



MJenV

**Directoraat-Generaal
Rechtspleging en
Rechtshandhaving**
Directie Rechtshandhaving en
Criminaliteitsbestrijding
Criminaliteit en Veiligheid

Datum
4 december 2023

Projectnaam
CCIII

Ons kenmerk
4941132

Bijlagen
1

nota

Beleidsreactie wetsevaluatie bevoegdheid tot het binnendringen in een geautomatiseerd werk

1. Aanleiding

U wordt verzocht een besluit te nemen over de verzending van de beleidsreactie op de door het WODC uitgevoerde wetsevaluatie inzake de bevoegdheid tot het heimelijk en op afstand binnendringen in een geautomatiseerd werk (hierna: de binnendringbevoegdheid, ook de 'hackbevoegdheid' genoemd). Deze bevoegdheid is op 1 maart 2019 in werking getreden. Het rapport van de procureur-generaal bij de Hoge Raad, het rechtsvergelijkend onderzoek van het WODC en het jaarlijkse verslag van de IJenV zijn ook onderdeel van de beleidsreactie. U bent eerder over de voortgang geïnformeerd via nota [4545885](#) en [4617770](#).

De toezegging is gedaan om voor het herfstreces de beleidsreactie te versturen. Met het vervallen van het herfstreces kan verzending gebeuren voor het verkiezingsreces 27 oktober. De brief is akkoord bevonden door de Korpsleiding en het College van Procureurs-Generaal.

2. Geadviseerd besluit

U wordt geadviseerd akkoord te gaan met verzending van de beleidsreactie op de wetsevaluatie voor 27 oktober 2023.

Ten eerste, omdat de typen misdrijven waartegen de binnendringbevoegdheid kan worden ingezet vragen om een effectief middel als onderdeel van het beschikbare instrumentarium.

Ten tweede, wordt er een wijziging voorgesteld in het beleid van de aanschaf van binnendringsoftware. Deze wijziging dient de effectiviteit en is goedkoper.

Ten derde, op de onderwerpen toezicht en de keuring van technische hulpmiddelen wordt de politie gevraagd om nadere uitwerking. Deze uitwerking kan met de verzending van de brief beginnen. Het is wel waarschijnlijk dat deze uitwerking pas onder een volgend kabinet gereed is, waardoor het aan een volgend kabinet is om definitief over deze beleidswijzigingen te besluiten.

3. Kernpunten

De kernpunten uit de brief zijn:

1. De binnendringbevoegdheid heeft in relatief korte tijd haar meerwaarde in de digitale opsporing bewezen. De binnendringbevoegdheid is een steeds belangrijker instrument in de strijd tegen de georganiseerde criminaliteit. Van de 25 van de door het WODC onderzochte inzetten was er in 22 inzetten sprake van ondermijnende of daaraan gerelateerde criminaliteit.

- De overige inzetten waren tegen terrorisme, seksueel kindermisbruik en computervredebreuk.
2. Voor binnendringsoftware komt de beperking tot aanschaf voor een specifieke zaak te vervallen. Dit betekent dat software niet meer na gebruik in de specifieke zaak hoeft te worden verwijderd of dat de licentie verbruikt is, maar dat software in volgende zaken kan worden ingezet. Voor een effectieve uitvoering van de bevoegdheid bestaat er een mate van afhankelijkheid van deze software, waardoor toegang tot deze software noodzakelijk is. Tegelijkertijd maakt deze wijziging de aanschaf van deze software goedkoper en blijft de inzet van deze software een uiterste middel waardoor van lichtzinnig gebruik geen sprake is.. Hierdoor wordt het betreden van de markt van dergelijke software tot een minimum beperkt en zal aanschaf goedkoper zijn, zodat de markt voor onbekende kwetsbaarheden zo min mogelijk wordt gestimuleerd. Tevens blijven waarborgen om te voorkomen dat deze software van producten wordt afgenomen die leveren aan dubieuze regimes in stand gehouden.
 3. De politie stelt een visie op voor een intern kwaliteitssysteem, zodat systeemtoezicht van de Inspectie JenV de norm wordt.
 4. De politie, inclusief de keuringsdienst, wordt gevraagd een nieuwe systematiek uit te werken voor het keuren van technische hulpmiddelen waarbij in beginsel alle hulpmiddelen ter keuring worden aangeboden, maar het uitgangspunt dat sprake moet zijn van een goedgekeurd hulpmiddel komt te vervallen.

**Directoraat-Generaal
Rechtspleging en
Rechtshandhaving**
Directie Rechtshandhaving en
Criminaliteitsbestrijding
Criminaliteit en Veiligheid

Datum
4 december 2023

Ons kenmerk
4941132

4. Toelichting

Op de kernpunten 2,3 en 4 volgt een nadere toelichting

Ad 2: Binnendringsoftware van externe leveranciers

Het huidige beleid wordt bepaald door het regeerakkoord van Rutte-2. Het gebruik van binnendringsoftware van externe leveranciers is beperkt tot een aanschaf in een specifieke zaak (bijvoorbeeld een licentie-model), daarna moet de software worden verwijderd (of is de licentie verbruikt). Daarnaast mogen leveranciers deze software niet leveren aan dubieuze regimes en doet de AIVD naslag naar hen. Deze regeling had tot doel om het betreden van de markt van dergelijke software tot een minimum te beperken, zodat de markt voor onbekende kwetsbaarheden zo min mogelijk wordt gestimuleerd. In het regeerakkoord is wel opgenomen dat deze regeling wordt geëvalueerd waarna aanschaf voor algemeen gebruik wordt overwogen.

De IJenV, het WODC en de PGHR vermelden alle drie dat deze systematiek naar alle waarschijnlijkheid duurder is dan aanschaf voor algemeen gebruik. Het WODC stelt in de wetsevaluatie dat het de vraag is of dit model er wel toe leidt dat de markt van onbekende kwetsbaarheden minder gestimuleerd wordt. Hiermee zou het huidige beleid het tegenovergestelde effect hebben als dat in het regeerakkoord in Rutte-2 was beoogt.

Het WODC en de IJenV schrijven dat binnendringsoftware cruciaal is voor het verkrijgen van toegang tot met name telefoons.

Vanwege het kostbare licentiemodel en de mate van afhankelijkheid voor de effectiviteit van de bevoegdheid wordt u geadviseerd om aanschaf voor algemeen gebruik mogelijk te maken. Daarbij wordt u ook geadviseerd om de naslag van de AIVD en de toets door de politie of deze leveranciers leveren aan dubieuze regimes in stand te houden. Zoals terecht gesteld door de PGHR is deze toets niet

waterdicht, de politie is immers deels afhankelijk van de antwoorden van de leverancier zelf, maar dit is wel een waardevolle inspanning. Ook blijft het ministerie van JenV jaarlijks rapporteren over het gebruik van dit type software. Als laatste blijft dit type software een uiterste middel in het instrumentarium om binnen te dringen conform motie Recourt (PvdA). Echter gezien de ernst van de criminaliteit zoals ondermijning, terrorisme, seksueel kindermisbruik en computervredebreuk waartegen de binnendringbevoegdheid wordt ingezet is relatief vaak het gebruik van binnendringsoftware proportioneel en subsidiair bevonden.

Ad 3) Toezicht door de IJenV

Binnen het huidige beleid houdt de IJenV nalevingstoezicht. Dat wil zeggen dat voor elke inzet de rechtmatigheid wordt nagegaan. Dit toezicht heeft de wetgever voorafgaand aan de inwerkingtreding gewild. Zeker in de beginjaren van de bevoegdheid (sinds 2019) heeft dit toezicht bijgedragen aan de bestending van de bevoegdheid binnen de politieorganisatie. Het toezicht dat de IJenV houdt op de binnendringbevoegdheid is (erg) intensief wanneer men dit vergelijkt met andere (heimelijke) bevoegdheden.

Het WODC vermeldt onder andere dat het beeld bestaat dat de IJenV zich richt op de naleving van regels en niet op de uitvoerbaarheid van die regels. De politie ervaart dit als lastig, omdat een deel van de regels in haar ogen niet uitvoerbaar is en zij dus nooit aan die regels zal (kunnen) voldoen. Het WODC benoemt een patstelling tussen de politie en de IJenV in haar wetsevaluatie. Navraag leert dat deze patstelling door de politie en de IJenV niet wordt herkend.

U wordt geadviseerd een beweging in gang te zetten naar systeemtoezicht. Dat systeemtoezicht de norm wordt betekent dat de IJenV toezicht houdt via de interne systematiek van de politie om te controleren dat rechtmatig aan het bevel wordt voldaan, in plaats van zelf tijdens en na elke inzet dit te controleren. De omslag naar systeemtoezicht moet het intensieve karakter voor alle partijen verminderen. De verschuiving naar systeemtoezicht doet niets af aan de bevoegdheid van de IJenV om naar eigen inzicht verdiepend onderzoek uit te voeren.

Het beter op orde hebben van een intern kwaliteitssysteem binnen de politie is voor bovenstaand advies een voorwaarde. Dit kwaliteitssysteem moet passend zijn voor de politieorganisatie en voldoende solide zijn om te waarborgen dat de politie zich houdt aan de kaders van het bevel. De IJenV is in de afgelopen verslagen kritisch geweest op de voortgang van dit kwaliteitssysteem door de politie. Om deze reden wordt de politie nu expliciet verzocht om hierop een visie te ontwikkelen en dit te bespreken met de IJenV. Totdat het kwaliteitssysteem op orde is zal sprake zijn van nalevingstoezicht door de IJenV zoals dat nu wordt ingevuld.

Ad 4) Keuring van technische hulpmiddelen

Nadat de politie is binnengedrongen op een geautomatiseerd werk moet de informatie die relevant is voor de opsporing worden vergaard. Dit kan via een technisch hulpmiddel. Via dit middel wordt de informatie gedetecteerd, geregistreerd en getransporteerd. De vergaring moet op een betrouwbare, herleidbare en integere manier gebeuren. In het huidige beleid moet in beginsel sprake moet zijn van een vooraf goedgekeurd hulpmiddel bij een inzet.

**Directoraat-Generaal
Rechtspleging en
Rechtshandhaving**
Directie Rechtshandhaving en
Criminaliteitsbestrijding
Criminaliteit en Veiligheid

Datum
4 december 2023

Ons kenmerk
4941132

De keuring van technische hulpmiddelen heeft de meeste aandacht gekregen in de rapporten die in de beleidsreactie worden behandeld. Dit wordt als een grote belemmering ervaren door de opsporingsinstanties in de uitvoering van de binnendringbevoegdheid. Er doen zich drie problemen voor bij de keuring van technische hulpmiddelen bij de binnendringbevoegdheid: de tijd die het kost om te keuren, de noodzaak voor de ruimte om de configuratie van het hulpmiddel aan te passen tijdens de inzet, het 'black box' karakter van commerciële technische hulpmiddelen. Op Zweden na vindt in ieder land een vorm van keuring of toetsing plaats van het te gebruiken technisch hulpmiddel. Nederland kent de meest gedetailleerd beschreven keuring van technische hulpmiddelen. Geen enkel ander land kent een keuring door een onafhankelijke keuringsdienst waarbij deze keuringsdienst voorafgaand aan een inzet, aan de hand van een uitgebreid keuringsprotocol, de technische hulpmiddelen dient te onderzoeken.

**Directoraat-Generaal
Rechtspleging en
Rechtshandhaving**
Directie Rechtshandhaving en
Criminaliteitsbestrijding
Criminaliteit en Veiligheid

Datum
4 december 2023

Ons kenmerk
4941132

De politie, inclusief de keuringsdienst, wordt gevraagd om de volgende beleidsmaatregel uit te werken: alle middelen die automatisch informatie detecteren, registreren en transporteren (tenzij de aard van het hulpmiddel zich tegen keuring verzet) worden ter keuring aangeboden, echter het huidige uitgangspunt dat voorafgaand aan een inzet sprake moet zijn van een *goedgekeurd* technisch hulpmiddel komt te vervallen. Middelen worden toch ter keuring aangeboden zodat inzicht wordt verkregen in welke mate aan de eisen uit het Besluit onderzoek geautomatiseerd werk wordt voldaan. Hiervan wordt een rapport opgemaakt. Op deze manier wordt de integriteit en de werking van het middel geanalyseerd en gecontroleerd door een derde partij en de relevante factoren voor de bewijswaarde inzichtelijk en toetsbaar gemaakt.

Bovenstaande werkwijze betekent niet dat per definitie de waarborgen rondom de bewijswaarde verminderen. Dit geeft namelijk de volgende mogelijkheden bij het gebruik van technische hulpmiddelen. Is het middel goedgekeurd, dan wordt een goedgekeurd middel ingezet. Als het middel niet of ten dele is goedgekeurd kan de officier van justitie op basis van dit rapport bepalen óf aanvullende verificatiemaatregelen kunnen worden genomen zodat alsnog aan de eis kan worden voldaan, óf dat de officier van justitie en de rechter inzicht wordt verstrekt in de bewijswaarde in de rechtszaal. De zaakofficier kan in dit laatste geval inschatten of aanvullend bewijs nodig is om de zaak voordat de zaak wordt voorgelegd aan de rechter. Dit vereist een wijziging in het Besluit onderzoek geautomatiseerd werk en zal daarom ook in gezamenlijkheid met alle betrokken partijen worden voorbereid.

4.1 Politieke context

De Eerste Kamer heeft aandacht voor de invulling van het toezicht en vraagt in een brief duidelijkheid over de invulling hiervan. Verder heeft D66 tijdens de behandeling in de Tweede Kamer (toen in de oppositie) tegen het wetsvoorstel gestemd dat de binnendringbevoegdheid regelde. Voornamelijk vanwege kritiek op het gebruik van binnendringsoftware. In de Eerste Kamer, met de regeling in het regeerakkoord Rutte-2 inzake binnendringsoftware, heeft D66 voor gestemd.

In het kader van binnendringsoftware meldt Omtzigt (NSC) in een recent artikel in de NRC: "De diensten hebben het nodig tegen bijvoorbeeld staatsondermijnende activiteiten. Helemaal verbieden is niet realistisch. Maar je moet het gebruik en de verkoop ontzettend strak reguleren en effectief toezicht houden, want dit is echt de overtreffende trap van afluisteren." In de week van 11 oktober as. brengt het Assemblee van de Raad van Europa aanbevelingen uit

voor de omgang met binnendringsoftware. Eerder heeft ook het Europees Parlement uitgangspunten geformuleerd.

De beleidswijziging die wordt voorgesteld op binnendringsoftware van externe leveranciers is niet de wijze van aanschaf zoals voorgeschreven in het regeerakkoord van Rutte-2. Maar juist vanwege de mogelijke nadelige effecten van deze inperking is in het regeerakkoord de evaluatietermijn verkort van vijf naar twee jaar en is expliciet aangegeven dat aanschaf voor algemeen gebruik wordt overwogen.

Aanvullend kan nog worden gemeld dat vanuit de Tweede Kamer vragen zijn gesteld over de mogelijkheden voor de inzet van binnendringsoftware voor repressie in de internationale context, bijvoorbeeld door het lid Cuijk (CDA) en recent door de SGP en PVDA/GroenLinks. Belangrijk hierbij te vermelden is dat het kabinet misbruik van dit soort software afkeurt en een diplomatieke inzet pleegt om dit tegen te gaan, bijvoorbeeld via schriftelijke verklaringen van de Freedom Online Coalition. Echter, rechtmatig gebruik door de Nederlandse politie komt de criminaliteitsbestrijding ten goede, zeker gezien het belang van deze software in de strijd tegen ernstige en georganiseerde criminaliteit. Als minder ingrijpende opsporingsmiddelen niet voldoen is binnendringsoftware een noodzakelijk laatste redmiddel. Effectieve criminaliteitsbestrijding zorgt er in deze gevallen juist voor dat burgers van hun rechten en vrijheden kunnen genieten, bijvoorbeeld de uitoefening hiervan door slachtoffers.

**Directoraat-Generaal
Rechtspleging en
Rechtshandhaving**
Directie Rechtshandhaving en
Criminaliteitsbestrijding
Criminaliteit en Veiligheid

Datum
4 december 2023

Ons kenmerk
4941132

4.7 Implementatie

Op enkele punten is deze brief afdoende om de beleidswijziging in gang te zetten. Een meerderheid van de punten vereist nadere uitwerking door de politie, OM of het departement. De coördinatie van het beleid ligt bij de beleidsmedewerker van DRC en werkt hierin goed samen met DWJZ en DGPenV. DGPenV is als beheer verantwoordelijke van de politie nauw betrokken.

4.8 Communicatie

Geen communicatie voorzien.

5. Informatie die niet openbaar gemaakt kan worden

De persoonsgegevens van de betrokken ambtenaren worden niet openbaar gemaakt ter bescherming van de persoonlijke levenssfeer.

Bijlage

Meer specialistische toelichting:

Misdrijven waartegen de binnendringbevoegdheid is ingezet:

Soorten misdrijven, totaal 25 inzetten maart 2019-2021	
Misdrijf	Aantal inzetten
Traditionele criminaliteit	
Moord/doodslag en of poging daartoe en of voorbereiding	7
Combinatie met WWM en brandstichting	1
Opiumwet	3
Combinatie met omkoping en witwassen	1
Combinatie met omkoping, heling, witwassen en criminele organisatie	1

Combinatie met opium, witwassen, valsheid in geschrifte en WWM	1
Combinatie met WWM en criminele organisatie	1
Combinatie met witwassen	1
Valsheid in geschrifte en oplichting	1
Lidmaatschap criminele organisatie	2
Witwassen	2
Combinatie met criminele organisatie	1
Zeden	1
Organisatie terroristisch misdrijf	1
Cybercriminaliteit in enge zin	
Computervrederebreuk	1

**Directoraat-Generaal
Rechtspleging en
Rechtshandhaving**
Directie Rechtshandhaving en
Criminaliteitsbestrijding
Criminaliteit en Veiligheid

Datum
4 december 2023

Ons kenmerk
4941132

Ontwikkeling aantal inzetten per jaar:

Inzet van de binnendringbevoegdheid per jaar inclusief commerciële binnendringsoftware.				
	2019	2020	2021	2022 ¹
Opsporingsonderzoeken	8	13	24	26
Commerciële binnendringsoftware	3	10	16	22
Aantal softwarelicenties	7	11	13	16
<p><i>We tellen een opsporingsonderzoek in het jaar waarin de aanvangsdatum van het eerste bevel valt. Een bevel dat wordt gegeven op 30/12/2020 en een ingangperiode heeft voor de uitvoering van de bevoegdheid per 7/1/2021 telt mee voor 2021. Als een zaak in meer dan 1 jaar loopt, tellen we hem alleen mee in het eerste jaar. Een nieuw geautomatiseerd werk of een nieuwe verdachte in een zaak tellen we in beginsel niet als nieuwe inzet. We tellen geen zaken waarin gewerkt is voor andere landen in het Koninkrijk. We tellen geen zaken waarin sprake is geweest van een uitgaand rechtshulpverzoek en de uitvoering door een ander dan DIGIT is gedaan.</i></p>				

Algemene toelichting beleidsreactie

Ten aanzien van de inhoud kan worden aangegeven dat de inzet van de binnendringbevoegdheid beperkt is tot het type misdrijven zoals van tevoren was voorzien, namelijk voornamelijk tegen ernstige en georganiseerde criminaliteit. De binnendringbevoegdheid is een specialistische, gerichte, streng genormeerde en gereguleerde inzet en geen 'silver bullet' of panacee. In 2022 is bijvoorbeeld in 31 zaken een bevel afgegeven om de bevoegdheid toe te passen.

De beleidsreactie kent zes sporen: 1) de manier waarop wordt binnengedrongen, 2) de inzet van commerciële middelen [binnendringsoftware], 3) de meldplicht van onbekende kwetsbaarheden die volgt uit artikel 126ffa Sv, 4) het toezicht

¹ Dit aantal wijkt af van de aantallen genoemd door de IJenV. Het jaarverslag van het ministerie van Justitie en Veiligheid komt altijd eerder dan het verslag van de IJenV daar wordt een andere telling aangehouden.

door de Inspectie Justitie en Veiligheid, 5) de keuring van technische hulpmiddelen en 6) procedurele of aanvullende waarborgen, vernietigen van gegevens en overige punten. Deze sporen zijn geïdentificeerd naar aanleiding van de bevinden van het WODC.

De brief bestaat uit twee delen. In de hoofdbrief worden de rapporten geïntroduceerd, de maatschappelijke toegevoegde waarde van de binnendringbevoegdheid toegelicht en per spoor worden de grotere beleidswijzigingen of -voornemens benoemd. In de bijlage worden per spoor de bevindingen van het WODC, de PGHR of de IJenV weergegeven en van een reactie voorzien. Dit zorgt voor een lange bijlage. Daarbovenop zijn er enkele (doorgaans technische) wensen vanuit de opsporinginstanties.

Overzicht van het systeem van toezicht en controle

Voor de volledigheid wordt geschetst hoe het toezicht en controle op de inzet eruit zien: een zaakofficier maakt een afweging of de binnendringbevoegdheid aangewezen is. Nadat de officier van justitie deze afweging heeft gemaakt wordt de voorgenomen inzet van de bevoegdheid voorgelegd aan de Centrale Toetsingscommissie (CTC) van het openbaar ministerie, die het College van procureurs-generaal over die inzet adviseert. Na een positief oordeel zal de rechter-commissaris toetsen of de inzet strikt noodzakelijk is om het gestelde doel te bereiken en er geen minder ingrijpende middelen beschikbaar zijn. Alleen dan wordt voor de inzet een machtiging afgegeven. Het OM heeft een speciale officier van justitie aangesteld voor de controle op de uitvoering van het bevel. Ook de IJenV houdt toezicht op de uitvoering van bevel door de politie. Als het strafrechtelijke onderzoek waarin de inzet heeft plaatsgevonden voor de rechter komt, oordeelt de zittingsrechter over de rechtmatigheid van de inzet. De IJenV voert, op dit moment, nalevingstoezicht uit en publiceert hierover jaarlijks een verslag. De procureur-generaal bij de Hoge Raad heeft in het kader van de toezichthoudende taak die voortvloeit uit artikel 122 lid 1 van de Wet op de rechterlijke organisatie (Wet RO), een onderzoek uitgevoerd. De binnendringbevoegdheid blijft, met deze wijzigingen een gerichte, streng genormeerde en gereguleerde inzet die wordt aangewend in zaken die zien op ernstige of georganiseerde criminaliteit.

Toelichting keuringsproblematiek

Er zijn op dit moment enkele technische hulpmiddelen goedgekeurd. De ervaring tot nu toe is dat het vrij veel tijd kostte om aan de verwachtingen te voldoen en dat het ook nodig was om het middel meerdere keren aan te bieden. Soms kan een inzet snelheid vereisen en is deze tijd er niet.

Daarbovenop is het geautomatiseerde werk waarop wordt binnengedrongen in de regel onbekend. Pas wanneer toegang is verkregen krijgt de politie een beeld van de software die het individu gebruikt en de versie daarvan. Het kan zo zijn dat afhankelijk hiervan het technisch hulpmiddel op een bepaalde manier geconfigureerd moet worden en daarmee niet meer functioneert op een wijze die vooraf bij de keuringsdienst is getest.

Het kan ook zijn dat het functioneren niet valt terug te herleiden, omdat de werking van het technische hulpmiddel onbekend is (het black box karakter). Dit kan het geval zijn bij commerciële technische hulpmiddelen waarbij de veelzijdige werking onderdeel is van het intellectueel eigendom van de leverancier. Een maatregel dat de betrouwbaarheid, herleidbaarheid en integriteit van het bewijs

**Directoraat-Generaal
Rechtspleging en
Rechtshandhaving**
Directie Rechtshandhaving en
Criminaliteitsbestrijding
Criminaliteit en Veiligheid

Datum
4 december 2023

Ons kenmerk
4941132

in dit geval kan waarborgen is dat bijvoorbeeld een forensische kopie wordt gemaakt van de informatie die wordt vergaard.

Daarnaast benoemt de IJenV ook het risico dat leveranciers niet technisch kunnen worden uitgesloten van mogelijke toegang tot de gegevens die verkregen worden. Dit geldt ook voor de mogelijkheid zelfstandig updates uit te voeren of de controle over het geautomatiseerde werk over te nemen.

In de beleidsreacties wordt erkend dat dit een dilemma is omdat onmisbare expertise op deze terreinen bij commerciële partijen ligt. Dit dilemma beperkt zich niet tot de opsporing. De Nederlandse overheid is vaker afhankelijk van goede samenwerking met commerciële partijen vanwege de onmisbare expertise. Voor de betrokken commerciële partijen zijn de belangen om een betrouwbare partner voor de overheid te zijn en zich te houden aan de afspraken evident. De politie heeft een onderhoudscontract bij een leverancier. Voordeel hiervan is dat de continuïteit van de werking van de software zo veel mogelijk gewaarborgd kan blijven. In dat contract worden ook strikte afspraken gemaakt over de toegang van de leverancier tot componenten van het product dat is geleverd aan de politie. Deze afspraken en de mogelijkheid deze in rechte af te dwingen vormen waarborgen om onbevoegde toegang van de leverancier tot componenten van het product tegen te gaan. Op deze manier wordt gezocht naar een balans tussen effectieve toegang tot noodzakelijke software in de opsporing en het voorkomen dat producten worden afgenomen van ongewenste leveranciers.

Regeerakkoord Rutte-2

Voor de uitvoering van de Wet Computercriminaliteit III komt 10 miljoen euro extra beschikbaar. Daarbij zal slechts in een specifieke zaak hacksoftware worden ingekocht door opsporingsdiensten. Leveranciers van dergelijke software worden gescreend door de AIVD en verkopen niet aan dubieuze regimes. Statistieken over het gebruik van hacksoftware worden jaarlijks openbaar gemaakt. Bij de evaluatie van de wet na twee jaar wordt gezien in hoeverre deze regeling de effectiviteit van de wet ernstig aantast. In dat geval wordt alsnog de aanschaf van hacksoftware voor algemeen gebruik overwogen.

**Directoraat-Generaal
Rechtspleging en
Rechtshandhaving**
Directie Rechtshandhaving en
Criminaliteitsbestrijding
Criminaliteit en Veiligheid

Datum
4 december 2023

Ons kenmerk
4941132