BITS OF FREEDOM
Voor jouw internetvrijheid

Datum:
4 oktober 2019
Versie:
0.9

Bits of Freedom
Prinseneiland 97hs
1013 LN Amsterdam

Rejo Zenger
+31 6 3964 2738
rejo@bitsoffreedom.nl

bitsoffreedom.nl
IBAN: NL73 TRIO 0391 1073 80
KVK: 34 12 12 86, Amsterdam

Advies Bits of Freedom over het wetsvoorstel voor een Wet Zerodays Afwegingsproces

Bits of Freedom heeft met veel belangstelling kennisgenomen van het wetsvoorstel dat moet leiden tot een overheidsbreed afwegingskader voor het geheim houden van onbekende kwetsbaarheden.[1] We zijn het met de voorsteller eens dat zo'n kader ontzettend belangrijk is, gegeven de enorme risico's die verbonden zijn aan het geheim houden van zulke kwetsbaarheden. Maar juist ook vanwege die risico's acht Bits of Freedom het essentieel dat het kader allesomvattend, genuanceerd en glashelder is. Het voorliggende voorstel kan wat ons betreft in dat opzicht sterk verbeterd worden. Hieronder volgen enkel suggesties.

Opmerkingen van algemene aard

1. Hoewel Bits of Freedom blij is met het uitgangspunt dat onbekende kwetsbaarheden gemeld moeten worden aan de maker van de kwetsbare software, willen we benadrukken dat het "melden" op zichzelf nog geen kwetsbaarheid dicht. We begrijpen ook wel dat dit ook niet de achterliggende gedachte van het wetsvoorstel is, maar toch is het belangrijk om dit altijd scherp in het achterhoofd te houden. Het is naast het melden ook, of misschien wel vooral, belangrijk om in te zetten op het verbeteren van het hele proces van het uitrollen van beveiligingsupdates.[2] Dit voorstel beperkt zich tot het melden van kwetsbaarheden, zonder dat het ook maar iets doet aan het daadwerkelijk gedicht krijgen van de kwetsbaarheden. De veiligheid van onze digitale infrastructuur zou vooral gebaat zijn met wetgeving die ervoor zorgt dat bekende kwetsbaarheden sneller weggewerkt zijn.

2. Bits of Freedom is verder verbaasd over de keuze om een groot deel van de structuur van het afwegingskader buiten de formele wettekst te laten. Hoewel een deel van de invulling vastgelegd moet gaan worden in een algemene maatregel van bestuur, lijkt voor het overige vooral de toelichting op het wetsvoorstel leidend. Die toelichting is bijvoorbeeld lang niet altijd even helder. Het is bijvoorbeeld niet duidelijk of het technisch orgaan, zoals beschreven op pagina 24, onderdeel vormt van het orgaan dat ondergebracht wordt bij het NCSC of dat het een onderdeel is van de overheidsinstantie die de onbekende kwetsbaarheid geheim wil houden. Omdat het erg belangrijk is dat de afwegingen zorgvuldig gemaakt worden, ligt het wat ons betreft voor de hand om bijvoorbeeld de structuur van het afwegingsproces juist in de tekst van de wet vast te leggen. Datzelfde geldt ook voor andere aspecten, zoals de afwegingen die gemaakt moeten worden.

1 Tweede Kamer, dossier 35257
2 Bits of Freedom publiceerde een lijst van 12 broodnodige updates voor het updateproces.

Wanneer vallen kwetsbaarheden vallen onder het kader?

1. Het uitgangspunt moet zijn dat bestuursorganen alle onbekende kwetsbaarheden meldt waarvan zij kennis krijgt. Die melding moet bovendien gedaan worden, kort nadat de kennis verkregen is. Dat is iets anders dan nu in artikel 2, lid 1 is voorgesteld. Daar staat namelijk dat een overheidsinstantie een onbekende kwetsbaarheid meldt indien zij "voor het binnendringen in een geautomatiseerd werk gebruik zal maken van een onbekende kwetsbaarheid." Strikt genomen betekent dat als een overheidsinstantie kennis krijgt van een onbekende kwetsbaarheid, de overheidsinstantie deze kwetsbaarheid niet zou hoeven te melden als zij niet ook voornemens is om *een* kwetsbaarheid te gebruiken voor het binnendringen in een geautomatiseerd werk. De logica van artikel 2, lid 1 en 2, zou dus eigenlijk moeten zijn:
    1. Als de overheidsinstantie kennis krijgt van een onbekende kwetsbaarheid, dient de overheidsinstantie deze kwetsbaarheid te melden bij de maker van de kwetsbare software.
    2. Als de overheidsinstantie de hiervoor bedoelde kennis verkrijgt en de onbekende kwetsbaarheid geheim wil houden om mogelijk eens te gebruiken voor het binnendringen in een geautomatiseerd werk, moet zij dit voornemen eerst voorleggen aan het afwegingsorgaan.
2. Het is belangrijk om een termijn vast te leggen waarin een onbekende kwetsbaarheid, die men geheim wil houden, aan het afwegingsorgaan moet zijn voorgelegd. Als de termijn ongebruikt is verstreken, moet de kwetsbaarheid gemeld worden. Deze termijn moet erg kort zijn, hooguit een paar dagen. De reden hiervoor is dat de tijd tussen het moment van ontdekking van de kwetsbaarheid en het misbruik ervan door kwaadwillenden, de *time to exploit*, soms kort is. Er zijn in het verleden ernstige kwetsbaarheden gevonden die binnen een of enkele dagen misbruikt werden.
3. Daar komt bij dat de feitelijk afweging, inclusief de adviesaanvraag bij de vertegenwoordigers van de vitale sector, ook nog eens kostbare tijd vergt. Idealiter wordt ook de termijn van deze processtap vastgelegd. Als deze termijn verstreken is, zonder dat er een beslissing tot geheimhouding is genomen, dient de kwetsbaarheid te worden gemeld. Los daarvan wordt uit de memorie van toelichting ook niet duidelijk welke termijn de voorsteller voor ogen heeft.
4. Op pagina 18 van de toelichting staat: "Zerodays die door derden aan de overheid worden gemeld met de intentie of verwachting dat de kwetsbaarheid wordt gedicht […] worden altijd aan de maker van de software gemeld." Dit is een fundamenteel beginsel[3] en zou daarom expliciet meegenomen moeten worden in de logica van artikel 2.
5. Het voorstel houdt bepaalde onbekende kwetsbaarheden onterecht buiten het afwegingskader. In de toelichting staat dat onbekende kwetsbaarheden in software waarvan de broncode niet openbaar is en waarvan bekend is dat de software niet meer wordt ondersteund door de maker, niet gemeld hoeven te worden. Dit volgt impliciet ook uit de formulering van artikel 1. Bits of Freedom is van mening dat de zulke kwetsbaarheden ook gemeld moeten worden.

---

3 Overigens is dit beginsel te ongenuanceerd geformuleerd. Verwacht mag worden dat een kwetsbaarheid in kwaadaardige software, zoals een *trojaans paard*, juist *niet* wordt gemeld aan de maker van die software. Dit is overigens ook het staande beleid van het NCSC.

1. Het melden van zo'n kwetsbaarheid aan de maker van de software stelt de maker in de gelegenheid om, ondanks dat het de software formeel niet meer ondersteunt, toch de kwetsbaarheid te dichten. In mei 2019 dichtte Microsoft bijvoorbeeld een kwetsbaarheid in Windows XP, software die het al jaren niet meer ondersteunde.[4]
2. De publieke bekendmaking van zo'n kwetsbaarheid is een extra stimulans voor de gebruikers van zulke software om over te stappen op software die wel wordt ondersteunt door de maker.
3. De publieke bekendmaking van zo'n kwetsbaarheid stelt de gebruiker van de software ook in staat om extra beveiligingsmaatregelen te nemen ten einde zich tegen het misbruik van de kwetsbaarheid te beschermen. Dit kan noodzakelijk zijn indien de software niet vervangen kan worden door een gebrek aan alternatieven en/of indien de software door andere afhankelijkheden niet vervangen kan worden.

6. Wat Bits of Freedom betreft mag de enige uitzondering op het uitgangspunt om onbekende kwetsbaarheden te melden alleen gelden voor kwetsbaarheden die zich voordoen in een systeem dat i) alleen voor militaire doeleinden wordt gebruikt en ii) waarbij de kwetsbaarheid zich niet voordoet in een component dat ook niet-militair wordt ingezet, zoals een vrij te gebruiken softwarebibliotheek. Het is overigens aannemelijk dat dit soort kwetsbaarheden zich snel laten beoordelen door het afwegingsorgaan, waardoor het niet nodig lijkt om deze uitzondering op te nemen.
7. Het wetsvoorstel maakt niet duidelijk of een overheidsinstantie een onbekende kwetsbaarheid mag aankopen waarbij het kennis krijgt van de onbekende kwetsbaarheid, maar door de aankoop gehouden is aan een geheimhoudingsverklaring.[5] Het gaat hier dus niet om een technisch hulpmiddel zoals bedoel in artikel 3 van het voorstel, maar om de aankoop van de kennis over een onbekende kwetsbaarheid zelf. De toelichting verwijst naar het SNV-advies, dat stelt "dat overheden geen geheimhoudingsverklaringen zouden mogen tekenen om te voorkomen dat zerodays door het afwegingsproces beoordeeld worden." Bits of Freedom is dezelfde mening toegedaan en mist in het voorstel het expliciete verbod op de aankoop van onbekende kwetsbaarheden waarbij een geheimhoudingsverklaring getekend moet worden.

Welke belangen moeten worden afgewogen?

1. De belangen die zwaarwegender zouden kunnen zijn dan het belang van de melding van de kwetsbaarheid moet op voorhand vastgelegd zijn. In het huidige voorstel is in artikel 2, lid 2, slechts een niet-limitatief en *high level*-lijstje geformuleerd. Een limitatieve invulling is niet meer dan logisch, gegeven het beoogde "bias to disclosure". Dat kan ook niet bezwaarlijk zijn: het is onwaarschijnlijk dat deze belangen en de wijze waarop die belangen moeten worden afgewogen erg veranderlijk of onvoorzienbaar zijn. Mocht na verloop van termijn de behoefte bestaan om dit toch anders doen, kan dat,

4 Microsoft maakte in mei 2019 een patch beschikbaar voor een kwetsbaarheid in de Remote Desktop Services-functionaliteit van onder meer Windows XP. De gangbare versies van dat besturingssysteem werden al niet meer ondersteund sinds 2014.
5 Opsporings- en geheime diensten kunnen bij het bedrijf VUPEN security een abonnement op onbekende kwetsbaarhedenhttps://wikileaks.org/spyfiles/files/0/279_VUPEN-THREAD-EXPLOITS.pdf) nemen. En dienst moet voor het abonneren wel eerst een geheimhoudingsverklaring tekenen.

weloverwogen en met parlementaire instemming, met een wijzigingsvoorstel doorgevoerd worden.
2. Dat zelfde geldt ook voor de formulering van afwegingsfactoren, zoals beschreven in de toelichting op pagina's 24 en 25. Daar staat onder meer: "Initiatiefnemer stelt voor om een aantal categorieën van afwegingsfactoren wettelijk vast te leggen. Verdere uitwerking van de afwegingen, inclusief specifieke informatie die aangeleverd moet worden, wordt per AMvB nader uitgewerkt." Bits of Freedom ziet daar vervolgens geen uitwerking van terug in het wetsvoorstel. De genoemde categoriën zijn niet vastgelegd in de voorgestelde wet en de lijst van afwegingsfactoren in de toelichting is vrijblijvend ("kunnen aan bod komen").
3. Uit het voorstel wordt niet duidelijk of het risico op kennisdeling over een onbekende kwetsbaarheid wordt meegenomen in de afweging van belangen. Mocht de AIVD kennis verkrijgen van een onbekende kwetsbaarheid, dan kan op niet op voorhand worden uitgesloten dat zij de kennis hierover deelt met een andere geheime dienst. Het is ook niet ondenkbaar dat die geheime dienst een risico vormt voor het onbedoeld publiek worden van de kwetsbaarheid.

Wie zijn betrokken bij de afweging?

1. Bits of Freedom vindt het onverstandig om het afwegingsorgaan onder te brengen bij het NCSC. Het NCSC "voorkomt maatschappelijke schade en beperkt dreigingen", onder meer door "kennis breed toegankelijk te maken". Het NCSC is er dus vanuit haar kern erop gericht om kwetsbaarheden op verantwoorde wijze te melden bij de maker van de kwetsbare software en er aan bij te dragen dat deze kwetsbaarheden zo snel mogelijk gedicht worden. Het idee dat onbekende kwetsbaarheden onder omstandigheden geheim zouden kunnen worden gehouden, staat haaks hierop.

2. Het is niet duidelijk op grond waarvan sommige overheidsinstanties een plaats krijgen in het afwegingsorgaan. Zo maken de politie en het Openbaar Ministerie wel deel uit van het orgaan, maar het NFI weer niet. Dat is curieus, omdat ook het NFI soms onbekende kwetsbaarheden ontdekt en gebruikt. Dit geldt natuurlijk ook voor andere overheidsinstanties, zoals de FIOD.

3. Wat Bits of Freedom betreft wordt in het wetsvoorstel verhelderd dat niet de minister maar het afwegingsorgaan de feitelijke beslissing neemt om onbekende kwetsbaarheden al dan niet te melden. Dat de minister vervolgens de politieke verantwoordelijkheid draagt is vanzelfsprekend. Dit is niet duidelijk uit het artikel, ook niet indien gelezen in de context van pagina 26 van de toelichting.

4. De toelichting bespreekt niet de situatie waarin het adviesorgaan van betrokkenen die vitale infrastructuren beheren, adviseert een onbekende kwetsbaarheid bekend te maken, maar het afwegingsorgaan besluit de kwetsbaarheid alsnog geheim te houden. Het zou beter zijn als deze vertegenwoordigers duidelijk als belanghebbende in de zin van de Algemene wet bestuursrecht zijn aangemerkt en het besluit van de minister vatbaar is voor bezwaar en beroep.

Hoe worden besluiten genomen gemaakt?

1. Het lijkt ons een slecht idee om de beslissing van het afwegingsorgaan te baseren op een stemming. Het gaat hier immers om de afweging van enorme belangen, zoals de veiligheid van onze digitale infrastructuur en de veiligheid van de Staat. Dat zijn beslissingen die genomen moeten worden op basis van consensus. Indien er geen brede overeenstemming bestaat over de afweging van de belangen, moet de kwetsbaarheid gewoon gemeld worden.
2. De perverse consequentie van een systeem waarbij gestemd wordt, is dat de uitslag beïnvloed kan worden door de samenstelling van het afwegingsorgaan aan te passen.
3. Mocht de voorsteller vasthouden aan een stemming, dan is het belangrijk deze stemming met een andere stemverhoudingen in te richten (en dus niet “per meerderheid”). In de toelichting op het voorstel wordt gerefereerd aan de “belangrijke aanbevelingen” van de SNV.[6] Een van die belangrijke adviezen is “om het principe «bias towards disclosure» vast te leggen in de stemverhoudingen”. De wijze waarop zij dat invult: “een zeroday [wordt] openbaar gemaakt of gemeld als een robuuste minderheid (15% of meer) van de [leden] dat adviseert.” SNV’s advies wordt nu genegeerd.
4. Het is Bits of Freedom niet duidelijk hoe het proces ingericht moet gaan worden in een situatie waarbij onbekende kwetsbaarheden aangekocht worden (anders dan die deel uitmaken van een technisch hulpmiddel). Moet de AIVD of MIVD, die een onbekende kwetsbaarheid aankoopt, voor of na de verwerving van die kwetsbaarheid deze aan het afwegingsorgaan voorleggen? Een soortgelijk probleem: wat gebeurt er als een buitenlandse geheime dienst informatie over een onbekende kwetsbaarheid met de AIVD of MIVD deelt? Het voorgestelde kader verplicht de dienst deze kwetsbaarheid een bepaald proces te volgen, dat mogelijk strijdig is met de afspraken die tussen de diensten onderling geldt.
5. Ook vragen we ons af hoe gehandeld moet worden als de informatie over een onbekende kwetsbaarheid als staatsgeheim is gerubriceerd. Het is immers aannemelijk dat als de AIVD of MIVD kennis verkrijgt over een onbekende kwetsbaarheid, deze informatie als een staatsgeheim wordt aangemerkt. Hoe kan het technisch orgaan, zoals bedoeld op pagina 24 van de toelichting, haar afweging maken als zij niet ook de details van de kwetsbaarheid kent? En kan het afwegingsorgaan een goede beslissing nemen als zij niet over alle informatie beschikt? En welke impact heeft het verwerken van dit soort geheime informatie op de inrichting bij het NCSC (omdat het afwegingsorgaan daar ondergebracht zou moeten worden)?

Hoe lang mag een kwetsbaarheid geheim blijven?

1. Bits of Freedom mist de mogelijkheid om onbekende kwetsbaarheden voor een kortere periode dan één jaar geheim te houden. Op basis van het voorliggende voorstel kan het afwegingsorgaan besluiten dat de kwetsbaarheid direct te gemeld moet worden of dat de kwetsbaarheid geheim gehouden mag worden. Indien voor dat laatste wordt gekozen, vindt er na één jaar heroverweging van het besluit plaats. Het is veel verstandiger om flexibeler te zijn, zodat bijvoorbeeld ook bepaald kan worden: de kwetsbaarheid mag voor de duur van vier maanden geheim worden gehouden, waarna

de kwetsbaarheid gemeld moet zijn. Dat stelt de overheidsinstantie in staat om de kwetsbaarheid in die periode te gebruiken, maar zorgt tegelijkertijd ervoor dat de kwetsbaarheid niet langer dan strikt noodzakelijk geheim wordt gehouden. Dit past ook bij het principe «bias towards disclosure».

2. Daarnaast is de termijn van één jaar voor heroverweging van een eerder besluit tot geheimhouding veel te lang. In het voorstel wordt gesteld dat deze termijn “onder andere is gebaseerd op het feit dat volgens beschikbare studies de «collission rate» van een zeroday al binnen 1 jaar op een significant niveau ligt” en dat “er een kans is van 1 op 20 dat een zeroday binnen een jaar door een andere actor gevonden wordt.” Er zijn tenminste drie reden om deze termijn veel korter te maken, bijvoorbeeld drie maanden, of om te komen tot een complexer systeem waarbij risico’s doorlopend gemonitored worden.

    1. Naast de studie waar voorsteller naar verwijst, zijn er andere onderzoeken waaruit blijkt dat die termijn voor herontdekking vermoedelijk korter is. Onderzoek van bijvoorbeeld Herr, Schneier en Morris[7] laat zien dat 15 tot 20 procent van kwetsbaarheden die zijn ontdekt, binnen een jaar door een onafhankelijke derde nog eens ontdekt wordt. Datzelfde onderzoek laat ook zien dat voor sommige soorten software dat nog veel sneller gebeurt. Bijna 14 procent van kwetsbaarheden in het besturingssysteem Android worden binnen 60 dagen opnieuw ontdekt. Dat percentage stijgt naar boven de 21 procent in een tijdspanne van 120 dagen na de initiële ontdekking.
    2. Daarnaast is bekend dat op het moment dat een kwetsbaarheid wordt ontdekt, de kans groot is dat binnen relatief korte tijd gerelateerde kwetsbaarheden ontdekt worden. Dat heeft vermoedelijk te maken met het feit dat onderzoekers in het proces tot de ontdekking van de eerste kwetsbaarheid een beter begrip hebben gekregen van de inrichting van de kwetsbare software en diens (mogelijke) kwetsbaarheden. Dat betekent ook dat het risico op herontdekking van de geheim gehouden kwetsbaarheid aanzienlijk is verhoogd indien in de periode van geheimhouding een gerelateerde kwetsbaarheid gevonden wordt. Stel dat binnen drie maanden na het besluit om een bepaalde kwetsbaarheid geheim te houden, een nieuwe en vergelijkbare kwetsbaarheid bekend wordt, dan moet de geheimhouding van die eerste kwetsbaarheid worden heroverwegen omdat het risicoprofiel is veranderd.
    3. Een van de door de voorsteller aangehaalde “belangrijke aanbevelingen” van SNV luidt: “The protections should include a mechanism to accelerate disclosure in light of an event indicating that the existence of the vulnerability is known to others.” Dit is alleen mogelijk indien doorlopend gekeken wordt naar meldingen van tot dan toe onbekende kwetsbaarheden en de ontwikkelingen op de markt voor zulke kwetsbaarheden. Dat betekent dat een jaarlijks heroverwegingsproces absoluut ontoereikend is. En juist omdit een doorlopende aandacht vereist, moet vooraf nagedacht worden over de inrichting.

7 Trey Herr, Bruce Schneier and Christopher Morris, ``Taking Stock: Estimating Vulnerability Rediscovery'', juli 2017

Hoe is de melding vormgegeven?

1. Het wetsvoorstel laat in het midden hoe de melding van een onbekende kwetsbaarheid precies vormgegeven moet worden. Wat Bits of Freedom is dat proces gebaseerd op de huidige werkwijze van het NCSC. Dat betekent dat een overheidsinstantie dat een onbekende kwetsbaarheid moet melden, deze kwetsbaarheid meldt bij het NCSC. Het NCSC zorgt daarna voor een verantwoorde *disclosure* van de kwetsbaarheid. Dat doet zij door het informeren van de maker van de kwetsbare software en, zodra dat op verantwoord is, de beveiligingsgemeenschap door de publicatie van een zogenaamd beveiligingsadvies.[8]

Wat kan wel openbaar?

1. Het wetsvoorstel verplicht niet tot transparantie over de toepassing van het kader. De toelichting bespreekt dit bijzonder marginaal. Bits of Freedom vind het belangrijk dat nu al wordt nagedacht over de wijze waarop het afwegingsorgaan of de toezichthouder op zinvolle wijze transparant kan rapporteren over het proces en de genomen beslissingen. Zo is het “aantal geheimgehouden en het aantal vrijgegeven kwetsbaarheden” een vrijwel nietszeggende statistiek. Het is veel belangrijker om naast zulke statistieken ook informatie te publiceren over de afwegingen die zijn gemaakt en hoe risico’s en belangen ten op zichte van elkaar zijn afgewogen.

2. Ook is niet duidelijk hoe de toezichthouder om moet gaan met informatie over onbekende kwetsbaarheden die als staatsgeheim is geclassificeerd. Zal de toezichthouder statistische en andere informatie over deze kwetsbaarheden mogen publiceren? Of zegt deze informatie teveel over de modus operandi van de AIVD en MIVD en wordt die informatie achter de hand gehouden? Of als informatie daarover wordt samengevoegd met informatie over kwetsbaarheden bij andere diensten, hoeveel zegt de statistiek ons dan nog?

3. Wat Bits of Freedom betreft wordt in ieder geval ook gerapporteerd over de volgende punten.

    1. Het aantal en de aard van inbreuken op de beveiliging van de systemen die worden gebruik voor de bewaring van de onbekende kwetsbaarheden waarvan is besloten die niet te melden aan de maker van de software.
    2. Op welke wijze de betrokken minister het advies van “een of meer vertegenwoordigers van betrokkenen die vitale infrastructuur beheren” heeft meegenomen in zijn besluit om een onbekende kwetsbaarheid al dan niet geheim te houden.
    3. Op welke wijze de bestuursorganen kennis kregen van de onbekende kwetsbaarheden (eigen onderzoek, aankoop, melding door een derde, etc).
    4. Van welke bedrijven onbekende kwetsbaarheden zijn aangekocht (zodat onderzoek gedaan kan worden naar de overige activiteiten van deze bedrijven.)

8 Het NCSC publiceert regelmatig zogenaamde beveiligingsadviezen (of ``security advisories''): "Een beveiligingsadvies wordt door het NCSC gepubliceerd naar aanleiding van een recent gevonden kwetsbaarheid […]. In een beveiligingsadvies staat de beschrijving, de mogelijke gevolgen en mogelijke oplossingen van de kwetsbaarheid of dreiging.

5. De samenstelling van het advies- en afwegingsorgaan (aantal leden per organisatie).

4. Daarnaast ziet Bits of Freedom graag dat voor een kwetsbaarheden die in eerste instantie geheim gehouden werd maar na verloop van tijd alsnog gemeld word, in het publieke beveiligingsadvies een paragraaf wordt opgenomen over de geheimhouding. Deze paragraaf moet op zijn minst vermelden wanneer een of meer bestuursorganen voor het eerst kennis kregen van de kwetsbaarheid. Dit stelt onafhankelijke beveiligingsonderzoekers in staat om onderzoek te doen naar incidenten waarbij de bedoelde kwetsbaarheid een rol speelde, tijdens de periode van geheimhouding.

5. Ook zou Bits of Freedom graag zien dat wordt nagedacht over de transparantie naar situatie. Zo ziet Bits of Freedom niet of nauwelijks problemen bij transparantie over de gemaakte afweging die voorafgegaan zijn aan de aankoop door de politie van een technisch hulpmiddel waarvan aannemelijk is dat dit hulpmiddel gebaseerd is op een onbekende kwetsbaarheid. Dat de politie en het NFI over dit soort hulpmiddelen is algemeen bekend [9] en transparantie over de overwegingen van het afwegingsorgaan kan dus geen probleem zijn.

Overige opmerkingen

1. Uit de toelichting op het voorstel wordt niet duidelijk wat de verwachting is van het aantal kwetsbaarheden dat jaarlijks aan het afwegingsorgaan worden voorgelegd en voor welk deel daarvan verwacht wordt dat besloten wordt dat deze geheim gehouden worden. Het is belangrijk om daar een goede inschatting van te hebben, omdat een verkeerd beeld hiervan de kwaliteit van de uitvoering ernstig kan schaden. Immers, de voorsteller van het kader wil een technisch orgaan, een adviesorgaan, een afwegingsorgaan en een toezichthouder inrichten. De last op de daarbij betrokken partijen zal sterk afhankelijk zijn van het aantal kwetsbaarheden dat beoordeelt moet worden. Als bovendien de verwachting is dat veel van deze kwetsbaarheden geheim gehouden gaan worden, zal dat ook meerwerk betekenen vanwege de jaarlijkse heroverweging.

Vanzelfsprekend zijn we graag bereid een nadere toelichting te geven, mocht daartoe behoefte bestaan.

9 Op verzoek van Bits of Freedom maakte de politie in 2013 al eens documenten openbaar over de aanschaf van zulke hulpmiddelen, onder meer van de merken Cellebrite en Microsystemation.