevredenheid kunnen leven en zich kunnen ontplooien. Veiligheid is echter een 'delicaat krachtenspel', want te veel veiligheid kan initiatief en vrijheid beperken, terwijl te weinig veiligheid

9 https://www.nrc.nl/nieuws/2024/10/11/politiehack-als-een-vrijwilliger-of-de-stagiair-de-schuld-krijgt-is-er-echt-iets-mis-met-de-it-a4869054.

10 Digitalisering is 'de ontwikkeling die inhoudt dat geautomatiseerde werken op steeds meer plaatsen en op steeds meer verschillende manieren een rol spelen in het dagelijks leven' (Stol & Strikwerda 2017, p. 304).

tot chaos kan leiden (Ducheine, 2018). Ook hier is een goede balans dus nodig.

Volgens de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV, 2024) blijven digitale dreigingen onverminderd groot. Digitale dreigingen zijn er in verschillende soorten en maten. Naast datalekken, zoals reeds besproken, hebben we het dan vooral over criminaliteit[11] dat inmiddels voor een belangrijk deel een digitale component kent.[12] Denk bijvoorbeeld aan phishing-pogingen,[13] ransomware-aanvallen,[14] DDoS-aanvallen[15] en het hacken van systemen.[16] Dit kan leiden tot slachtofferschap onder burgers, faillissementen van bedrijven en algehele maatschappelijke ontwrichting. Digitale dreigingen hebben dus ook invloed op onze nationale veiligheid. Geopolitieke spanningen, zoals de oorlogen die momenteel gaande zijn, spelen hierbij eveneens een rol (NCTV, 2024).

Daarnaast zijn er tal van andere ontwikkelingen gaande rond de digitalisering van de maatschappij. Deze ontwikkelingen gaan steeds verder en brengen nieuwe veiligheidsuitdagingen met zich mee. Denk bijvoorbeeld aan generatieve AI (kunstmatige intelligentie), waarmee het plegen van online criminaliteit geoptimaliseerd kan worden – van geschreven tekst in phishingberichten[17] tot videocalls waarin deepfakes[18] worden toegepast om CEO-fraude te plegen[19] –, maar ook aan ontwikkelingen als robotica, nanotechnologie en kwantumcomputing. Let op dat deze ontwikkelingen ook kunnen worden ingezet ten behoeve van politiewerk, waarbij AI bijvoorbeeld kan helpen bij het

11 Met criminaliteit bedoel ik elke gedraging die als misdrijf strafbaar is gesteld.

12 Het internet heeft verschillende eigenschappen die de kans op criminaliteit vergroten (Leukfeldt, 2016; Yar, 2005). Het voert voor deze rede te ver om daar dieper op in te gaan.

13 Aanvallen waarbij middels een fraudeleuze actie via e-mail, berichten of nepwebsites persoonlijke gegevens, zoals wachtwoorden of creditcardinformatie, getracht wordt te ontfutselen door zich daarbij voor te doen als een betrouwbare entiteit.

14 Aanvallen waarbij kwaadwillende software een computer of netwerk versleutelt en de toegang blokkeert totdat er losgeld (bijv. in Bitcoin) wordt betaald.

15 Aanvallen waarbij een systeem wordt overbelast om het plat te leggen.

16 Aanvallen waarbij op ongeautoriseerde wijze wordt binnengedrongen in computers of netwerken om gegevens te stelen, schade aan te richten en/of controle over het systeem te verkrijgen.

17 https://www.europol.europa.eu/media-press/newsroom/news/criminal-use-of-chatgpt-cautionary-tale-about-large-language-models.

18 Een deepfake betreft 'inhoud (video, audio of anderszins) die volledig of gedeeltelijk is verzonnen of bestaande inhoud (video, audio of anderszins) die is gemanipuleerd' (Van der Sloot & Wagensveld, 2022, p. 1, vertaald uit het Engels).

19 https://www.bloomberg.com/opinion/articles/2024-02-05/a-25-million-hong-kong-deepfake-scam-on-zoom-shows-new-ai-risks.

overbruggen van taalbarrières, het verbeteren van kennismanagement, het bieden van ondersteuning in de taakuitoefening, en het bijdragen aan datagedreven werken.[20]

Ook virtuele werelden, waaronder de metaverse,[21] en de verdere integratie van digitale technologieën in en aan het lichaam[22] kunnen leiden tot nieuwe en/of aangepaste vormen van criminaliteit (Borwell et al., 2021a; Stol & Jansen, 2024; Van der Wagen, 2018).[23,24,25] Daarnaast zijn er kwesties zoals data-soevereiniteit[26] (en onze afhankelijkheid van technologie en software van bijv. de Verenigde Staten en China), online spionage en cyberoorlogvoering (NCTV, 2024), en fenomenen zoals polarisatie, haatzaaien en desinformatie, die kunnen leiden tot maatschappelijke spanningen en verstoringen van de openbare orde (Bantema, 2023). Tot slot zijn er schadelijke en immorele gedragingen waarmee de maatschappij wordt geconfronteerd, zoals cyberpesten en het eerder benoemde doxing (Van Huijstee et al., 2021).

Kortom
Digitale veiligheid is tegenwoordig van cruciaal belang voor een digitaal en onderling verbonden Nederland, Europa en wereld. Welvaart en vooruitgang zijn steeds meer afhankelijk geworden van digitalisering. Naarmate die afhankelijkheid groeit, neemt ook de potentiële impact toe wanneer het misgaat. Dit betekent dat we als samenleving weerbaar moeten zijn om met deze digitale uitdagingen om te gaan.

20 Generatieve AI kan ook worden ingezet ten behoeve van digitale weerbaarheid (NCTV, 2024).

21 De metaverse is een virtuele wereld waarin mensen kunnen interageren en activiteiten kunnen ondernemen via digitale avatars. De metaverse gebruikt verschillende technieken, zoals virtual reality, augmented reality en mixed reality. Deze technieken samen worden ook wel extended reality genoemd. Zie https://forwork.meta.com/nl/blog/difference-between-vr-ar-and-mr/.

22 Verbeek (2011, p. 14) benadrukt dat mens en technologie steeds verder verweven raken, 'zelfs zodanig dat het steeds lastiger wordt om een grens tussen beide te trekken'. Van Mensvoort (2019) onderkent dit en geeft daarbij aan dat technologie niet alleen onze omgeving verandert, maar ook de mens zelf. We merken dat al met mobiele telefoons die in relatief korte tijd de transitie maakten 'van onbekend naar vertrouwd naar onmisbaar' (Van Mensvoort, 2019, p. 63). Hij stelt dat hoewel dit apparaat niet in ons lichaam zit, het een verlengstuk is geworden van onze hersenen en beleving.

23 https://www.bbc.com/news/technology-44697788.

24 https://www.theguardian.com/commentisfree/2024/jan/05/metaverse-sexual-assault-vr-game-online-safety-meta.

25 https://www.upi.com/Health_News/2022/06/01/medical-devices-pacemakers-cybersecurity/70416536563 30/.

26 https://www.computable.nl/2024/10/21/overheid-herziet-cloudbeleid-wegens-zorgen-over-leveranciers-vs/.