Toezichtsrapport

Over de inzet van de hackbevoegdheid door de AIVD en MIVD in 2015

CTIVD nr. 53

8 maart 2017

Commissie van Toezicht
op de Inlichtingen- en
Veiligheidsdiensten

Commissie van Toezicht
op de Inlichtingen- en
Veiligheidsdiensten

CTIVD nr. 53

TOEZICHTSRAPPORT

**over de inzet van de hackbevoegdheid
door de AIVD en MIVD in 2015**

Inhoudsopgave

Commissie van Toezicht
op de Inlichtingen- en
Veiligheidsdiensten

CTIVD nr. 53

SAMENVATTING

**van het toezichtsrapport
over de inzet van de hackbevoegdheid
door de AIVD en MIVD in 2015**

De AIVD en de MIVD hebben de wettelijke bevoegdheid te hacken, dat wil zeggen binnen te dringen in geautomatiseerde werken. In dit toezichtsrapport komt de CTIVD tot de conclusie dat de AIVD en de MIVD doorgaans weloverwogen te werk gaan bij de inzet daarvan. Hacken blijkt een effectieve bevoegdheid, in die zin dat de inzet in de regel heeft geleid tot resultaten in het belang van de nationale veiligheid, die niet op een andere manier hadden kunnen worden behaald.

De AIVD en de MIVD zijn in het overgrote deel van de tientallen onderzochte hackoperaties in 2015 rechtmatig te werk gegaan. De diensten zijn zich in het algemeen bewust van de ernstige inmenging in de rechten en de belangen van betrokkene(n) die de inzet van de hackbevoegdheid met zich mee kan brengen. Daarbij moet in eerste plaats worden gedacht aan het recht op de bescherming van de persoonlijke levenssfeer, maar ook aan het belang van het bewaken van de integriteit van ICT-systemen.

Bij een aantal werkwijzen worden echter tekortkomingen gesignaleerd. De belangrijkste daarvan is dat de diensten structureel nalaten gegevens te vernietigen op momenten dat dit wel zou moeten. Bovendien hanteren beide diensten – ondanks eerdere toezeggingen aan de Tweede Kamer daarover – nog steeds geen (buitenwettelijke) bewaartermijnen voor door middel van een hack gekopieerde en opgeslagen ongeëvalueerde gegevens. Ook wordt nagelaten niet relevant beoordeelde en ten onrechte verwerkte gegevens te vernietigen. Hiermee handelen de diensten onrechtmatig.

Tekortkomingen bestaan ook in de omgang met onbekende kwetsbaarheden, zogenaamde *'zero day's'*. De werkwijze en de relevante afwegingen voor het al dan niet melden daarvan zijn intern niet uitgewerkt en vastgelegd. Bovendien vindt van de gemaakte afwegingen geen centrale verslaglegging plaats. Hierdoor is interne controle en extern toezicht op de gemaakte afwegingen niet goed mogelijk. Deze werkwijze is onzorgvuldig.

Ook de toestemmingsprocedure voor verlengingen van de inzet van de hackbevoegdheid schiet tekort. Door de inrichting van de administratieve processen wordt bij de AIVD niet de laatste stand van zaken in een onderzoek in de onderbouwing van het verzoek om verlenging van de toestemming meegenomen. Dit is onzorgvuldig. Bij de MIVD wordt de verlenging niet ter goedkeuring aan de minister voorgelegd. Daardoor kan het gebeuren dat de operatie na verloop van tijd een ander verloop of karakter krijgt dan waarvoor de minister aanvankelijk toestemming heeft gegeven. Dit wordt in één geval als onrechtmatig beoordeeld.

In dit rapport wordt tevens aandacht gevestigd op een aantal incidentele onrechtmatigheden. Dit betrof het te algemeen formuleren van het target en/of de geautomatiseerde werken waarop de inzet was gericht. Bovendien is in een beperkt aantal gevallen buiten de reikwijdte van de gegeven toestemming getreden. In één geval heeft de MIVD ongeëvalueerde gegevens verstrekt aan een buitenlandse dienst zonder de vereiste ministeriële toestemming hiervoor.

Commissie van Toezicht
op de Inlichtingen- en
Veiligheidsdiensten

CTIVD nr. 53

TOEZICHTSRAPPORT

**over de inzet van de hackbevoegdheid
door de AIVD en MIVD in 2015**

1 Inleiding

De hackbevoegdheid

De Algemene Inlichtingen- en Veiligheidsdienst (hierna: AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (hierna: MIVD) zijn bevoegd tot het binnendringen in geautomatiseerde werken. Deze bijzondere bevoegdheid staat beschreven in artikel 24 van de Wet op de inlichtingen en veiligheidsdiensten 2002 (Wiv 2002). Deze bevoegdheid wordt in het dagelijks taalgebruik van beide diensten en het in het politieke debat de 'hackbevoegdheid' genoemd. De CTIVD sluit hierbij aan. Voorbeelden van hacken zijn het binnendringen in een smartphone, e-mailaccount, laptop of een server. Bijzondere bevoegdheden, zoals hacken, worden doorgaans ingezet tegen zogenaamde targets of onderzoekssubjecten. Dit zijn personen of organisaties waarnaar de diensten op basis van de veiligheids- of inlichtingentaak onderzoek doen. In dit rapport zal hiervoor de overkoepelende term target worden gebruikt.

De aanleiding van het onderzoek

De hackbevoegdheid is al in eerdere rapporten van de CTIVD (als onderdeel van een groter onderzoeksterrein) aan de orde geweest. De belangrijkste hiervan zijn toezichtsrapport 38 inzake gegevensverwerking op het gebied van telecommunicatie door de AIVD en de MIVD en toezichtsrapport 39 met betrekking tot de onderzoeksactiviteiten door de AIVD op sociale media. De bevindingen in deze rapporten en de voortgaande technologische en maatschappelijke ontwikkelingen die ertoe leiden dat persoonlijke informatie steeds meer digitaal beschikbaar is, hebben aanleiding gegeven tot dit nadere diepteonderzoek.[1]

De reikwijdte van het onderzoek

De CTIVD heeft op 17 maart 2016 aangekondigd een diepteonderzoek naar de toepassing van de hackbevoegdheid door de AIVD en de MIVD te gaan verrichten.[2] Het onderzoek richt zich op *fysieke hacks*, waarbij het geautomatiseerd werk (tijdelijk) in handen is van één van de diensten en *hacks op afstand*, dat wil zeggen dat buiten het directe fysieke bereik wordt binnengedrongen, bijvoorbeeld via het internet. **Het onderzoek richt zich op de vraag of de AIVD en de MIVD de hackbevoegdheid in de onderzoeksperiode (1 januari 2015 tot 17 maart 2016) op een rechtmatige en zorgvuldige wijze hebben uitgeoefend.**

---

[1] Toezichtsrapport van de CTIVD nr. 38 inzake gegevensverwerking op het gebied van telecommunicatie door de AIVD en de MIVD, *Kamerstukken II* 2013/14, 29 924, nr. 105 (bijlage) en toezichtsrapport van de CTIVD nr. 39 inzake onderzoek door de AIVD op sociale media, *Kamerstukken II* 2013/2014, 29 924, nr. 114 (bijlage). Hierna aangehaald als: toezichtsrapporten nr. 38 en 39 van de CTIVD.

[2] Aanbiedingsbrief, beschikbaar op www.ctivd.nl

De methodiek

In bijlage I van dit rapport wordt verantwoording afgelegd over de in dit onderzoek gekozen methodiek. Er is kort gezegd onderzoek gedaan naar hackoperaties van de diensten die zijn gestart in het kalenderjaar 2015 en waarin het daadwerkelijk binnendringen voor de startdatum van dit onderzoek (17 maart 2016) is geslaagd. Omdat de MIVD de hackbevoegdheid op relatief bescheiden schaal inzet, zijn alle geslaagde operaties die de MIVD in de onderzoeksperiode heeft uitgevoerd bij het onderzoek betrokken. Uit de geslaagde operaties die de AIVD heeft uitgevoerd, is een selectie gemaakt op basis van de bijzondere feiten en omstandigheden die deze operaties kenmerkten. Hierbij moet worden gedacht aan specifieke (groepen) personen waartegen de hackbevoegdheid is uitgeoefend, zoals verschoningsgerechtigden, non-targets en derden, maar ook aan operaties waarbij gegevens ongericht (integraal) zijn overgenomen (gekopieerd en opgeslagen). Ook zijn operaties die volgens de AIVD bijzonder effectief zijn geweest, in de selectie opgenomen.[3] Deze selectie is daarna nog aangevuld met operaties op basis van het type hack (de gevolgde modus operandi) en de aandachtsgebieden van de AIVD.

De beoordeling van praktijk en werkwijze

In bijlage II bij dit rapport is het juridisch toetsingskader uiteengezet. Wanneer dat van toepassing is, wordt daarin ook de verbinding gelegd met het thans aanhangige wetsvoorstel Wiv 20..., de nieuwe Wet op de inlichtingen-en veiligheidsdiensten. Per hoofdstuk of onderwerp zullen in dit rapport de relevante rechtsregels uit het toetsingskader worden aangehaald. Op grond van dit kader wordt beoordeeld of een praktijk of werkwijze rechtmatig en zorgvuldig is geweest. Het oordeel *onzorgvuldig* houdt in dat de motivering voor de inzet van de hackbevoegdheid weliswaar een gebrek vertoont, maar de CTIVD op basis van eigen nader onderzoek tot de conclusie is gekomen dat de inzet van de bevoegdheid voldoet aan de vereisten van noodzakelijkheid, proportionaliteit en subsidiariteit. Van een onzorgvuldige werkwijze is sprake als deze rechtens tekortschiet, maar de risico's daarvan zich niet of nauwelijks hebben gerealiseerd. Bij het oordeel *onrechtmatig* is sprake van strijdigheid met de wet- of regelgeving of een zodanig gebrekkige motivering van de inzet dat herstel hiervan niet mogelijk is. Hierbij wordt rekening gehouden met de ernst van de inbreuk en aard van de belangen van de betrokkene(n), waarop een inbreuk wordt gemaakt.

Het openbare toezichtsrapport en de geheime bijlage

In dit toezichtsrapport is gekozen voor een systeemmatige benadering waar dat mogelijk was. Dit betekent dat eerst is gekeken naar beleid, werkwijzen en (vaste) praktijk en vervolgens naar de individuele geselecteerde operaties. De systeemmatige benadering heeft vooral haar beslag gekregen in Hoofdstuk 2 (algemeen beeld en effectiviteit), Hoofdstuk 5 (de toestemmingverlening) en Hoofdstuk 7 (het overnemen, beoordelen en vernietigen van gegevens). Voorts zijn naar vaste werkwijze van de CTIVD, alle geconstateerde onrechtmatigheden en onzorgvuldigheden in het openbare toezichtsrapport opgenomen. Vanwege de bescherming van de nationale veiligheid worden nadere details van een aantal operaties in de geheime bijlage beschreven. Deze geheime bijlage is beperkt in omvang (drie pagina's).

Het verloop van het onderzoek

Het onderzoek is met het opstellen van dit rapport afgerond op 23 december 2016. De ministers van Binnenlandse Zaken en Koninkrijksrelaties (hierna: BZK) en van Defensie zijn in de gelegenheid gesteld te reageren op de in het toezichtsrapport opgenomen bevindingen. De reactie van de minister van BZK is op 24 februari 2017 en de reactie van de minister van Defensie is op 22 februari 2017 ontvangen. Deze reacties hebben geleid tot een nader overleg met de MIVD en tot enkele wijzigingen, waarna het toezichtsrapport op 8 maart 2017 is vastgesteld.

---

[3] De redenen hiervoor worden in Hoofdstuk 2 en Bijlage I nader uiteengezet.

De leeswijzer

Het rapport is volgordelijk opgebouwd. Dat wil zeggen dat na het algemeen beeld (Hoofdstuk 2) en een korte weergave van het werkproces (Hoofdstuk 3) de volgorde van dit werkproces wordt aangehouden om de verschillende onderdelen van de inzet van de hackbevoegdheid te bespreken. Hoofdstuk 4 beschrijft de aanloop naar de inzet: het vooronderzoek en het opstellen van de motivering ten behoeve van een verzoek om toestemming, zowel in het algemeen als met betrekking tot bijzondere situaties, zoals de inzet van de hackbevoegdheid tegen organisaties, verschoningsgerechtigden, non-targets, derden respectievelijk in het geval sprake is van bijschrijvingen. In hoofdstuk 5 wordt ingegaan op de toestemmingsverlening, in Hoofdstuk 6 op de uitvoering van de hack en in Hoofdstuk 7 op de verdere verwerking van gegevens. Hoofdstukken 8 bespreekt het verstrekken van uit hacks afkomstige ongeëvalueerde gegevens. Tot slot worden in Hoofdstuk 9 en 10 de conclusies en aanbevelingen uit dit rapport weergegeven.

2 Algemeen beeld en effectiviteit

Algemeen beeld

De CTIVD constateert dat de AIVD en MIVD doorgaans weloverwogen en rechtmatig te werk gaan bij de uitvoering van de hackbevoegdheid. Dit komt allereerst doordat de diensten zich bewust zijn van de grote inmenging die met de hackbevoegdheid kan worden gemaakt in de grondrechten en belangen van de betrokkene(n). Bij die grondrechten moet in de eerste plaats worden gedacht aan de bescherming van de persoonlijke levenssfeer. De inmenging die plaatsvindt in de persoonlijke levenssfeer van betrokkene(n) kan doorgaans worden vergeleken met een doorzoeking en/of een tap. In het kader van de hackbevoegdheid is ook het bewaken van de integriteit van ICT-systemen een relevant belang, omdat voor het goed functioneren van de samenleving veilige en betrouwbare ICT-systemen onmisbaar zijn geworden. Deze integriteit wordt met name aangetast door het binnendringen zelf, maar kan ook het aanbrengen of in stand houden van kwetsbaarheden in die systemen betreffen. Daarnaast geldt dat hacken in de praktijk doorgaans arbeidsintensief en bewerkelijk is, een grote mate van deskundigheid vereist en het daadwerkelijk binnendringen niet altijd succesvol is. Deze factoren zorgen ervoor dat in de interne besluitvormings- en werkprocessen wegingsmomenten zijn ingebouwd voordat tot de daadwerkelijke inzet van de hackbevoegdheid wordt overgegaan. Daarmee is een werkwijze ontstaan die de rechtmatige inzet en uitvoering bevordert.

Effectiviteit

De CTIVD heeft zich in dit onderzoek de vraag gesteld of, en zo ja in welke mate, de hackbevoegdheid vanuit de nationale veiligheid bezien effectief is. Hierbij wordt gedoeld op effectiviteit als onderdeel van de rechtmatigheidstoets. Indien een bevoegdheid in bepaalde gevallen naar algemene ervaring weinig relevante opbrengsten oplevert, kan dit in (soortgelijke) concrete gevallen immers van invloed zijn op de vraag of de inbreuk die met deze bevoegdheid wordt gemaakt op de grondrechten en de belangen van betrokkene(n) wel opweegt tegen het doel waarvoor de bevoegdheid wordt ingezet (proportionaliteit).

Een eenduidige omschrijving van effectiviteit is niet voorhanden. Aan de (diverse) teams bij de diensten is daarom voorgelegd hoe zij dat zouden beschrijven. De gemene deler in de reacties was dat de hackbevoegdheid effectief is, omdat hiermee grote hoeveelheden waardevolle informatie met een hoog waarheidsgehalte kunnen worden verkregen, zonder dat daarvoor direct risico voor natuurlijke personen (agenten, informanten) ontstaat. Eenmaal in het geautomatiseerd werk binnengedrongen, kan de verlangde concrete informatie met meer precisie worden geselecteerd en gekopieerd, waarmee de inbreuk op de persoonlijke levenssfeer kan worden beperkt.

De CTIVD vindt voor (de onderbouwing van) deze redenering bevestiging in haar onderzoek. In een groot deel van de operaties zijn een of meer elementen van deze omschrijving van effectiviteit aangetroffen. Er zijn ook operaties aan te wijzen die duidelijk worden gekenmerkt door een bijzonder hoge mate van effectiviteit ten behoeve van de nationale veiligheid. Daarbij waren de specifieke mogelijkheden met het middel hacken vaak doorslaggevend voor het resultaat, in die zin dat de resultaten met geen enkele andere bevoegdheid hadden kunnen worden verkregen. Een voorbeeld daarvan is de situatie waarin twee gebruikers versleuteld met elkaar communiceren. Deze in transitie versleutelde communicatie is na het onderscheppen daarvan vaak niet leesbaar te maken. De hackbevoegdheid kan hier een oplossing in bieden.

Onrechtmatig- en onzorgvuldigheden

De constatering dat de hackbevoegdheid in de onderzoeksperiode doorgaans effectief is en rechtmatig is uitgeoefend, betekent echter niet dat in dit onderzoek geen onrechtmatig- en onzorgvuldigheden zijn aangetroffen. De geconstateerde structurele tekortkomingen, in aantal beperkt van omvang, worden over het algemeen veroorzaakt door dienstbrede werkwijzen die tekort schieten. De aangetroffen incidentele onrechtmatig- en onzorgvuldigheden hebben een gedifferentieerdere oorzaak. Zij laten zich in het algemeen verklaren door tijdsdruk tijdens de uitvoering na het binnendringen of onbekendheid met de juridische randvoorwaarden die specifiek gelden voor het inzetten van de hackbevoegdheid.

3 De hackbevoegdheid en het werkproces

De hackbevoegdheid

Bij hacken gaat het om het binnendringen in een geautomatiseerd werk. Binnendringen houdt in dat tegen de wil, zonder toestemming van de rechthebbende, in een geautomatiseerd werk naar binnen wordt gegaan. Een geautomatiseerd werk is een inrichting die bestemd is om langs elektronische weg gegevens op te slaan, te verwerken en over te dragen. Hierbij wordt dezelfde definitie aangehouden als binnen het strafrecht.[4] Inrichtingen die niet aan deze drie cumulatieve voorwaarden voldoen, worden volgens de wetgever niet als geautomatiseerd werk aangemerkt. Dit betekent dat inrichtingen die enkel gegevens overdragen (denk aan een eenvoudig telefoontoestel) of opslaan (bijvoorbeeld een usb-stick) niet als geautomatiseerd werk worden beschouwd. Desktopcomputers en laptops, maar ook tablets en de huidige generatie smartphones worden wél als geautomatiseerd werk aangemerkt. In de wetsgeschiedenis bij de Wiv 2002 wordt aangegeven dat het in de praktijk in het bijzonder zal gaan om het binnendringen in (standalone) computers en computernetwerken, waaronder ook servers.

De AIVD en de MIVD mogen de hackbevoegdheid alleen inzetten indien en voor zover dat in het belang van de nationale veiligheid voor de goede uitvoering van de veiligheids- of inlichtingentaak noodzakelijk is. De inlichtingentaak houdt in het doen van onderzoek naar andere landen en het potentieel en de strijdkrachten van andere mogendheden ten behoeve van het Nederlandse buitenlands- en veiligheidsbeleid danwel in het belang van de internationale rechtsorde of ten behoeve van een juiste opbouw en een doeltreffend gebruik van de krijgsmacht. Dit onderzoek wordt verricht door de AIVD, tenzij er sprake is van onderwerpen met een militaire relevantie. In dat geval wordt het onderzoek doorgaans door de MIVD uitgevoerd. De veiligheidstaak houdt in het onderkennen van dreigingen voor het voortbestaan van de democratische rechtsorde dan wel voor de veiligheid of andere gewichtige belangen van de staat (AIVD), of voor de veiligheid en de paraatheid van de krijgsmacht (MIVD).

Het werkproces

Om de verschillende onderwerpen die in dit rapport aan de orde komen en de onderlinge verhouding daartussen weer te geven, wordt het werkproces bij de diensten bij het inzetten van de hackbevoegdheid hieronder kort beschreven. Deze beschrijving is gebaseerd op het binnen de diensten vastgelegde beleid en de tijdens het onderzoek vastgestelde praktijk.

Zo was bij beide diensten een formele Mandaatregeling van kracht die het toestemmingsniveau bepaalde. Bij de AIVD was voor de operationele teams tevens en aantal beleidsstukken over onder meer het toestemmingsniveau, de samenloop van bevoegdheden alsmede een werkinstructie beschikbaar. Bij de MIVD was in de onderzoeksperiode voor de operationele teams nog geen beleid of werkinstructie op het gebied van hacken vastgesteld.

De hackoperaties worden uitgevoerd door de Joint Sigint Cyber Unit (hierna: JSCU). De JSCU is een uitvoeringseenheid van de AIVD en MIVD gezamenlijk op het gebied van sigint en cyber. Doordat ook de JSCU bepaalde vaste werkwijzen hanteert, kan van de verschillende fases in het werkproces het volgende beeld worden geschetst

[4] Zie art. 80sexies Sr. De definitie wordt in de Wet computercriminaliteit III aangepast aan de (bredere) definitie uit het Cybercrimeverdrag. Deze definitie wordt in de Wiv 20.. overgenomen. Zie daarvoor ook Bijlage II, p. 6 en Zienswijze van de CTIVD op het wetsvoorstel Wiv 20.., bijlage II (november 2016) , p. 10, beschikbaar op www.ctivd.nl

Het vooronderzoek (zie verder Hoofdstuk 4)

In vrijwel alle gevallen beslissen bij zowel de AIVD als bij de MIVD de verantwoordelijke operationele teams of zij de hackbevoegdheid willen aanwenden. De operationele teams gaan vervolgens in overleg met de JSCU over de technische mogelijkheden van een hack. Indien er mogelijkheden bestaan, voert de JSCU hierna een zogenaamd vooronderzoek uit.

Het verzoek om toestemming (zie verder Hoofdstuk 4)

Als wordt besloten de hackbevoegdheid in te zetten, wordt een uitgebreide motivering voor het verzoek om toestemming door het team opgesteld, waarbij de JSCU meeleest met betrekking tot de technische kant van de operatie. Het verzoek om toestemming wordt doorgaans geschreven door de desbetreffende bewerker (AIVD) of analist (MIVD) van het operationele team.

Toestemming (zie verder Hoofdstuk 5)

AIVD

Het verzoek moet worden goedgekeurd door het team- en het unithoofd. Als het een fysieke hack betreft, waarbij het geautomatiseerd werk (tijdelijk) in handen van de dienst is, kan de operatie vervolgens worden uitgevoerd. De toestemming voor een fysieke hack wordt slechts voor een éénmalige inzet gegeven. Betreft het een hack op afstand, dat wil zeggen op een geautomatiseerd werk buiten het directe fysieke bereik van de dienst, bijvoorbeeld via internet, dan is de toestemming van de directeur-generaal (het hoofd) van de AIVD nodig. Nadat de directeur-generaal akkoord heeft gegeven wordt in de regel door de afdeling Juridische Zaken een samenvatting van het verzoek gemaakt. Deze samenvatting wordt tezamen met die van andere verzoeken driemaandelijks gebundeld aan de minister van BZK voor toestemming voorgelegd. In spoedgevallen wordt het verzoek in zijn geheel of mondeling aan de minister aangeboden. Het is de minister die de uiteindelijke toestemming moet geven voor een hack op afstand. De toestemming voor (eventuele) verlengingen voor hacks op afstand zijn bij de AIVD evenzeer op het niveau van de minister belegd.

MIVD

Bij de MIVD wordt in de toestemmingsprocedure geen onderscheid gemaakt tussen fysieke hacks en hacks op afstand. Alle opgestelde verzoeken worden na accordering van het teamhoofd, het bureauhoofd, het afdelingshoofd, de Stafafdeling Juridische Zaken en de directeur ter toetsing voorgelegd aan de Directie Juridische Zaken en de Secretaris-Generaal van het Ministerie van Defensie alvorens schriftelijk toestemming wordt verzocht aan de minister van Defensie. Als de hackbevoegdheid is aangevraagd voor plaatsen buiten gebruik van het ministerie van Defensie, is ook toestemming van de minister van BZK vereist. Voor (eventuele) verlengingen van zowel fysieke hacks als hacks op afstand is bij de MIVD de directeur bevoegd.

Bijschrijven (zie verder Hoofdstuk 4)

Met het zogenaamde bijschrijven worden andere geautomatiseerde werken bedoeld (van dezelfde persoon of organisatie), die een aanvulling zijn op of in de plaats treden van de in het initiële verzoek om toestemming genoemde geautomatiseerde werken. Deze bijschrijving moet voldoen aan de criteria die daarvoor in de toestemming voor de fysieke hack of de hack op afstand worden genoemd. Dit leidt ertoe dat nieuwe geautomatiseerde werken onder de toestemming kunnen vallen, zonder dat de minister om nadere toestemming wordt verzocht. Dit bijschrijven vindt plaats bij zogenaamde brede toestemmingen (bijvoorbeeld omdat op voorhand nog niet duidelijk is welke geautomatiseerde werken relevant zijn voor het onderzoek) of verzoeken die betrekking hebben op (geautomatiseerde werken van) nog ongekende leden van een organisatie.

Bij de AIVD worden de bijschrijvingen intern goedgekeurd door het unithoofd. Bij een eventuele verlenging van de hackoperatie, wordt de minister van BZK geïnformeerd over de geautomatiseerde werken of personen die bijgeschreven zijn onder het initiële verzoek.

Bij de MIVD beslist de betrokken analist of een geautomatiseerd werk bijgeschreven kan worden onder de initiële last. In de praktijk overlegt de analist vaak met het bureauhoofd en de Stafafdeling Juridische Zaken voordat de bijschrijving plaatsvindt. De bijschrijvingen worden vervolgens ook bij de aanvraag voor verlengingen gevoegd, die ter goedkeuring aan de directeur worden voorgelegd.

De uitvoering en de verwerking van gegevens (zie verder Hoofdstuk 6 t/m 8)

Als de toestemming op het juiste niveau is verkregen, kan de JSCU de hack uitvoeren. Over het algemeen worden de keuzes en technische handelingen met betrekking tot de hack grotendeels handmatig bijgehouden. Bij operationele keuzes in de uitvoering van de hack die de inhoud raken en voor het team van belang zijn, wordt met het team overleg gevoerd. Gegevens die met de operatie worden binnengehaald, worden (via applicaties) aan het team ter beschikking gesteld. De teams beoordelen of de informatie relevant is voor het onderzoek. Deze gegevens kunnen eventueel, met toepassing van de rechtsregel daarvoor, ook worden verstrekt aan buitenlandse diensten.

4 Het opstellen van het verzoek om toestemming

4.1 Vooronderzoek

Toetsingskader (paragraaf 4.1, p. 9, van bijlage II):

- Bij het verrichten van vooronderzoek ten behoeve van het binnendringen in een geautomatiseerd werk, mag geen kennis worden genomen van de inhoud van gegevens.

Bevindingen

Indien het operationeel team van oordeel is dat een hack noodzakelijk is, vindt overleg met de JSCU plaats over de technische mogelijkheden daarvan. De JSCU voert vervolgens doorgaans een vooronderzoek uit. In het kader van dit vooronderzoek schat de JSCU de benodigde capaciteit en de technische haalbaarheid (de slagingskans) in. Daarbij worden eventuele risico's zoals het aanrichten van schade aan ICT-systemen en het gevaar van onderkenning meegewogen.

In het vooronderzoek wordt in principe niet binnengedrongen, maar wordt het geautomatiseerd werk van buitenaf (de publieke kant) bekeken. In sommige gevallen wordt getest of bepaalde inloggegevens toegang verschaffen tot een geautomatiseerd werk. Met dit zogenoemde valideren van credentials wordt weliswaar formeel binnengedrongen, maar wordt geen kennis genomen van de gegevens op het geautomatiseerd werk. Het operationeel team krijgt alleen te weten of de credentials juist zijn. Deze praktijk wordt als zorgvuldig en rechtmatig beoordeeld. Er zijn geen situaties aangetroffen waarbij in het vooronderzoek kennis is genomen van de inhoud van gegevens.

4.2 Verzoeken om toestemming voor de inzet van de hackbevoegdheid in het algemeen

Als de operatie, gelet op de uitkomsten van het vooronderzoek en het belang voor de nationale veiligheid, voldoende prioriteit heeft om te worden uitgevoerd, stelt het operationele team een verzoek om toestemming op. Het verzoek om toestemming bevat de motivering voor de inzet van de hackbevoegdheid. Het belang van de motivering is gelegen in het toetsbaar vastleggen van de afwegingen die de diensten volgens de wet dienen te maken voordat een bijzondere bevoegdheid wordt ingezet. Het gaat daarbij om de noodzaak tot de inzet van de bevoegdheid, de vraag of de inbreuk op grondrechten en belangen van de betrokkene(n) opwegen tegen het doel van de inzet (proportionaliteit) respectievelijk of minder inbreukmakende middelen of werkwijzen voorhanden zijn (subsidiariteit).

De motivering dient zowel een intern als een extern belang. Intern is het een belangrijke waarborg dat door te motiveren stil wordt gestaan bij de vraag of de inzet echt noodzakelijk, proportioneel en subsidiair is. Ook dwingt het de opsteller te overwegen wat het doel is van de bijzondere bevoegdheid en welke inbreuk daarmee wordt gemaakt. Van belang is ook dat de uitvoering van de bevoegdheid (vaak) niet in handen ligt van diegene die het operationeel onderzoek verricht. Om de uitvoerder van voldoende richting en begrenzing te voorzien, moet in de motivering duidelijk worden aangegeven met welk concreet doel de bevoegdheid wordt ingezet en wat de reikwijdte van de te verkrijgen toestemming is.

De externe functie van de motivering is gelegen in de informatieverschaffing aan een ieder die minder bekend is met het concrete onderzoek, bijvoorbeeld de minister. In de motivering wordt duidelijkheid verschaft over de feiten en omstandigheden die tot het verzoek om toestemming hebben geleid. Aan de hand van de opgestelde motivering kan zowel de uiteindelijk hiërarchisch als

de politiek verantwoordelijke toetsen of de toestemming binnen de daarvoor geldende wettelijke vereisten kan worden gegeven. De toestemmingsverlener kan eventueel ook nadere voorwaarden (bijvoorbeeld in tijdsduur of met betrekking tot de mate van inbreuk) stellen voordat deze voor de inzet de verantwoordelijkheid neemt. Daarnaast maakt de motivering het mogelijk (extern) toezicht uit te oefenen door de CTIVD op de inzet van de bevoegdheid.

Toetsingskader (paragraaf 4.2, p. 10, van bijlage II):

- In het verzoek om toestemming dient gemotiveerd te worden op welke personen of organisaties en geautomatiseerde werken de inzet van de hackbevoegdheid zich richt en zo concreet mogelijk het doel van de inzet te worden aangegeven alsmede welke informatie wordt beoogd te worden verkregen met de inzet van de hackbevoegdheid.

Bevindingen

Bij de AIVD was in de onderzoeksperiode een eenvoudige werkinstructie beschikbaar voor het opstellen van een verzoek om toestemming. Tevens bood het door de bewerkers gebruikte bijbehorende sjabloon een zekere houvast de noodzakelijke elementen in het verzoek om toestemming op te nemen. Bij de MIVD ontbraken dergelijke werkinstructies en werden verzoeken gebaseerd op eerdere goedgekeurde verzoeken. De noodzaak van de operatie werd doorgaans zeer uitgebreid toegelicht, waarbij ook de proportionaliteit en subsidiariteit werden betrokken. De verzoeken van de MIVD hadden naar het oordeel van de CTIVD bondiger en gestructureerde gekund. Zij vindt de eerst ná de onderzoeksperiode ontwikkelde formats een adequaat instrument om dit te bewerkstelligen.

De onderzochte verzoeken om toestemming van zowel de AIVD als de MIVD blijken doorgaans voldoende gemotiveerd met betrekking tot de noodzaak, proportionaliteit en subsidiariteit van de inzet. In de (interne) verzoeken om toestemming wordt door beide diensten over het algemeen ook opgenomen op welke geautomatiseerde werken de inzet is gericht en op welke personen of organisaties de inzet betrekking heeft. Kenmerkend aan de hackbevoegdheid is dat van tevoren vaak niet exact kan worden aangegeven welke gegevens in de geautomatiseerde werken zullen worden aangetroffen. Het gevolg daarvan is dat een aantal initiële verzoeken om toestemming slechts abstract vermeldden welke informatie de diensten wilden overnemen. Daaraan gaven zij verder inhoud door in de verzoeken om toestemming tot verlenging de ontwikkelingen en de opbrengsten van de operatie weer te geven.

4.3 Het verzoek om toestemming voor de inzet tegen onbekende personen of organisaties

In bepaalde gevallen ontbreekt in de verzoeken om toestemming tegen welke persoon of organisatie de hackbevoegdheid werd ingezet. Dit kan het geval zijn wanneer het geautomatiseerd werk wel bekend is, maar niet duidelijk is welke personen of organisaties daar gebruik van maken.

Toetsingskader (paragraaf 4.2, p. 10, van bijlage II):

- Indien het niet direct mogelijk is aan te geven tegen welke personen of organisaties de hackbevoegdheid wordt ingezet, zal de dienst, zodra de gegevens betreffende de identiteit van de gebruiker(s) wel bekend zijn, de motivering met betrekking tot het verzoek om toestemming onverwijld moeten aanvullen en ter kennis van de toestemmingsverlener moeten brengen.

Bevindingen
In een aantal onderzoeken startten zowel de AIVD als de MIVD een operatie gericht op het binnendringen in een geautomatiseerd werk zonder dat bekend was bij wie dit in gebruik was. Soms hadden de diensten wel een vermoeden. Een voorbeeld daarvan bij de MIVD is een IP-adres dat werd gebruikt voor een cyberaanval. In een ander geval drong de AIVD een internetaccount binnen dat werd gebruikt om jihadistische propaganda te verspreiden.

Ondanks een eerdere toezegging van de ministers daartoe[5] vond in het algemeen geen directe afzonderlijke kennisgeving aan de toestemmingsverlener (minister of directeur) plaats op het moment dat de identiteit van een gebruiker bekend wordt. Uit nader onderzoek is wel gebleken dat deze identiteit (telkens) bij de afwegingen is betrokken, indien die informatie relevant was voor het nemen van beslissingen in het kader van het verdere verloop van de operatie. Evenmin is gebleken van operaties die op basis van het bekend worden van de identiteit gestopt hadden moeten worden en waarbij dit niet is gebeurd. Het nalaten van de onverwijlde kennisgeving heeft dus niet geleid tot situaties waarin de operaties niet (meer) noodzakelijk, proportioneel en subsidiair waren. De werkwijze van de AIVD en de MIVD is daarom op dit punt onzorgvuldig. De diensten wordt aanbevolen hun werkwijze met de toezeggingen van de ministers in overeenstemming te brengen.

4.4 Het verzoek om toestemming voor de inzet tegen onbekende geautomatiseerde werken

Bij de AIVD en de MIVD zijn zogenoemde brede verzoeken om toestemming aangetroffen waarin de personen en organisaties specifiek worden omschreven, maar ruimte werd gelaten voor de geautomatiseerde werken die het betrof.

Toetsingskader (paragraaf 4.2, p. 11, van bijlage II):

- Indien het niet direct mogelijk is het verzoek om toestemming toe te spitsen op (een) bepaald(e) geautomatiseerd(e) werk(en), zal de dienst het verzoek om toestemming (door middel van een bijschrijving) gemotiveerd moeten aanvullen zodra deze wel bekend worden.

Bevindingen
De operaties waarin een brede toestemming is gegeven, kunnen in grofweg twee categorieën worden opgedeeld. Allereerst zijn dat verzoeken om toestemming voor het fysiek hacken en het daarbij eenmalig overnemen (kopiëren) van de op de geautomatiseerde werken aanwezige gegevens. De tweede categorie betrof hacks op afstand die tot doel hadden of waarin voorzienbaar was dat met de operatie nieuwe aan hetzelfde target te relateren geautomatiseerde werken zouden worden onderkend.

Fysieke hacks
Bij de fysieke hacks bestond telkens het vermoeden dat specifieke targets over geautomatiseerde werken beschikten, maar was niet geheel duidelijk welke en hoeveel geautomatiseerde werken zouden worden aangetroffen. Een voorbeeld daarvan is het verzoek om toestemming voor het hacken van alle aan te treffen geautomatiseerde werken op een bepaalde locatie.

Gelet op het eenmalige karakter en de daarmee doorgaans korte duur van de inzet, is het niet onbegrijpelijk dat alle aangetroffen geautomatiseerde werken bij fysieke hacks niet alsnog op het verzoek

[5] Toetsingskader (paragraaf 4.2, p. 10 van bijlage II)

worden bijgeschreven. In het merendeel van de onderzochte operaties was er echter – bij met name de AIVD – sprake van een gebrekkige verslaglegging ten aanzien van de aangetroffen en binnengedrongen geautomatiseerde werken. Deze informatie was dikwijls niet op een eenduidige en/of toegankelijk wijze in de daarvoor bestemde systemen geregistreerd. Uit nader eigen onderzoek is echter niet gebleken van gevallen waarin buiten de gegeven toestemming is getreden of die anderszins tot een nadere proportionaliteitstoets noodzaakten. Dit gebrek aan verslaglegging is daarmee onzorgvuldig en de diensten wordt aanbevolen deze plicht tot verslaglegging in een werkinstructie op te nemen.

Hacks op afstand
Doorgaans bleek bij de hacks op afstand uit de motivering waarom voor een brede toestemming werd gekozen. Het ging in het algemeen om operaties waarin de mate van de dreiging en/of de verwachte dynamiek zodanig waren dat de diensten snel en efficiënt moesten kunnen handelen. Hierbij kan worden gedacht aan operaties waarin sprake was van aanwijzingen voor concrete gewelddadige acties of waarbij een target (bewust) met hoge frequentie van geautomatiseerde werk wisselde.

Zowel de AIVD als de MIVD hebben van deze vorm van brede toestemming gebruik gemaakt. In de motivering hebben zij het target telkens duidelijk omschreven en werd aangegeven welke informatie met de operatie werd beoogd. Daarnaast was voor een bijschrijving een duidelijke relatie met het target een vereiste. Daarmee waren de operaties in de praktijk voldoende begrensd om te kunnen oordelen dat deze, naast noodzakelijk en subsidiair, ook proportioneel waren. De werkwijze van de AIVD en de MIVD wordt op dit punt dan ook als rechtmatig beoordeeld.

Bijschrijvingen op brede toestemmingen
Hoewel de praktijk van het bijschrijven van gerelateerde nader onderkende geautomatiseerde werken op zichzelf dus rechtmatig is, moet daarbij wel telkens kritisch worden gekeken of de bijschrijving onder de verleende toestemming valt. Indien dit niet het geval is, moet eerst afzonderlijk toestemming worden gevraagd alvorens kan worden binnengedrongen.

AIVD
De AIVD heeft in een aantal operaties geautomatiseerde werken bijgeschreven onder eerdere verzoeken, waarvoor geen brede toestemming was gegeven. In deze gevallen was in het initiële verzoek alleen een specifiek geautomatiseerd werk genoemd en werd juist niet gerefereerd aan (nog te onderkennen) andere geautomatiseerde werken. Een voorbeeld daarvan was een operatie waarbij op een toestemming voor het hacken van een laptop een daarvan losstaand internetaccount van hetzelfde target werd bijgeschreven. In een andere operatie werden meerdere e-mailaccounts bijgeschreven, terwijl toestemming was gevraagd voor het hacken van één specifiek e-mailaccount. In één geval was in het interne verzoek om toestemming het binnendringen van gerelateerde, nader te onderkennen, e-mailaccounts opgenomen, maar is dit in de samenvatting van het verzoek aan (en daarmee in de toestemming van) de minister weggevallen.

Hoewel de bijschrijvingen via de verlenging in de meeste gevallen wel door de minister zijn geautoriseerd, is met het daarvóór reeds binnendringen van deze geautomatiseerde werken door de AIVD onrechtmatig gehandeld, omdat daarmee buiten de initieel door de minister verleende toestemming is getreden.

MIVD
Bij de MIVD is één operatie aangetroffen waarin wel een brede toestemming was gegeven, maar waarbij de bijgeschreven aan derden toebehorende geautomatiseerde werken niet onder de omschrijving vielen. Nadat deze geautomatiseerde werken waren binnengedrongen, zijn deze – onder aanpassing van de brede toestemming – door de betreffende analist, in overleg met de uitvoerder van de hack, wel op het verzoek bijgeschreven. Middels de verlenging is deze bijschrijving door de directeur van de MIVD geautoriseerd. De minister is daarvan niet op de hoogte gesteld. De MIVD heeft in deze operatie

onrechtmatig gehandeld door buiten de door de minister verleende toestemming te treden. De MIVD wordt aanbevolen in ieder geval een procedure in te richten waarbij de toestemming voor een bijschrijving hiërarchisch op een hoger niveau wordt belegd dan dat van de individuele medewerker, te weten op dat van het bureauhoofd.

4.5 Het verzoek om toestemming voor de inzet tegen organisaties

Omdat de wet voorziet in het verrichten van onderzoek naar personen én organisaties, is het mogelijk ook bijzondere bevoegdheden in te zetten tegen een organisatie. Daarbij wordt een onderscheid gemaakt tussen vaste en fluïde organisaties. Een vaste organisatie is een organisatie met een (min of meer) vaste structuur en personele samenstelling. Een fluïde organisatie betreft een meer informele organisatie naar samenstelling en tijd. Voor de inzet van de hackbevoegdheid tegen organisaties gelden bijzondere eisen aan de motivering.

Toetsingskader (paragraaf 4.2.1, p. 11, van bijlage II):

- Indien de bevoegdheid tegen (leden van) een organisatie wordt ingezet moet in het verzoek om toestemming worden gemotiveerd waarom sprake is van een organisatie en moet worden aangegeven onder welke omstandigheden tegen welke categorie van leden de hackbevoegdheid kan worden ingezet.

Inzet tegen vaste organisaties

Voor hacken geldt – meer dan bij andere bevoegdheden – dat goed voorstelbaar is dat de bevoegdheid wordt ingezet tegen een organisatie als geheel. Hierbij kan worden gedacht aan organisaties met een geheel eigen infrastructuur of systeem van geautomatiseerde werken, die relevant zijn voor de veiligheids- of inlichtingentaak van de diensten. Een voorbeeld daarvan is een officiële stichting die betrokken is bij het financieren van terrorisme.

Bevindingen

Zowel de AIVD als de MIVD hebben de hackbevoegdheid ingezet tegen dit type organisaties. In de onderzochte gevallen bleek uit de (gemotiveerde) omschrijving van het target dat evident sprake was van een organisatie. Deze duidelijk kenbare organisaties kwamen telkens in aanmerking voor onderzoek in het kader van een goede uitvoering van de veiligheids- of inlichtingentaak van de diensten.

Vaak beschikte de organisatie zelf over een uitgebreide digitale infrastructuur die op voorhand van buitenaf niet of weinig inzichtelijk was. In de verzoeken om toestemming werden daarom doorgaans de beoogde informatie en de (mogelijk) aan te treffen (onderdelen van) geautomatiseerde werken die voor onderzoek in aanmerking kwamen duidelijk beschreven. Pas nadat in de systemen was binnengedrongen, kon worden aangegeven welke specifieke delen van de systemen voor de diensten relevant waren. Aan deze nadere specificering (trechtering) werd in de motiveringen voor de verlengingen van de operaties voldoende aandacht besteed.

In die gevallen dat in de motivering concrete personen of functies binnen de organisatie werden genoemd, diende dit doorgaans om aan te geven welke (delen van) geautomatiseerde werken van de organisatie voor het onderzoek mogelijk relevante informatie bevatten. De aanduiding van de functies was daarbij telkens dermate concreet dat duidelijk was welke leden van de organisatie daarmee werden bedoeld. Deze functionarissen of functievermeldingen waren of evident of door de nadere motivering telkens relevant in het kader van de veiligheids- of inlichtingentaak.

De algemene werkwijze van de AIVD en de MIVD wordt op dit punt als rechtmatig beoordeeld. De reikwijdte van de inzet werd telkens voldoende beperkt door de relatie met het target, namelijk de desbetreffende organisatie. In combinatie met de nadere beperkingen voor de inzet die in de motiveringen voor de verlenging(en) werden aangebracht, is het vereiste van proportionaliteit gedurende de operaties voldoende in het oog gehouden. In het overgrote merendeel van de operaties woog het belang van nationale veiligheid op tegen de inbreuk op grondrechten en de belangen van de betrokkene(n).

Bij de AIVD is één en bij de MIVD zijn twee operaties aangetroffen, waarbij de reikwijdte van de inzet onvoldoende was begrensd. Daarbij ging het telkens om gevallen waarin een te abstracte beschrijving werd gegeven van de organisatie of onvoldoende duidelijk werd omschreven welk soort of aantal geautomatiseerde werken het betrof. Omdat bij de uitvoering van de hackoperatie binnen toelaatbare grenzen is gebleven, is feitelijk geen gebruik gemaakt van deze (te) brede toestemming. Dit heeft in de praktijk dan ook uiteindelijk niet tot ongeoorloofde inbreuken geleid. Om die reden is geen sprake van onrechtmatig-, maar van onzorgvuldigheden.

In de geheime bijlage wordt nader ingegaan op de aard van deze organisaties en de functies van de leden daarvan.

Inzet tegen fluïde organisaties

Naast de inzet van de hackbevoegdheid tegen een duidelijk gestructureerde organisatie, kan de hackbevoegdheid ook worden ingezet tegen zogenaamde fluïde organisaties. Bij zo een organisatie moet worden gedacht aan een (wisselende) groep aanhangers van dezelfde ideologische stroming, die zich hebben verenigd, zonder een duidelijke organisatorische of functionele structuur, bijvoorbeeld rond een jihadistisch webforum.[6] Binnen de onderzoekscriteria van dit rapport heeft alleen de AIVD de hackbevoegdheid ingezet tegen dit type organisaties.

Toetsingskader (paragraaf 4.2.1, p. 11, van bijlage II):

- In het geval van een fluïde (informele) organisatie dient een aparte motivering te worden opgesteld voor de bijschrijving van een persoon.

Bevindingen

Bij de AIVD was sprake van de inzet van de hackbevoegdheid tegen twee fluïde organisaties. Deze organisaties konden evident als zodanig worden aangemerkt. Naast duidelijk omschreven rollen of achtergronden die personen konden hebben om als lid te worden aangemerkt, was in de verzoeken om toestemming opgenomen dat deze zich ook richtten op “aanhangers die gezien hun handelingen in de toekomst mogelijk aansluiting zoeken bij de organisatie”. De CTIVD is van oordeel dat dit van onvoldoende gewicht is om als lid van een organisatie te worden aangemerkt. Het in het verzoek opnemen van een dergelijke vage relatie is onzorgvuldig en werkt onrechtmatigheden in de hand.

Daarbij moet wel worden opgemerkt dat de teams hebben aangegeven dat zij deze omschrijving zelf ook te onbepaald vinden om een persoon als lid aan te merken. Uit eigen onderzoek is gebleken dat van deze benadering ook geen gebruik is gemaakt bij de inzet van de bevoegdheid: voor alle in de onderzoeksperiode bijgeschreven personen waren concrete aanwijzingen aanwezig voor een specifiek

[6] Het kan ook voorkomen dat de organisatie achter een forum desalniettemin hiërarchisch is opgebouwd. Daarbij zijn er enkele sleutelfiguren die als moderator optreden en toezien op de naleving van de opgestelde regels binnen een forum.

in het verzoek genoemde substantiëlere rol, zodat zij terecht als lid van de organisatie konden worden aangemerkt.

Bijschrijvingen
Zoals bij fluïde organisaties is vereist, is voor de bijschrijving telkens een aparte motivering voor de inzet van de hackbevoegdheid tegen specifiek dat lid van de organisatie opgesteld. De motiveringen bevatten de noodzaak, subsidiariteit en proportionaliteit voor deze inzet en voldeden daarmee aan de eisen daarvoor. De toestemming is telkens minimaal op het niveau van unithoofd gegeven.

In één geval waren er zowel indicaties als contra-indicaties voor het lidmaatschap van de organisatie. De CTIVD is van oordeel dat indien de relatie met de organisatie onvoldoende vaststaat, een persoon niet op het verzoek mag worden bijgeschreven. Voor onderzoek dat (mede) inhoudt het vaststellen *of* een persoon wel lid is van een organisatie, moet apart toestemming aan de minister worden gevraagd. Dit betekent dat de toestemming in dit geval niet op het juiste niveau is gegeven. Daarmee heeft de AIVD onrechtmatig gehandeld.

4.6 Het verzoek om toestemming voor de inzet tegen verschoningsgerechtigden

De CTIVD heeft in haar onderzoek bijzondere aandacht gehad voor zowel het direct als het indirect hacken van verschoningsgerechtigden. Verschoningsgerechtigden zijn personen met een maatschappelijke vertrouwensfunctie, in die zin dat eenieder vertrouwelijk met deze personen moet kunnen communiceren. Voorbeelden daarvan zijn artsen en advocaten. Op grond van deze functie komt aan de communicatie van en met deze personen extra bescherming toe.

Toetsingskader (paragraaf 4.2.2, p. 13, van bijlage II):[7]

- Bij het direct hacken van een verschoningsgerechtigde geldt in algemene zin een verzwaarde proportionaliteitstoets: er moet in het concrete geval sprake zijn van operationele belangen die zwaarder wegen dan het verschoningsrecht. Bij zwaarwegende operationele belangen kan gedacht worden aan situaties waarin sprake is van één of meer concrete aanwijzingen voor een direct gevaar voor de nationale veiligheid. De toestemming is maximaal één maand geldig.
- Indien bij het indirect hacken van een verschoningsgerechtigde voorzienbaar is dat met de inzet toegang wordt verkregen tot informatie waarop het verschoningsrecht van toepassing is, dienen de diensten hier bij de motivering ten behoeve van de toestemming en (eventuele) verlengingen nadrukkelijk aandacht aan te besteden.
- Zowel bij direct als bij indirect hacken is het uitwerken van gegevens waarop het verschoningsrecht van toepassing is, slechts toegestaan indien aan het verzwaarde proportionaliteitsvereiste is voldaan. Dit dient schriftelijk gemotiveerd te worden. Het teamhoofd (AIVD) of bureauhoofd (MIVD) moet bij deze afweging betrokken worden en dient goedkeuring aan de uitwerking te verlenen.

[7] Vanaf 1 januari 2016 is de Tijdelijke regeling onafhankelijke toetsing bijzondere bevoegdheden Wiv 2002 jegens advocaten en journalisten van toepassing. Op grond van deze regeling moet de toestemming van de minister voor de inzet van (ook) de hackbevoegdheid jegens advocaten en journalisten (voor zover gericht op het achterhalen van een bron) ter bindend advies worden voorgelegd aan de Tijdelijke Toetsingscommissie. Deze situatie heeft zich in de onderzochte hackoperaties niet voorgedaan en wordt daarom in dit rapport, dat zich hoofdzakelijk richt op de inzet en verlengingen in het jaar 2015, buiten beschouwing gelaten. Er is tevens gekozen voor een uniform toetsingscriterium voor alle verschoningsgerechtigden. Voor de specifieke invulling daarvan bij advocaten en journalisten zie rapport nr. 52 over de inzet van bijzondere bevoegdheden jegens advocaten en journalisten.

- Overgenomen (gekopieerde) gegevens waarop het verschoningsrecht van toepassing is die niet aan de verzwaarde proportionaliteitstoets voldoen, moeten terstond verwijderd en vernietigd worden.

Bevindingen

In het onderzoek zijn bij de AIVD en de MIVD met betrekking tot de (motivering van de) directe inzet van de hackbevoegdheid tegen verschoningsgerechtigden geen onrechtmatigheden of onzorgvuldigheden geconstateerd. Ditzelfde geldt voor die gevallen van indirect hacken waarin op voorhand voorzienbaar was dat met de operatie verschoningsgerechtigde communicatie(gegevens) zou kunnen worden verkregen. In de systemen van de diensten waarin relevant bevonden informatie wordt opgeslagen, is geen uit hacks afkomstige uitgewerkte verschoningsgerechtigde communicatie aangetroffen. Dit betekent dat er geen aanwijzingen zijn dat uit deze hacks afkomstige verschoningsgerechtigde communicatie(gegevens) zijn gebruikt in het operationeel proces.

4.7 Het verzoek om toestemming voor de inzet tegen non-targets

In het onderzoek is ook bijzondere aandacht besteed aan hacks op geautomatiseerde werken van non-targets. Non-targets zijn doorgaans personen uit de (directe) omgeving van een target. Daarbij kan het bijvoorbeeld gaan om familieleden, vrienden of kennissen. Zij zijn dus zelf niet in onderzoek bij de diensten, maar de inzet is wel op hen gericht. Uit hun communicatie, informatiepositie of handelingen wordt geprobeerd informatie over het target te krijgen (bijvoorbeeld over de verblijfplaats van het target).

Toetsingskader (paragraaf 4.2.3, p. 14, van bijlage II):

- Uit de motivering van het verzoek om toestemming moet blijken dat het een hack op een non-target betreft.
- Bij het hacken van non-targets geldt een verzwaarde proportionaliteitstoets: er moet sprake zijn van operationele belangen die zwaarder wegen dan het belang van de bescherming van de grondrechten en de belangen van het non-target. Bij zwaarwegende operationele belangen kan gedacht worden aan situaties waarin sprake is van één of meer concrete aanwijzingen dat er ten aanzien van het uiteindelijke target een direct gevaar voor de nationale veiligheid bestaat. Deze belangenafweging dient in de motivering van het verzoek om toestemming en eventuele verlengingen tot uitdrukking te komen.
- Gegevens die geen zicht (kunnen) geven op het target, worden niet uitgewerkt. Deze randvoorwaarde moet ook uit het verzoek om toestemming blijken.[8]

Bevindingen

De MIVD heeft in de onderzoeksperiode van dit rapport geen non-targets gehackt. De AIVD heeft dit in beperkte mate gedaan. In het algemeen was telkens sprake van concrete aanwijzingen dat van het uiteindelijke target een direct gevaar voor de nationale veiligheid uitging, terwijl het voor de diensten niet mogelijk was om daarover inlichtingen te verkrijgen door zich direct op het target te richten. Voorbeelden daarvan betreffen onderzoeken naar uitreizigers naar of (mogelijke) terugkeerders uit jihadistische strijdgebieden, waarbij de diensten voor het verrichten van onderzoek geen andere aanknopingspunten hadden dan de contacten die deze targets hadden met hun omgeving.

[8] Gegevens die niet relevant zijn voor de veiligheids- en inlichtingentaak dienen te worden verwijderd en vernietigd. Deze (algemene) voorwaarde van gegevensverwerking wordt in Hoofdstuk 7 besproken.

In drie hackoperaties tegen een non-target was weliswaar geen sprake van een direct gevaar, maar wel van een overigens rechtens relevant zwaarwegend operationeel belang. In de verzoeken om toestemming voor deze operaties, werd telkens gemotiveerd aangegeven waarom sprake was van zwaarwegende operationele belangen in het kader van de nationale veiligheid. In de motiveringen werd steeds ingegaan op de inlichtingbehoefte waaruit de dringende operationele noodzaak van de beoogde informatie kon worden afgeleid. Aangegeven werd voor welke onderdelen en (soort) operaties binnen de diensten de toegang tot deze informatie cruciaal was. Ook werd uitgebreid stilgestaan bij de beperkte risico's voor de betrokkene(n) en de mate waarin de integriteit van de systemen van de betrokkene(n) werden aangetast. De operationele belangen om toegang te verwerven tot de gegevens waren voldoende zwaarwegend om de inbreuk op grondrechten en de belangen van de betrokkene(n) te rechtvaardigen.

In de geheime bijlage wordt nader op de aard en achtergrond van deze zwaarwegende operationele belangen ingegaan.

In vrijwel alle gevallen is voldoende duidelijk vermeld en/of gemotiveerd dat het binnen te dringen geautomatiseerd werk aan een non-target toebehoorde. Ook werd aangegeven naar welke informatie het operationele team op zoek was en onder welke – al dan niet abstract geformuleerde – voorwaarden deze informatie zou worden uitgewerkt. Uit het onderzoek naar de uitvoering is gebleken dat de diensten in de systemen waarin zij relevante informatie opslaan alleen gegevens stonden die gerelateerd waren aan het (onderzoek naar het) target.

In één operatie bleek uit de motivering alleen impliciet dat de hack op een non-target was gericht en was onvoldoende duidelijk dat de hack alleen zou worden gebruikt om zicht te krijgen op het target. Om misverstanden bij de toestemmingsverlener, onder wie de minister, en de uitvoerder van de hack te voorkomen, had dit expliciet moeten worden vermeld. Uit nader onderzoek blijkt dat de noodzakelijke belangenafweging intern (binnen het team) wel heeft plaatsgevonden en dat uiteindelijk alleen gegevens zijn uitgewerkt die betrekking hadden op het (onderzoek naar) het uiteindelijk target. Deze operatie heeft daarmee niet tot ongeoorloofde inbreuken geleid. Het ontbreken van de expliciete vermelding van het doel van de operatie in het verzoek om toestemming wordt daarom niet onrechtmatig, maar als onzorgvuldig beoordeeld.

4.8 Het verzoek om toestemming voor de inzet tegen derden

Bij de inzet van de hackbevoegdheid kunnen ook derden in beeld komen bij de diensten. Derden zijn anders dan non-targets geen doel van een operatie, maar een middel om bij het target te komen. De inzet van de hackbevoegdheid is niet op hen gericht. Gelijk aan de (toelichting op) de Wiv 20... worden derden gedefinieerd als technisch gerelateerde partijen wier geautomatiseerde werken worden gebruikt om binnen te kunnen dringen in het geautomatiseerd werk van het target. Zo kunnen de diensten gebruik maken van het geautomatiseerde werk van een derde als *stepping stone* om via deze bij het geautomatiseerde werk van het target te komen, bijvoorbeeld via een netwerkverbinding tussen beide geautomatiseerde werken. Daarnaast ook kunnen de diensten een geautomatiseerd werk van een derde hacken waarin technische gegevens zijn opgeslagen die gebruikt kunnen worden om het geautomatiseerd werk van het target binnen te dringen (bijvoorbeeld een IP-adres of wachtwoord). In haar Zienswijze op de Wiv 20... heeft de CTIVD aangegeven dat het hierna te noemen toetsingskader moet worden gehanteerd en in de nieuwe wet zou moeten worden verankerd.[9]

[9] Zienswijze van de CTIVD op het wetsvoorstel Wiv 20., bijlage I (november 2016) , p. 29-30, beschikbaar op www.ctivd.nl

Toetsingskader (paragraaf 4.2.4, p. 15, van bijlage II):

- Voor het binnendringen van het geautomatiseerde werk van een derde ten behoeve van het binnendringen van het geautomatiseerde werk van het target, geldt een verzwaarde subsidiariteitstoets. Binnendringen in het geautomatiseerd werk van de derde is alleen toegestaan indien en voor zover dit onvermijdelijk is voor het binnendringen van het werk van het target. Er mag geen andere reële mogelijkheid zijn. Een en ander moet uit de motivering van het verzoek om toestemming blijken.
- Indien gegevens van de betreffende derde worden overgenomen die geen betrekking hebben op het binnendringen van het geautomatiseerd werk van het target, en ook niet relevant zijn voor het onderzoek waarvoor zij zijn verworven, worden deze niet uitgewerkt.[10]

Bevindingen

Zowel de AIVD als de MIVD heeft in de onderzoeksperiode van dit rapport geautomatiseerde werken van derden gehackt om uiteindelijk binnen te kunnen dringen bij targets. Het hacken via het geautomatiseerde werk van een derde heeft op beperkte schaal en alleen na een gemotiveerde belangenafweging dienaangaande plaatsgevonden. In tegenstelling tot de in de reacties op de Wiv 20.. vaak geuite zorg daaromtrent, betrof dit in geen van de gevallen een individuele burger.

In de onderzochte operaties zijn door de JSCU middels een vooronderzoek eerst de haalbaarheid en de eventuele risico's van een rechtstreekse hack op het target in kaart gebracht. Alleen wanneer dit niet of te moeilijk realiseerbaar bleek, bijvoorbeeld omdat dit een uitzonderlijk onevenredige capaciteit vroeg of grote risico's met zich meebracht, hebben de diensten gebruik gemaakt van het geautomatiseerde werk van een derde. Bij deze risico's moet worden gedacht aan een (te) langdurig proces om complexe beveiliging te doorbreken, de reële kans dat met een directe hack schade in systemen wordt aangericht of de reële verwachting dat de hack wordt onderkend.

In sommige gevallen is het geautomatiseerd werk van de derde alleen gebruikt als *stepping stone*. In andere gevallen zijn ook gegevens overgenomen. In de gevallen dat bij het hacken ook gegevens zijn overgenomen, ging het telkens om gegevens die nodig waren om bij het uiteindelijk target binnen te dringen. In een enkel geval zijn bij een *stepping stone*, die zich niet alleen technisch, maar ook feitelijk in de omgeving van het target bevond, gegevens overgenomen die inhoudelijk relevant waren voor het onderzoek naar het target. De CTIVD is van oordeel dat – toetsend aan de onvermijdelijkheid – de AIVD en MIVD rechtmatig hebben gehandeld bij het binnendringen in geautomatiseerde werken van derden.

[10] Deze gegevens dienen tevens te worden verwijderd en vernietigd. Deze voorwaarde van gegevensverwerking wordt in Hoofdstuk 6 besproken.

5 De toestemmingsverlening

Voordat de hackbevoegdheid kan worden ingezet moet het verzoek tot toestemming op het juiste niveau worden gegeven.

Initiële verzoeken om toestemming

Toetsingskader (paragraaf 4.3 p. 17, van bijlage II):

- Bij de AIVD moet het verzoek om toestemming voor een hack op afstand door de minister en voor een fysieke hack door de betrokken directeur worden goedgekeurd.
- Bij de MIVD moet het verzoek tot toestemming voor een hack (op afstand en fysiek) door de minister worden goedgekeurd.

Bevindingen

Het is bevorderend voor de rechtmatigheid dat de toestemming voor de initiële inzet van de hackbevoegdheid in vrijwel alle gevallen op het hoogst mogelijk niveau is gelegd, te weten dat van de minister. Dit doet recht aan de grote inbreuk die met hacken op de grondrechten en belangen van de betrokkene(n) kan worden gemaakt.

Alleen voor fysieke hacks is bij de AIVD toestemming van een directeur voldoende. De verzoeken om toestemming worden in deze gevallen niet aan de minister voorgelegd. Hoewel deze werkwijze niet in strijd is met de wet en in concrete gevallen ook niet tot onrechtmatigheden heeft geleid, is de argumentatie van de AIVD om fysieke hacks op een lager toestemmingsniveau te beleggen niet overtuigend. Hoewel het eenmalige karakter van een fysieke hack een zekere mate van beperking aanbrengt, is daarmee niet gezegd dat met de inzet minder inbreuk op de grondrechten en belangen van de betrokkene(n) wordt gemaakt. Integendeel, in het onderzoek zijn operaties aangetroffen waarin de inbreuk op rechten en belangen in aard en omvang minimaal vergelijkbaar was met die van hacks op afstand. De AIVD wordt daarom aanbevolen, vooruitlopend op de Wiv 20.., alle verzoeken om toestemming voor hacks op het niveau van de minister te beleggen.

Verzoeken om verlengingen van de toestemming

Toetsingskader (paragraaf 4.3 p. 17, van bijlage II):

- Bij de AIVD moet het verzoek om verlenging van de toestemming voor een hack op afstand door de minister worden goedgekeurd.
- Bij de MIVD moet het verzoek om verlenging van de toestemming voor een hack door de (plaatsvervangend) directeur worden goedgekeurd.

Bevindingen

De CTIVD heeft naast alle initiële verzoeken om toestemming, ook de verzoeken om verlenging van de geselecteerde hackoperaties bestudeerd. Zij stelt vast dat zowel bij de AIVD als de MIVD in voldoende mate aandacht wordt besteed aan de noodzaak, proportionaliteit en subsidiariteit van de verlenging, met vermelding van eventuele opbrengsten. Ten aanzien van zowel de AIVD als de MIVD zijn echter enkele aanmerkingen te maken op de werkwijze bij het verlengen van hackoperaties.

AIVD
Bij de AIVD is het administratief proces zo ingericht, dat de verzoeken om verlenging van de toestemming voor de inzet van de hackbevoegdheid, zo veel mogelijk samengevoegd met alle andere verzoeken voor (verlenging van de) de inzet van bijzondere bevoegdheden in lopende onderzoeken, aan de minister worden voorgelegd. In de praktijk komt het er op neer dat de minister een keer per drie maanden een door de afdeling Juridische Zaken sterk samengevatte bundeling van alle verzoeken (waaronder verlengingen van de hackbevoegdheid) krijgt voorgelegd. Om het samenvatten en bundelen tijdig te kunnen uitvoeren, stelt de afdeling Juridische Zaken een termijn waarbinnen de verzoeken bij haar moeten zijn aangeleverd. Deze termijn ligt rond de zes weken voor de datum waarop de verlengingen in moeten gaan.

Deze werkwijze betekent dat de teams gedwongen worden kort na het opstellen van het initiële verzoek om toestemming, een verzoek om verlenging in te dienen. De hackoperatie loopt dan nog maar net en heeft op dat moment vaak nog geen opbrengsten gegenereerd. In de praktijk betekent dit dat de motivering van de verlenging nagenoeg identiek is aan de motivering van de initiële aanvraag. Zouden de teams eerst kort voor het verloop van de toestemming (duur drie maanden) het verzoek om verlenging hoeven op te stellen, zou dit tot een beter te motiveren verzoek leiden dan nu het geval is. Op dat moment is immers meer bekend over wat de betreffende hack al dan niet oplevert, en kan de motivering van de verlenging daarop worden toegespitst. De eerste verlenging heeft nu inhoudelijk weinig meerwaarde en de minister krijgt in feite een beperkt gemotiveerd verzoek voorgelegd. Hierdoor is hij in beginsel onvoldoende geïnformeerd om de verlengingsbeslissing te kunnen nemen, hetgeen onrechtmatigheden in de hand kan werken. Van concrete onrechtmatigheden is overigens niet gebleken.

Deze werkwijze is onzorgvuldig. Aanbevolen wordt de procedure zo aan te passen dat de inhoud van de verzoeken om verlenging van de toestemming zo recent als redelijkerwijs mogelijk is. Van de AIVD is overigens vernomen dat de procedure op dit moment wordt herzien.

MIVD
Bij de MIVD worden de verzoeken om verlenging van de toestemming niet aan de minister, maar aan de directeur voorgelegd. Bij de MIVD is het administratief proces voor verlengingen zo ingericht dat de directeur het volledige verzoek voorgelegd krijgt. Ook laat het administratief proces bij de MIVD ruimte om relatief kort voor het indienen van het verzoek de laatste informatie over het verloop en de opbrengst van de operatie in het verzoek op te nemen. Het aan de directeur voorleggen van het gehele verzoek maakt dat deze kennis kan nemen van alle feiten en omstandigheden die aan het verzoek ten grondslag liggen. Op deze wijze kan er geen verschil ontstaan tussen de inhoud van het verzoek om verlenging en de toestemming. Deze werkwijze is zorgvuldig.

De keuze bij de MIVD om de verlengingen niet aan de minister voor te leggen is formeel niet in strijd met de wet of de Mandaatregeling. Desondanks werkt deze praktijk onrechtmatigheden in de hand, omdat de operaties gedurende het proces, niet zozeer wat betreft het doel, maar wel in de wijze waarop dat doel wordt bereikt, kunnen veranderen. Daardoor kan het gebeuren dat de operatie na verloop van tijd een ander verloop, karakter of focus krijgt dan de operatie waarvoor de minister initieel toestemming heeft gegeven.

Naar het oordeel van de CTIVD waren de wijzigingen in het verloop van één operatie dermate significant dat deze (bij de verlenging) aan de minister had moeten worden voorgelegd. Deze had dan opnieuw de afweging moeten maken over de gevolgen voor subsidiariteit en de proportionaliteit van de operaties en of toestemming daarvoor (nog steeds) op zijn plaats was. Dit is onrechtmatig en de MIVD wordt aanbevolen, vooruitlopend op de wet Wiv 20.., de Mandaatregeling en/of het beleid zo aan te passen dat alle verzoeken om verlenging van hackoperaties aan de minister worden voorgelegd.

6 De uitvoering

De uitvoering

Nadat op het juiste niveau toestemming is verkregen, kunnen de medewerkers van de JSCU de hack gaan uitvoeren. Een beschrijving van de wijze van deze uitvoering raakt per definitie het belang van de nationale veiligheid, omdat daarmee inzicht wordt gegeven in de modus operandi van de diensten. Volstaan moet hier dan ook worden met algemeen omschreven bevindingen.

Bevindingen

De voortgang van de (technische) uitvoering van een hack wordt doorgaans door de betreffende medewerker van de JSCU individueel en handmatig bijgehouden. Er vindt overleg plaats met het operationele team wanneer voor de verdere uitvoering van de hack operationele kennis noodzakelijk is. Het operationeel team houdt handmatig in een logboek bij op welke wijze zij de uitvoerder begeleiden en welke informatie zij van de uitvoerder over het verloop van de operatie hebben gekregen. Anders dan bij een continu geautomatiseerde integrale vastlegging van gegevens over de uitvoering en de verrichte technische handelingen van een hack, het zogenaamde loggen, is het (interne) toezicht op de uitvoering grotendeels afhankelijk van de nauwkeurigheid van de verslaglegging door de medewerkers van de JSCU en het operationele team. Naar analogie van het wetsontwerp Wet Computercriminaliteit III is het echter, om de uitvoering van de hackbevoegdheid volledig inzichtelijk en objectief toetsbaar te maken, noodzakelijk deze in het vervolg geautomatiseerd te loggen.

Kwetsbaarheden

Teneinde binnen te dringen, om bij het niet publiek toegankelijke deel van het geautomatiseerd werk te komen, moet vrijwel altijd enige vorm van beveiliging worden doorbroken. Hierbij kan gebruik worden gemaakt van kwetsbaarheden in het geautomatiseerd werk. Dit wil zeggen: langs een weg die de aanwezige beveiliging niet of onvoldoende afsluit, waarbij die opening inherent kan zijn aan het systeem of veroorzaakt kan zijn door de binnendringer zelf. Bij het gebruik van deze kwetsbaarheden is in het parlementaire debat uitgebreid stilgestaan.[11] Daarbij is vooral de aandacht uitgegaan naar het gebruik van kwetsbaarheden die noch algemeen noch bij de fabrikant zelf bekend zijn, zogenaamde zero days of onbekende kwetsbaarheden.

Toetsingskader (paragraaf 3.3, p. 7, van bijlage II):

- De AIVD en de MIVD dienen belangendragers te informeren over geconstateerde onbekende kwetsbaarheden, tenzij wettelijke argumenten of operationele redenen daaraan (tijdelijk) in de weg staan. Hierbij dient de verhouding tussen de gerechtvaardigde belangen van de diensten en (het gevaar van) het laten voortbestaan van de kwetsbaarheden voor (alle) gebruikers van het internet te worden betrokken.

[11] Zie voor de vindplaatsen van de parlementaire stukken: Toetsingskader, p. 7 van bijlage II

Bevindingen

Bij het hacken wordt vrijwel altijd een bepaalde kwetsbaarheid in het te hacken geautomatiseerd werk gezocht. Dit is in veel gevallen een reeds algemeen bekende kwetsbaarheid. In een beperkt aantal gevallen wordt een onbekende kwetsbaarheid gebruikt. Deze kan door de uitvoerders van de hack zelf zijn ontdekt, maar kennis daarover kan ook zijn aangekocht. Daarnaast is het mogelijk dat malware wordt aangekocht die is gebaseerd op het uitbuiten van (onbekende) kwetsbaarheden.

In de geheime bijlage wordt nader op het gebruik van (onbekende) kwetsbaarheden ingegaan.

Het uitgangspunt is dat onbekende kwetsbaarheden worden gemeld middels het door het NCSC opgestelde beleid van *responsible disclosure*.[12] Indien bij het hacken een onbekende kwetsbaarheid wordt geconstateerd, wegen de medewerkers van de JSCU – al dan niet na onderling overleg – het gevaar van het voortbestaan van de kwetsbaarheid af tegen het operationeel belang en de wettelijke argumenten de kwetsbaarheid niet te melden. Bij beide moet worden gedacht aan de bescherming van het actueel kennisniveau, een werkwijze of bronnen. In deze afweging speelt mee of de kwetsbaarheden zich in door particulieren en bedrijven veelgebruikte of door de Nederlandse overheid gebruikte producten bevinden. In die gevallen wordt sneller tot het informeren van belangendragers overgegaan. Dit informeren is tijdens de onderzoeksperiode niet en vóór de onderzoeksperiode eenmaal gebeurd.

De door de medewerkers van de JSCU te volgen werkwijze is echter niet vastgelegd. Daarnaast zijn de relevante afwegingen niet in intern beleid nader geconcretiseerd of uitgewerkt. Ook wordt de uitkomst van de afweging niet centraal geadministreerd. In de praktijk is het melden van onbekende kwetsbaarheden daarmee sterk afhankelijk van de door de individuele medewerkers van de JSCU gemaakte afwegingen en is het niet goed mogelijk daar interne controle en extern toezicht op uit te oefenen. Ook kan het gebeuren dat kwetsbaarheden niet alsnog worden gemeld nadat het operationeel belang voor het niet-melden is verminderd of weggevallen. Deze werkwijze is onzorgvuldig. In het onderzoek zijn overigens geen operaties aangetroffen waarin, naar het oordeel van de CTIVD, tot het informeren van de belangendragers had moeten worden overgegaan.

De JSCU en daarmee zowel de AIVD als de MIVD wordt aanbevolen beleid en werkwijzen te ontwikkelen waarin relevante afwegingen met betrekking tot het al dan niet informeren van belangendragers over geconstateerde onbekende kwetsbaarheden worden geconcretiseerd en vastgelegd. Daarnaast dient (centrale) verslaglegging van de geconstateerde onbekende kwetsbaarheden en van de daarbij gemaakte afwegingen plaats te vinden. Voor niet gemelde onbekende kwetsbaarheden dient een periodieke toetsingstermijn te worden bepaald, waarbinnen wordt beoordeeld of – indien nog opportuun – het operationeel belang nog steeds dient te prevaleren.

[12] Praktijk van het verantwoord melden van aangetroffen beveiligingslekken. Hierbij worden afspraken gehanteerd die doorgaans hierop neerkomen dat de melder de ontdekking niet deelt met derden totdat het lek verholpen is, en de getroffen partij geen juridische stappen tegen de melder zal ondernemen. Meer informatie op www.ncsc.nl

7 Het overnemen, beoordelen en vernietigen van gegevens

In de vorige hoofdstukken is beschreven tegen wie en op welke wijze de hackbevoegdheid wordt ingezet met de nadruk op bijzondere categorieën van personen en/of organisaties daarbij. Daarin is ook aangegeven dat de gegevens uit de gehackte geautomatiseerde werken werden gekopieerd en op de systemen van de AIVD en MIVD werden opgeslagen (het overnemen van gegevens). In dit hoofdstuk wordt vanuit een systeembenadering beschreven hoe de diensten het proces om deze gegevens op hun relevantie te beoordelen hebben ingericht. Daarbij wordt stilgestaan bij de vraag hoe wordt omgegaan met methoden van functiescheiding en compartimentering bezien vanuit het waarborgprincipe van need-to-know ten behoeve van het operationeel proces en met het bewaren en vernietigen van gegevens die in het verwerkingsproces niet (meer) relevant zijn bevonden of die in het geheel niet zijn beoordeeld. Een gevolg van deze benadering is dat de conclusies en aanbevelingen met name betrekking zullen hebben op het aanpassen en/of invoeren van (geautomatiseerde) procedures.

7.1 Het overnemen van gegevens

Het doel van het inzetten van de hackbevoegdheid is het verwerven van informatie die relevant is voor de veiligheids- en inlichtingentaken van de diensten. Dit wordt bereikt door het overnemen van gegevens uit de gehackte geautomatiseerde werken. Dit betreft het kopiëren van de gegevens van het gehackte geautomatiseerd werk en de opslag daarvan in de systemen van de diensten. Dit overnemen van gegevens is in artikel 24 van de Wiv 2002 expliciet als bevoegdheid opgenomen.

Toetsingskader (paragraaf 5.1 p. 17/18, van bijlage II):

- Bij het ongericht overnemen van gegevens, geldt een verzwaarde proportionaliteitstoets: de operationele belangen moeten zwaarder wegen dan het belang van de bescherming van de grondrechten en de belangen van in het bijzonder die personen of organisaties van of over wie informatie in de gegevens voorkomt en geen target van de diensten zijn. Bij zwaarwegende operationele belangen kan gedacht worden aan situaties waarin sprake is van één of meer concrete aanwijzingen dat er een direct gevaar voor de nationale veiligheid bestaat. Deze belangenafweging dient in de motivering van het verzoek om toestemming en eventuele verlengingen tot uitdrukking te komen.

Bevindingen

De door middel van de hackbevoegdheid overgenomen gegevens worden niet als zodanig geregistreerd. Om de herleidbaarheid van de herkomst en de wijze van het overnemen van de gegevens te kunnen waarborgen, moet ook het proces van het overnemen van gegevens integraal worden gelogd. Dit maakt tevens (intern) toezicht daarop mogelijk. Ondanks het ontbreken van logging kan op basis van de handmatige verslaglegging en nader onderzoek een algemeen beeld worden geschetst van hoe de selectie van de over te nemen (te kopiëren) gegevens in de praktijk tot stand komt. Daartoe laten zich een gerichte en een ongerichte methode onderscheiden, die in de praktijk van de diensten ook zo worden toegepast. Deze verschillende methoden van overnemen worden hieronder toegelicht.

Het gericht overnemen van gegevens

In een enkel geval is het mogelijk precies die informatie te kopiëren die voor het operationele team van belang is. Daarbij kan worden gedacht aan het vanuit een e-mailaccount alleen overnemen van

een paar door het operationeel team verzochte specifieke berichten. In veel gevallen echter laat de beveiliging niet toe dat alleen de voor het onderzoek relevante informatie wordt overgenomen, vanwege de daarvoor noodzakelijke activiteiten en bewerkingen in de binnengedrongen geautomatiseerde werken. De medewerker van de JSCU die de hack uitvoert, heeft ook vaak onvoldoende operationele kennis om te kunnen bepalen naar welke informatie het operationele team precies op zoek is. In het overgrote deel van de gevallen wordt er daarom (al dan niet in overleg met het team) voor gekozen een *grove selectie* te maken van de over te nemen gegevens die voor het onderzoek mogelijk relevant zijn. Een voorbeeld daarvan is het vanuit een laptop, die ook door huisgenoten wordt gebruikt, alleen kopiëren van bestanden van het target. Ook kan worden gedacht aan het overnemen van alle berichten uit een e-mailaccount dat uitsluitend door een target wordt gebruikt. De CTIVD vindt deze werkbare en rechtmatige handelwijze nog zodanig toegespitst op bepaalde gegevensvergaring, dat zij dit rangschikt als gericht overnemen.

Het ongericht overnemen van gegevens
Het uitgangspunt is dat het overnemen van gegevens zo gericht als redelijkerwijs mogelijk plaatsvindt. In sommige situaties echter worden de gegevens *integraal* (in bulk) ongericht overgenomen. In die gevallen kan op voorhand niet worden aangegeven welke gegevens in het geautomatiseerd werk aan het target en/of onderzoek zijn te relateren danwel daarvoor mogelijk relevant zijn. In deze operaties is vaak van tevoren wél duidelijk dat het overgrote deel van de integraal over te nemen gegevens betrekking heeft op personen en/of organisaties die *geen* target van de diensten zijn. Daarbij kan worden gedacht aan een algemeen webforum, waarop personen communiceren van wie vermoed wordt dat zij een terroristische aanslag voorbereiden, of het overnemen van een hele e-mailserver, waarvan enkele e-mailaccounts worden gebruikt voor een cyberaanval.

De AIVD is in twee operaties en de MIVD in één operatie tot het ongericht overnemen van gegevens overgegaan. In alle gevallen was het redelijkerwijs niet mogelijk de gegevens gerichter over te nemen. Er was telkens sprake een direct gevaar voor de nationale veiligheid, te weten een ernstige terroristische dreiging en een cybervaanval, die tot het overnemen van de gegevens noodzaakte. Het belang van nationale veiligheid prevaleerde boven het belang van de bescherming van de grondrechten en de belangen van de personen of organisaties van of over wie informatie in de gegevens voorkwam en die geen target van de diensten waren. Deze operaties zijn derhalve als rechtmatig beoordeeld.

In de geheime bijlage wordt nader op deze operaties ingegaan.

7.2 Ontsluiten van ongeëvalueerde gegevens voor het operationeel proces

De gegevens zijn op het moment van overnemen dus vaak nog niet op relevantie voor de veiligheids- en inlichtingentaak beoordeeld. Dit betekent dat het ongeëvalueerde gegevens betreft. Om de overgenomen ongeëvalueerde gegevens op relevantie te kunnen beoordelen, moeten ze aan de operationele teams ter beschikking worden gesteld. Om de inbreuk op de grondrechten en de belangen van de betrokkene(n) binnen aanvaardbare grenzen te houden, is het noodzakelijk dat aan de toegang tot deze ongeëvalueerde gegevens nadere voorwaarden worden verbonden.

Toetsingskader (paragraaf 5.2, p. 18 van bijlage II):

- De diensten dienen invulling te geven aan de voorwaarde dat medewerkers alleen toegang hebben tot die ongeëvalueerde gegevens, voor zover dat noodzakelijk is voor een goede uitvoering van de hun opgedragen taken (need-to-know).

- Indien de ongeëvalueerde gegevens ongericht zijn overgenomen en (naar verwachting) hoofdzakelijk gegevens zullen bevatten die niet relevant zijn voor de goede taaktuitvoering van de diensten, dient daaraan tevens de nadere voorwaarde van functie- en/of taakscheiding te worden verbonden. Deze randvoorwaarde moet uit het verzoek om toestemming blijken.

Bevindingen

Autorisaties voor toegang tot ongeëvalueerde gegevens
De JSCU gebruikt voor het ter beschikking stellen van ongeëvalueerde gegevens aan de operationele teams over het algemeen systemen van de AIVD, die ook ter beschikking staan van de MIVD. Deze interne systemen zijn beveiligd en afgeschermd en niet voor (interne) derden toegankelijk. De gegevens worden in het overgrote deel van de gevallen in de binnen deze systemen reeds bestaande applicaties (software) geplaatst. In sommige operaties worden nieuwe applicaties of methoden ontworpen om de ontsluiting van de gegevens in een specifiek geval mogelijk te maken.

Voordat medewerkers van het operationele team toegang hebben tot deze applicaties moeten zij eerst worden geautoriseerd. Binnen de AIVD worden deze autorisaties door het teamhoofd gegeven en binnen de MIVD door of namens het afdelingshoofd. Dit betekent in de praktijk dat alleen die medewerkers voor wie dit op basis van hun werkzaamheden noodzakelijk is, toegang hebben tot een applicatie en de daarin geplaatste ongeëvalueerde gegevens. Dit zijn doorgaans de bewerkers of analisten die de hackoperatie hebben aangevraagd.

In sommige applicaties kunnen de gegevens door leden van andere operationele teams worden doorzocht op basis van een systeem van “hit / no hit”. De medewerker krijgt dan alleen te zien dat bepaalde gegevens mogelijk relevante informatie bevatten. Deze kan vervolgens op de gebruikelijke wijze autorisatie voor het gebruik van de gegevens vragen. In bepaalde applicaties kan een individuele medewerker (in de praktijk vaak een bewerker of analist) die gebruik maakt van bepaalde ongeëvalueerde gegevens op zijn beurt weer medewerkers (ook van andere operationele teams) autoriseren.

Deze procedures zijn in beginsel een zorgvuldige invulling van het vereiste van need-to-know. Gelijk aan de eisen bij andere bijzondere bevoegdheden zijn de daaruit afkomstige ongeëvalueerde gegevens op deze wijze immers alleen toegankelijk voor die medewerkers die de taak hebben deze op relevantie te beoordelen. Ter vergelijking kan worden gedacht aan de bevoegdheid tot gerichte interceptie (bijvoorbeeld een telefoontap), waarbij de desbetreffende medewerkers van het operationele team toegang hebben tot alle verworven ongeëvalueerde gesprekken om deze daarna op relevantie uit te luisteren.

Kanttekeningen worden geplaatst bij die gevallen waarin de toestemming voor het gebruik van bepaalde ongeëvalueerde gegevens kan worden gegeven op het niveau van de individuele medewerker. Gelet op het belang dat aan de vereisten van need-to-know moet worden gehecht op het moment dat wordt gewerkt met ongeëvalueerde gegevens, wordt aanbevolen de toestemming in die gevallen op een hoger niveau te beleggen, te weten op die van het team- of bureauhoofd.

Functie- en taakscheiding bij ongericht overgenomen ongeëvalueerde gegevens
Analoog aan de vereisten voor het gebruik van gegevens, die ongericht zijn geïntercepteerd (satellietcommunicatie), dienen bij door middel van een hack ongericht overgenomen gegevens – naast autorisaties – additionele interne procedures van functie- en taakscheiding te worden gevolgd. Deze dienen zoveel mogelijk te voorkomen dat informatie van of over personen en organisaties die geen target zijn in het operationeel proces terechtkomen.

Bij de AIVD hebben alleen een aantal technisch beheerders en specialisten bij de JSCU volledige toegang tot alle ongericht overgenomen gegevens. De bewerkers van het team die de hack hebben aangevraagd worden tot zekere hoogte evenzeer geautoriseerd, echter niet tot het directe gebruik van de gegevens. De applicatie (software) waarmee de gegevens voor de bewerkers wordt ontsloten werkt op basis van zoekslagen en –vragen. Gegevens van personen of organisaties die geen relatie hebben met het onderzoek zijn daarmee niet voor het operationele proces beschikbaar. Deze randvoorwaarden die aan het gebruik van de gegevens zijn verbonden, waren – zij het in abstracte zin – ook in de verzoeken om toestemming vermeld. De AIVD heeft hiermee een zorgvuldige invulling gegeven aan de randvoorwaarden van functie- en taakscheiding voor het gebruik van door middel van een hack ongericht overgenomen gegevens.

Bij de MIVD zijn de ongericht overgenomen gegevens in opdracht van de analisten van het operationele team door de JSCU op relevantie doorzocht. Aan het team zijn alleen de voor het onderzoek (mogelijk) relevante gegevens gerapporteerd. Het gevolg van deze werkwijze is dat er sprake is van een technische scheiding tussen de systemen voor ongeëvalueerde gegevens bij de JSCU en de systemen die de MIVD gebruikt voor het opslaan van relevante gegevens. Hiermee is voorkomen dat de ongericht overgenomen gegevens in hun geheel door het operationele team van de MIVD konden worden gebruikt. Deze rechtmatige werkwijze werd echter niet als randvoorwaarde in het verzoek om (verlenging van de) toestemming vermeld. Dit wordt als onzorgvuldig beoordeeld.

7.3 Het beoordelen, bewaren en vernietigen van gegevens

Toetsingskader (paragraaf 5.3, p. 18/19 van bijlage II):

- Het uitwerken van de gegevens is alleen toegestaan als zij als relevant zijn beoordeeld voor het onderzoek waarvoor ze zijn overgenomen of ten behoeve van een ander lopend onderzoek dat onder de veiligheids- of inlichtingentaak valt.
- Gegevens die niet als relevant zijn beoordeeld dienen terstond te worden verwijderd en vernietigd.
- Gegevens die op enig moment als relevant zijn beoordeeld, maar ten onrechte blijken te zijn verwerkt of – na verloop van tijd – hun betekenis hebben verloren, dienen terstond te worden verwijderd en vernietigd, tenzij regels omtrent bewaring daaraan in de weg staan.

Bevindingen

Niet alle overgenomen gegevens die in de applicaties worden geplaatst, worden dus door de operationele teams op relevantie beoordeeld. De grote hoeveelheid gegevens maakt dat het in het algemeen doelmatiger is met zoektermen te werken en alleen de resultaten daarvan op relevantie te beoordelen. Gegevens die wel als evident relevant worden beoordeeld, worden doorgaans naar daarvoor bestemde systemen geëxporteerd. In de systemen waarin relevant bevonden gegevens worden vastgelegd, zijn geen uit een hack afkomstige gegevens aangetroffen die op het moment van vastleggen niet als zodanig hadden mogen worden aangemerkt.

Geconstateerd is dat bij zowel de AIVD als de MIVD in het geheel geen beleid, laat staan werkwijzen bestaan om verzamelde gegevens al dan niet na verloop van tijd te verwijderen en te vernietigen. Dit geldt zowel voor uit hacks afkomstige gegevens die op enig moment op relevantie zijn beoordeeld, als voor die waarbij een beoordeling in het geheel niet heeft plaatsgevonden.

Ook voor deze laatste categorie, de ongeëvalueerde gegevens, worden dus geen bewaartermijnen gehanteerd. Dat wil zeggen dat alle gegevens die niet zijn beoordeeld gewoon bewaard blijven.

Dit geldt tevens voor gegevens van bijvoorbeeld non-targets, derden en ongericht overgenomen gegevens. Deze praktijk staat in contrast met de toezegging aan de Tweede Kamer die in 2014 door de minister van BZK is gedaan om vooruitlopend op de inwerkingtreding van de nieuwe wet (Wiv 20..) (buitenwettelijke) bewaartermijnen vast te stellen.[13]

Ten onrechte verwerkte gegevens worden evenzeer niet vernietigd. Zo werd in een operatie van de AIVD op enig moment door het operationele team bemerkt dat twee gehackte e-mailaccounts (toch) niet aan het target toebehoorden. Bij de constatering daarvan is aan de JSCU direct verzocht de operatie stop te zetten. De JSCU is niet verzocht tot vernietiging van de gegevens over te gaan, hetgeen dan ook niet heeft plaatsgevonden. Gegevens uit deze e-mailaccounts zijn eveneens in de systemen voor relevante informatie blijven staan. De AIVD heeft in deze operatie onrechtmatig gehandeld (artikel 43 lid 2 Wiv 2002).

In een operatie bij de MIVD is in één geval een hack doorgelopen, terwijl de toestemming voor de operatie niet was verlengd. Op het moment dat de MIVD dat constateerde is de JSCU direct gevraagd de operatie stop te zetten. In het logboek over deze operatie is aangegeven dat de MIVD geen kennis meer heeft genomen van deze gegevens. De JSCU is echter niet verzocht tot vernietiging over te gaan. Ook deze gegevens zijn in de systemen van de JSCU nog steeds beschikbaar. De MIVD heeft daarmee onrechtmatig gehandeld (artikel 43 lid 2 Wiv 2002).

Het ontbreken bij beiden diensten van een werkwijze en praktijk voor het vernietigen van gegevens, waaronder het nalaten van het terstond vernietigen van niet relevante en ten onrechte verwerkte gegevens, is zonder meer onrechtmatig. Voor de AIVD geldt tevens dat dit is nagelaten, ondanks eerdere toezeggingen in 2014 aan de Tweede Kamer dat bewaartermijnen voor ongeëvalueerde gegevens zouden worden vastgesteld.

De CTIVD beveelt de AIVD (nogmaals) en de MIVD aan, vooruitlopend op de nieuwe wet (Wiv 20..), bewaartermijnen voor ongeëvalueerde gegevens van maximaal één jaar vast te stellen en deze te handhaven. Daarbij geldt dat deze interne handhaving van de bewaartermijnen volledig en toetsbaar moet zijn. Een effectieve werkwijze zou zijn, het op herkomst (in de zin van bron en tijdstip) labelen van gegevens met een daaraan gekoppelde geautomatiseerde vernietiging en verslaglegging daarvan. Een dergelijke werkwijze kan een wezenlijk onderdeel zijn van de zorgplicht voor geautomatiseerde gegevensverwerking zoals in de Zienswijze op de Wiv 20.. van de CTIVD is beschreven.[14]

Daarnaast dienen beide diensten beleid en/of een werkinstructie te ontwikkelen waarin wordt vastgelegd op welke wijze en door wie tot de verwijdering en vernietiging van niet relevante en ten onrechte verwerkte gegevens wordt overgegaan. Datzelfde geldt voor gegevens die hun aanvankelijke betekenis hebben verloren. Vervolgens dient er intern op te worden toegezien dat de daarvoor aangemerkte gegevens ook daadwerkelijk terstond worden vernietigd.

---

[13] Naar aanleiding van toezichtsrapport 38, zie Toetsingskader, p. 19 van bijlage II

[14] Zienswijze van de CTIVD op het wetsvoorstel Wiv 20., bijlage I (november 2016) , p. 23-25 beschikbaar op www.ctivd.nl

8 Het verstrekken van ongeëvalueerde gegevens

In dit onderzoek is expliciet aandacht besteed aan verstrekkingen van uit hacks afkomstige ongeëvalueerde, nog niet op relevantie beoordeelde, gegevens aan buitenlandse diensten. Bij hacken kan dit bijvoorbeeld gaan om een volledig webforum, maar ook om de inhoud van een server of computer.

Toetsingskader (Hoofdstuk 6, p. 20, van bijlage II):

- Voor het verstrekken van ongeëvalueerde gegevens aan een buitenlandse dienst dient de minister vooraf toestemming te geven.

Bevindingen

In de onderzochte operaties heeft de AIVD geen uit een hack afkomstige ongeëvalueerde gegevens verstrekt aan buitenlandse diensten. De MIVD heeft dit in één geval wel gedaan.

In deze operatie heeft de MIVD in het kader van een gezamenlijke operatie uit een hack afkomstige ongeëvalueerde gegevens verstrekt aan twee buitenlandse partnerdiensten. Hoewel de minister middels het verzoek om toestemming van de (nauwe) samenwerking met deze buitenlandse diensten op de hoogte was, volgde hieruit niet dat ook ongeëvalueerde gegevens konden worden gedeeld. Dit stond ook niet expliciet in het verzoek vermeld. De MIVD heeft dan ook niet vooraf om toestemming voor de verstrekking van ongeëvalueerde gegevens verzocht. Dit had wel gemoeten. De MIVD heeft hiermee onrechtmatig gehandeld.

9 Conclusies

De CTIVD trekt in dit rapport de navolgende conclusies:

Hoofdstuk 2: algemeen beeld en effectiviteit

De AIVD en de MIVD hebben de wettelijke bevoegdheid te hacken, dat wil zeggen binnen te dringen in geautomatiseerde werken. Hacken blijkt in het algemeen een effectieve bevoegdheid, in die zin dat de inzet in de regel heeft geleid tot resultaten in het belang van de nationale veiligheid, die niet op een andere manier hadden kunnen worden behaald.

De AIVD en de MIVD zijn in het overgrote deel van de tientallen onderzochte operaties in 2015 bij de inzet van de hackbevoegdheid weloverwogen en rechtmatig te werk gegaan. De diensten zijn zich bewust van de ernstige inmenging in de rechten en belangen van betrokkene(n) die de inzet van de hackbevoegdheid met zich mee kan brengen. Daarbij moet in eerste plaats worden gedacht aan het recht op de bescherming van de persoonlijke levenssfeer, maar ook aan het belang van het bewaken van de integriteit van ICT-systemen. Over het algemeen gaan de diensten derhalve zorgvuldig om met de inzet van de bijzondere bevoegdheid en vindt er een juiste afweging plaats tussen het belang van de nationale veiligheid en de in het geding zijnde belangen van de betrokkene(n).

Hoofdstuk 4: het opstellen van het verzoek om toestemming

Het verrichten van het zogenaamde technisch vooronderzoek, dat er op gericht is de technische mogelijkheden voor een hack ten behoeve van de interne besluitvorming tot de inzet daarvan te verkennen, vindt op rechtmatige wijze plaats. Doorgaans worden de verzoeken om toestemming voor de inzet van de hackbevoegdheid op zorgvuldige wijze gemotiveerd en is daarin opgenomen op welke geautomatiseerde werken van welke personen of organisaties de inzet is gericht, voor welk doel de inzet plaatsvindt en welke informatie daarmee wordt beoogd te verkrijgen. In een beperkt aantal gevallen zijn door de AIVD en MIVD geautomatiseerde werken binnengedrongen of bijgeschreven die niet onder de initiële toestemming vielen. Dit is onrechtmatig. Daarnaast schieten beide diensten tekort – in het geval ten tijde van de toestemmingsverlening het niet mogelijk was aan te geven tegen welke personen of organisaties de hackbevoegdheid zou worden ingezet – in de verplichte afzonderlijk kennisgeving aan de minister daarover bij het nadien bekend worden van die identiteiten. Dit wordt als onzorgvuldig beoordeeld. Bovendien schiet de verslaglegging bij de uitvoering van fysieke hacks bij beide diensten tekort. Dit is onzorgvuldig.

De werkwijze van de diensten met betrekking tot de inzet van de hackbevoegdheid tegen (leden van) organisaties is over het algemeen rechtmatig. In een beperkt aantal gevallen was de reikwijdte van de motivering en daarmee van de toestemming onvoldoende begrensd doordat de beschrijving van (leden van) de organisaties of van de binnen te dringen geautomatiseerde werken te algemeen was. Omdat echter van de gegeven toestemming in de uitvoering binnen toelaatbare grenzen gebruik is gemaakt, acht de CTIVD dit niet onrechtmatig, maar onzorgvuldig.

Met betrekking tot het direct of indirect hacken van verschoningsgerechtigden zijn geen onrechtmatig- of onzorgvuldigheden geconstateerd.

De AIVD heeft in de onderzoeksperiode in beperkte mate non-targets gehackt. Dit is alleen gebeurd wanneer er concrete aanwijzingen waren voor een direct gevaar voor de nationale veiligheid van het uiteindelijke target zelf dan wel sprake was van overige zwaarwegende operationele belangen. Deze werkwijze van de AIVD is rechtmatig. In één operatie had in het verzoek om toestemming explicieter moeten worden aangegeven wat het doel van de operatie was. Omdat uiteindelijk alleen gegevens zijn uitgewerkt die betrekking hadden op het target zelf is dit onzorgvuldig.

De AIVD en de MIVD hebben rechtmatig gehandeld bij het binnendringen in geautomatiseerde werken van derden. Dit was in alle onderzochte operaties onvermijdelijk om uiteindelijk in het geautomatiseerd werk van het uiteindelijke target te kunnen binnendringen. Gedurende de onderzoeksperiode heeft geen inzet plaatsgevonden tegen individuele burgers als derde.

Hoofdstuk 5: de toestemmingsverlening

Vanwege administratieve processen binnen de AIVD dienen verzoeken om verlenging van de inzet van de hackbevoegdheid intern dusdanig ruim van tevoren te worden opgesteld dat een recente stand van zaken in het onderzoek niet in de toestemmingsprocedure voor de verlenging kan worden betrokken. Dit is onzorgvuldig.

Bij de MIVD wordt de verlenging van de inzet van de hackbevoegdheid niet ter goedkeuring aan de minister voorgelegd. Daardoor kan het gebeuren dat de operatie na verloop van tijd een ander verloop of karakter krijgt dan waarvoor de minister toestemming heeft gegeven. Dit heeft een onrechtmatigheid opgeleverd.

Hoofdstuk 6: de uitvoering

De werkwijze en de relevante afwegingen voor het al dan niet melden van onbekende kwetsbaarheden (*zero day's*) zijn intern niet uitgewerkt en vastgelegd. Bovendien vindt van de gemaakte afwegingen geen centrale verslaglegging plaats. Hierdoor is interne controle en extern toezicht op de gemaakte afwegingen niet goed mogelijk. Ook kan het gebeuren dat kwetsbaarheden niet alsnog worden gemeld nadat het belang voor het niet-melden is verminderd of weggevallen. Dit is onzorgvuldig.

Hoofdstuk 7: beoordelen, bewaren en vernietigen van gegevens

De ontsluiting van gegevens aan medewerkers in het operationeel proces vindt in het algemeen op zorgvuldige wijze plaats. Bij de MIVD is bij de ontsluiting van ongericht overgenomen gegevens de randvoorwaarde van functie- en taakscheiding niet in het verzoek tot toestemming voor de inzet van de hackbevoegdheid vermeld. Dit is onzorgvuldig.

Het ontbreken van een werkwijze en praktijk voor het vernietigen van gegevens, waaronder het niet terstond vernietigen van niet relevante en ten onrechte verwerkte gegevens, is bij beide diensten zonder meer onrechtmatig. Bovendien is bij de AIVD het niet vaststellen van bewaartermijnen voor ongeëvalueerde gegevens, ondanks toezeggingen in 2014 van de minister van BZK aan de Tweede Kamer daartoe wel (buitenwettelijk) over te gaan, onrechtmatig.

Hoofdstuk 8: verstrekken van ongeëvalueerde gegevens

De MIVD heeft in één gezamenlijke operatie niet expliciet vooraf om ministeriële toestemming verzocht om ongeëvalueerde gegevens te verstrekken aan een buitenlandse dienst. Dit is onrechtmatig.

10 Aanbevelingen

De CTIVD doet in dit rapport de navolgende aanbevelingen:

Hoofdstuk 4: het opstellen van het verzoek om toestemming

1. De AIVD en MIVD dienen hun werkwijze in overeenstemming te brengen met eerdere toezeggingen van de ministers met betrekking tot het afzonderlijk direct kennisgeven aan de toestemmingsverlener bij het bekend worden van identiteiten, die ten tijde van de toestemming nog niet bekend waren.

2. De diensten moeten de verplichting tot verslaglegging van de bij fysieke hacks binnengedrongen geautomatiseerde werken in een werkinstructie opnemen.

3. De MIVD dient een procedure in te richten waarbij de toestemming voor een bijschrijving op een hoger niveau wordt belegd dan dat van de individuele medewerker.

Hoofdstuk 5: de toestemmingsverlening

4. De AIVD moet, vooruitlopend op de nieuwe wet (Wiv 20..), de toestemming voor fysieke hacks op het niveau van de minister beleggen.

5. De MIVD dient, vooruitlopend op de wet Wiv 20.., de Mandaatregeling en/of het beleid zo aan te passen dat ook de verzoeken om verlengingen van een hackoperatie aan de minister worden voorgelegd.

Hoofdstuk 6: de uitvoering

6. Zowel de AIVD als de MIVD dienen tot logging (het continu geautomatiseerd integraal vastleggen van gegevens met betrekking tot) van de uitvoering van de hackbevoegdheid en de daarbij verrichte technische handelingen over te gaan.

7. De diensten dienen beleid en werkwijzen te ontwikkelen waarin relevante afwegingen met betrekking tot het al dan niet informeren van belangendragers over geconstateerde onbekende kwetsbaarheden (zero day's) worden geconcretiseerd en vastgelegd. Daarnaast dient (centrale) verslaglegging van de geconstateerde onbekende kwetsbaarheden en de daarbij gemaakte afwegingen plaats te vinden. Voor niet gemelde onbekende kwetsbaarheden dient een periodieke toetsingstermijn te worden bepaald, waarbinnen wordt beoordeeld of – indien nog opportuun – het operationeel belang nog steeds dient te prevaleren.

Hoofdstuk 7: het overnemen, beoordelen en vernietigen van gegevens

8. De AIVD en MIVD moeten het toestemmingsniveau met betrekking tot het interne gebruik van uit hacks afkomstige ongeëvalueerde gegevens in alle gevallen op het niveau van het teamhoofd/bureauhoofd beleggen in plaats van op het niveau van een bewerker of analist.

9. De beide diensten dienen, vooruitlopend op de nieuwe wet (Wiv 20..), buitenwettelijke bewaartermijnen voor ongeëvalueerde gegevens van maximaal één jaar vast te stellen en deze nadrukkelijk te handhaven.

10. De AIVD en de MIVD dienen beleid en/of een werkinstructie te ontwikkelen, waarin wordt vastgelegd op welke wijze tot de verwijdering en vernietiging van niet relevant beoordeelde of ten onrechte verwerkte gegevens moet worden overgegaan. Datzelfde geldt voor gegevens die hun aanvankelijke betekenis hebben verloren.

T 070 315 58 20 | **F** 070 381 71 68
E info@ctivd.nl | www.ctivd.nl