Ministerie van Justitie en Veiligheid

> Retouradres Postbus 20301 2500 EH Den Haag

Aan de Voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

Directoraat-Generaal Politie en Veiligheidsregio's

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv

Onze referentie
5855113

Uw referentie
2024Z14837

Datum 8 november 2024
Betreft Antwoorden Kamervragen over hack bij de politie

In antwoord op uw brief van 2 oktober 2024, nr. 2024Z14837, deel ik u mede dat de vragen van de leden Van der Werf (D66), Mutluer (GroenLinks-PvdA), Michon-Derkzen (VVD), Van Nispen (SP) en Aardema (PVV) over het bericht 'Politiehack van 62.000 medewerkers is gevaarlijk: naam agent is handelswaar' worden beantwoord zoals aangegeven in de bijlage van deze brief.

De Minister van Justitie en Veiligheid,

D.M. van Weel

Antwoorden van de minister van Justitie en Veiligheid op vragen van de leden Van der Werf (D66), Mutluer (GroenLinks-PvdA), Michon-Derkzen (VVD), Van Nispen (SP) en Aardema (PVV) over het bericht 'Politiehack van 62.000 medewerkers is gevaarlijk: naam agent is handelswaar' (ingezonden 2 oktober 2024, 2024Z14837)

Directoraat-Generaal Politie en Veiligheidsregio's

Datum
8 november 2024

Onze referentie
5855113

Vraag 1
Welke informatie is er nu exact vrijgekomen als gevolg van het datalek?[1]

Antwoord op vraag 1
Er is een politieaccount gehackt. Daarbij zijn de werkgerelateerde contactgegevens van alle politiemedewerkers buitgemaakt, de zogenoemde *global address* list met daarin de outlook-visitekaartjes. Het betreft in enkele gevallen privé(contact)gegevens die personen met een politieaccount zelf in hun visitekaartje hebben gezet. Het kan bijvoorbeeld gaan om privételefoonnummers en vermoedelijk ook om (profiel)foto's. Ook zijn de e-mailadressen van een aantal ketenpartners buitgemaakt. Er zijn op dit moment nog altijd geen aanwijzingen dat er naast de gegevens uit de *global address list* nog andere gegevens zijn buitgemaakt.

Vraag 2
Hoeveel meldingen zijn er inmiddels gekomen bij het meldpunt?

Antwoord op vraag 2
Sinds het openen van het meldpunt op zaterdag 28 september tot en met vrijdag 25 oktober zijn 1.639 vragen bij het meldpunt binnengekomen.

Vraag 3
Wanneer was de korpsleiding op de hoogte van het datalek en waarom is pas in het weekend een mail gestuurd aan alle medewerkers?

Antwoord op vraag 3
In het belang van de lopende onderzoeken kan ik daar geen uitspraken over doen.

Er is op vrijdag 27 september een bericht op intranet geplaatst en korte tijd later ook extern op de politie website. Op zaterdag 28 september heeft de korpschef alle medewerkers per e-mail geïnformeerd. In een poging iedereen zorgvuldig te informeren via de gebruikelijke lijn(en), ging het nieuws sneller dan verwacht. Een deel van de politiemedewerkers moest het nieuws via de media horen. De korpschef betreurt dit.

Vraag 4
Wanneer was u op de hoogte van het datalek?

Antwoord op vraag 4
Zoals ik u in mijn brief van 27 september jl.[2] heb laten weten, heeft de korpschef mij op 26 september jl. geïnformeerd.

[1] Algemeen Dagblad, 27 september 2024, 'Politiehack van 62.000 medewerkers is gevaarlijk: naam agent is handelswaar', www.ad.nl/politiek/politiehack-van-62-000-medewerkers-is-gevaarlijk-naam-agent-is-handelswaar~ac7d6588/
[2] Kamerstukken II 2024-25, 29 628, nr. 1221

Vraag 5
Is bekend op welke wijze iemand een politieaccount heeft binnengedrongen?

Vraag 6
Was de hack mogelijk vanwege nalatigheid van een beheerder van het betreffende politieaccount, vanwege een fout in het systeem of allebei?

Vraag 7
Zijn er verdere conclusies naar aanleiding van het onderzoek van de politie naar de oorzaak en de impact? Zo nee, wanneer worden deze verwacht?

Antwoord op vragen 5, 6 en 7
De politie doet momenteel onderzoek naar de aard, omvang en gevolgen van het cyberincident. Het Team High Tech Crime van de Eenheid Landelijke Opsporing en Interventies doet onderzoek naar de toedracht en de daders.

Uit het onderzoek van Team High Tech Crime is inmiddels gebleken dat de daders vermoedelijk gebruik hebben gemaakt van een zogenoemde *pass-the-cookie*-aanval. Het doel van zo'n aanval is om toegang te krijgen tot het account of de applicatie van een gebruiker zonder dat inloggen met een wachtwoord opnieuw vereist is. Bij een succesvolle *pass-the-cookie*-aanval wordt een actieve sessie van een account overgenomen met de bijbehorende rechten.

Het verkrijgen van toegang kan op verschillende manier gebeurd zijn, bijvoorbeeld door phishing. Na een succesvolle aanval kan malware worden geïnstalleerd, die data, zoals cookies, doorstuurt naar de hacker.

Ik kan op dit moment geen nadere uitspraken doen over dit onderzoek.

Vraag 8
Wat zijn de risico's voor de individuele agent?

Vraag 9
Welke maatregelen worden genomen om de risico's te ondervangen?

Vraag 10
Wat betekent dit datalek voor de familie van de agenten en welke maatregelen worden genomen om ook directe gezinsleden veiligheid te bieden?

Antwoord op vragen 8, 9 en 10
De politie heeft op dit moment geen aanwijzingen voor concrete dreigingen tegen politiemedewerkers of hun familie.

De politie heeft meteen maatregelen getroffen nadat zij was geïnformeerd door de inlichtingen- en veiligheidsdiensten. De maatregelen die worden getroffen, zijn afgestemd op het huidige beeld, namelijk dat de inlichtingen- en veiligheidsdiensten het zeer waarschijnlijk achten dat een statelijke actor verantwoordelijk is voor het cyberincident bij de politie en dat de daders vermoedelijk gebruik hebben gemaakt van een zogenoemde *pass-the-cookie*-aanval.

Het betreft onder meer ICT-maatregelen en maatregelen op het vlak van bewustwording, bijvoorbeeld een oproep tot extra waakzaamheid van

politiemedewerkers op phishingmails en verdachte telefoontjes en berichten. Tevens monitort de politie of de buitgemaakte gegevens elders verschijnen. Tot slot blijft de politie alert op mogelijk nieuwe aanvallen. Daartoe monitort de politie haar systemen continu.

Vraag 11
Hoe worden agenten meegenomen en geüpdatet tijdens het onderzoek?

Antwoord op vraag 11
Politiemedewerkers worden op diverse manieren van het cyberincident op de hoogte gehouden. Op 27 september zijn medewerkers geïnformeerd via het intranet van de politie. Op 28 september, 2 oktober en 9 oktober heeft de korpschef een e-mail naar alle medewerkers gestuurd over de actuele situatie. Medewerkers worden via intranet ook gelijktijdig met deze berichtgeving aan uw Kamer geïnformeerd over de laatste stand van zaken.

Ook is op het politie-intranet een themapagina met informatie over het cyberincident ingericht. Tot slot kunnen medewerkers met zorgen en vragen terecht bij hun leidinggevende en is er een speciaal meldpunt ingericht.

Vraag 12
In de Kamerbrief van 27 september jl. (Kamerstuk 29628, nr. 1221) staat dat aanvullende maatregelen getroffen worden als blijkt dat deze nodig zijn, maar betekent dat dat er al maatregelen genomen zijn en zo ja, welke zijn dit?

Antwoord op vraag 12
Zie het antwoord op de vragen 8 t/m 10.

Vraag 13
Zijn ook agenten die undercover werken, bij de Mobiele Eenheid of op een andere wijze verhoogd risico lopen bij het openbaar maken van hun gegevens betrokken bij dit lek en wordt er direct actie ondernomen om te voorkomen dat zij gevaar lopen of hinder ondervinden in het uitoefenen van hun functie?

Antwoord op vraag 13
De werkgerelateerde gegevens van undercoveragenten zijn afgeschermd en zijn derhalve niet opgenomen in de *global address list* van outlook. Deze gegevens zijn dus niet buitgemaakt.

De werkgerelateerde outlook-gegevens van alle andere politiemedewerkers zijn wel buitgemaakt, bijvoorbeeld van politiemedewerkers die werkzaam zijn bij de Mobiele Eenheid.

Vraag 14
Op basis waarvan baseerde de minister-president zijn uitspraak dat hij ervan uitgaat dat "mensen geen gevaar lopen" terwijl het onderzoek naar de oorzaak en de impact van het lek nog lopende is?

Vraag 15
Blijkt dit statement dat mensen geen gevaar lopen naar aanleiding van het onderzoek ook te kloppen?

Antwoord op vragen 14 en 15
Zie het antwoord op de vragen 8 t/m 10.

Vraag 16
Welke acties lopen er om de dader van dit hack op te sporen?

Antwoord op vraag 16
Het OM is een strafrechtelijk onderzoek gestart, dat wordt uitgevoerd door het Team High Tech Crime van de Eenheid Landelijke Opsporing en Interventies van de politie. Dit team doet onderzoek naar de toedracht en de daders van de hack. Ik kan op dit moment geen nadere uitspraken doen over dit onderzoek.

Vraag 17
Wat is de reactie van de Autoriteit Persoonsgegevens op de melding van dit lek?

Antwoord op vraag 17
Zoals gemeld in mijn brief van 27 september 2024 heeft de politie melding gemaakt van het datalek bij de Autoriteit Persoonsgegevens (AP). De AP heeft in reactie daarop contact gezocht met de politie en gevraagd haar nader te informeren over de informatie die tot nu toe is verstrekt aan betrokkenen over het datalek.

Vraag 18
Waarom is aan de Kamer in eerste instantie gemeld dat er alleen werkgerelateerde contactgegevens zijn buitgemaakt, terwijl op dat moment de impact van het lek nog niet goed bekend was en later bleek uit berichtgeving van de NOS dat het datalek ook incidenteel privégegevens van agenten betreft?

Antwoord op vraag 18
Ik hecht grote waarde aan het tijdig informeren van uw Kamer. Ik heb uw Kamer op de hoogte gesteld van nieuwe inzichten op 2 en 9 oktober jl., zo snel deze uit het onderzoek van de politie naar voren kwamen. Ook over de laatste stand van zaken heb ik uw Kamer, gelijktijdig met de beantwoording van deze vragen, geïnformeerd, zodra dit bekend was.

Vraag 19
Zijn er daadwerkelijk ook privégegevens gestolen? Zo ja, hoe omvangrijk is dat precies?

Antwoord op vraag 19
Zie het antwoord op vraag 1.

Vraag 20
Zijn naar aanleiding van dit nieuwe bericht aanvullende maatregelen getroffen?

Antwoord op vraag 20
Zie het antwoord op de vragen 8 t/m 10.

Vraag 21
Bestaat het risico dat er meer privégegevens achterhaald kunnen worden indien de gestolen gegevens door hackers kunnen worden gekoppeld aan elders gelekte gegevens?

Antwoord op vraag 21
Het is theoretisch mogelijk dat de actor achter de hack de buitgemaakte

informatie koppelt aan openbaar te vinden privégegevens. Daarvoor zijn op dit moment geen aanwijzingen.

Vraag 22
Waarom is ervoor gekozen om het systeem zo in te richten dat vanuit één account de contactgegevens van alle agenten makkelijk ingezien kunnen worden en is daarbij rekening gehouden met het risico op een datalek?

Antwoord op vraag 22
Zie het antwoord op de vragen 5 t/m 7.

Vraag 23
Zijn er meer systemen binnen de overheid, en met name bij de veiligheidsdiensten, de rechtspraak en het Openbaar Ministerie, die op een manier werken waarbij één account met een lage drempel een grote hoeveelheid vertrouwelijke contactgegevens kan inzien?

Antwoord op vraag 23
Het delen van contactgegevens tussen collega's in outlook is noodzakelijk om samenwerking te faciliteren en ten behoeve van de werking van systemen, zoals mailsystemen.

Binnen de Rijksoverheid wordt ook de Rijksadresgids gebruikt. De Rijksadresgids bevat, zoals bij de meeste organisaties ook in outlook het geval is, standaard alleen de naam en e-mailadres van de betrokken collega's.

Vraag 24
Welke maatregelen worden genomen om in het vervolg binnen de overheid, en met name bij de veiligheidsdiensten, de rechtspraak en het Openbaar Ministerie, te voorkomen dat hackers zelfs bij het binnendringen van één politieaccount niet direct een hele lijst van contactgegevens van alle medewerkers kunnen bemachtigen?

Antwoord op vraag 24
Het is de verantwoordelijkheid van de organisaties zelf om op basis van risicomanagement de nodige preventieve maatregelen te nemen. Lijsten van contactgegevens in outlook zijn echter niet te voorkomen in een zakelijke omgeving, aangezien deze noodzakelijk zijn om samenwerking te faciliteren en ten behoeve van de werking van (mail)systemen. Wel zal worden bezien welke informatie daarin zichtbaar dient te zijn.

Het Nationaal Cyber Security Centrum (NCSC) heeft partijen binnen de Rijksoverheid en vitale sectoren geïnformeerd over (generieke) maatregelen die naar aanleiding van dit incident kunnen worden getroffen.

Misbruik van deze gegevens kunnen met detectieve maatregelen ontdekt worden. Grote Rijksorganisaties hebben hiervoor een zogenaamde Security Operating Centers (SOC). Binnen de Rijksoverheid worden deze organisaties ondersteund o.a. door het programma Versterkt SOC Stelsel Rijk (VSSR).

Het hebben van een zeer volwassen SOC is evenwel geen garantie dat dergelijke zaken nooit kunnen gebeuren. Het is hierdoor ook van belang om blijvend te investeren in de digitale weerbaarheid van ICT-systemen, maar ook van medewerkers.