# Tweede Kamer der Staten-Generaal

**2**

Vergaderjaar 2020–2021

**Aanhangsel van de Handelingen**


**Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden**

## 3748

Vragen van de leden **Kathmann** (PvdA) en **Van Ginneken** (D66) aan de Minister van Justitie en Veiligheid over *het bericht dat Russen ten tijde van het MH17-onderzoek door een hack diep in de systemen van de politie zaten* (ingezonden 15 juni 2021).

Antwoord van Minister **Grapperhaus** (Justitie en Veiligheid) (ontvangen 16 augustus 2021). Zie ook Aanhangsel Handelingen, vergaderjaar 2020–2021, nr. 3483.

Vraag 1, 2, 3, 4, 6, 7, 8
Bent u bekend met het feit dat Russische hackers toegang hadden tot de politiesystemen door een hack?[1]
Wat vindt u van de uitspraak dat de politiesystemen voor de hack slecht beveiligd waren?
Hoe kan het zijn dat de politiesystemen zo slecht beveiligd waren?
Waarom monitorde de politie niet structureel of de systemen veilig waren?
Wat vindt u van de keuze van de politie om de Russen er eerst uit te jagen, gelet op het feit dat we niet weten waar de Russen naar op zoek waren?
Klopt het dat Russische hackers ook toegang hebben proberen te krijgen tot de digitale systemen van het Openbaar Ministerie (OM)? Zo ja, is dit gelukt?
Klopt het dat de politie zelf controle houdt over het oplossen van de hack en dat daarom kostbare tijd verspild is?

Antwoord 1, 2, 3, 4, 6, 7, 8
Ik heb kennisgenomen van de berichtgeving door de Volkskrant. Het is algemeen bekend dat (buitenlandse) statelijke actoren voortdurend proberen bij (overheids)organisaties binnen te dringen om toegang te krijgen tot organisatiegeheimen of gerubriceerde (staatsgeheime) informatie.
Het is geen geheim dat Nederland en andere Westerse landen in het vizier staan van onder meer Russische en Chinese inlichtingendiensten. Alle betrokken organisaties zijn zich bewust van de digitale dreigingen. Vanwege staatsveiligheid kan ik geen uitspraken doen over de specifieke maatregelen die de onder mij ressorterende diensten treffen.

[1] Website De Volkskrant, 7 juni 2021 (Russen zaten ten tijde van MH17-onderzoek door hack diep in systemen politie | De Volkskrant)


ah-tk-20202021-3748
ISSN 0921 - 7398
's-Gravenhage 2021

Voor zover uw vragen zien op concrete incidenten met statelijke actoren zoals die in de berichtgeving van de Volkskrant worden beschreven, kan ik op deze vragen geen antwoord geven.

Vraag 5
Onderzoekt de regering structureel of de digitale beveiligingsystemen op orde zijn? Zo nee, waarom niet en bent u hiertoe bereid? Zo ja, zijn er meer overheidssystemen die slecht beveiligd zijn? Zo ja, welke?

Antwoord 5
Overheidsorganisaties zijn gehouden aan de Baseline Informatiebeveiliging Overheid (BIO). In de BIO worden eisen gesteld aan het beoordelen van de technische naleving van beveiligingsbeleid en -normen. Door middel van kwetsbaarheidsanalyses, pentesten of ethische hackoperaties (Red Teaming) wordt de feitelijke veiligheid van kritische systemen en netwerken regelmatig beproefd.
Daarnaast is door CISO Rijk in samenwerking met een groep experts binnen de rijksoverheid en de departementen een handreiking opgesteld en vastgesteld voor het inrichten van een doorlopende kwetsbaarhedenscan bij rijksoverheidsorganisaties. Dit wordt waar nodig ondersteund met praktische tooling.

Vraag 9, 10, 11
Klopt het dat het aandringen van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) tot snelle beveiligingsmaatregelen bij de politie tot frictie leidde?
Is er vaker frictie tussen de politie en veiligheidsdiensten?
Wat doet u eraan om deze frictie op te lossen, zodat er in de toekomst sneller gehandeld kan worden bij hacks?

Antwoord 9, 10, 11
Er is geen sprake van frictie tussen de politie en veiligheidsdiensten, de samenwerking verloopt goed.
Net als iedere andere organisatie binnen het veiligheidsdomein, neemt ook de politie zowel organisatorische als technische maatregelen om blijvend te anticiperen op de veranderende dreigingen in de buitenwereld. Zoals in de bijlage bij het recent verstuurde Halfjaarbericht Politie staat, investeert de politie in de verbetering van detectie- en incidentenrespons[2].
Er wordt onafgebroken geïnvesteerd in het steeds beter en sneller te kunnen omgaan met (pogingen tot) hacks. Zo heeft de implementatie van EDR (Endpoint Detection & Response) het afgelopen jaar een significante bijdrage geleverd aan de digitale veiligheid van de politie.

Vraag 12, 13, 14
Klopt het dat niet alle voorgestelde beveiligingsvoorstellen zijn ingevoerd door de politie?
Welke beveiligingsmaatregelen zijn nog niet ingevoerd bij de politie?
Wat is het gevolg van het nog niet invoeren van beveiligingsmaatregelen op de digitale weerbaarheid van de politie?

Antwoord 12, 13, 14
Zoals u zult begrijpen kan ik om veiligheidsredenen in het openbaar geen antwoord geven op deze vragen.

Vraag 15
Zijn de belangrijkste data van de politie nu wel veilig? Zo nee, welke data zijn niet veilig en wat doet u eraan om dit zo snel mogelijk op te lossen?

Antwoord 15
Geen enkele organisatie kan zich voor 100% wapenen tegen hacks of andere ongeoorloofde toegang tot systemen. Door een combinatie van verschillende maatregelen, van geavanceerde beveiligingsoplossingen tot personeel dat getraind is in en bekend is met technieken voor social engineering, wordt het

[2] Kamerstuk 29.628 nr. 1030.

beveiligingsniveau zo hoog mogelijk gehouden. Hierop wordt dan ook voortdurend ingezet door de politie.
De politieorganisatie heeft gezien de aard van de organisatie te maken met zogeheten Advanced Persistent Threats (APT). APT is een verzamelnaam voor dreiging door een groep aanvallers die niet alleen over geavanceerde technische middelen en voldoende geld beschikt, maar ook een sterke motivatie heeft om organisatiegeheimen of gerubriceerde (staatsgeheime) informatie te bemachtigen. Er zijn specifieke kenmerken (de Indicators Of Compromise, IOC) te onderscheiden van een aanval vanuit Advanced Persistent Threats. Deze IOC's worden voortdurend vertaald naar detectie- en monitoringoplossingen zoals het optimaliseren van een Security Information & Event Management Systeem (SIEM).
Digitale kwetsbaarheid en hackpogingen om misbruik van te maken van die kwetsbaarheid nemen overal toe en de impact van hack- en ransomware aanvallen wordt steeds zichtbaarder. Met het Programma Cyber Security richt de politie zich op het digitaal weerbaarder maken van de politieorganisatie door onder andere extra beveiligingsmaatregelen te implementeren en bewustwording over de digitale dreigingen te vergroten. Daarbij wordt bijvoorbeeld geïnvesteerd in de verbetering van detectie- en incidentrespons.

Vraag 16
Bent u bereid om structureel ethische hackers in te zetten om te zoeken naar gaten in de digitale systemen?

Antwoord 16
Binnen de politie worden – net als bij vrijwel alle overheidsorganisaties – ethische hackers ingezet. Dit wordt gedaan in de vorm van Red Teaming. Red Teaming zorgt voor een analyse van zwakke plekken en kwetsbaarheden in (hoog-risico) organisaties vanuit het perspectief van de opponent. Het geeft inzicht in de werkwijze van de tegenstander en in het beveiligingsniveau van de organisatie. Met dit inzicht kunnen op strategisch-, tactisch- en operationeel niveau beleidsbeslissingen worden aangescherpt en kan de veiligheid binnen de organisatie verder worden vergroot.