Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Aan de Voorzitter van de Tweede kamer der Staten-Generaal
Postbus 20018
2500 EA Den Haag

Ons kenmerk
951ac9e8-or1-1.3

Uw kenmerk

Bijlagen
1

Datum 23 december 2022
Betreft Beantwoording vragen Leijten en Van Dijk (SP) inzake spionage met gebruik van Pegasus- of vergelijkbare software

Hierbij bieden we u, mede namens de minister van Defensie, de antwoorden aan op de schriftelijke vragen die zijn gesteld door de leden Leijten en Van Dijk (SP) over spionage met gebruik van Pegasus- of vergelijkbare software. Deze vragen werden ingezonden op 10 november 2022, met als kenmerk 2022Z21645.

De minister van Binnenlandse Zaken en Koninkrijksrelaties,

Hanke Bruins Slot

De minister van Justitie en Veiligheid,

D. Yeşilgöz-Zegerius

2022Z21645

Vragen van de leden Leijten en Jasper van Dijk (beiden SP) aan de ministers van Binnenlandse Zaken en Koninkrijksrelaties, van Justitie en Veiligheid en van Defensie over spionage met gebruik van Pegasus- of vergelijkbare software (ingezonden 10 november 2022).

Vraag 1
Klopt het dat er geen onderscheid in veiligheidsrisico wordt gemaakt tussen ministers, topambtenaren en ander rijkspersoneel als het gaat om digitale veiligheid? Geldt dit beleid Rijksbreed? Zo ja, waarom wordt er geen onderscheid gemaakt, terwijl het zeer goed voorstelbaar is dat hooggeplaatste functionarissen over meer essentiële informatie beschikken en daardoor eerder het doelwit van spionage of een hack zullen zijn?

Iedere overheidsorganisatie is in eerste plaats zelf verantwoordelijk voor haar digitale veiligheid, en die van haar medewerkers. Voor zowel Rijksoverheden als medeoverheden biedt onder meer de Baseline Informatiebeveiliging Overheid (BIO) wel een aantal kaders en regels. De BIO bevat een palet aan maatregelen die iedere overheidsorganisatie moet nemen, inclusief een risicobeoordeling. De BIO richt zich hiermee niet alleen op specifieke personen of middelen, maar leidt voor iedere organisatie tot een integrale risicogebaseerde aanpak. Voor de Rijksoverheid zien de Audit Dienst Rijk (ADR) en de Algemene Rekenkamer (ARK) hierop toe. CISO Rijk monitort, vanuit het CIO-stelsel Rijk, de implementatie van beleid op het gebied van dataveiligheid bij de departementen.

Hierbij geldt nog een specifieke set regels voor omgang met gerubriceerde informatie bij de Rijksoverheid. Dit is vastgelegd in het Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie (VIRBI), dat voorschrijft hoe met gerubriceerde informatie moet worden omgegaan. Dit geldt voor alle rijksambtenaren die vanuit hun werk incidenteel of structureel met gerubriceerde informatie moeten werken. Om het werken met dergelijke informatie mogelijk te maken worden er ook onder meer technische, facilitaire en organisatorische maatregelen genomen, en worden er specifieke middelen en netwerken ter beschikking gesteld om veilig met dergelijke informatie te kunnen werken.

Het gaat hier om kaders die in overeenstemming met de ministerraad zijn vastgesteld om te kunnen waarborgen dat de ministers hun verantwoordelijkheid voor de digitale veiligheid en een zorgvuldige omgang met gerubriceerde informatie waar kunnen maken. Bij hun aantreden krijgen bewindspersonen instructies over veiligheidsrisico's. In het 'Blauwe Boek' worden bewindspersonen gewezen op het Voorschrift Informatiebeveiliging Rijksdienst/Bijzondere Informatie (VIR-BI).[1] Ook krijgen zij middelen aangeboden zoals telefoons.

[1] Het Blauwe Boek, Handboek voor bewindspersonen; www.rijksoverheid.nl/documenten/richtlijnen/2022/01/25/handboek-voor-bewindspersonen

Vraag 2
Deelt u de mening van de beveiligingsspecialist die stelt dat het met het huidige beveiligingsniveau niet te achterhalen is of digitale apparatuur gehackt is met geavanceerdere hacksoftware zoals Pegasus? Kunt u uw antwoord uitgebreid toelichten?

In de in het antwoord op vraag 1 genoemde Baseline Informatiebeveiliging Overheid (BIO) worden drie beveiligingsniveaus onderkend, de zogenaamde basisbeveiligingsniveaus (BBN). Er is sprake van basisbeveiligingsniveau 2 wanneer er wordt gewerkt met (departementaal) vertrouwelijke informatie. In dat geval gaat de BIO uit van het concept *'assume breach'*. In feite houdt men er rekening mee dat een systeem vroeg of laat kan worden binnengedrongen door een geavanceerde kwaadwillende actor. Dat betekent dat maatregelen zoals detectie moeten worden ingeregeld, zodat achteraf effectief kan worden opgetreden. Zoals ook toegelicht in het antwoord op vraag 1 zijn departementen zelf verantwoordelijk voor het implementeren van relevante maatregelen zoals detectiemechanismen.

Garanties zijn echter niet te geven. Dat geldt zeker voor mobiele telefoons, waar binnendringsoftware zoals Pegasus op is gericht. Er is sprake van een continue wedloop van geavanceerde digitale actoren die hun werkwijzen zo aanpassen dat ze niet of moeilijk gedetecteerd kunnen worden. Bovendien maakt een mobiele telefoon per definitie gebruik van een publiek netwerk en is er beperkte controle mogelijk op de software die aanwezig is op een telefoon en is detectie van *malware* op een telefoon ingewikkeld. De AIVD adviseert daarom terughoudend te zijn met het voeren van (bedrijfs)gevoelige gesprekken via of in de aanwezigheid van een mobiele telefoon.

Vraag 3
Gaat u de beveiligingsmaatregelen verhogen? Kunt u uw antwoord toelichten?

Het kabinet neemt de statelijke dreiging en risico's rondom digitale veiligheid bij de overheid serieus. Dat betekent dat het stelsel van maatregelen continu in ontwikkeling blijft. Informatiebeveiliging bij de overheid is dan ook een belangrijk element in de Werkagenda waardengedreven digitalisering en de Nederlandse Cyber Security Strategie, waaruit verschillende acties volgen. Voor de gehele overheid worden wettelijke eisen voor veiligheid ingericht, ook in lijn onder meer met de Europese richtlijn voor Netwerk- en Informatiebeveiliging (NIB). Het gevolg hiervan zal zijn dat de hiervoor genoemde BIO in de wet als eis geborgd zal zijn. Er wordt verder generiek toezicht ingericht en ook dit wordt via een wettelijke verankering geborgd.

Vraag 4
Wordt er naar aanleiding van nieuwe beschikbare informatie over landen die zich schuldig maken aan ernstige schendingen van mensenrechten of internationaal humanitair recht een nieuwe afweging gemaakt of de inzet van bepaalde software nog gerechtvaardigd is, als blijkt dat dergelijke landen gebruik maken van dezelfde software?

Het is van belang dat opsporings-, inlichtingen- en veiligheidsdiensten beschikken over effectieve bevoegdheden voor het uitvoeren van hun wettelijke taak. Die bevoegdheden worden vormgegeven door de Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017) en de Wet Computercriminaliteit III. Daarin

zijn naast de bevoegdheid van het binnendringen in een geautomatiseerd werk ook de bijbehorende waarborgen verankerd. Voor de uitvoering van deze bevoegdheden kunnen politie, AIVD en MIVD gebruik maken van specifieke soft- en hardware. De rechtmatigheid daarvan volgt dus uit juridische grondslagen met bijbehorende waarborgen uit hierboven genoemde wetgeving. De rechtmatigheid van de inzet van een bevoegdheid wordt niet bepaald door de gebruikte technologie maar door het geheel van juridische en operationele aspecten van de specifieke casus die gewogen wordt.

Zoals aangegeven in de Kamervragen van de leden Omtzigt (CDA) en van Dijk (SP) (kamerstuk 2022Z10593) mogen leveranciers van binnendringsoftware die wordt ingekocht door opsporingsdiensten niet leveren aan dubieuze regimes. Het gaat om landen die zich schuldig maken aan ernstige schendingen van mensenrechten of internationaal humanitair recht.[2] Om deze reden voert de politie een toets uit voordat over wordt gegaan tot de aanschaf van binnendringsoftware. In deze toets wordt de leverancier gevraagd niet te hebben geleverd aan landen waartegen vanuit de EU of de VN restrictieve sancties bestaan en wordt gecontroleerd of in het land waar de leverancier is gevestigd een exportcontroleregime bestaat waar het respecteren van mensenrechten een onderdeel is in de beoordeling voor het verstrekken van een exportvergunning.[3] De politie past dit beleid toe en eist van leveranciers een bevestiging dat niet aan dergelijke landen wordt geleverd. Aanvullend hierop wordt door de politie deze toets periodiek herhaald. De Wet computercriminaliteit III is recentelijk geëvalueerd en naar verwachting kan in het voorjaar 2023 de beleidsreactie aan uw Kamer worden gezonden.[4]

De inlichtingen- en veiligheidsdiensten kunnen ten behoeve van hun wettelijke taakuitvoering en omgeven door waarborgen bijzondere bevoegdheden inzetten. Over de wijze waarop deze organisaties gebruik maken van hun wettelijk toegekende bijzondere bevoegdheden, en over de afwegingen die daarbij worden gemaakt, kan in het openbaar geen mededeling worden gedaan.

Vraag 5
Deelt u de mening dat het gebruik van dergelijke software de democratische rechtstaat veel schade kan berokkenen, als het wordt ingezet tegen de eigen onschuldige inwoners of het gebruikt wordt om functionarissen van andere lidstaten te bespioneren? Zo nee, kunt u uw antwoord uitgebreid toelichten?

Het kabinet acht het onrechtmatig gebruik van binnendringsoftware onaanvaardbaar. Dit geldt ook wanneer het om onrechtmatige inzet tegen advocaten, politici, mensenrechtenverdedigers en journalisten gaat. Naast de nationale wetgeving is ook het Europees Verdrag van de Rechten van de Mens belangrijk in de weging van de rechtmatigheid. In het geval van onrechtmatig gebruik kan de inzet van dit soort software de democratische rechtsstaat schade berokkenen.

Het uitvoeren van de bevoegdheid tot binnendringen in een geautomatiseerd werk door Nederlandse overheidsdiensten is aan strenge voorwaarden en stevige waarborgen gebonden. Deze bevoegdheid kan alleen worden ingezet wanneer

[2] Handelingen I 2017/18, 34, item 5, p. 29.
[3] Kamerstukken, TK, 2018/2019, Aanhangsel van de Handelingen nummer 3537.
[4] Kamerstukken TK, 2021-2022, 34372, nr. 30

minder ingrijpende bevoegdheden niet bruikbaar zijn voor het gestelde doel, en de inzet noodzakelijk en proportioneel is. Voor de voorwaarden en waarborgen die gelden bij de eventuele inzet van binnendringsoftware wordt verwezen naar Kamervragen van de leden Omtzigt (Omtzigt) en Van Dijk (SP) of de samenvatting in antwoord op vraag 6.[5] Tegelijkertijd is de rechtmatige inzet van de bevoegdheid tot binnendringen in een geautomatiseerd werk van belang voor onze democratische rechtsstaat. Criminelen en kwaadwillende statelijke actoren zijn een reële bedreiging voor onze maatschappelijke orde, de nationale veiligheid, de mogelijkheid van burgers om vrijelijk van hun rechten te genieten en ons verdienvermogen.

Vraag 6
Deelt u de mening dat het wenselijk is dat deze software ofwel in het geheel niet gebruikt wordt, dan wel aan strikte regels en toezicht onderworpen wordt, zowel op nationaal als internationaal niveau? Zo nee, waarom niet?

Gegeven het belang van de rechtmatige inzet van binnendringsoftware voor onze democratische rechtsstaat zoals beschreven in antwoord op vraag 5 is het onwenselijk om het gebruik van binnendringsoftware categoriaal te verbieden. Ook deelt het kabinet de opvatting dat inzet van dergelijke software enkel wenselijk is wanneer deze is gebonden aan strikte regels omtrent proportionaliteit, subsidiariteit en noodzakelijkheid, en er sprake is van onafhankelijk toezicht. Effectief en gedetailleerd toezicht op de inzet van middelen door opsporings-, inlichtingen- en veiligheidsdiensten kan echter, gezien de benodigde toegang tot bijzondere informatie, enkel nationaal vormgegeven zijn.

In de opsporing vindt de uitvoering van de binnendringbevoegdheid plaats onder het gezag van de officier van justitie. Die houdt voor, tijdens en na de inzet door de politie toezicht op de rechtmatigheid van de opsporing en daarmee op de uitvoering van deze bevoegdheid. Een officier van justitie mag een bevel voor het binnendringen in een geautomatiseerd werk slechts geven na voorafgaande machtiging door een rechter-commissaris. Deze rechter toetst een voorgenomen inzet eveneens vooraf. Na afronding van een inzet wordt deze door de politie in processen-verbaal verantwoord. Tijdens de behandeling ter terechtzitting kan de rechter de rechtmatigheid van de inzet beoordelen. De afweging van de proportionaliteit en subsidiariteit van de inzet van de software is in eerste instantie aan de officier van justitie, die na machtiging van de rechter-commissaris bevoegd is tot het bevelen van het onderzoek in een geautomatiseerd werk. Deze afweging wordt getoetst door de Centrale Toetsingscommissie bij het OM die het College van Procureurs-generaal adviseert.

De Inspectie Justitie en Veiligheid (IJenV) houdt eveneens toezicht op de inzet van binnendringsoftware door het technisch team van de politie. De afweging van het Openbaar Ministerie valt buiten de bevoegdheid van de IJenV. Toezicht op het Openbaar Ministerie wordt op grond van artikel 122 van de wet RO door de procureur-generaal van de Hoge Raad der Nederlanden verricht.

De AIVD en de MIVD mogen onder strikte wettelijke voorwaarden bijzondere bevoegdheden inzetten ten behoeve van de nationale veiligheid. Deze bevoegdheden zijn aan voorwaarden gebonden, die zijn vastgelegd in de Wiv 2017. De Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten

[5] Kamerstukken TK, 2021-2022, Aanhangsel 3252

(CTIVD) houdt toezicht op de juiste toepassing van die wet. De Toetsingscommissie Inzet Bevoegdheden (TIB) richt zich op toetsing voorafgaand aan de inzet van bepaalde bevoegdheden, waaronder het binnendringen in een geautomatiseerd werk. De CTIVD houdt toezicht tijdens en na afloop van inzet van een bevoegdheid.

Verder kan worden gewezen op de internationale afspraken die zijn gemaakt in het kader van toezicht op de handel in binnendringsoftware, zoals de recent geactualiseerde dual-use verordening van de Europese Unie en het Wassenaar Arrangement.

Vraag 7
Deelt u de mening dat globale transparantie over of dergelijke software aangekocht is en gebruikt wordt wenselijk is, zodat het parlement de controlerende taak kan uitvoeren? Kunt u uw antwoord uitgebreid toelichten?

In de opsporing worden ten behoeve van de transparantie jaarlijks statistieken van het gebruik van binnendringsoftware openbaar gemaakt. Het verstrekken van informatie aan derden over welke specifieke software de politie beschikt en gebruikt bij de inzet van deze bijzondere opsporingsbevoegdheid, brengt onaanvaardbare risico's met zich mee voor de inzetbaarheid van die middelen en daarmee het opsporingsbelang. De verwerving van binnendringsoft- en hardware vindt bij de politie onder geheimhouding plaats. Het is voor de afscherming van middelen en methodieken niet mogelijk om openbaar inzicht te geven in welke software de politie gebruikt bij de uitvoering van deze bevoegdheid.

Ook voor de AIVD en de MIVD is transparantie belangrijk. Daarom publiceren de diensten een openbaar jaarverslag en wordt waar mogelijk in de openbaarheid verantwoording afgelegd over het werk van de inlichtingen- en veiligheidsdiensten. Tegelijkertijd zijn beide diensten ook wettelijk gehouden aan geheimhouding, onder andere over de werkwijze. Dat geldt dus ook voor de inzet van de bevoegdheid tot het binnendringen in een geautomatiseerd werk. De CTIVD en TIB houden toezicht op de taakuitvoering van de diensten. De openbare (jaar)verslagen van de CTIVD en de TIB worden met de Kamer en het publiek gedeeld. Parlementaire controle op de taakuitvoering van de inlichtingen- en veiligheidsdiensten vindt, wanneer nodig vanwege de geheime aspecten, via de geëigende kanalen plaats.

Vraag 8
Kunt u aangeven of volgens u het gebruik van dit soort software van Israëlische makelij past binnen de aangenomen Kamermotie waarin uitdrukkelijk de wens is uitgesproken om dergelijke apparatuur niet aan te schaffen uit landen zoals Israël?

In de verzamelbrief politie van 19 oktober jl. wordt geschetst hoe uitvoering wordt gegeven aan de motie Van Nispen waarin de regering wordt verzocht bij aanbestedingen voor apparatuur, zoals afluisterapparatuur, drones en ANPR-camera's, aan veiligheidsvereisten een zwaarder belang toe te kennen en te streven naar apparatuur uit Nederland of op z'n minst uit landen binnen de Europese Unie.[6] Zoals in de verzamelbrief is gemeld, moeten Nederlandse overheden en uitvoeringsdiensten zo nodig kunnen beschikken over kwalitatief

[6] Kamerstukken TK, 2022-2023, 29 628, 1127

hoogwaardige producten en diensten, ook van buitenlandse leveranciers, of over producten en diensten die deels in het buitenland zijn ontwikkeld of geproduceerd. Het uitgangspunt is dat het gebruik van apparatuur en programmatuur veilig moet zijn en dat eventuele risico's beperkt en/of gemonitord worden. Er kunnen bijvoorbeeld technische beveiligings- of organisatorische maatregelen worden getroffen binnen de eigen organisatie. Ook kunnen strenge eisen gesteld worden aan de beveiliging van producten en diensten en kunnen ondernemers gevestigd in bepaalde landen uitgesloten worden van aanbestedingsprocedures. Voorgaande wordt bij alle eventuele aanschaf van binnendringsoftware in acht genomen.

Specifiek in het kader van binnendringsoftware kan ten eerste worden gewezen op de specifieke regelgeving voor de aanschaf van binnendringsoftware genoemd in antwoord op vragen 3 en 4. Ten tweede wordt het doel onderschreven om het betreden van de markt van dergelijke software tot een minimum te beperken. Ten derde dient een technisch hulpmiddel beveiligd te zijn tegen wijziging van geregistreerde gegevens en kennisneming hiervan door onbevoegden.