Bijlage III

Begrippenlijst

bij het 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

BIJLAGE III

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

Afdelingshoofd (MIVD)	Functionaris binnen de MIVD die hiërarchisch als volgt is ingebed in de organisatie: directeur, afdelingshoofd, bureauhoofd, sectiehoofd.
Applicatie	Een computerprogramma waarmee bepaalde taken uitgevoerd kunnen worden (bijvoorbeeld Microsoft Word, waarmee tekst verwerkt kan worden). De diensten maken gebruik van applicaties voor bijvoorbeeld de opslag, ontsluiting en analyse van gegevens.
Bewerker (AIVD)	De bewerker is de dienstmedewerker die onder meer nieuwe gegevens beoordeelt en op basis daarvan de aanzet doet voor inlichtingenproducten, de koers van het team en de eventuele inzet van bevoegdheden. Bij de MIVD kan deze taak zijn belegd bij een analist.
Bijschrijven	Met het bijschrijven worden andere geautomatiseerde werken (van dezelfde persoon of organisatie) of andere leden van een organisatie in een verzoek om toestemming opgenomen, die een aanvulling zijn op of in de plaats treden van de daarin al genoemde.
Bijzondere bevoegdheid	Een bevoegdheid van de dienst die een specifieke inbreuk op de persoonlijke levenssfeer maakt. De toepassing van een bijzondere bevoegdheid heeft veelal een geheim karakter. De bijzondere bevoegdheden en de voorwaarden waaronder deze mogen worden toegepast zijn neergelegd in de artikelen 20 t/m 30 van de Wiv 2002 (bijvoorbeeld tappen of de inzet van een agent). Zie ook “directe inzet”/”indirecte inzet”.
Buitenlandse dienst	Een inlichtingen- en/of veiligheidsdienst van een ander land.
Bulkdata	Ongeëvalueerde gegevens; in de regel grote hoeveelheden metadata.
Bureauhoofd (MIVD)	Functionaris binnen de MIVD die hiërarchisch als volgt is ingebed in de organisatie: directeur, afdelingshoofd, bureauhoofd, sectiehoofd.
Compartimentering	Het in de praktijk brengen van het need to know beginsel uit artikel 35 Wiv 2002 in de zin dat binnen de AIVD of de MIVD ervoor wordt zorg gedragen dat informatie alleen aan medewerkers verstrekt wordt voor zover dat noodzakelijk is voor een goede uitvoering van de aan hen opgedragen taken.
Credentials	Inloggegevens (bijvoorbeeld gebruikersnaam en wachtwoord).
Cyber	Datgene dat samenhangt met de digitale of virtuele wereld, waaronder het internet.

Derde	Personen of organisaties die zelf niet een target zijn en waartegen geen bijzondere bevoegdheden worden ingezet. Deze derden kunnen wel in een onderzoek van de AIVD of de MIVD betrokken raken, bijvoorbeeld doordat zij gebruik maken van dezelfde communicatiemiddelen. In het kader van de hackbevoegdheid gaat het dan doorgaans om een technische gerelateerde partij wier geautomatiseerde werk wordt gebruikt om binnen te dringen in het geautomatiseerd werk van het target.
Directe inzet	De inzet van een bijzondere bevoegdheid die specifiek is gericht op een verschoningsgerechtigde zelf.
Directeur (AIVD)	Functionaris binnen de AIVD die hiërarchisch als volgt is ingebed in de organisatie: directeur-generaal, *directeur*, unithoofd, teamhoofd.
Directeur-Generaal (AIVD)	Functionaris die de leiding heeft over de AIVD, ook wel het hoofd genoemd. Binnen de AIVD is de directeur-generaal hiërarchisch als volgt ingebed in de organisatie: directeur-generaal, directeur, unithoofd, teamhoofd.
Directeur (MIVD)	Functionaris die de leiding heeft over de MIVD. Binnen de MIVD is de directeur hiërarchisch als volgt ingebed in de organisatie: directeur, afdelingshoofd, bureauhoofd, sectiehoofd.
E-mailaccount	E-mail is elektronisch postverkeer. Een e-mailgebruiker gebruikt een account om e-mails te verzenden en te ontvangen. Een e-mailaccount kan aangevraagd worden bij een Internet Service Provider (bijvoorbeeld KPN) of een andere aanbieder van e-maildiensten (bijvoorbeeld Hotmail of Gmail).
Encryptie	Het versleutelen van informatie om deze onleesbaar te maken voor onbevoegden.
Exploit	Software, gegevens of opeenvolging van commando's die gebruikmaken van een kwetsbaarheid in software en/of hardware om ongewenste functies en/of gedrag te veroorzaken.
Fysieke hack	Een hack waarbij het geautomatiseerd werk (tijdelijk) in handen is van één van de diensten.
Geautomatiseerd werk	Een inrichting die bestemd is om langs elektronische weg gegevens op te slaan, te verwerken en over te dragen (bijvoorbeeld een computer, een computernetwerk, een mobiele telefoon of een server).
Geëvalueerde gegevens	Gegevens die op relevantie zijn beoordeeld.
Gegevensverwerking (verwerking van gegevens)	Elke handeling of elk geheel van handelingen met betrekking tot gegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding, of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens (artikel 1 sub f Wiv 2002).
Gericht	Als van tevoren kan worden aangegeven op welke personen, organisatie of technisch kenmerk de gegevensverwerving gericht is.
Hack op afstand	Een hack op een geautomatiseerd werk buiten het directe fysieke bereik van de diensten, bijvoorbeeld via het internet.
Hacken	Het binnendringen in een geautomatiseerd werk.

Indirecte inzet	De inzet van een bijzondere bevoegdheid die niet specifiek is gericht op een verschoningsgerechtigde zelf, maar waarbij wel vertrouwelijke communicatie van of met hen wordt onderschept omdat de persoon jegens wie de inzet is gericht contact heeft me een verschonings-gerechtigde, (bijvoorbeeld) een cliënt van de advocaat of een bron van de journalist is.
Inlichtingentaak	Het doen van onderzoek naar andere landen en het potentieel en de strijdkrachten van andere mogendheden (zie artikel 6, tweede lid, aanhef d en artikel 7, tweede lid, aanhef a en e Wet op de inlichtingen- en veiligheidsdiensten).
IP-adres	Iedere afzonderlijke computer die via IP met andere computers communiceert heeft een uniek adres, het IP-adres. Het IP-adres identificeert de aansluiting van de computer met het internet, vergelijkbaar met een telefoonnummer.
JSCU	Joint Sigint Cyber Unit, gezamenlijke eenheid van de AIVD en de MIVD die zich bezighoudt met de verwerking van gegevens op het gebied van sigint en cyber.
Kwetsbaarheid	Eigenschap van een informatiesysteem (of een onderdeel daarvan) die een kwaadwillende partij de kans geeft om de legitieme toegang tot informatie of functionaliteit te verhinderen en te beïnvloeden dan wel ongeautoriseerd te benaderen.
Logging	Het volledig geautomatiseerd integraal vastleggen van gegevens over de uitvoering van een hack.
Malware	Samentrekking van malicious software. Malware is de term die tegenwoordig als generieke aanduiding wordt gebruikt voor onder andere virussen, wormen en Trojaanse paarden.
Non-target	Een persoon of organisatie uit de omgeving van het target jegens wie een bijzondere bevoegdheid wordt ingezet ten einde via deze persoon of organisatie zicht te krijgen op een target. Een non-target is zelf niet in onderzoek bij de AIVD of MIVD.
Ontsluiting	Het toegankelijk of doorzoekbaar maken van gegevens.
Ongeëvalueerde gegevens	Alle gegevens – zowel metagegevens als inhoudelijke gegevens en zowel gericht als ongericht verworven gegevens – die nog niet zijn beoordeeld op relevantie voor de taakuitvoering.
Ongericht	Als niet van tevoren kan worden aangegeven op welke persoon, organisatie of technisch kenmerk de gegevensverwerving gericht is.
Onrechtmatig	De CTIVD komt tot het oordeel onrechtmatig als sprake is van strijdigheid met de wet of als de motivering zodanig gebrekkig is dat herstel ervan niet mogelijk is. Hierbij wordt rekening gehouden met de aard van de belangen waarop een inbreuk wordt gemaakt. De CTIVD ziet haar aanbevelingen, indien en voor zover zij door de betrokken minister(s) zijn overgenomen, ook in de berichtgeving aan het parlement, als onderdeel van de op de AIVD en de MIVD toepasselijke wet- en regelgeving. Het handelen van de AIVD en de MIVD dat hiermee niet in overeenstemming is, is derhalve ook onrechtmatig.

Onzorgvuldig	De CTIVD komt tot het oordeel onzorgvuldig als sprake is van een tekortkoming die herstelbaar is. In eerdere toezichtsrapporten ging het dan meestal om een gebrekkige motivering. Op basis van eigen nader onderzoek van de CTIVD bleek dan dat ondanks een tekortkoming in de motivering toch aan de wettelijke vereisten (beginselen van noodzakelijkheid, proportionaliteit en subsidiariteit) is voldaan. Van een onzorgvuldige werkwijze is sprake als deze rechtens tekortschiet, maar de risico's daarvan zich niet of nauwelijks hebben gerealiseerd.
Operationeel proces	Het combineren van verworven gegevens met andere (reeds beschikbare) gegevens waarna de gegevens worden geduid en geanalyseerd om rapportages op te stellen die desgewenst aan de verantwoordelijke instanties kunnen worden verstrekt.
Organisatie	Een duurzaam samenwerkingsverband met een gemeenschappelijke doelstelling, die kenbaar is voor zijn leden.
Patch	Een patch (letterlijk: 'pleister') kan bestaan uit reparatiesoftware of kan wijzigingen bevatten, die direct in een programma worden doorgevoerd om het desbetreffende programma te repareren of te verbeteren.
Responsible disclosure	Praktijk van het verantwoord melden van aangetroffen beveiligings-lekken. Hierbij worden afspraken gehanteerd die er doorgaans op 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.
Server	Een computer of een programma dat diensten verleent aan andere programma's (of gemeenschappelijke voorzieningen levert).
Signals intelligence (sigint)	Inlichtingen die verzameld worden uit opgevangen elektronische signalen.
Taakuitvoering	De uitvoering van de taken zoals die zijn omschreven in artikel 6 lid 2 Wiv 2002 (AIVD) en artikel 7 lid 2 Wiv 2002 (MIVD).
Target	Een persoon of organisatie waar de AIVD en MIVD onderzoek naar verricht (artikel 13 Wiv 2002).
Teamhoofd (AIVD)	Functionaris binnen de AIVD die hiërarchisch als volgt is ingebed in de organisatie: directeur-generaal, directeur, unithoofd, *teamhoofd*.
Uitwerken	De schriftelijke verslaglegging van de opbrengst van de inzet van een bijzondere bevoegdheid.
Unithoofd (AIVD)	Functionaris binnen de AIVD die hiërarchisch als volgt is ingebed in de organisatie: directeur-generaal, directeur, *unithoofd*, teamhoofd.
Veiligheidstaak	Taak gericht op het onderkennen van dreigingen voor het voort-bestaan van de democratische rechtsorde (artikel 6, tweede lid, aanhef d Wet op de inlichtingen- en veiligheidsdiensten), dan wel voor de veiligheid of andere gewichtige belangen van de staat, of voor de veiligheid en de paraatheid van de krijgsmacht (artikel 7, tweede lid, aanhef c Wet op de inlichtingen- en veiligheidsdiensten).
Verschoningsgerechtigde	Een persoon met een maatschappelijke vertrouwensfunctie, in die zin dat eenieder vertrouwelijk met deze persoon moet kunnen communiceren. Op grond van deze functie komt aan zijn communicatie extra bescherming toe.

Vertrouwelijke communicatie	Communicatie toevertrouwd aan een verschoningsgerechtigde, maar niet in zijn hoedanigheid als privépersoon of andere professionele hoedanigheid.
Webforum	Digitale publieke discussiepagina's op het internet. Op sommige forums dienen bezoekers zich aan te melden om toegang te krijgen. Via deze pagina's kunnen de bezoekers veelal ook onderling berichten uitwisselen.
Werkwijze	Het schriftelijke beleid van de diensten en/of de werkwijze die in de praktijk wordt gehanteerd.
Wiv 2002	Wet op de inlichtingen- en veiligheidsdiensten 2002. Deze wet geldt ten tijde van het onderzoek door de CTIVD.
Wiv 20..	Voorstel voor een nieuwe Wet op de inlichtingen- en veiligheids-diensten, dat in oktober 2016 bij de Tweede Kamer is ingediend en op 14 februari 2017 door de Tweede Kamer is aangenomen.
Zero day kwetsbaarheid	Een kwetsbaarheid waarvoor nog geen patch beschikbaar is, omdat de maker daarvan nog geen tijd heeft gehad om een patch maken en/of omdat deze hem nog niet bekend is. Dit wordt ook wel een onbekende kwetsbaarheid genoemd.

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