Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2024–2025

29 628 Politie

Nr. 1242

VERSLAG VAN EEN COMMISSIEDEBAT

Vastgesteld 9 januari 2025

De vaste commissie voor Justitie en Veiligheid heeft op 27 november 2024 overleg gevoerd met de heer Van Weel, Minister van Justitie en Veiligheid, over:

- **de brief van de Minister van Justitie en Veiligheid d.d. 27 september 2024 inzake datalek politie (Kamerstuk 29 628, nr. 1221);**
- **de brief van de Minister van Justitie en Veiligheid d.d. 2 oktober 2024 inzake nadere informatie over hack bij de politie (Kamerstuk 29 628, nr. 1222);**
- **de brief van de Minister van Justitie en Veiligheid d.d. 9 oktober 2024 inzake update over hack bij de politie (Kamerstuk 29 628, nr. 1223);**
- **de brief van de Minister van Justitie en Veiligheid d.d. 8 november 2024 inzake update hack bij de politie (Kamerstuk 29 628, nr. 1236).**

Van dit overleg brengt de commissie bijgaand geredigeerd woordelijk verslag uit.

De voorzitter van de commissie,
Pool

De griffier van de commissie,
Brood

kst-29628-1242
ISSN 0921 - 7371
's-Gravenhage 2025

Voorzitter: Pool
Griffier: Van Tilburg

Aanwezig zijn acht leden der Kamer, te weten: Aardema, Helder, Michon-Derkzen, Mutluer, Van Nispen, Pool, Six Dijkstra en Van der Werf,

en de heer Van Weel, Minister van Justitie en Veiligheid.

Aanvang 16.01 uur.

De **voorzitter**:
Dames en heren, hartelijk welkom bij het commissiedebat Datalek bij de politie. Allereerst een hartelijk woord van welkom aan de Minister. Fijn dat u bij ons bent. Een woord van welkom aan de leden en aan ons publiek op de tribune. We hebben hier vandaag tot 19.00 uur de tijd. De spreektijden staan op vier minuten, met drie interrupties in deze eerste termijn. Ik vraag u gezien de tijd kort en bondig te interrumperen. Dan geef ik nu als eerste het woord aan mevrouw Van der Werf.

Mevrouw **Van der Werf** (D66):
Dank, voorzitter. Politieagenten zetten zich elke dag in voor een veilig Nederland. Ze draaien daarbij lange dienstem, geven hun weekenden op en maken veel mee waar je niet altijd vrolijk van wordt. Dat doen ze allemaal om onze veiligheid te garanderen. Het is pijnlijk dat juist zij het slachtoffer zijn geworden van dit lek.
Voorzitter. Ik stoor me dan ook aan de communicatie naar agenten toe na het ontdekken van het lek. Sommige politiemensen moesten in de krant lezen dat hun gegevens op straat lagen. De Kamer en de media wisten het nieuws hierover soms eerder dan de mensen om wie het ging. Uit de praktijk hoor ik nu gelukkig dat die updates een stuk beter verlopen. Daarom complimenten dat dat goed wordt opgepakt. Wel vraag ik de Minister hoe dit nou in het vervolg beter kan gaan.
Voorzitter. Hoogstwaarschijnlijk is een statelijke actor verantwoordelijk voor deze hack, maar verder is er weinig informatie beschikbaar. De voor de hand liggende vraag is: is dit datalek onderdeel van een groter geheel, een digitale oorlogsvoering? Kan de Minister hier iets over zeggen? In de Kamerbrief staat dat de korpschef werd geïnformeerd door de AIVD en de MIVD, maar er is niet gedeeld hoe zij die hack op het spoor zijn gekomen. Kwamen ze die gegevens ergens tegen of hebben ze direct doorgehad dat het account was gehackt? Kan de Minister uitleggen hoe ze precies achter dit lek zijn gekomen en wanneer dit heeft plaatsgevonden?
Voorzitter. Dan het punt waar ik mij het meest over verbaas. De Minister zegt in de beantwoording van onze vragen erg stellig dat er geen veiligheidsrisico is voor onze agenten. Ik vraag mij af waar die stelligheid vandaan komt. Hoe kan een Minister zo goed weten dat een statelijke actor geen kwade bedoelingen heeft? En dat er nu geen risico is, betekent toch niet dat het risico er niet gaat komen? Is de Minister dat met mij eens? Gegevens van politiemensen zijn kostbaar en kwetsbaar. Er zijn partijen die veel geld overhebben voor deze informatie. Foto's en andere gegevens kunnen ook gebruikt worden voor bijvoorbeeld gezichtsherkenning. Het wordt makkelijk om bijvoorbeeld agenten te chanteren met activiteiten in hun vrije tijd. Al deze personen, maar liefst 62.000 mensen, kunnen misschien wel nooit meer worden ingezet als undercoveragent. Deze dienders hebben recht op het hele verhaal. Ik hoor dan ook graag welke risico's zich in de toekomst kunnen voordoen als gevolg van dit datalek, waaronder de risico's voor gezichtsherkenning, de risico's bij de inzet van nieuwe undercoveragenten en de risico's in de aanloop naar bijvoorbeeld de NAVO-top.
Voorzitter. De politie is hard aan het werk om haar digitale bewustzijn te vergroten. De eenheid Amsterdam werkt bijvoorbeeld aan een regionale

digitale vakdag. Zouden dit soort dagen niet veel meer overheidsbreed georganiseerd kunnen worden?
Voorzitter. Tot slot. Eén keer in de zoveel tijd laait deze discussie weer op. Sommige agenten zouden graag anoniem onder een nummer willen werken, in plaats van onder hun naam. Dat is best te begrijpen, want hoe makkelijk maken we het kwaadwillende criminelen die nog een appeltje te schillen hebben als de gegevens van een agent op straat liggen. In Engeland wordt momenteel al gewerkt met zo'n dienstnummer. Ik ben benieuwd of de Minister in Nederland deze mogelijkheid ook als optie ziet.

De **voorzitter**:
Ik dank u hartelijk voor uw bijdrage en ik geef het woord aan de heer Aardema.

De heer **Aardema** (PVV):
Dank u wel, voorzitter. Eind september werd de politie geconfronteerd met een hack, een inbraak in het systeem, waarbij gegevens over politiemensen werden buitgemaakt. Dat is op zich al opmerkelijk omdat je er als politieambtenaar op mag vertrouwen dat dergelijke gegevens veilig achter slot en grendel zitten. Dit had natuurlijk nooit mogen plaatsvinden. Mensen die ons land veilig moeten houden, mogen niet zelf het slachtoffer worden. Dat mag zeker niet als je een bijzondere functie hebt, bijvoorbeeld als je werkt onder een dekmantel of bij een observatieteam. Dan mag het niet zo zijn dat je gegevens zomaar worden buitgemaakt. Dat kan voor die functiecategorieën vergaande gevolgen hebben voor de werkzaamheden en de eigen veiligheid. Mijn vraag aan de Minister is dan ook of politiemensen echt in gevaar zijn geweest en wat de genomen maatregelen waren. Ik snap dat het lastig is om daarover in het openbaar uitspraken te doen. Als de Minister daar nu op antwoordt dat hij daar meer over kan zeggen, maar niet in het openbaar, dan ga ik via het procedureoverleg hierover een besloten gesprek aanvragen. Opmerkelijk is dat de hack al uitgebreid werd gecommuniceerd met de buitenwereld, terwijl de betreffende politiemensen pas drie dagen later via een mailtje werden geïnformeerd. Ik wil graag weten wat de overwegingen waren om hier zo lang mee te wachten.
In de jaarverslagen van de AIVD en MIVD werd al langer gewaarschuwd voor offensieve cyberactiviteiten. Wat is er met die signalen gedaan? Wat gaat er nu concreet gebeuren om dergelijke hacks in de toekomst te voorkomen? In de laatste brief van de Minister zegt hij dat er is gebleken dat er sprake was van een pass-the-cookieaanval. Als je even zoekt op internet, blijkt dat dit niet echt hogere krijgskunde is maar redelijk simpel te doen. Je kunt ook simpele tegenmaatregelen nemen, zoals een multifactorauthenticatie bij het inloggen. Dat zou toch heel gemakkelijk kunnen met de persoonlijk op naam uitgereikte diensttelefoons? Was deze er, en is dat nu beter geregeld? Er is ook een ISO 27001-certificering die de gaten kan dichten. Dat is een internationale standaard voor informatiebeveiliging. Is die er nu en was die er toen ook? Misschien kan de Minister daar nog wat meer over zeggen.
Ten slotte wil ik opmerken dat veiligheid voor de PVV topprioriteit heeft, niet alleen voor onze burgers, maar zeker ook voor onze politiemensen en andere hulpverleners.
Dank u wel.

De **voorzitter**:
U bedankt. Mevrouw Helder, aan u het woord.

Mevrouw **Helder** (BBB):
Dank u wel, voorzitter. «Op 26 september ben ik door de korpschef geïnformeerd dat een politieaccount is gehackt», aldus de Minister in zijn brief van 26 september jongstleden. Het gevolg is dat werkgerelateerde

contactgegevens van alle, alle politiemedewerkers zijn buitgemaakt. Dat een account gehackt kon worden, is al ernstig; daar kom ik dadelijk nog op terug. Wat ook ernstig is en wat BBB betreft ook verwijtbaar, is dat niet alle politiemedewerkers als eersten zijn geïnformeerd, maar de Minister en de media. Agenten moesten het nieuws via de media horen. Gedurende het proces bleek dat ook privégegevens zijn buitgemaakt, en ook e-mailadressen van een aantal ketenpartners. Tot zover het proces.
Voorzitter. Dan de inhoud. Een dergelijke hack met deze immense gevolgen had natuurlijk nooit mogen gebeuren. Ik ga ervan uit dat de Minister dat met BBB eens is. Voor de goede orde: ik mis die scherpe bewoordingen in de drie brieven die de Minister hierover naar de Kamer heeft gestuurd. Er is de afgelopen jaren veel geïnvesteerd in cybersecurity, dus de vraag hoe dit heeft kunnen gebeuren, is des te dringender. Anno 2024 kan het excuus echt niet meer zijn dat de knappe IT-koppen allemaal bij het bedrijfsleven zitten en niet bij de overheid. De vraag is dus: hebben de mensen aan de knoppen wel voldoende deskundigheid?
Voorzitter. Als de informatie die ik heb, juist is, zijn de ter zake verantwoordelijken wel degelijk gewaarschuwd en zijn er signalen geweest met als kern: waarom staan deze velden in Outlook open? Met andere woorden: die hadden dus dichtgezet moeten worden. Dan was deze hack niet mogelijk geweest. In ieder geval zouden de gevolgen niet zo groot zijn geweest. Is de Minister het met BBB eens dat de eindverantwoordelijke met IV of ICT – ik weet niet hoe de naam daar luidt – in zijn portefeuille aan een functie elders moet gaan denken? Het kan toch niet zo zijn dat het negeren van deze signalen met deze gevolgen zonder gevolg blijft en dat de korpschef hiervoor de klappen moet opvangen? Niet alleen alle politieagenten, maar ook de korpsleiding en de samenleving moeten erop kunnen vertrouwen dat een dergelijke situatie niet meer zal kunnen gebeuren. Daarom moeten ter zake deskundige personen aan de knoppen zitten en moet degene die eindverantwoordelijk is, vervangen worden.
Voorzitter. Ik verwijs naar een artikel in de NRC van 11 oktober jongstleden met de veelzeggende titel «Politiehack: als een stagiair of een vrijwilliger de schuld krijgt, is er echt iets mis met de IT». Een citaat uit dat artikel: «Een hack is zelden de schuld van een individuele medewerker, tenzij iemand bewust de boel saboteert. Belangrijker is: wie heeft bedacht dat het een goed idee is dat een politievrijwilliger bij het hele adresboek van alle medewerkers kan?» Ik zal echt niet beweren dat de eindverantwoordelijke dat een goed idee vond, maar wel dat duidelijke signalen hierover niet zijn opgevolgd. Dat is toch echt onacceptabel. Wat gaat de Minister op dat punt doen?
In de laatste brief, van 8 november jongstleden, schrijft de Minister dat de daders vermoedelijk gebruik hebben gemaakt van een zogenoemde pass-the-cookieaanval en dat het vrij zeker is dat er niet meer gegevens zijn gestolen dan nu bekend is. Ik heb begrepen dat dit een vrij standaard aanval is; de vorige spreker zei dit ook al. Ik heb echter twee vragen. Hoe lang heeft deze aanvaller zich opgehouden in het netwerk? Hoe weet men zo zeker dat er niet meer gegevens zijn gestolen? Ik sluit me aan bij de vorige woordvoerders en hun vragen over het gevaar voor met name agenten bij werken onder dekmantel, nu en in de toekomst.
Dank u wel.

De **voorzitter**:
U bedankt. Het woord is aan mevrouw Mutluer.

Mevrouw **Mutluer** (GroenLinks-PvdA):
U hoort heel veel eensgezindheid, voorzitter. Gegevens, tot aan privégegevens toe, worden door derden gekaapt. Alleen al dat is verschrikkelijk en al helemaal als het gaat om mensen in gevoelige functies, zoals politiemensen. Ik moet zeggen dat ik me ook kapot geschrokken ben van deze hack die onze politieorganisatie met ruim 62.000 medewerkers is

overkomen. Dat had nooit mogen gebeuren. Het maakt ons gewoon enorm kwetsbaar. Ik weet dat het onderzoek nog in volle gang is, maar uit de eerste berichten maken we al op dat het om een pass-the-cookieaanval zou gaan, waardoor de dader toegang kreeg tot in ieder geval de Outlookadressen van alle politiemensen en ook de privégegevens en extra contacten.
Ik hoop dat we zo snel mogelijk het antwoord op die vraag krijgen. Mijn eerste vraag is dan ook: wanneer kunnen we die verwachten? Was er sprake van een kwetsbaarheid in het systeem, een lek dat de politie nog niet kende, maar de dader wel, zodat hij deze kennis kon uitbuiten? Was de kwetsbaarheid wel al bekend en was de oplossing daarvoor, de patch, nog niet gedraaid? Zeker in dat laatste geval moet de politie sneller reageren op de door de softwareleverancier gemelde kwetsbaarheden.
Worden de systemen van de politie gemonitord op het stelen van session cookies? Hoe weet de Minister dat er naast de gegevens uit de lijst van adressen van Outlook geen andere adressen zijn buitgemaakt? Ik denk dat dat ook de grootste zorg was van menig politieagent. Want waarom zouden de hackers niet ook de mails van de politiemensen ingezien kunnen hebben en daaruit meer vertrouwelijke gegevens kunnen vissen?
Een nieuwe aanval moet voorkomen worden, ook al weet ik dat menselijke fouten nooit zijn uit te sluiten. Dat laat echter onverlet dat het systeem zelf zo veilig mogelijk moet zijn. We hebben eerder inspectierapporten gezien waarin werd gemeld dat de ICT van onze justitiële partners te wensen overliet. Het vraagt echt om versnelling en prioritering om dit zo snel mogelijk voor elkaar te krijgen. Ik doel dan ook op de wijze waarop onze justitiële partners met elkaar communiceren.
Voorzitter. Daarbij zou ik ook willen stellen dat er alarmbellen moeten afgaan als in één keer een enorme hoop persoonsgegevens van alle politiemensen wordt gekaapt. Daarom vraag ik de Minister ook of er wel monitoringstools waren die alarm konden slaan als er signalen werden gevonden die wezen op een veiligheidsprobleem? Waarom is het nodig dat politiemensen bij de persoonsgegevens van ál hun collega's kunnen? Kan dat inderdaad onder een nummer worden geschaard?
Voorzitter. Tot zover een beetje de technische kant van het probleem. Digitale onzorgvuldigheid van mensen kan een minstens zo groot risico zijn. Dat zien we overal om ons heen. Daarom vind ik het heel erg belangrijk dat onze politiemedewerkers ook op de gevaren worden gewezen. Zij moeten getraind worden om hiermee om te gaan. Daar wil ik graag een reactie op van de Minister. Ook wil ik dat de Minister ingaat op de kwetsbaarheden van andere schakels van de justitiële keten, zoals het Openbaar Ministerie, de rechters en ook het gevangeniswezen, dat gevoelige gegevens heeft over hoe en waar criminelen opgesloten zitten, die niet misbruikt mogen worden om ze te laten ontsnappen. Ik wil van de Minister weten of hij bereid is om de ICT van al deze justitiële partners door te lichten, zodat we kunnen kijken of daar zo snel mogelijk verbeteringen in moeten worden doorgevoerd.
Dan kom ik op de menselijke kant, namelijk die van de politiemedewerkers van wie privégegevens in verkeerde handen zijn gekomen. De communicatie liet echt te wensen over. Dat moet in de toekomst veel, veel en veel beter. Zijn er nu signalen dat hun gegevens door externen misbruikt worden? Wat is er gedaan om schade te voorkomen om deze mensen te beschermen? Hebben ze bijvoorbeeld nieuwe e-mailadressen en nieuwe telefoonnummers gekregen? Dat wil ik gewoon graag weten.
Voorzitter. Ik rond af. We krijgen bericht over de stand van zaken van het strafrechtelijk onderzoek naar de daders. Als je kijkt naar de rapportage van de AIVD en de MIVD, dan zie je dat er waarschijnlijk statelijke actoren zaten achter de hack. Dat vind ik heel erg zorgelijk, ook in het licht van de NAVO-top die er aankomt. Graag ook daar een reactie op, voor zover dat kan.

De **voorzitter**:
Dank u wel voor uw bijdrage. Dan de heer Six Dijkstra.

De heer **Six Dijkstra** (NSC):
Dank, voorzitter. Het is goed dat we dit debat met elkaar voeren. Een cyberaanval van vermoedelijk een statelijke actor op onze politie, waarbij de gegevens van politiemensen en ketenpartners op straat komen te liggen, heeft een grote impact op alle betrokkenen. Ik begrijp heel goed dat politiemedewerkers hier last van hebben. Ik zie ook het risico dat, als meer datalekken als dit plaats zouden vinden, dit ook de aangiftebereidheid van burgers zou kunnen schaden. De veiligheid van onze politiesystemen is in dat licht van het hoogste belang. Ik sluit me dan ook graag aan bij de zorgen die eerder gedeeld zijn door mijn voorgangers.
Ik heb een aantal verduidelijkende en inhoudelijke vragen over de informatie die de Minister heeft aangeleverd. Uit de kabinetsbrieven blijkt dat er een politieaccount is gehackt, maar het valt me in de brieven op dat er nog onzekerheid is over de initiële toegang. De toegang kan bijvoorbeeld door phishing komen, zegt de Minister, maar naar ik begrijp is daar nog geen uitsluitsel over. Verwacht de Minister hier later meer duidelijkheid over te krijgen of zijn de logbestanden daarvoor ontoereikend? Zijn de detectiecapaciteiten van de politie toereikend om de initiële toegang bij dergelijke aanvallen in principe vast te stellen? Waar en hoe kunnen deze capaciteiten nog versterkt worden? Heeft het NCSC in het kader van het Nationaal Detectie Netwerk hier bijvoorbeeld duidelijke standaarden voor. Zijn die in dit geval ook nageleefd?
Voorzitter. Na een succesvolle aanval kan malware worden geïnstalleerd voor exfiltratie van data, kunnen we lezen in de brief. Dat staat wederom beschreven als mogelijkheid en niet als zekerheid. Kan de Minister al bevestigen of dit daadwerkelijk is gebeurd? Zo ja, kan de Minister dan ook iets delen over de gebruikte malware? Is dat het type malware dat generiek en breed beschikbaar is of wijst de malware naar een specifieke actor of een specifiek land? Begrijp ik de Minister goed dat via malware session cookies zijn verzameld en geëxfiltreerd of bestaat ook de kans dat deze cookies op een andere wijze verkregen zijn? Kan de Minister delen of de aanvallers ook malware hebben geplaatst voor persistente toegang of laterale beweging binnen het netwerk? Is inmiddels zeker dat alle malware uit het systeem is of bestaat het risico dat de actor nog steeds toegang heeft? Wederom stel ik de vraag in welke hier sprake is van dekkend zicht. Zo nee, hoe komen we daar?
Waarschijnlijk was er sprake van een statelijke actor. Als het gaat om staatsgeheime informatie, dan begrijp ik dat de Minister niet zomaar alles kan delen, maar ik wil wel graag een dringend appel doen dat het, zodra dit kan, ook wel zinvol zou zijn om publiekelijk te attribueren. Bij een eerdere casus, de hack op een Defensiesysteem, heeft de regering Chinese actoren publiekelijk geattribueerd. Dat vond ik een krachtig signaal. Ziet de Minister mogelijkheden voor de uitbreiding van het beleid omtrent publieke attributie van cyberaanvallen? Zijn er duidelijke afspraken? Wie staat daar in Nederland voor aan de lat?
Tot slot wil ik het nog graag hebben over de vervolgstappen. Nu lijkt de omvang van de hack op basis van de aan de Kamer verstrekte informatie gelukkig beperkt te zijn tot de mailomgeving, maar de samenleving moet wel kunnen vertrouwen op de weerbaarheid van het politieapparaat. In dat kader wilde ik het onderwerp aanstippen dat eerder bij het mondelinge vragenuur aan de orde is geweest, namelijk de langetermijnopslag van politiegegevens ten behoeve van cold cases en PTSS-behandeling. De Minister gaat daarmee aan de slag. Er komt nieuwe wetgeving aan. Dat zullen we zeker aanmoedigen. De Autoriteit Persoonsgegevens heeft in de media echter al wel zorgen geuit over de manier waarop gegevens zeer lang worden opgeslagen. Als deze data door een hack op straat komen te liggen, kunnen de gevolgen daarvan desastreus zijn, zowel voor de

nabestaanden als voor de getuigen en voor de politiemensen zelf. Daarom vraag ik de Minister of hij bereid is om de AP om een nader te advies te vragen over de veiligheid van het regime waarmee informatie ten behoeve van cold cases voor zeer lange termijn opgeslagen is. Daarbij heb ik het dus niet over wat wettelijk mag, want we weten dat de wetgeving in gebreke is en er nieuwe in de maak is. Ik heb het dan concreet over de manier waarop de gegevens afgeschermd en toegankelijk zijn.
Voorzitter, dat was het van mijn kant. Dank u wel.

De **voorzitter**:
Dank u wel. U heeft nog een vraag van de heer Van Nispen.

De heer **Van Nispen** (SP):
Dan wordt dit toch nog een beetje een debat, misschien, al is dit meer een verhelderende vraag dan een scherpe politieke, zo realiseer ik mij. De heer Six Dijkstra doet eigenlijk een appel op de Minister om, zodra dat kan, bekend te maken om welke statelijke actor het gaat. Daar kan ik me van alles bij voorstellen. Ik heb daar echter nog over nagedacht. Ten eerste moet je dat dan wel heel zeker weten en kan het niet zomaar een verdenking zijn. Je moet het dus heel zeker weten. Ten tweede ga ik de heer Six Dijkstra toch ook de vraag stellen welke gevolgen hij daar dan aan verbindt. Ik kan me er van alles bij voorstellen. Je wilt het graag weten, maar wat doe je daar dan mee? Waarom vindt de heer Six Dijkstra dat zo belangrijk?

De heer **Six Dijkstra** (NSC):
Ik denk dat dit een terechte vraag is. Ik sluit me natuurlijk helemaal aan bij het standpunt van de heer Van Nispen dat je het wel zeker moet weten. Het moet meer zijn dan een aanleiding en daarom moeten we volgens mij heel terughoudend zijn met die stap. Ik vraag daarom niet aan de Minister om het nu kenbaar te maken, maar ik vraag wel wanneer dat kan, zeker omdat dit in het verleden ook heeft plaatsgevonden. Ik denk dat er meerdere signalen van uitgaan, ook een signaal richting de burger, namelijk dat we niet naïef moeten zijn over de intenties van bepaalde statelijke actoren. Verder draagt het ook bij aan de geloofwaardigheid van de informatie van de regering dat bepaalde landen een offensief cyberprogramma richting Nederland hebben. Andere landen doen dit veel proactiever. Een land als Amerika doet daadwerkelijk een aanklacht tegen een ander land. Ik weet niet of we zo ver moeten gaan, maar ik denk dat het wel een pad is om uit te lopen om te kijken wat de verschillende mogelijkheden zijn. In het kader van transparantie, zeker omdat het gaat over een strafrechtelijk onderzoek, denk ik dat het in sommige gevallen wel nuttig zou kunnen zijn.

De **voorzitter**:
Is dit voldoende, meneer Van Nispen? Ja. Dan heeft de heer Aardema ook nog een interruptie voor u.

De heer **Aardema** (PVV):
Ik heb een vraag in het vervolg hiervan. De wat-alsvraag is altijd lastig te beantwoorden, maar zou het misschien in een besloten deel plaats kunnen vinden, als we weten wie het is?

De heer **Six Dijkstra** (NSC):
Ik denk dat dat afhankelijk is van een aantal factoren waaronder waarschijnlijk de zekerheid van de verdenking. Het liefst gebeurt het natuurlijk zo openbaar mogelijk. Wat mij betreft doen we het openbaar als het openbaar kan. Maar ik kan mij voorstellen dat met enige mitsen en maren, die bij een onderzoek als dit beschikbaar zijn en waarbij sommige

dingen ook onzeker zullen blijven, er maatwerk geleverd moet worden, ook richting ons als Kamer.

De **voorzitter**:
Dank u wel. Dan is nu het woord aan de heer Van Nispen voor zijn inbreng.

De heer **Van Nispen** (SP):
Dank u wel, voorzitter. Er werd kort na het lek steeds meer duidelijk over dat datalek bij de politie: dat er veel gegevens zijn gestolen, zelfs privégegevens, dat er waarschijnlijk een ander land achter zit. Maar daarna werd het wat stiller. We weten ook nog heel veel niet: wat is precies de impact van deze datadiefstal, hoe kan die bijvoorbeeld tegen ons gebruikt worden? Zijn die analyses al gemaakt en wat kan er dan van gedeeld worden? Een van de zorgen is dat als hackers zicht hebben op mailinglijsten, er mogelijk ook zaken te zien zijn als welke agenten onderzoek doen naar een bepaalde criminele organisatie, welke politiemensen belast zijn met de beveiliging van een bedreigde politicus of rechter en wie er deel uitmaken van het Team Internationale Misdrijven. De Minister schreef dat de werkgerelateerde gegevens van undercoveragenten afgeschermd zijn. Die gegevens zijn dus niet buitgemaakt, maar de gegevens van alle andere politiemedewerkers wel. Dat maakt de vraag die ik net stelde volgens mij wel een gerechtvaardigde vraag. Ik hoop dus dat daar antwoord op kan komen.
Wat precies de gevolgen van het datalek zijn voor de agenten en de organisatie is nog niet helemaal duidelijk. Wat wel duidelijk is, is dat de politie erdoor in het hart getroffen is, in het hart van de organisatie en van al die mensen die dag in, dag uit zorgen voor onze veiligheid. Zij zijn nu zelf het slachtoffer, met alle onzekerheid van dien. Dat doet natuurlijk iets met die mensen; verschillende sprekers hebben daar terecht al op gewezen. Het is heel belangrijk dat we agenten en ook hun families duidelijkheid en veiligheid bieden. Welke maatregelen worden er getroffen om de agenten te beveiligen of te beschermen, en hoe wordt beoordeeld of dat nodig is?
Ik sluit mij aan bij de vraag die mevrouw Van der Werf ook al stelde over het werken onder nummer als wens vaker mogelijk te maken. Want nu er namen en gegevens naar buiten zijn gegaan, is er nog meer zorg dat daders naam en achternaam lezen in het proces-verbaal. Dat maakt die wens begrijpelijk. Ik ben benieuwd naar de reactie van de Minister hierop.
Wat ten slotte ook nog niet duidelijk is wat ons betreft – het is een open deur – is hoe ervoor wordt gezorgd dat het hierbij blijft, dus eens maar nooit weer. Ik vrees dat de Minister dat niet kan beloven, hoe graag hij dat ook zou willen. Maar het zou natuurlijk eigenlijk wel moeten. Deskundigen zeggen ook dat de aandacht voor en urgentie van cyberbeveiliging veel hoger zou moeten. Worden er passende maatregelen getroffen om de politie en andere diensten ook digitaal beter te beveiligen? Hoe wordt dataopslag veiliggesteld? Wordt de datahuishouding doorgelicht en geanalyseerd op kwetsbaarheden, ook richting de NAVO-top straks? Kortom, welke lessen worden hiervan geleerd en wordt hier wel voldoende in geïnvesteerd?
Voorzitter. Ten slotte een wat ongemakkelijke vraag: als dit zelfs bij de politie kan gebeuren, waar dan allemaal nog meer?
Dank u wel.

De **voorzitter**:
U bedankt. Dan is tot slot het woord aan mevrouw Michon-Derkzen.

Mevrouw **Michon-Derkzen** (VVD):
Voorzitter. Het is juist de politie die dag in, dag uit voor onze veiligheid zorgt. Deze mannen en vrouwen waren slachtoffer van een datalek

waardoor niet alleen hun werkgerelateerde informatie maar soms zelfs ook hun privégegevens op straat kwamen te liggen. Hierdoor hebben zij maar ook hun naasten, hun familie, direct last van hun werk. We moeten dus met alles wat we in ons hebben zien te voorkomen dat zij risico lopen. We moeten ervoor zorgen dat zij hun werk veilig kunnen doen.
Ik heb dus heel veel begrip voor de bezorgdheid en de verwarring bij al die politiemedewerkers. De eerste reactie van de korpsleiding vond ik absoluut onder de maat. Collega's hebben dit hier al gezegd en ik sluit mij daarbij aan. Ik hoop dat de Minister er ook een reflectie op kan geven. Als klap op de vuurpijl kwam daar de politievrijwilliger bij, die werd neergezet als degene die iets verkeerd zou hebben gedaan. Ook dat vind ik echt ongepast. Het feit dat je dit dus kán doen, wie er dan ook achter de computer zat, is natuurlijk al een gotspe en zou niet moeten kunnen en mogen.
Criminelen en andere kwaadwillenden kunnen met dit soort gegevens aan de haal. Is het niet nu dan misschien, morgen, of volgende maand of over een halfjaar. Het risico op doxing en op bedreiging neemt toe, zeker in teams die met zware criminaliteit te maken hebben. Graag een reactie hierop. Hoe staat de korpsleiding al deze mensen ook nu, vandaag de dag nog bij? Heeft het datalek ook implicaties voor lopende onderzoeken en wat doen we daaraan?
Het gaat in mijn optiek ook over de mate waarin de politie haar eigen ICT-systeem heeft beveiligd; dat hoorden we ook eerder. Natuurlijk zit er een deel geautomatiseerde beveiliging in, maar er zit altijd een menselijke kant aan. Hoe werken die samen en hoe zorgen we ervoor dat we het optimaal veilig houden? Juist deze hack laat weer zien dat we de vitale infrastructuur – ik vind ook onze politie-ICT vitale infrastructuur – moeten beschermen tegen allerlei dreigingen. Die opgave wordt natuurlijk steeds complexer en die dreiging wordt steeds intenser, maar de impact wordt ook steeds groter. Ik hoor graag van de Minister hoe we nu en in de toekomst bestand zijn tegen gerichte aanvallen op het politiesysteem, niet in de laatste plaats omdat we juist de ICT bij de politie zo hard nodig hebben om efficiënt en effectief te kunnen optreden. Er is juist heel veel meer ICT nodig om ervoor te zorgen dat de politieagent op straat direct kan optreden. Graag een reactie van de Minister hoe het nu staat met de innovatieve kant van de ICT-ontwikkeling en met, waar we het ook heel vaak in de Kamer over hebben gehad, de basis op orde qua ICT van de politie. Kunnen zij op een voldoende manier met elkaar werken?
Voorzitter, dank u wel.

De **voorzitter**:
U bedankt. U heeft nog een interruptie van mevrouw Mutluer.

Mevrouw **Mutluer** (GroenLinks-PvdA):
Toen wij als rapporteurs de parlementaire verkenning deden naar de vastgelopen strafrechtketen, was een van de conclusies die we trokken dat de ICT niet goed was bij onze justitiële partners, dat ze daarin achterlopen en dat daar enorm in moet worden geïnvesteerd. Is mijn collega het met mij eens – ik noemde het ook in mijn eigen bijdrage – dat het belangrijk is om opnieuw met het OM, de politie en de rechtspraak te kijken waar de kwetsbaarheden zitten? Ik noem dat dan doorlichting; we kunnen het anders noemen. Staat mijn collega daar ook welwillend tegenover? We weten ook dat ICT-projecten heel lang kunnen duren.

Mevrouw **Michon-Derkzen** (VVD):
Dank aan mevrouw Mutluer voor haar vraag. In mijn optiek is zelfs de ICT bij de politie nog niet eens op orde, laat staan dat de ICT-systemen in de strafrechtketen met elkaar kunnen werken en op elkaar zijn aangepast. Ik vrees dat we nog heel ver weg zijn van een goedwerkend ICT-systeem voor de strafrechtketen. Het zou goed zijn om in dit debat een reactie van

de Minister daarop te horen. We steken wel enorm veel geld in de ICT politie. Ik vind het overigens niet te veel geld. ICT is de basis van politiezorg, dus ik zou zeggen: geef aan wat nodig is en dan hebben we hier de discussie erover of we dat er ook voor vrijmaken. Ik heb eerder gezegd dat er nog steeds 13% van het totale budget naar ICT gaat. Ik heb geen idee of dat niet een beetje omhoog zou moeten, omdat het een veel meer ICT-gedreven organisatie wordt. Maar ik zou vooral willen dat de politie het zichzelf minder moeilijk maakt – laat ik het zo zeggen – en ervoor zorgt dat de basis aan ICT op orde is, opdat dat het begin is om beter te kunnen samenwerken in de strafrechtketen.

Mevrouw **Mutluer** (GroenLinks-PvdA):
Ik hoor mijn collega zeggen dat we in beeld moeten brengen waar de politie maar denk ik ook het OM en de rechtspraak tegen aanlopen. Als we dat in beeld hebben, moeten we prioriteren en daar voldoende in investeren om ze voor de korte termijn zo hackproof mogelijk te maken en voor de langere termijn de basis veel meer op orde te hebben. Ik ben daar zelf een groot voorstander van en hoor mijn collega hetzelfde zeggen. Ik ben dus ook benieuwd naar de antwoorden van de Minister op dat vlak.

De **voorzitter**:
Nog een reactie van mevrouw Michon-Derkzen? Is het voldoende zo?

Mevrouw **Michon-Derkzen** (VVD):
Ik denk dat het goed is dat de Minister in dit debat een toelichting geeft op de stand van zaken ICT politie. Ik ben het ermee eens dat wij de vinger aan de pols moeten houden, maar volgens mij doen we dat hier ook in de reguliere commissiedebatten over de politie.

De **voorzitter**:
Goed. Dan zijn we daarmee aan het einde van de eerste termijn van de Kamer. Ik kijk naar de Minister hoelang hij... U kunt gelijk door? Helemaal goed. Dan is het woord aan de Minister voor zijn beantwoording in eerste termijn.

Minister **Van Weel**:
Dank, voorzitter. Ik ga in één keer door, omdat ik boven op dit onderwerp zit. Ik laat me daar regelmatig over informeren sinds 26 september. Daarom zijn de vragen die u heeft gesteld voor mij geen verrassing. Dat zijn de vragen die ik mezelf ook heb gesteld en waarop ik dus antwoorden heb gekregen. Ik zal die hier zo goed als mogelijk geven. Daarbij maak ik één disclaimer. Er zijn ook zaken die ik hier niet kan zeggen omdat onderzoeken nog lopen of omdat het karakter van de informatie zich niet verhoudt tot het openbare karakter van deze meeting. Wanneer dat zo is, zal ik dat eerlijk aangeven. Dan weet u in ieder geval waarom ik daar geen antwoord op kan geven.
Deze episode begon voor mij met een telefoontje, laat op 26 september, van de korpschef. Als de korpschef belt na negen uur 's avonds, dan is dat meestal geen goed nieuws, en dat was het nu ook niet. Ik ken deze telefoontjes wel. Ik was bij de NAVO verantwoordelijk voor cybersecurity en was dus ook degene die als eindverantwoordelijke werd gebeld, als er ergens in de organisatie sprake was van een hack of een lek. Dat zijn hele vervelende telefoontjes, want je weet dat het meteen impact heeft op mensen en op een organisatie. En je weet in zo'n eerste telefoontje niet wat de impact is. Hoe groot is dit? Komen we ervan af? Komen we erachter of we ervan afkomen? Hoe zijn we erachter gekomen? Het begint altijd met duizenden vragen en nog heel weinig antwoorden. Tegelijkertijd voel je meteen de druk dat dit naar buiten moet. Je kunt mensen niet verrassen hiermee. Het gaat over informatie, mogelijk persoonsgegevens.

Je weet nog niet tot welke diepte, maar je hebt een verplichting om je personeel in te lichten over dit soort zaken.
Dat alles heeft geleid tot het briefje en de communicatie die u een dag later, dus op 27 september, heeft gekregen en die de medewerkers toen ook hebben gekregen. Dat is dus niet via de media gegaan. Tegen diegenen die zeggen dat sommige agenten of vele agenten dat wel via de media hebben moeten lezen, zeg ik dat het begon met een bericht op het intranet. Ik zit ook niet permanent op het intranet, dus de kans was groot geweest dat ik het ook via de media had gelezen en niet op het intranet. Dat is iets waar we lering uit kunnen trekken. Er is later ook meer gerichte communicatie geweest aan medewerkers, onder andere via de e-mail, om ze daar nadrukkelijker op te wijzen.
Wat zet je dan in de eerste communicatie? Altijd minder dan je zou willen, gewoon omdat je nog niet precies weet wat de omvang van het lek is. De eerste communicatie bevatte alleen informatie die we op dat moment hadden; daarom heeft u nog twee of drie aanvullende stukken gekregen. Het nadeel daarvan is dat je weet dat het een open einde bevat, dat je weet dat mensen op basis van de informatie die je dan kunt geven geen volledige zekerheid hebben over: wat is er nu buitgemaakt, wat is er nu weg? Dat creëert onrust in de organisatie. Dat is een afweging die je dan maakt als eindverantwoordelijke tussen de verplichting om je personeel en de Autoriteit Persoonsgegevens te informeren over een hack en als gevolg van een hack een lek en de zekerheid die je kunt geven over: wat is nu de impact op mijn veiligheid? Alle begrip voor de onrust die dat in de organisatie heeft opgeleverd.
Ik ben wel blij dat ik kan constateren dat we in de weken die daarna volgden uiteindelijk meer zekerheid hebben gekregen over de omvang van de gelekte data. Het is geen gegeven bij een hack, zeg ik u, dat je die informatie nog zo goed terug kunt halen, maar in dit geval hebben we wel enige mate van zekerheid kunnen krijgen over welke informatie is verdwenen.
Een aantal zaken moeten meteen gebeuren en wel nog voordat je naar buiten gaat. Eén. Weten we zeker dat dit...

De **voorzitter**:
U had nog een interruptie van mevrouw Mutluer.

Mevrouw **Mutluer** (GroenLinks-PvdA):
Het ging met name om de communicatie. Ik vond zelf dat de communicatie te wensen overliet. Er werd pas een paar dagen later een meldpunt in het leven geroepen waar politieagenten zich konden melden. We hoorden van bijvoorbeeld criminologen die met politieagenten samenwerken dat zij niks hadden gehoord en dat hun gegevens ook in die systemen staan, en eventueel een aantal officieren van justitie. We kunnen het nu niet terugdraaien, maar stel dat een calamiteit als deze zich weer zou voordoen. Dan moeten de protocollen en de communicatiestrategie richting je mensen toch al klaar zijn, zodat je dit soort onrust zo veel als mogelijk kunt beperken? Ik vind echt dat dat een gemiste kans is geweest.

De **voorzitter**:
Hartelijk dank. En voor de duidelijkheid: we hebben de schorsing overgeslagen, dus ik zou graag vier interrupties aan de leden willen gunnen. Dan weet u dat u dat kunt doen. De Minister.

Minister **Van Weel**:
Ik vertelde over de communicatie dat je een afweging maakt tussen hoe volledig je kunt zijn op dat moment en de plicht die je voelt om je medewerkers te informeren. In dit geval hebben we ervoor gekozen om de medewerkers te informeren de dag nadat ik werd geïnformeerd door de korpschef. Dat kon omdat we wisten dat het lek inmiddels was gedicht.

Als dat niet zo is, dan moet je nog heel erg oppassen met communiceren naar je medewerkers of naar buiten. Je kan iemand die dan nog in je systeem zit juist de gelegenheid bieden om grote hoeveelheden data weg te trekken voordat je «m uit het systeem hebt. Dat is één. Ik ga niet communiceren op het moment dat dat lek er nog is, maar we wisten nu dat dat niet het geval was.
Twee. Je probeert medewerkers dan zo gericht mogelijk te vertellen wat er aan de hand is. Wij wisten in die eerste dagen wel dat het te maken had met het Outlookadressenbestand, maar de volledige omvang daarvan was nog niet duidelijk. Toch hebben we ervoor gekozen om ermee naar buiten te gaan. U vraagt: had dat dan niet beter gekund richting ketenpartners et cetera? Dat is informatie die in de dagen daarna langzaam naar boven kwam. Toen kwamen we erachter dat in dat Outlookadressenbestand ook mailinglisten zaten en dat er in die mailinglisten ook e-mailadressen voorkwamen van externe ketenpartners. Langzaam vervolmaakte dat beeld zich dus. Dat geldt ook voor privégegevens. In eerste instantie dachten we bij Outlook niet aan privégegevens, maar wat bleek? Er waren wel degelijk mensen geweest die zelf in Outlook een privénummer of een profielfoto hadden toegevoegd. U zult hier in de Tweede Kamer ook mensen hebben die dat hebben gedaan.
De ongemakkelijkheid dat je communiceert en weet dat je niet volledig bent, voelde ik dus vanaf het begin. Die voel ik ook met u mee. Ik heb wel de afweging gemaakt om het op deze manier te doen, om in ieder geval niet achteraf verweten te kunnen worden dat we de medewerkers niet tijdig in staat hebben gesteld om kennis te nemen van de betreffende data. Dat heeft zeker onrust met zich meegebracht. Had dat meldpunt eerder in het leven geroepen kunnen worden? Dat is een les die we zeker meenemen voor een volgende keer, net als het idee om in plaats van iets te plaatsen op intranet, wellicht een e-mail te sturen naar het hele bestand, zodat mensen eerder en persoonlijk op de hoogte worden gesteld. Zo leren we continu van dit soort afhandelingen.

De **voorzitter**:
De heer Aardema had eerst nog een vervolgvraag.

De heer **Aardema** (PVV):
De Minister schetst nu een heel mooi tijdpad van wanneer hij dingen heeft gehoord en gedaan. Volgens mij zitten er enkele dagen tussen, tenminste voordat de algemene mail naar alle medewerkers ging. Dat was pas op zaterdagmiddag om iets over tweeën, meen ik. Heeft de Minister in de dagen meteen nadat hij het te weten kwam, bijzondere maatregelen genomen ten voor bijzondere diensten binnen de politie?

Minister **Van Weel**:
Zeker. Op basis van de informatie die er was, zeg ik daar wel bij. We hebben natuurlijk elke keer gekeken welke informatie er weg was en wat we moesten doen. Je gaat daarbij uit van het ergste scenario. We wisten wel vrij snel dat het beperkt was gebleven tot de Outlookomgeving. Dan ga je dus kijken welke informatie daar dan te vinden is. Een van de eerste vragen die natuurlijk extern maar ook bij ons intern speelde, was: hoe zit het met mensen die werken onder een dekmantel? Dat is de meest kwetsbare groep. Ik moet eerlijk zeggen dat ik al hoopte dat die niet onder een naam in het systeem zouden staan. Dat bleek gelukkig ook niet het geval te zijn. Daarmee was dus het acute gevaar voor die operaties geweken.
Ten tweede hebben we gekeken wat je als statelijke actor met deze informatie ... Ik bedoel als actor, want we wisten natuurlijk nog niet dat het een statelijke actor was. Wat zou je als actor nou met die informatie kunnen doen? Wat brengt die informatie? Dan ga je nadenken: als je namen en e-mailadressen hebt, is het dus eenvoudiger geworden om

bijvoorbeeld een hele gerichte phishingmail te sturen. Je kunt je dan immers voordoen als iemand anders van wie je het e-mailadres en de functie hebt. Als ik aan u een e-mail stuur die lijkt te komen van David van Weel terwijl ik dat niet ben, bent u eerder geneigd om daarop in te gaan dan op een mail van iemand anders. Vandaar dat een van de eerste maatregelen die we hebben getroffen, is dat we iedereen erop wijzen dat het risico op phishing mogelijk is toegenomen doordat deze informatie in verkeerde handen is gevallen. Zo hebben we elke keer gekeken wat de aard van de informatie die weg was, betekent voor het mogelijke risico dat mensen lopen.
Daar kwam vervolgens de vraag vandaan, van velen van u, over de fysieke veiligheid. Waarom hebben we die nou ingeschat als laag? Dat is omdat er uiteindelijk geen privéadressen of Facebookpagina's met foto's van familieleden et cetera buitgemaakt zijn. Dat soort informatie, die echt wijst naar de privéomgeving van een agent, is hiermee niet buitgemaakt. Het betreft informatie die je ook hier in de Tweede Kamer kunt vinden op een visitekaartje in Outlook. Dat geeft niet onmiddellijk aanleiding voor een dreiging voor de fysieke veiligheid van agenten. Vandaar dat we dat risico lager hebben ingeschat, in combinatie met het feit dat we op een gegeven moment met vrij grote zekerheid wisten dat het een statelijke actor betrof en geen criminele. Ook dan speelt mee wat waarschijnlijk de intentie geweest is van het vergaren van informatie. Die intentie is waarschijnlijk geweest om grotere toegang te krijgen via deze eerste hack.

De **voorzitter**:
Dank u wel. Mevrouw Michon-Derkzen heeft eerst nog een interruptie.

Mevrouw **Michon-Derkzen** (VVD):
Ik kan de Minister goed volgen, maar ik begrijp hem niet. De toon waarop gezegd wordt «het was nu via intranet en volgende keer zou het beter kunnen» vind ik niet oké. Ik zou heel erg denken dat op dit soort kwesties is geoefend, dat het in draaiboeken zit en dat we vooraf met elkaar hebben afgesproken hoe je ervoor zorgt dat iedereen zo snel mogelijk op de hoogte is en hoe je ervoor zorgt dat risico's geminimaliseerd worden. Ik snap dat je van elk incident leert, maar nu lijkt het alsof we eigenlijk door dit incident procedures gaan aanscherpen of wellicht gaan maken. Dat kan toch niet de bedoeling zijn? Ik zou verwachten dat we in alarmfase 1 zitten als er zoiets gebeurt, wat een direct risico is voor het werk van een agent, en dat we daar zo alert op zijn dat je de kans minimaliseert op de fouten die na de hack en het lek in deze communicatie zijn gemaakt. Mag ik daar een reflectie op van de Minister?

Minister **Van Weel**:
Elke hack, elk lek, is anders, zo ook deze. Het feit dat met deze gerichte hack alle medewerkers van de politie werden geraakt, is vrij ongekend. Er zijn heel veel hacks en datalekken, bij heel veel organisaties. Daar zijn ook draaiboeken voor. Bij een vrij gericht lek van informatie krijg je daar gewoon een standaard informerend bericht over. U heeft hem ongetwijfeld ook weleens gehad van bol.com of andere bedrijven. Dit lek raakte alle politiemedewerkers. In het begin was ook nog niet helemaal duidelijk op welke wijze zij werden geraakt. Dat maakte dit uniek. We hebben daarin keuzes gemaakt, waarbij een aantal makkelijk via het draaiboek zijn af te werken, namelijk het dichten van het lek en het nemen van digitale maatregelen om te voorkomen dat het nog een keer zo gaat plaatsvinden. Die technische kant staat helemaal vast in draaiboeken om het systeem zo snel mogelijk weer veilig te maken. De personele kant was hier uniek. Daar hebben we zeker van geleerd. Hoe bereik je nu 62.000 mensen op zo'n manier dat er geen paniek uitbreekt, maar dat er wel urgentie doorklinkt? Hoe geef je handelingsperspectief aan mensen?

Mevrouw **Michon-Derkzen** (VVD):
Waarom kwam het bericht op intranet, als men op donderdagavond of vrijdagochtend wist dat het iedereen betrof? Er hebben ongetwijfeld ook mensen naar gekeken in de uren dat andere mensen sliepen. Waarom kwam er pas zaterdagmiddag een mail? Waarom ging dan pas zondag de helpdesk open? Daar zit toch geen enkel begin van urgentie in? Gelukkig is er niets gebeurd, maar als de hack nou echt gericht was op het schaden van individuele agenten en je als agent even met andere dingen bezig was, dan had je tot maandag niet geweten wat er aan de hand was. Dat vind ik echt heel zorgelijk. Ik begrijp dat de Minister zegt dat dit uniek is, maar dit en ook de risico's van al die cyberaanvallen wetende – ik hoor de Minister daar ook vaak over en hij heeft de urgentie daarvan op zijn netvlies staan – moeten we toch als de wiedeweerga aan de gang om een sneller en beter handelingsperspectief richting personeel op te zetten?

Minister **Van Weel**:
Ik heb hier al gezegd dat het bericht op intranet wat mij betreft volgende keer gewoon een directe mail aan iedereen is. Dat hebben we hiervan geleerd. Hadden we dat van tevoren kunnen bedenken? Mogelijk. Ik had graag gewild dat er iemand was geweest in het crisisteam waarin we zaten die had gezegd: misschien moeten we gewoon een directe mail sturen aan iedereen. Dan hadden we dat gedaan. Daar was natuurlijk niks op tegen. Nu hebben we dat reactief gedaan, omdat we erachter kwamen dat intranet te vrijblijvend was. Daarom is er zaterdag meteen ter correctie een mail uitgegaan naar alle medewerkers en is in reactie op de vraag «waar moet ik dan heen?» op zondag de helpdesk ingesteld. Men vond namelijk dat men via de eigen lijn niet snel genoeg informatie verkreeg, wat aanvankelijk wél het idee was. Ik denk dus dat er elke keer gereageerd is. Hadden we dit allemaal in één keer beter willen doen? Heel graag! Hebben hiervan geleerd? Zeker! Zouden we het een volgende keer, die hopelijk nooit meer komt, anders doen? Absoluut!

De **voorzitter**:
Dank u wel. Voldoende zo? Mevrouw Van der Werf heeft nog een vraag.

Mevrouw **Van der Werf** (D66):
Ja, voorzitter, omdat ik echt verbaasd ben over de antwoorden van de Minister. Hij geeft aan dat hij vanuit zijn eerdere functie en positie ervaring heeft met dit soort hacks. Dan begrijp ik echt niet waarom de Minister zich geen zorgen maakt over de gegevens die nu gestolen zijn. Ik weet niet of u het boek Het is oorlog maar niemand die het ziet van Huib Modderkolk kent, maar daarin gaat het veelvuldig over het verrijken van datasets door inlichtingendiensten. Dan gaat het dus niet alleen maar om blokjes data, maar gaat het erom een compleet beeld te krijgen van mensen in bepaalde landen. Een statelijke actor maakt dus per definitie helemaal niet minder kwetsbaar dan een groep criminelen. Ik begrijp dus niet dat de Minister dat aangeeft.
Wat ik ook niet goed begrijp, is het volgende. Het gaat niet om de Facebookpagina van mensen; het gaat erom dat de identiteit van bijna al onze politiemensen nu in handen is van een statelijke actor die het de moeite waard vond om deze gegevens van ons te stelen. Ik zou dus wel van de Minister een ietwat minder optimistische afdronk willen horen dan dat dit in de toekomst niets voor de veiligheid van deze mensen zou betekenen. Want die opmerking begrijp ik echt niet.

Minister **Van Weel**:
Ik snap de vragen van mevrouw Van der Werf. Maar ik denk dat het juist mijn kennis en mijn ervaring zijn en wat ik op dit moment weet van deze hack waardoor ik ook een werkgeversverantwoordelijkheid heb om mensen niet onnodig ongerust te maken. Als ik aanleiding had om

ongeruster te zijn dan ik nu overkom, zou ik die ongerustheid ook uiten. Ik ben hier helemaal niet om zaken te downplayen of om ze mooier te laten lijken for the sake of it. Ik probeer het echte verhaal neer te zetten. Wat ik u vertel, is het echte verhaal, op basis van de risicoanalyses die we hebben gemaakt op basis van de informatie waarvan we weten dat die weg is en het risico dat mensen daar mogelijk door lopen. En zoals ik al zei, achten wij het risico voor de fysieke veiligheid klein. Dat is ons oordeel. Dat is niet om het mooier te laten lijken; dat is het professionele oordeel dat wij aan deze hack geven.

Mevrouw **Van der Werf** (D66):
Met het risico dat dit een ingewikkeld debat wordt, want ik kan mij voorstellen dat de Minister op dit punt niet het achterste van zijn tong kan laten zien, waar ik alle begrip voor heb, toch nog een vraag. Ook al zou de Minister aanleiding hebben om te zeggen dat het op dit moment geen gevaar betekent, die gegevens zijn wel weg. Die zouden in combinatie met andere gegevens, die online vindbaar zijn, of die al in het bezit zijn van die statelijke actor wel voor een gevaarlijke situatie kunnen zorgen in de toekomst. Deze mensen hebben niet in een keer een andere naam of andere basisgegevens dan die nu buit zijn gemaakt. Als die gegevens niet de moeite waard zouden zijn, begrijp ik sowieso niet waarom ze dan gestolen zijn, maar dat terzijde. Kan de Minister hier niet iets meer over vertellen, waardoor hij de Kamer geruststelt dat dit niets voor de veiligheid van deze mensen betekent?

Minister **Van Weel**:
Voor zover ik dat kan doen, ga ik proberen om dat te doen. Ten eerste. Ja, we gaan ervan uit dat deze informatie in handen is van deze statelijke actor, maar zoals we ook aangeven in de Kamerbrief in antwoord op vragen van u, monitoren wij erg goed of de informatie daar ook blijft. Wij speuren dus continu op alle plekken waar we denken dat dat zou kunnen, of deze informatie ergens opduikt. Want natuurlijk zou dat op dat moment wel kunnen leiden tot een andere risico-inschatting. Tot op heden – ik heb dit vandaag nog met de korpschef besproken – is die informatie nog nergens aangetroffen, waardoor wij ervan uitgaan dat die nog in handen is van de statelijke actor.
Als we kijken naar de intentie van de statelijke actor, is het vermoeden, kijkend naar de modus operandi van dit soort statelijke actoren, dat het hier gaat om informatievergaring en dus niet om het direct lastigvallen van individuen in de organisatie. Daar komt dat idee vandaan.
Als u mij vraagt – maar dan ga ik deels speculeren – waarom men dan zo'n adreslijst pakt: precies om wat ik zojuist zei, het is een fantastische gelegenheid om op basis van die informatie te proberen om veel gerichter zo'n organisatie binnen te komen. Daarom zagen we ook echt als het grootste risico dat specifiek met phishing, doordat men zich voordoet als collega, de informatie verrijkt kon worden op basis van deze gegevens. Daarom hebben we dat ook als het hoogste risico aangemerkt en daar ook maatregelen tegen genomen, door mensen alert te maken en de cyberbeveiliging nog verder op te schroeven om er zo beter zicht op te hebben.
Als je kijkt naar de informatie die is buitgemaakt, dan zie je dat het niet gaat om politiedata. Dat hoorde ik wel in een paar vragen. Het gaat niet om onderzoeksdata. Het gaat niet om data uit strafrechtelijke processen. Die zijn echt op een andere manier beveiligd. Het gaat hier echt om de Outlookadreslijst. Niet alleen in de politieorganisatie, maar in de meeste organisaties is die vrij makkelijk toegankelijk. Waarom? Omdat je met elkaar moet kunnen communiceren. Dat zeg ik ook tegen de mensen die vroegen waarom elke medewerker toegang heeft tot die gegevens. Dat is omdat je in de organisatie waar je werkt, mensen wilt kunnen opzoeken. Dat kun je hier in de Tweede Kamer ook doen. Als ik de heer Aardema wil

mailen, en ik weet zijn e-mailadres niet, dan typ ik «aa» in in Outlook en dan ben ik blij dat de heer Aardema daarin opduikt. Als ik wil weten of het de goede is, omdat er vier Aardema's staan, dan klik ik met mijn rechtermuisknop en ga ik naar properties. Dan zie ik dat de heer Aardema, Tweede Kamerlid voor de PVV, de goede is. Zo voorkom je dus ook dat er communicatie in verkeerde handen komt. Deze informatie is geen hooggerubriceerde informatie en is echt wat anders dan politie-informatie. Dat wil ik hier toch nog een keer markeren.
Naar aanleiding hiervan heeft de politie gekeken naar het schonen van die informatie om te voorkomen dat daar onnodig privéinformatie bij zit en om te voorkomen dat er onnodig foto's in staan. Voor sommige mensen is een foto deel van hun werk. Als wijkagent wil je niet onder een nummer bekend staan, maar juist als Jan de wijkagent, want je wilt dat mensen je herkennen en je weten te bereiken. Maar als je in een wat meer afgeschermde omgeving werkt, dan is dat natuurlijk heel anders.
Enkelen vroegen hoe het zit met werken onder nummer en vroegen of we dat ook kunnen uitbreiden. In het hoofdlijnenakkoord staat dat we gaan kijken hoe we dat kunnen uitbreiden, zeker in de strafrechtelijke onderzoeken. Het OM gaat bepalen waar ruimte ligt om dit voor mensen mogelijk te maken, om te voorkomen dat ze privé worden aangesproken op het werk dat ze in alle neutraliteit doen.

De **voorzitter**:
Mevrouw Van der Werf, had u nog een vervolgvraag?

Mevrouw **Van der Werf** (D66):
Politieagent zijn is gewoon een gevoelig beroep. Ik begrijp het punt dat de Minister maakt over die Outlooklijst wel, maar dit is wel wat anders dan de Outlooklijst van de Albert Heijn. Volgens mij zit daar precies de gevoeligheid. Dat maakt die informatie interessant. Ook al zitten mensen niet meteen in een functie waarbij de operatie in gevaar komt, dan wil dat niet zeggen dat het niet buitengewoon interessant is om te weten welke 62.000 Nederlanders bij de politie werken. Ik denk dat heel veel landen en partijen dat zouden willen weten. Dat maakt dat die informatie ook geld waard is. De Minister suggereert hier net dat wij erbovenop zitten en zouden kunnen zien wanneer die informatie verschuift of beweegt. Ik denk dat we nooit weten wat we niet weten of niet kunnen zien. Misschien is die informatie inmiddels wel bij een derde partij terechtgekomen die daar belangstelling voor heeft of wiens dataset daarmee verrijkt zou kunnen worden. Ik wil de Minister dus toch nog een keer vragen hoe hij de veiligheid van mensen kan garanderen, ook als zij in de toekomst bij de politie met iets aan de slag willen, waardoor het gevoelig is dat zij daar werken.

Minister **Van Weel**:
Even kijken hoe ik deze vraag op een goede manier beantwoord. We kijken op een bepaalde manier – ik kan niet zeggen op welke manieren, maar op internet – of deze informatie ergens beschikbaar komt. Je zou je kunnen voorstellen dat er marktplaatsen zijn waar je dit soort informatie kunt verkopen. Criminelen of statelijke actoren kunnen elkaar daar vinden om dit soort data aan elkaar te verkopen, of het nou gaat om data die bij Albert Heijn, bij Bol.com of anderszins is buitgemaakt. Datahacks en datalekken zijn aan de orde van de dag in onze maatschappij en daar is gewoon een business voor.
De politie weet waar dit soort marktplaatsen, deze zwarte markten, zijn. Dus die hangt daar ook rond, net als we op echte zwarte markten proberen present te zijn en kijken naar de contrabande die daar rondgaat. Op die manier en op andere manieren proberen we daar zicht op te houden en op de vraag of deze data ergens opduiken. En als dat zo is, wat gaan we daar dan mee doen en wat zijn de risico's? Ik kan dus geen

garanties geven dat die data nergens opduiken, maar ik hoop wel dat we er zicht op hebben op het moment dat dit zou gebeuren. Het is overigens de vraag of dit het doel van een statelijke actor zou zijn. Ik kan dat niet honderd procent uitsluiten. Het zou niet de meest logische stap zijn, maar ik zou ze ook zeker niet op ideeën willen brengen door het debat dat we hier nu hebben. Dat is één.
Twee is de aard van de data en wat dit betekent voor de veiligheid van mensen. De data vertellen inderdaad welke namen er werken bij de politie. Dat kan gevoelig zijn; daar wil ik absoluut niet voor weglopen. Tegelijkertijd is er ook niet méér informatie te vinden dan dat iemand werkt bij de politie en mogelijk op welke plek in de politie. Wat je daarmee zou kunnen doen, is die informatie gebruiken om een verder beeld van iemand op te bouwen, als je dat zou willen. Dat is het risico dat agenten sowieso lopen, ook als ze op straat lopen met hun naamkaartje en gefilmd worden.
In deze wereld, waarin met facial recognition mensen gevonden worden en waarin socialmedia-accounts worden gecombineerd, is dit in algemene zin een uitdaging voor agenten. Ik merk dat ook. U noemde zelf al de wens om te werken onder nummer. Mensen die in de frontlinie staan en gefilmd worden bij al het werk dat ze doen, moeten al enorm uitkijken met hoe ze verder digitaal, online, vindbaar zijn, omdat er mensen zijn die hen willen benaderen. Daar zou ook deze informatie aan kunnen bijdragen als die in handen van de verkeerde mensen valt. Dat risico zie ik dus zeker.

De **voorzitter**:
Dit is uw laatste interruptie, mevrouw Van der Werf.

Mevrouw **Van der Werf** (D66):
Dat is zeer spijtig, maar volgens mij is dit wel de kern van waar het debat over gaat. Ik ga die laatste mogelijkheid dus toch gebruiken. De Minister zegt net dat er altijd een risico voor agenten is dat hun identiteit bekend wordt, maar dat is natuurlijk iets heel anders dan dat een statelijke actor nu hun gegevens van ons heeft gestolen. Dat is natuurlijk iets heel anders dan dat ze zomaar op straat lopen en altijd het risico lopen dat iemand hun naam vindt. Ik vind het dus wel echt kwalijk dat de Minister dit zo bagatelliseert, want dat is hoe ik dat hoor.
Ik vind het ook interessant dat de Minister op 3 oktober aangaf dat het veiligheidsrisico werd ingeschat als «heel gering» en dat hij net zei dat hij natuurlijk geen garanties kan geven dat die statelijke actor er niets mee doet. Dat lijkt mij het eerlijke verhaal, want die garanties hebben we natuurlijk helemaal niet. Die statelijke actor is ook niet gek. Natuurlijk gaat die niet op de zwarte marktplaats zitten waarvan hij weet dat onze inlichtingendiensten daar gaan checken of zij de gegevens doorverkopen. Wij weten natuurlijk niet wat daarmee gebeurt op het moment dat zij die gegevens toch op een andere manier gaan gebruiken.
De Minister kan ook helemaal niet garanderen dat dit in de toekomst niet gebeurt. Dus wat is zijn boodschap aan de 62.000 politiemensen om wie dit gaat? Wat zouden zij met deze wetenschap moeten doen en wat gaat de Minister eraan doen om ons hiervan goed op de hoogte te houden? Want het eerder door hem geschetste veiligheidsrisico is in mijn ogen gewoon niet realistisch.

Minister **Van Weel**:
Mijn appreciatie verandert niet. Het zou vreemd zijn als ik daar nu in één keer een andere inschatting van zou hebben. Ik acht de kans dus nog steeds zeer gering dat er uiteindelijk een fysiek veiligheidsrisico ontstaat voor agenten op basis van de informatie die hier gestolen is en door wie die is gestolen. Dat is het geheel. Het enige wat ik nu probeer te doen in het debat met u, is afpellen.

Eén. Hoe zit het met die actor, wat is daar het risico en welke mitigerende maatregelen hebben we daar om eventueel zicht te krijgen op waar die informatie heen gaat? Een ander deel van de puzzel is: als die informatie in handen is van mensen die kwaad zouden willen, wat zouden zij dan met die informatie kunnen doen? Zo kwamen we op het construct. Ik pel het dus zover af als ik kan om inzicht te geven: als er risico's zouden zijn, wat zouden die dan zijn? De overallconclusie blijft dezelfde. Daarmee bagatelliseer ik helemaal niks.
Ik vind het ontzettend vervelend dat deze informatie is buitgemaakt en ik zou willen dat we dit debat niet hadden gehad, maar dat is niet de realiteit. Maar daarbinnen ga ik mensen ook niet onnodig ongerust maken alsof ze nu op hun thuisadres in één keer ongewenst bezoek kunnen verwachten op basis van deze hack. Ze lopen dus een zeer gering risico op hun veiligheid. Dat zeg ik dus wel in deze brief en dat herhaal ik in dit debat.

De heer **Aardema** (PVV):
Mevrouw Van der Werf schetst de ernst van de hack op het gebied van Outlook. Kan de Minister mij garanderen dat er geen doorstap is gemaakt naar de salarisadministratie, waarbij waarschijnlijk wel privéadressen kunnen worden buitgemaakt, of naar SUMMIT, waarin rechercheprocessen staan, weliswaar geschot maar toch. Kan de Minister garanderen dat dat niet het geval is?

Minister **Van Weel**:
Dat kan ik met aan zekerheid grenzende waarschijnlijkheid doen. Dat zeg ik u omdat we een redelijk zicht hebben kunnen krijgen op de exfiltratie van data. Zonder al te technisch te worden: je kunt in loggegevens wel zien wat er over netwerken heen gaat. Wij weten dus vrijwel zeker dat dit is wat er weg is. En met «dit» bedoel ik dus de hele global address list en alles wat daaraan hangt. Het zijn dus geen andere systemen, zoals de politiedata zelf of salarisadministratiesystemen.

Mevrouw **Helder** (BBB):
De Minister heeft heel in het begin van zijn beantwoording gezegd: we monitoren of buitgemaakte gegevens ergens opduiken. Dat blijkt tot op heden niet het geval te zijn. Hoelang blijven we dat dan monitoren? Ik zou bijna zeggen: permanent. Dan regeert de Minister dus wel een beetje over zijn graf heen. Dat is natuurlijk heel flauw om te zeggen want de Minister zit er net, maar we moeten dit natuurlijk wel blijven monitoren.

Minister **Van Weel**:
Ja, absoluut. Overigens zijn dit plekken die de politie sowieso graag monitort, maar waar zij nu natuurlijk extra alerts op heeft gezet waar het gaat om deze informatie. Regeer ik daarmee over mijn graf heen? Ja, maar dat doe ik met de volle zekerheid dat wie er ook na mij komt, dat niet anders zal willen. Uiteindelijk gaat dit immers om de veiligheid van de medewerkers. We willen daar dus gewoon zicht op houden.

Mevrouw **Helder** (BBB):
Dan nog een andere vraag, die ook voortkomt uit een antwoord van de Minister. Hij had het over de personele kant, en hij zei dat van 62.000 agenten de gegevens in één keer buitgemaakt zijn. Dat willen we dus gaan voorkomen. Ik heb ook gevraagd waarom al deze velden in Outlook openstaan. Een van de antwoorden van de Minister was: nou goed, dan doen we het misschien niet meer via intranet maar via een directe mail aan iedereen. Nou ben ik jurist en geen ICT-deskundige, maar als je met één mail iedereen bereikt, betekent dat dan niet dat die velden nog steeds openstaan? Dat is dan weliswaar vanuit de andere kant, vanuit de organisatie zelf, maar dat is dan toch ook niet handig?

Minister **Van Weel**:
In de tijd dat ik bij Defensie werkte, had je in de global address list nog een all user account. Ongeveer één keer in het jaar was er iemand die grappig dacht te zijn bij zijn afscheid of zijn pensioen, en in dat account zei: nou, tot ziens. En dan waren er altijd weer een paar duizend mensen die daaroverheen dan weer grappig wilden antwoorden. Die mogelijkheden kennen de meeste bedrijven al niet meer. Je kunt als werkgever dus wel separatie aanbrengen terwijl je daarachter toch één bestand hebt waar het allemaal in staat. Daardoor kun je dus wel individuen zoeken, maar kun je alleen als dat moet, bijvoorbeeld als ik dat als Minister zou willen, een mail naar de hele organisatie sturen. Niet iedere medewerker kan meteen iedereen met één e-mail bereiken.
Dan de velden die openstonden. Dat ging dus met name over het kunnen invullen van die privéinformatie. We zijn er dus achter gekomen dat dat niet wenselijk is en dat je dus als werkgever verantwoordelijkheid wil nemen in welke informatie mensen daadwerkelijk kunnen toevoegen aan zakelijke Outlookadressen. Dat bedoelde ik met het opschonen van dat bestand, om te voorkomen dat mensen extra kwetsbaar zijn vanwege de informatie die daarin staat.

Mevrouw **Helder** (BBB):
Dat leidt dan bijna tot de vraag: dan zit het lek toch ook daar? Die vraag plopte tegelijkertijd bij mij en bij de heer Aardema op. Misschien stel ik die dus mede namens hem. Het zit dan dus niet bij de vrijwilliger.

Minister **Van Weel**:
Waar het lek zit ... Ik wijs hier helemaal niemand aan als schuldige en het onderzoek loopt nog, maar er is via een device toegang verkregen via de beruchte pass-the-cookiemethode. Wat betekent dat? We klikken allemaal meerdere malen per dag op cookieverzoeken, die je nu eenmaal krijgt. Ik klik dan meestal op «ik ga akkoord», vrees ik. Die cookies hebben een bepaalde geldigheidsduur. Als jij dus binnen tien minuten op dezelfde website terugkomt, hoe je niet opnieuw «ik ga akkoord» aan te klikken. Van die geldigheidsduur kun je dus gebruikmaken op het moment dat je zo'n bestand weet te krijgen, om in dit geval dus toegang te krijgen tot Outlook en daarmee die address list te krijgen. Dat is de manier waarop het gegaan is. Dat kan via phishing zijn gebeurd. Dat kan ook op andere manieren gebeurd zijn. Het kan dus zo zijn dat er geklikt is door een medewerker. Het kan ook op een andere manier gebeurd zijn. Dat onderzoek loopt nog. Daar kan ik nu verder nog niks over vertellen. Dat komt hopelijk als dat onderzoek is afgerond.

De **voorzitter**:
Voldoende zo, mevrouw Helder?

De heer **Six Dijkstra** (NSC):
Misschien komt de Minister er nog op terug, maar ik ben benieuwd naar het volgende. In zijn brief benoemt hij expliciet phishing, waarbij hij zegt dat het dat niet hoeft te zijn, maar dat het een manier kan zijn. Ik kan nog wel twintig andere manieren verzinnen; het kan ook malware zijn. Waarom heeft hij in zijn bewoordingen zo'n specifiek scenario uitgewerkt terwijl er nog veel onzeker is?

Minister **Van Weel**:
Omdat het vanaf het begin wel daarop lijkt. Nogmaals, omdat het onderzoek nog loopt, kan ik er nog niet conclusief over zijn, maar dat is de reden dat het is opgenomen in die beantwoording en die brief.

De **voorzitter**:

Duidelijk zo? Zijn er op dit moment nog vragen van de leden op dit punt? Nee. Gaat u dan vooral verder met uw beantwoording.

Minister **Van Weel**:
Dan waren er een aantal vragen over de statelijke actor. Er werd gezegd dat diensten hier al vaker op hebben gewezen. Hebben we daar dan niet eerder maatregelen op kunnen nemen? Hoe gaan we om met de attributie van deze statelijke actor? Het is absoluut bekend dat de AIVD en de MIVD maar ook andere organisaties al langer waarschuwen voor de dreiging die uitgaat van statelijke actoren wat betreft cyberaanvallen. Zoals ik zei, heb ik er ook in mijn tijd bij de NAVO vele van meegemaakt. Er zijn een toenemend aantal statelijke actoren, zou ik willen zeggen, bezig toegang te verkrijgen tot onze systemen. Dan gaat het niet alleen om politiesystemen of Defensiesystemen, maar ook om vitale infrastructuur en toegang verkrijgen tot de telecomsector en tot drinkwatervoorzieningen. De voorbeelden zoals ze naar buiten zijn gekomen, zijn er te over. Dat dreigingsbeeld staat dus, en daar moeten we ons tot verhouden. Op basis van dat algemene dreigingsbeeld zijn er maatregelen genomen en monitoren de diensten delen van ons netwerk.
Uiteindelijk zijn het de diensten geweest die de politie hebben kunnen alerteren op deze hack. Het goede nieuws is dus dat die hack gedetecteerd is. Het slechte nieuws is dat er wel gehackt is en informatie is buitgemaakt. Zodra daar meer helderheid over was, is die informatie via het NCSC doorgegeven aan hun doelgroepen om te voorkomen dat anderen op dezelfde manier door deze actor zouden kunnen worden gehackt. In algemene zin, los van deze hack, gaat het erom dat je als verantwoordelijke voor cybersecurity het feit dat een organisatie gehackt wordt uit de schaamte haalt. Door heel snel te acteren en snel bekendheid te kunnen geven over hoe dat gebeurd is, help je namelijk te voorkomen dat anderen kunnen worden gehackt. Je maakt het een actor moeilijk door zo snel mogelijk zijn modus operandi te verspreiden en iedereen zich te laten wapenen. Ik denk dat we dat alleen maar meer moeten gaan doen naarmate de dreiging toeneemt.
Op dit moment loopt het strafrechtelijk onderzoek naar de dader nog. Hangende dat onderzoek zal er geen attributie worden gedaan. Dat onderzoek zal dus eerst worden voltooid, maar wij denken wel degelijk na over publieke attributie. We moeten alleen kijken – dat doen wij op een case-by-casebasis, ook in het geval van de Chinese hack – wanneer dat opportuun is, wie we meenemen in deze attributie, wat het betekent voor de informatiepositie van de diensten et cetera. Dat wegen we allemaal mee in de afweging omtrent wanneer we ermee naar buiten gaan en op welke manier. Ik geloof in publieke attributie, omdat het niet alleen voor die landen – die weten wel wat ze gedaan hebben – maar ook voor onze eigen bevolkingen heel erg inzichtelijk maakt wat hier gebeurt en wie dat doet.

De **voorzitter**:
Er is een vraag van de heer Six Dijkstra.

De heer **Six Dijkstra** (NSC):
Het is mooi dat de Minister dat onderschrijft. Ik had nog één vraag over het vorige punt. Ik snap dat de Minister niet bij alles in detail kan treden, maar hij zei in ieder geval dat er monitoring plaatsvindt op delen van het netwerk. Eerder gaf hij aan: uit exfiltratie hebben wij kunnen opmaken dat er niet meer gedeeld is dan enkel dat adresboek. Uit de bewoording «delen van het netwerk» maak ik op dat er vast ook delen van het netwerk zullen zijn waar dat niet zo is. Kan de Minister zoals hij eerder aangaf met aan zekerheid grenzende waarschijnlijkheid te kunnen zeggen dat het niet zo is, zeggen dat het niet mogelijk is dat er delen van het politienetwerk bestaan waarlangs een statelijke actor een separaat exfiltratiekanaal heeft,

waar dan andere gevoelige data gedeeld kan worden? Kan hij ons dat comfort bieden?

Minister **Van Weel**:
Dat is een vraag met een hoop lagen erin. Zonder al te technisch te willen worden, wil ik het volgende zeggen. De informatie waar nu toegang toe is verkregen, is de laagdrempeligste informatie die binnen de politieorganisatie beschikbaar is. Het betreft namelijk de Outlookinformatie waartoe iedereen die een e-mailadres van de politie heeft, uiteindelijk toegang heeft. Daar is de beveiligingsdrempel lager en zitten er minder lagen tussen dan als je daadwerkelijk in de politiedatabases zou willen komen. In die zin is het wel logisch dat als je dan een hack vindt, dat op deze plek gebeurt, omdat dat nu eenmaal de plek van de minste weerstand is. Desondanks is het ook daar opgemerkt. We hebben achteraf construerend dus kunnen zien welke data zijn verdwenen en waarheen. Dat laatste kan altijd met terugwerkende kracht, want je kunt gewoon je logs teruglezen, als dat niet te lang geleden is, om te kijken wat voor data eroverheen gegaan is. Op dat detecteren kan ik niet al te diep ingaan, maar daar zitten onze diensten wel bovenop.

De **voorzitter**:
Ja. Helder zo. Gaat u dan vooral verder met uw beantwoording.

Minister **Van Weel**:
Tegen mevrouw Mutluer zeg ik dus ook dat dit niet te maken had met patching, maar meer met de wijze van toegang verkrijgen. Daarom hebben we ook zo snel mogelijk daarna die informatie gedeeld met andere diensten, om te voorkomen dat anderen daar ook slachtoffer van zouden kunnen worden.
Geldt die kwetsbaarheid dan ook voor andere overheidsdiensten? Nou, ik hoop dus niet meer, niet van deze actor en niet op deze manier. In algemene zin zijn we, denk ik, allemaal kwetsbaar voor hacks. Er zijn een hoop dingen die we kunnen doen om dat makkelijker te maken. Patching is daar een van. Het is belangrijk dat organisaties dat gewoon meteen doen bij elke software-update. Een tweede ding dat helpt, is logging, dus back-ups maken van je systemen. We hebben het nu bijvoorbeeld wel kunnen zien. We hebben met honderd procent zekerheid kunnen zeggen: het lek is dicht. Maar er zijn ook hacks waarbij je niet weet hoe diep de hacker zit. Dan rest je uiteindelijk niets anders dan je hele systeem opnieuw opbouwen. Als je dan een back-up hebt van 24 uur geleden, dan kun je vrij snel je operatie hervatten. Heb je die niet en moet je een jaar terug, dan kun je je voorstellen dat het bij een organisatie als de politie of het OM enorme impact heeft. Dat is dus nog iets wat je kunt doen.
De heer Aardema noemde al de multifactor authentication. De politie heeft ook daarnaar gekeken en in een aantal gevallen de policy daarop aangescherpt, dus dat je wel multifactorauthenticatie nodig hebt. Ik heb mij ook weleens laten bezoeken door hackers die gingen kijken of ze mijn passwords konden raden. Dat is in alle gevallen gelukt. Dus ook op dat vlak maak ik hier toch maar weer van de gelegenheid gebruik om, via u, voorzitter, tegen iedereen te zeggen: de naam van je kinderen, hun geboortejaren, de eerste letters van iedereen in de familie en je huwelijksdag; het is allemaal vrij eenvoudig te achterhalen, dus werk echt met goede passwords.

De **voorzitter**:
Mevrouw Mutluer, had u nog een interruptie?

Mevrouw **Mutluer** (GroenLinks-PvdA):
Ja, juist omdat de Minister een aantal maatregelen noemt. Wellicht ga ik hiermee weer terug naar de eerste discussie, over het beschermen van

onze politiemensen. Want ik ben het met u eens: het is gewoon een gegeven dat die 62.000 gegevens ergens liggen. We kunnen het niet tot het einde der jaren blijven monitoren. Die moeten ergens opduiken voordat we er daadwerkelijk acties op kunnen ondernemen. Ik hoor de Minister met een aantal maatregelen komen die de risico's dat onze agenten in een onveilige situatie kunnen komen, kunnen verminderen. Volgens mij kunnen we daar allerlei beelden bij hebben en scenario's over uittekenen. De concrete vraag die ik heb, is de volgende. Ik weet niet of de Minister daarop kan antwoorden, maar wordt er ook verder nagedacht? Ik noemde zelf als voorbeeld andere e-mailadressen en andere nummers. Over dat werken onder nummer heeft de Minister al wat antwoorden gegeven. Ze gaan dat uitbreiden. Daar ben ik een groot voorstander van. Welke concrete acties worden er, naast de acties die zojuist door de Minister zijn genoemd, genomen om die risico's zo veel mogelijk te beperken?

Minister **Van Weel**:
Dat is een hele heldere vraag. Deels kan ik daar antwoord op geven en deels doe ik dat niet, ook omdat de maatregelen die wij nemen, inzicht bieden voor diegenen die kwaad willen met die informatie. Dan heb ik het over wat wij ertegen hebben gedaan. Daarin wil ik hen natuurlijk niet wijzer maken. Ik noemde al de awarenessmaatregelen. We hebben mensen ervan bewust gemaakt dat ze juist op dit moment alert moeten zijn op e-mails van «collega's» van anderen, die mogelijk dus niet van collega's zijn. Daarbij is de boodschap dus ook: klik niet op links op het moment dat je twijfelt. Dat is in het algemeen een hele goede tip voor ons allemaal, maar die is nu natuurlijk des te belangrijker.
Ik vertelde al dat er gekeken is naar het opschonen van de Outlookinformatie. Er is dus echt bekeken welke informatie daarin moet zitten, welke informatie daar niet in moet zitten en hoe we ervoor kunnen zorgen dat daarmee het risico op een lek van bijvoorbeeld privéinformatie zo klein mogelijk is. Er zijn een aantal monitoringsmaatregelen ingesteld – daar ga ik hier niet al te diep op in – om vast te kunnen stellen wat er gebeurt op onze netwerken. Ik noemde al de tweefactorauthenticatie. Ik kan u ook zeggen dat deze maatregelen allemaal zijn genomen binnen de politieorganisatie, onder andere in consultatie met het NCSC. Er wordt op dit moment ook nog gevalideerd door een derde partij of we hiermee echt alle maatregelen hebben genomen die zij kunnen bedenken. Dus op die manier is de politieorganisatie hiermee omgegaan.

De **voorzitter**:
Dank. Dat is voldoende voor nu. Continueert u.

Minister **Van Weel**:
Voorzitter. Ik zit even te kijken welke vragen ik nog heb openstaan. De heer Six Dijkstra vroeg naar de coldcase-informatie. Hij vroeg of de AP daar nader onderzoek naar moet doen. Nogmaals, in dit geval is er geen toegang geweest tot politiedata, tot politiesystemen zelf. Dat geldt ook voor de data die gebruikt worden voor cold cases. Daar zit een poortwachtersfunctie op – dat heb ik ook in het vragenuur met uw Kamer gewisseld – die gewoon met menselijke interventie bepaalt wie toegang mag krijgen tot die data. Daarbij is een hack dus niet eens mogelijk. Daar zit gewoon een persoon tussen, die bepaalt of iemand een bepaalde navraag mag doen in die data. We weten dat de Autoriteit Persoonsgegevens zich al heeft uitgelaten over het bewaren van deze informatie. Dat gaat dus niet over de wijze waarop, maar over het bewaren an sich. We zijn inderdaad bezig met nadere wetgeving, die hopelijk snel naar de Raad van State gaat, om die lacune te dichten.
Voorzitter. Ik denk dat ik daarmee de meeste vragen heb beantwoord, maar ik zie er nog een paar openstaan.

De **voorzitter**:
Ik maak even een ronde langs de velden om de onbeantwoorde vragen bij de leden op te halen. Allereerst mevrouw Van der Werf.

Mevrouw **Van der Werf** (D66):
Wat betreft de langetermijnrisico's heb ik de Minister gevraagd om specifiek in te gaan op de risico's voor gezichtsherkenning, de inzet van nieuwe undercoveragenten die misschien uit deze groep zouden komen en de risico's in aanloop naar de NAVO-top.

De **voorzitter**:
Dank u wel. Ik haal ze allemaal even op. De heer Aardema. Nee? Mevrouw Helder.

Mevrouw **Helder** (BBB):
Ik heb de Minister gevraagd: hebben de mensen aan de knoppen wel voldoende deskundigheid? Dat zeg ik met alle respect. Ik ben zelf geen deskundige, maar ik zit daar dan ook niet. Ik had ook gevraagd: wie heeft bedacht dat het een goed idee is dat een politievrijwilliger bij het adressenboek van medewerkers kan? Duidelijke signalen hierover zijn blijkbaar niet opgevolgd. Dat vind ik wel een hele belangrijke vraag. Daar wil ik graag een antwoord op. En ik had ook gevraagd: hoelang heeft deze aanvaller zich opgehouden in het netwerk?

Mevrouw **Mutluer** (GroenLinks-PvdA):
Ik vraag de Minister graag om nog even in te gaan op de vragen over de NAVO-top. Ik had zelf nog een onbeantwoorde vraag – die is wellicht deels beantwoord – over de inspectie. Die heeft eerder aangegeven dat de ICT bij de justitiële partners niet op orde is en dat dat prioritering en investering behoeft. Ik hoop dat we nog meer wakker zijn geworden door die politiehack. Welke acties mogen we ook van deze Minister op dat vlak verwachten, zodat we de basis op orde kunnen krijgen?

De heer **Six Dijkstra** (NSC):
Ik denk dat mijn vragen beantwoord zijn, voor zover de Minister die kon beantwoorden, omdat hij op sommige dingen natuurlijk wat terughoudend is. Op zijn laatste punt had ik nog wel een vervolgvraag. Dan gebruik ik even een interruptie, met uw toestemming, voorzitter. Dat gaat om de coldcase-informatie. Begrijp ik de Minister goed dat het echt gaat om een fysieke persoon? Ik bedoel dat die systemen niet digitaal met elkaar verbonden zijn, maar dat er altijd iemand tussen moet zitten? Kan hij garanderen dat het niet via het internet toegankelijk is?

De **voorzitter**:
Dan beantwoorden we die even met de rest, als u dat goedvindt. De heer Van Nispen. Niet? Mevrouw Michon-Derkzen.

Mevrouw **Michon-Derkzen** (VVD):
Ik had nog gevraagd naar de stand van de huidige ICT binnen de politie en naar innovatieve ontwikkelingen binnen de ICT, die zo hard nodig zijn.

De **voorzitter**:
Dank u wel. Het woord is aan de Minister voor de onbeantwoorde vragen.

Minister **Van Weel**:
Ja. Excuses dat ik die niet allemaal heb meegenomen in mijn eerste beantwoording. Dat krijg je als je je ambtenarenapparaat buitenspel zet en spontaan doorgaat.
De risico's. Laat ik beginnen met de NAVO-top, want daar is door een tweetal van u naar gevraagd. Wij zijn absoluut alert op wat wij kunnen

gaan meemaken, niet alleen tijdens de NAVO-top, maar ook in de aanloop daarnaartoe. We weten dat er op dit moment al sprake is van hybride aanvallen en cyberaanvallen op alle NAVO-lidstaten. We hebben vorige week nog de kabelbreuk gehad tussen Duitsland en Finland, waarover we de conclusies nog te weten moeten komen. Maar het duidt wel op hybride aanvallen. Zo kan ik nog wel twintig voorbeelden noemen van het afgelopen jaar in Europese landen.
Het feit dat de NAVO-top naar Nederland komt, gaat ons meer in het vizier brengen, vermoedelijk voornamelijk bij Rusland. Daar moeten we dus op voorbereid zijn, niet alleen in de fysieke wereld, maar ook in het digitale domein. Daar bereiden we ons dus ook op voor. Wat dat betreft is deze hack dus ook een heel goede wake-upcall, zeg ik tegen degenen die dat noemden, om te zorgen dat we daar volop op voorbereid zijn. We nemen ook extra maatregelen in het licht van de NAVO-top, maar daar kan ik in dit gremium dan weer geen uitspraken over doen.
De risico's op gezichtsherkenning. Als u dat in algemene zin vraagt, denk ik dat dat een enorme uitdaging wordt voor de toekomst, niet alleen voor politieagenten. Het gaat grote impact hebben op velen van ons, het feit dat je met vrij eenvoudige software en grote scans van grote datasets mensen kunt matchen en daardoor een extra biometrische laag aanboort die ineens voor iedereen beschikbaar is. Het gaat ook dingen oplossen. Zoals met alle technologie zal het voor het goede worden gebruikt en voor het slechte. Dus we zullen cold cases oplossen op basis van gezichtsherkenningstechnologie. Mensen zullen lang verloren familieleden terugvinden door middel van deze technologie, omdat je door heel grote datasets met mensen heen kunt gaan. Maar we gaan ook krijgen dat mensen die niet gevonden willen worden, om goede redenen of omdat ze in een getuigenbeschermingsregeling zitten of zo, ook risico lopen dat ze door deze technologie ergens opduiken via een vakantiefoto van iemand. Datzelfde geldt voor agenten.
U kunt zich voorstellen dat alle eisen die nu worden gesteld aan biometrie en paspoorten al een uitdaging zijn voor inlichtingendiensten als het gaat om het proberen om mensen onder een andere identiteit te laten rondlopen. Dus de goede dingen die deze technologieën brengen, brengen ook een uitdaging voor het werk dat we doen. Ik denk dat dat ook zo zal zijn voor mensen die undercover werken. Dus we moeten er goed over nadenken hoe we dat mitigeren en welke wettelijke beperkingen we willen opleggen aan het gebruik van die technologieën. Dat geldt voor artificial intelligence – daarbij zijn we al een stap verder, denk ik, met de Europese AI Act – maar ook zeker voor gezichtsherkenning. Als het gaat om deze specifieke data, betreft het overwegend emailadressen en functiebenamingen. Maar wat betreft diegenen die een profielfoto erin hadden zitten: dat is fotomateriaal, dus in die zin zou je daar wat mee kunnen als het gaat om gezichtsherkenning.
Is er voldoende deskundigheid bij de politieorganisatie, vroeg mevrouw Helder. Ik denk het wel. Dat baseer ik op mijn ervaringen tussen het ondervinden en onderkennen van de hack en de maatregelen die er genomen zijn. Ik denk dat de grootste lessen die ik voor mezelf hieruit trek, gaan over de communicatie richting de medewerkers en hoe we dat doen. Dat kan ik de deskundigen niet aanrekenen. Ik zou niet willen zeggen dat dat überhaupt niet in hun competentieprofiel hoort, maar het is uiteindelijk natuurlijk aan de korpsleiding en aan mij om die communicatie op een goede manier te doen. Maar als ik kijk naar de mitigerende maatregelen die zijn genomen na het ondervinden van de hack – dat zie ik dan maar als de deskundigen die daar zitten – dan denk ik dat dat op een goede manier is gebeurd. Het geeft mij in ieder geval vertrouwen.

De **voorzitter**:
Er is toch nog een vervolgvraag van mevrouw Helder.

Mevrouw **Helder** (BBB):
Dat is aan de achterkant, maar mijn vraag ging erover dat het aan de voorkant überhaupt niet had mogen gebeuren. Daar vloeide de vraag ook uit voort, juist vanwege het feit dat mij ter ore is gekomen dat er wel degelijk voor gewaarschuwd is dat die velden openstonden met deze mogelijke, grote gevolgen. Dan stel ik volgens mij terecht de vraag. Als de betreffende verantwoordelijken gewaarschuwd zijn en blijkbaar niet voldoende geacteerd hebben – laat ik het voorzichtig zeggen – dan kun je de hack wel onderkennen ... Misschien is dat zelfs door andere mensen gedaan en ik vind het fijn dat het onderkend is en er maatregelen genomen zijn. Maar als er gewaarschuwd is, is er dus gezien dat er dingen openstonden, wat niet had gemogen. Dáár had op geacteerd moeten worden. Dan blijft mijn vraag dus nog steeds overeind.

Minister **Van Weel**:
Met het gevaar dat ik ernaast zit omdat ik niet de waarschuwingen heb ontvangen die u heeft ontvangen: ik denk dat met de openstaande velden werd gedoeld op het feit dat je zelf inhoudelijk je visitekaartje kon aanpassen, dus dat dat de openstaande velden waren. Dat heeft ertoe geleid dat mensen privéinformatie hebben toegevoegd, waarvan we nu hebben gezegd: dat moet je dus niet willen. Dat is dus opgeschort. Dat is niet de oorzaak van de hack geweest. Die is niet gekomen doordat die informatie kon worden toegevoegd. Er is echt via een andere weg toegang verkregen tot het systeem, waarmee uiteindelijk die informatie is buitgemaakt. Ik denk dat het zo zit, maar als het anders zit, hoor ik het graag. Dan gaan we erachteraan.

De **voorzitter**:
U bent door uw interrupties heen, mevrouw Helder, tenzij het heel belangrijk is om het nog te verduidelijken. Kort.

Mevrouw **Helder** (BBB):
Dan kort, voorzitter. Ik heb van de Minister onder andere begrepen dat er is binnengekomen via «pass the cookie wall», doordat iemand privégegevens heeft ingevuld. Dat zeg ik als verduidelijking.

Minister **Van Weel**:
Nee. Dat strookt niet met mijn beeld over hoe de hack is ontstaan.

De **voorzitter**:
Goed. Dan hebben we dat zo uit de wereld geholpen.

Minister **Van Weel**:
Dan de vraag naar de inspectie, justitiële partners en de stand van de ICT. Die discussie moeten we zeker voeren. Die moeten we overigens rijksbreed voeren. Daar hebben we ook het overleg Digitale Zaken over, onder andere. Daar moeten we periodiek op terugkomen, wat mij betreft ook in de commissiedebatten Politie. Maar het staat voor mij wel los van de cybersecurityhoek, die te maken heeft met hoe deze hack heeft kunnen ontstaan.
In algemene zin – dan beantwoord ik ook meteen de vraag van mevrouw Michon – gaan we een enorme uitdaging hebben om als overheid up-to-date te blijven met alle snelle ontwikkelingen die er zijn in IT-land. Daar voeg ik dan eufemistisch aan toe: de overheid heeft niet de beste trackrecord als het gaat om heel grote IT-projecten. Dus dat is een enorme uitdaging. Ik denk dat er wel verbeteringen zijn doorgevoerd, ook rijksbreed, om meer grip te krijgen op aanbestedingen en hoe je voorkomt dat dit soort systemen eindeloos uitlopen in de tijd en tegen de tijd dat ze ingevoerd worden alweer achterhaald zijn. Op het moment dat we ze hebben, zijn ze zo specialistisch dat we ons een breuk betalen om ze

allemaal up-to-date te houden, terwijl je eigenlijk ziet dat de buitenwereld veel sneller gaat qua informatie. Dat zijn allemaal lessen die we moeten leren. Die worden geleerd. Maar het strekt wel breder dan dit debat.
Als het gaat om innovatie, dan heb ik daar persoonlijk een visie op. Ook in het kader van de intensiveringen, bijvoorbeeld de 100 miljoen, hebben we daar geld voor vrijgemaakt om te kijken hoe de politie op een betere manier kan innoveren. Dat gaat breder dan IT, zeg ik erbij, maar het valt er wel onder. Wat je eigenlijk ziet in de buitenwereld, is dat commerciële technologie veel sneller ontwikkeld wordt dan wat welke overheid dan ook maar doet. Ik noem als voorbeeld SpaceX, dat natuurlijk NASA en gevestigde bedrijven op een ongelofelijke manier van de troon heeft gestoten, of Starlink, dat in één keer een communicatiemogelijkheid heeft geboden die van overheidswege gewoon niet beschikbaar was. We moeten dus vertrouwen op de innovatieve kracht die er is en de massa van de markt die uiteindelijk ervoor zorgt dat dit soort enorme projecten ook van de grond kunnen komen.
Dan moeten we goed kijken naar onszelf als overheid en naar hoe wij onze behoeftestellingsprocessen hebben ingericht, namelijk heel erg lang, hoe we onze aanbestedingsprocedures hebben ingericht, namelijk heel gecompliceerd, en naar hoe die twee werelden zich tot elkaar verhouden. Als we dat niet doen, dan lopen we het risico dat we met de technologie van gister aanlopen achter criminelen die met hun enorm diepe zakken met de technologie van morgen aan de haal gaan. Dat is een risico. Ik heb hoop in sommige opzichten. Ik denk dat het kraken van EncroChat en andere diensten een goed voorbeeld is van hoe we de criminelen dicht op de hielen zitten. Maar we hebben ook al uitbraakpogingen met drones gezien. We gaan te maken krijgen met gezichtsherkenning als uitdaging. Als de kwantumcomputer er komt, gaan we een probleem krijgen met onze gecodeerde communicatiesystemen. Dus er zijn ontzettend veel uitdagingen, waarbij ik geloof dat de beste technologie op de markt aanwezig is. De uitdaging wordt: hoe maken we de politie kundig om dat ook aan te kunnen pakken?
Dan de vraag van de heer Six Dijkstra over de cold case. Daar kom ik op terug, want die was heel technisch, namelijk of er ook fysiek een scheiding is tussen die specifieke informatie en de rest van de systemen. Die vraag beantwoord ik separaat. Ik zou niet durven speculeren.

De **voorzitter**:
En daarmee zijn alle vragen beantwoord. Goed. Dan zijn we daarmee aan het einde van de eerste termijn van de Minister. We hebben de toezegging aan de heer Six Dijkstra genoteerd. Daarmee komen we bij de tweede termijn aan de zijde van de Kamer. We zitten goed in de tijd en het is een belangrijk onderwerp, dus ik zou u daarvoor graag twee minuten willen geven, met twee interrupties onderling. Dan hebben we ook nog goed de tijd voor de termijn met de Minister. Mevrouw Van der Werf, aan u het woord.

Mevrouw **Van der Werf** (D66):
Voorzitter, dank u wel. Ik ben een optimistisch mens, maar ik ben hier echt niet gerust op, in ieder geval niet zo gerust als de Minister lijkt te zijn. Dat komt omdat hij toch een aantal voorbeelden aandraagt die mij niet de kern van de zaak lijken. Kijk, ik begrijp dat mensen op Facebook vindbaar zijn, dat je als agent ook op straat of op andere plekken het risico loopt dat iemand je beroep kent en dat de kans klein is dat er iemand voor hun deur staat. Maar daar gaat het nu toch niet om? Laten we ook even eerlijk zijn. Het lijkt mij toch dat we liever niet hadden gehad dat er nu 62.000 namen in handen zijn van een statelijke actor die het de moeite waard vond om die van ons te stelen. Dat brengt risico's met zich mee.
Ik zou de Minister dus willen vragen om toch nog eens in te gaan op wat hij nu gaat doen voor met name de mensen waarvoor het buitengewoon

onaantrekkelijk is dat hun naam nu bekend is, of dat nou is omdat ze bijvoorbeeld in de toekomst bij een undercoveroperatie zouden willen meedoen of omdat ze al jaren bij de politie werken en erg hun best hebben gedaan om dat in de anonimiteit te doen. De Minister gaf net aan dat dit op het gebied van gezichtsherkenning een probleem kan zijn. Ik zou willen weten wat we gaan doen op het moment dat er wél aanwijzingen zijn dat die datasets op meerdere plekken in handen is en dat die gekoppeld gaan worden. Wat gaat de Minister dan ondernemen? En hoe gaan wij daarover als Kamer worden geïnformeerd?

De **voorzitter**:
Ik dank u hartelijk. De heer Aardema.

De heer **Aardema** (PVV):
Dank u wel, voorzitter. Ik ga mijn hele inleidende tekst niet herhalen, want dat is al veelvuldig gedaan, ook door anderen, denk ik. De Minister heeft duidelijk gezegd dat de communicatie beter kon en dat dat ook gaat gebeuren in de toekomst, mocht het helaas nog een keer gebeuren; ik hoop niet dat dat zo is. De Minister heeft duidelijke antwoorden gegeven op mijn prangende vragen. Het is ook duidelijk welke maatregelen zijn genomen, ondanks dat hij die niet allemaal kenbaar kan maken om begrijpelijke reden.
Coldcasezaken zijn per definitie niet digitaal, omdat het vaak gaat om meterslange ordners en verhuisdozen vol met bewijsstukken. Veel rechercheurs zouden willen dat ze digitaal waren, denk ik, want dan is makkelijker om te zoeken in zo'n berg. Ik heb van de Minister begrepen dat daar geen doorstap op is geweest en ook niet bij andere bestanden die kunnen leiden naar echte privégegevens van politiemedewerkers. Wat dat betreft heeft mij dat dus wel gerustgesteld, maar het blijft natuurlijk altijd een hele slechte zaak dat datgene wat nu gebeurd is, is gebeurd. Ik hoop dat het niet weer gebeurt.
Dank u wel.

De **voorzitter**:
U bedankt. Mevrouw Helder.

Mevrouw **Helder** (BBB):
Dank u wel, voorzitter. Dank aan de Minister voor de duidelijke antwoorden. Ik denk dat niemand van mijn collega's geheel gerustgesteld zal zijn; ik ook niet. De Minister verwijst terecht naar EncroChat, Exclu en al die cryptocommunicatiediensten die door medewerkers van de Landelijke Eenheid en soms door de recherche in Amsterdam zijn gekraakt. Hulde voor hun werk. Dat juist hun gegevens op straat komen te liggen, is natuurlijk heel pijnlijk. Die deskundigheid is er dus wel, maar ik had gevraagd naar de deskundigheid van de eindverantwoordelijken op de betreffende plek.
Op dat punt ben ik niet blij met de antwoorden van de Minister. Hij zegt: die informatie heb ik niet. Dat kan. Misschien klopt de informatie die ik heb gekregen niet, maar ik kan dit geen open einde laten zijn. Ik ga geen vertrouwelijke briefing geven – dat klinkt natuurlijk heel raar – maar ik ben wel bereid om de Minister wat nader hierover te informeren. Ik zal ook bij diegene navragen of dat akkoord is, want dit kan ik niet laten lopen. De Minister kan daar geen antwoord op geven.
Ik ben bereid om dan maar als tussenpersoon te fungeren. Ik ben het namelijk met collega Aardema eens, en ik denk alle collega's met mij, dat dit in ieder geval niet meer mag gebeuren. Maar dit open einde heb ik nog steeds. Die deskundigheid is er naar mijn mening nog steeds niet en dus kan het nog steeds gebeuren. De Minister zegt dat hij vertrouwen heeft in de deskundigheid gebaseerd op de onderkenning van de hack, maar ik wil toch echt aan de voorkant terechtkomen.

Dank u wel.

De **voorzitter**:
Dank u wel. Mevrouw Mutluer.

Mevrouw **Mutluer** (GroenLinks-PvdA):
Dank, voorzitter. De schrik zit er best wel goed in. Het gaat namelijk om ruim 62.000 agenten die voor onze veiligheid staan. Als zij kwetsbaar zijn, dan is de samenleving kwetsbaar. Als er een dergelijke hack plaatsvindt, dan verwacht ik dat de communicatie er ligt en dat er een draaiboek ligt. Dan verwacht ik dat er protocollen zijn waar snel op kan worden teruggevallen, waarin meerdere scenario's zijn uitgewerkt en waarmee het allemaal goed gaat, of in ieder geval beter gaat dan nu. Ik wil graag die toezegging hebben, want dat lijkt mij de meest logische stap binnen zo'n grote organisatie.
Ik ben ook ongerust. Ik maak mij zorgen om de toekomst, om waar en hoe die gehackte informatie straks gaat opduiken en om wat dit eventueel zou kunnen betekenen voor de veiligheid van de agenten. Ik hoor de Minister duidelijk aangeven: we gaan echt wel een aantal maatregelen nemen. Ik ga ervan uit dat de Minister periodieke overleggen heeft met de politieorganisatie. Mijn verzoek is dan ook dat deze hack een vast onderwerp wordt bij die overleggen. Mijn verzoek is dat de maatregelen om de negatieve effecten en risico's te beperken constant worden gemonitord, dat er gekeken wordt wanneer moet worden bijgestuurd en dat de monitoring zolang die risico's bestaan niet wordt afgeschaald.
Ook het hackproof maken van de ICT bij de politie, het OM en justitie staat bij mij nog hoog op de agenda. Daarom denk ik dat ik zelf nog met een tweeminutendebat zou willen komen, voor zover dat nog niet is aangevraagd, zodat we daar ook wat concretere voorstellen voor kunnen indienen.

De **voorzitter**:
Hartelijk dank. Dat is inderdaad het geval, dus we zullen u daar als eerste spreker noteren. De heer Six Dijkstra.

De heer **Six Dijkstra** (NSC):
Dank, voorzitter. Ik dank ook de Minister voor zijn beantwoording. Tegelijkertijd deel ik ook de onrust die veel van mijn collega's al benoemd hebben. Als het gaat om hacks, moeten we natuurlijk altijd voorbereid en waakzaam zijn. Maar we moeten het ook nooit normaal gaan vinden, zeker niet als het zo'n impact op mensenlevens heeft. Het is goed dat deze impact onderkend is, wilde ik zeggen.
Ik hoor de Minister zeggen dat dat ook via een onderkenning vanuit de diensten was. Wat dat betreft werkt het systeem. Daar ben ik al heel blij om, want we zien natuurlijk niet wat we niet zien, en als we meer dingen zien, kan dat ook betekenen dat we beter zicht krijgen. Het is wat dat betreft goed dat we daar, waar mogelijk, openlijk over spreken en dat we uit de taboesfeer komen als het gaat om ingrijpende hackoperaties. Ik hoop dan ook dat we als Kamer worden meegenomen wanneer verdere openbaarwording mogelijk is, zowel als het gaat om de modus operandi als de attributie van de actor en de verdere gevolgen van zowel specifiek deze hacks als soortgelijke hacks.
Dank u wel.

De **voorzitter**:
U bedankt. De heer Van Nispen.

De heer **Van Nispen** (SP):
Dank u wel, voorzitter. Ik begin toch met een korte opmerking over de eerste communicatie. Ik ben het namelijk wel een beetje eens met onder

andere de kritische vraag van mevrouw Michon-Derkzen. Een draaiboek voor wat je doet als zoiets zich voordoet, had eigenlijk al klaar moeten liggen. Want nu wordt gezegd: dat zouden we de volgende keer misschien beter doen door wel direct een mail te sturen. Ik zou toch denken dat zoiets al klaar had kunnen of moeten liggen. Misschien is dit iets uit de categorie «achteraf praten is altijd makkelijk», maar hiervan denk ik dat dat toch wel gerechtvaardigd is.
Vervolgens blijf ik nog wel zitten met de vraag wat er nou echt wordt gedaan om dit in de toekomst te voorkomen. Dat is natuurlijk ook een verschrikkelijk moeilijke vraag; dat snap ik. Ik geloof niet zozeer dat ik deze Minister moet aanmoedigen om voldoende aandacht te hebben voor cyberveiligheid. Die urgentie zal er echt zijn. Toch is mij nog niet geheel duidelijk welke echt concrete lessen hier nou van zijn geleerd en of er inderdaad voldoende in wordt geïnvesteerd. Ik weet dat er meer in wordt geïnvesteerd, maar worden dit soort hacks daar voortaan echt mee voorkomen? Hoe wordt voorkomen dat dit bij de politie of elders nog een keer zo kan gebeuren? Misschien is dat ook niet helemaal uit te sluiten – daar moet de Minister dan ook eerlijk over zijn – maar ik ben toch benieuwd wat hij hierop kan antwoorden.

De **voorzitter**:
Dank u wel. Mevrouw Michon-Derkzen.

Mevrouw **Michon-Derkzen** (VVD):
Voorzitter. Ik denk dat de korpsleiding van de politie ontzettend blij mag zijn met deze Minister, die heel veel verstand heeft van cyberaanvallen en van ICT. Hij legt hier dingen uit en gaat op onze vragen in op een manier die heel vertrouwenwekkend is. Tegelijkertijd hoop ik dat datzelfde kennis- en expertiseniveau ook bij de politie aanwezig is, tot en met de korpsleiding van de politie.
Op mijn vragen over hoe een draaiboek eruitziet als zoiets gebeurt en dat dat er niet lijkt te liggen, en over hoe we weten wat er met die data is gebeurd, krijgen we als antwoord: dat houden we in de gaten. Maar ik denk dus dat cyberveiligheid hét topic van de aankomende jaren is. Het wordt alleen maar erger. De basis van de ICT is dus eigenlijk nog niet op orde. Ik begrijp de ratio in de antwoorden van de Minister, maar het hele pakket stemt wel zorgelijk. Ik denk dat we het hier met elkaar over moeten blijven hebben in commissieverband. Ik zou de Minister willen vragen of hij ons kan informeren met een soort ICT-agenda van de politie. We hoeven niet elk systeem mee te ontwikkelen, maar we willen wel zicht houden op waar de ICT-uitdagingen zitten en of de budgetten kloppen, zoals ik ook in eerste termijn vroeg. Zo willen we vinger aan de pols houden bij wat er nodig is voor ICT bij de politie. Dat is essentieel en tegelijkertijd moet het voor mensen die daar werken ook veilig zijn, zoals we aan de actualiteit van dit debat zien.
Dank u wel, voorzitter.

De **voorzitter**:
Dank u wel. Dat was de tweede termijn van de Kamer. Dan is het woord aan de Minister. We zitten goed in de tijd, dus ik zou u graag drie interrupties willen geven in de tweede termijn van de Minister.

Minister **Van Weel**:
Dank, voorzitter, en wederom dank voor de inbreng in tweede termijn. Laat ik nóg een keer zeggen dat het echt niet mijn bedoeling is om zaken te bagatelliseren. Ik had gewild dat ik hier niet had gezeten en dat deze hack niet had plaatsgevonden. Dat was mij veel liever geweest, zeg ik ook tegen alle 62.000 politieagenten. Het enige wat ik hier heb willen doen, is niet onnodig ongerustheid zaaien onder die 62.000 politieagenten. Dat is waarom ik de duiding heb gegeven zoals ik die in de brief heb gegeven.

Dat neemt niet weg dat de risico's niet nul zijn, ook dat heb ik hier gezegd. Ik acht ze zeer gering, zeker zolang de data niet elders opduiken, maar ze zijn niet nul. Daarom zullen we dat blijven monitoren. Zoals ik al eerder gezegd heb, zal dat ook gebeuren over mijn graf heen. Afhankelijk van hoe de data opduiken en in welke vorm, zullen we ook mitigerende maatregelen moeten treffen.
Belemmert de informatie die daarin staat mensen om in de toekomst onder dekmantel te gaan werken? Ik denk van niet, want op dat moment verdwijnen ze uit deze database. Dat gebeurt met mensen die we onder dekmantel brengen. Dan zijn ze dus niet meer vindbaar. Wat hun oude identiteit ook was, zonder enige aanwijzing dat iemand nu onder dekmantel werkt, zou deze gelekte informatie voor iemand die onder dekmantel gaat werken, geen aanvullend risico moeten opleveren. Het is sowieso risicovol werk, maar het zou dus geen aanvúllend risico moeten opleveren. Dat zeg ik in reactie op mevrouw Van der Werf.

De **voorzitter**:
Mevrouw Van der Werf heeft nog een interruptie voor u.

Mevrouw **Van der Werf** (D66):
Natuurlijk begrijp ik dat de Minister mensen niet onnodig ongerust wil maken. Dat wil ik ook niet. Ik stel heel kritische vragen en ik kan me voorstellen dat dat ongemakkelijk is. Ik wil voor de luisteraars benadrukken dat het niet mijn intentie is om mensen ongerust te maken, maar ik vind dat wij als parlement hier wel uitermate kritisch op moeten zijn, omdat het niet niks is.
Dat gezegd hebbende: het is natuurlijk gewoon heel kwetsbaar dat die gegevens weg zijn, ook als dat betekent dat er niet morgen iemand voor de deur van een agent staat. Het is gewoon heel kwetsbaar dat die gegevens weg zijn. Ik kan me voorstellen dat als je weet dat jouw naam ergens bekend is en dat het onduidelijk is of die informatie ooit wordt doorgegeven of doorverkocht aan derden, je minder snel de stap zet om een spannendere functie binnen de politie – ik zeg het maar even plat – te gaan doen dan op het moment dat dit niet was gebeurd. Het betekent gewoon wat voor de motivatie van mensen en voor het veiligheidsgevoel van mensen, ook al is niet meteen te herleiden of je onder dekmantel gaat werken. Daar wil ik graag een reflectie op van de Minister.

Minister **Van Weel**:
We hebben hier te maken met twee dingen. Een: wat zijn de klinische risico's en feiten die we zien? En twee: wat betekent de wetenschap dat deze informatie weg is en dat jouw naam en functie daarin voorkomt, voor mensen? Ik heb daar alle begrip voor. Daarom hebben we dat meldpunt ingesteld. Dat hadden we inderdaad eerder moeten doen, zeg ik tegen iedereen die dat zei. Het komt ook zeker in de draaiboeken voor de toekomst.
Binnen de politie is de openheid om het gesprek aan te gaan met degenen die ongerust zijn er nog steeds. Ik hoorde vorige week voorbeelden van mensen die niet op vakantie waren gegaan vanwege deze hack. Daar moeten we het over kunnen blijven hebben. Ik wil de gevoelens van onveiligheid die mensen hebben helemaal niet wegnemen. We staan ervoor open om daar het gesprek over aan te gaan. Dat staat los van de duiding die ik heb geprobeerd te geven over wat ik denk dat er nu met deze informatie zou kunnen gebeuren. Ik hoop dat die twee naast elkaar kunnen bestaan. Ik hoop dat ik daarmee medewerkers de beste informatie geef die ik kan bieden.

Mevrouw **Van der Werf** (D66):
Toch voel ik een blijvend ongemak – ik kan me voorstellen dat dat ook voor de politiemedewerkers geldt – omdat ook na dit debat de belang-

rijkste vraag eigenlijk niet is beantwoord. Dat er nu geen risico is, betekent namelijk niet dat dat risico zich niet alsnog gaat aandienen, simpelweg omdat je – ook al monitoren we van alles – niet weet wat je niet ziet. Daarom begrijp ik dus ook niet dat de Minister niet wat terughoudender en voorzichtiger is in zijn beantwoording richting ons en daarmee ook richting de politie over het feit dat het allemaal wel meevalt. Ik wil de Minister toch nog één keer uitdagen om erop te reflecteren dat het natuurlijk heel goed mogelijk is dat we ook níét kunnen weten wat er met die datasets gebeurt.

Minister **Van Weel**:
Dat klopt. Daarom bestaat mijn weging ook uit twee factoren. Eén. Waar is die informatie en waar weten we of die opduikt? Nou, daar doen we wat we kunnen. Honderd procent zekerheid hebben we daar niet. De andere kant is: als je die informatie hebt, is de vraag welke informatie je dan hebt van mensen, en wat voor risico je op basis daarvan dan loopt. Als we hadden gedacht dat mensen een heel groot risico lopen op basis van hun e-mailadres en hun functienaam, dan had het natuurlijk niet gewoon in Outlook gestaan. Dan was die informatie beter afgeschermd geweest en dan had je niet 62.000 medewerkers gehad die daar toegang toe hebben. Dus ik probeer een weging te maken. Als die informatie in verkeerde handen belandt, welk risico lopen mensen dan? Dat risico is niet nul. En wat is het risico dat die informatie ergens anders belandt? Dat risico is ook niet nul. Dus die twee balanceer ik. In beide zit een risico, en dat heb ik geprobeerd te duiden.

De **voorzitter**:
Gaat u verder, als u wil.

Minister **Van Weel**:
Mevrouw Helder had het over de informatievoorziening. Ik herhaal nogmaals dat ik erg open sta voor die informatie, want dan kan ik die ook nalopen. In welke vorm u dat wilt doen, laat ik aan u, maar dan neem ik dat zeer serieus.
Mevrouw Mutluer vroeg om draaiboeken. Ook de heer Van Nispen vroeg daarom. Ja, daar kijken we naar. We kijken zowel naar technische lessen die we hieruit kunnen trekken als naar lessen voor de mensen. Kunnen we mensen dus nog beter opleiden en voorbereiden hierop, om te voorkomen dat dit gebeurt? Ten derde kijken we natuurlijk ook naar de organisatie: hebben we de goede organisatie staan, hebben we de goede verbanden en mechanismen staan? Voor mij was dit ook weer het eerste event van deze soort in deze baan, dus ook ik heb voor mezelf geleerd. Dus dit gaan we allemaal neerleggen in draaiboeken, zodat we een volgende keer beter zijn voorbereid, niet alleen technisch maar ook op de andere aspecten.
De heer Six Dijkstra vroeg of we nog terugkomen met meer informatie, dus of we nog meer te horen krijgen. Ja, op een aantal momenten. Het eerste moment is als er informatie komt die we nu niet kennen en die aanvullend is op alles wat ik u heb gemeld. Dan kom ik bij u terug, zoals ik de afgelopen keren totdat het beeld stabiel werd, ook elke keer naar u ben teruggekomen. Dus daarvan kunt u verwachten dat dat onverwijld gebeurt. Als we overgaan tot attributie, dan is dat natuurlijk ook een moment waarop we met uw Kamer communiceren. Datzelfde geldt, vermoed ik, voor het OM op het moment dat zij het strafrechtelijk onderzoek hebben afgerond of in een volgende fase willen brengen. Dan vermoed ik dat...
We hebben een hack!

De **voorzitter**:
Het was wat rumoerig, maar de situatie is onder controle.

Minister **Van Weel**:
Een fysieke hack. Oké, dan ga ik verder. Dus er zullen nog momenten zijn dat we hierover komen te spreken. Daarbij zeg ik ook: op het moment dat wij zouden zien dat er iets gebeurt met die dataset, dan is dat ook een moment voor communicatie. Een en ander is natuurlijk afhankelijk van de wijze waarop dat gebeurt en of het dan niet schaadt op het moment dat we daar ruchtbaarheid aan zouden geven. Ik denk dus niet dat we voor het laatst met elkaar gesproken hebben hierover.
Dan de IT-agenda in bredere zin, zeg ik zowel tegen mevrouw Mutluer als tegen mevrouw Michon. Ik wil wel kijken of we in het volgende halfjaarbericht – daarmee bedoel ik niet het halfjaarbericht dat u over een paar dagen krijgt, maar het bericht dat voor het zomerreces uw kant op gaat – uitgebreider kunnen stilstaan bij de stand van de IT bij de politieorganisatie. Ik denk ook dat dat nuttig kan zijn voor het debat dat we met uw Kamer over die berichten hebben.
Dat waren volgens mij de antwoorden, voorzitter.

De **voorzitter**:
Ik dank u hartelijk. Ik kijk nog even of er onbeantwoorde vragen zijn. De heer Van Nispen?

De heer **Van Nispen** (SP):
Nee, voorzitter, ik heb een hele korte aanvullende vraag. Ik hecht altijd heel erg aan informatievoorziening aan de Kamer. Ik ben altijd kritisch als de Kamer niet tijdig is geïnformeerd. In dit geval zou ik iets anders zeggen. Als de politieagenten bij ontwikkelingen rondom dit datalek eerder dan de Kamer worden geïnformeerd, dan zal ik daar niet over mopperen. Laat ik het zo zeggen. Ik vind dat in dit geval namelijk echt belangrijker. Ik wil uiteraard wel dat de Kamer daar meteen op volgt, maar ik vind dat aspect echt belangrijker. Ik hecht eraan om dat te zeggen.

De **voorzitter**:
Waarvan akte. Hartelijk dank daarvoor. Dan zijn we aan het einde gekomen van de tweede termijn van de Minister en daarmee ook aan het einde van dit debat. Mevrouw Mutluer heeft een tweeminutendebat aangevraagd. We gaan dat inplannen en zij zal daar de eerste spreker zijn. We hebben enkele toezeggingen van de Minister die ik graag even met u doorloop om te kijken of we die op deze wijze correct hebben doorgegeven.
– De Minister informeert de Kamer blijvend als er nieuwe ontwikkelingen zijn rondom het datalek.

Minister **Van Weel**:
Voor zover de veiligheid dat toelaat.

De **voorzitter**:
Ja, uiteraard.

Minister **Van Weel**:
Dat is het enige voorbehoud dat ik wil maken.

De **voorzitter**:
Dat voorbehoud zetten we erbij. Hartelijk dank voor die aanvulling.
– De Minister informeert de Kamer naar aanleiding van de vragen van het lid Six Dijkstra over de cold cases en de fysieke scheiding tussen de systemen.
De vraag aan de Minister is nog wanneer dat zal geschieden.

Minister **Van Weel**:

Dat kan op korte termijn. We proberen dat zelfs al mee te nemen in het halfjaarbericht. Dat moet niet moeilijk zijn.

De **voorzitter**:
Dank. Six Dijkstra is daarmee akkoord. Dan gaan we dat zo noteren.
– In het halfjaarbericht politie van zomer 2025 informeert de Minister de Kamer over de stand van de ICT bij de politie.

De Minister knikt en de Kamerleden ook. Dan zijn dit de toezeggingen.
Ik dank de Minister voor zijn komst en voor het inhoudelijke debat dat wij hier hebben kunnen voeren. Hartelijk dank aan de leden. Het is een belangrijk onderwerp en het heeft hier ook mooi gewicht gekregen. Dank aan het publiek, natuurlijk onze politieagenten die dit hebben gevolgd en onze ondersteuning.

Sluiting 17.58 uur.