Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2018–2019

35 257 Voorstel van wet van het lid Verhoeven houdende een regeling voor een afwegingsproces voor het gebruik van onbekende kwetsbaarheden in geautomatiseerde werken door de overheid (Wet Zerodays Afwegingsproces)

Nr. 3

MEMORIE VAN TOELICHTING

I. ALGEMEEN

1. Inleiding

Programmeren is mensenwerk. Dat betekent dat softwarecode vrijwel altijd fouten bevat. Zerodays, of onbekende kwetsbaarheden, zijn fouten in software die nog onbekend zijn bij de maker van de software (de maker heeft nul dagen gehad om het gat te dichten). Deze zerodays kunnen gebruikt worden om de werking van de betreffende software te manipuleren, oftewel te hacken. Daarvoor is een zogeheten «exploit» nodig; een stuk software dat gemaakt is om gebruik te maken van de zeroday om het apparaat of software te kunnen «binnendringen». Onder andere overheden, criminelen, terroristen of andere kwaadwillenden gebruiken dergelijke «zeroday exploits» om te kunnen hacken.

Als overheden zerodays vinden of aankopen ontstaat er een dilemma. Moet de zeroday worden gemeld bij de producent of leverancier zodat het gat in de software gedicht kan worden en het betreffende product of apparaat veilig gemaakt worden tegen hacks? Of moet de overheid de zeroday niet melden om zelf te gebruiken om te hacken? Het laten dichten kan in het belang zijn van de cyberveiligheid van de vitale infrastructuur, in het economisch belang van ondernemingen of in het privacy belang van mensen. Een beslissing om een zeroday open te houden en te gebruiken om te hacken kan bepaalde belangen van nationale veiligheid of opsporing dienen.

Op dit moment zijn de AIVD en MIVD gebonden aan een afwegingskader om ervoor te zorgen dat er zorgvuldige afwegingen gemaakt worden. Dit afwegingskader is ingericht met als uitgangspunt «melden, tenzij», ook wel een «bias towards disclosure» genoemd. Hierbij wordt gekeken naar het risico van de kwetsbaarheid voor de Nederlandse samenleving, de toegevoegde waarde van de kwetsbaarheid voor het inlichtingen werk en eventuele wettelijke beperkingen zoals bronbescherming of het afschermen van de modus operatie van de diensten.

kst-35257-3
ISSN 0921 - 7371
's-Gravenhage 2019

Terwijl de AIVD en MIVD wel gehouden zijn aan dit afwegingskader, hoeven bijvoorbeeld de Politie zich niet aan dit kader te houden. Dit brengt grote risico's met zich mee. Een zeroday die de politie openhoudt om verdachten op te sporen kan bijvoorbeeld de belangen van de AIVD schaden. Of een zeroday die Defensie wil gebruiken kan onze vitale infrastructuur in gevaar brengen.

Daarom wil initiatiefnemer een wettelijk geborgd afwegingskader voor alle zerodays die de overheid ontdekt, aankoopt of anderszins in bezit krijgt. Zo kan er een goede, objectieve afweging plaatsvinden tussen de verschillende belangen die gemoeid zijn bij het geheimhouden of laten dichten van zerodays. Hiertoe wordt een nieuw orgaan opgericht onder het Nationaal Cyber Security Centrum, waarin de verschillende belangen op het gebied van opsporing en inlichtingen, privacy, economie, vitale infrastructuur en cybersecurity vertegenwoordigd zijn. Daarnaast krijgen vertegenwoordigers van partijen uit de vitale infrastructuur een adviserende rol om ervoor te zorgen dat beslissingen over zerodays met voldoende informatie over de vitale infrastructuur genomen worden. Tot slot wordt in de wet een aantal belangen opgenomen die meegenomen moeten worden om tot een goede beslissing te komen. Dit zijn belangen als de operationele voordelen op het gebied van opsporing of inlichtingen van gebruik van de zeroday, belangen met betrekking tot de negatieve gevolgen op het gebied van cybersecurity van het gebruik van de zeroday, belangen aangaande alternatieve belangen rondom gebruik van de zeroday, zoals privacy, economie of andere veiligheidsbelangen en technische overwegingen aangaande het gebruik van de zeroday.

2. Achtergrond en aanleiding van het wetsvoorstel

2.1 Wat zijn zerodays?

Zerodays zijn fouten in software die nog onbekend zijn bij de maker van die software. Als een zeroday ontdekt wordt, heeft de maker van de software letterlijk nul dagen gehad om de fout te dichten. Dit soort softwarefouten ontstaan vanzelf als programmeurs fouten maken bij het schrijven van code. Programmeren is immers mensenwerk en veel software bestaat uit miljoenen regels code. Dan zijn fouten niet te voorkomen. Het gemiddeld aantal fouten ligt tussen de 0.5 en de 25 fouten per 1000 regels code.[1] In Open Source Software (OSS) ligt dat gemiddeld iets lager dan in Close Source Software.[2] Het is daarom aannemelijk dat in vrijwel alle software die we gebruiken dergelijke fouten zitten. Zodra een zeroday gemeld wordt aan de maker van de software of publiek bekend wordt dan spreekt men van een bekende kwetsbaarheid, waarna de maker van de software de mogelijkheid heeft om de kwetsbaarheid te dichten en hacks te voorkomen.

De AIVD en MIVD gebruiken in het afwegingskader dat zij gebruiken de volgende definitie: «*Een onbekende kwetsbaarheid is een kwetsbaarheid in een geautomatiseerd werk die kan worden gebruikt om dat geautomatiseerde werk binnen te dringen én waarvan het aannemelijk is of verondersteld kan worden dat die niet bekend bij de producent of leverancier.*»[3]

---

[1] http://software-lab.org/publications/ase2018_static_bug_detectors_study.pdf
[2] https://www.synopsys.com/content/dam/synopsys/sig-assets/reports/SCAN-Report-2017.pdf
[3] https://www.aivd.nl/binaries/aivd_nl/documenten/publicaties/2018/05/01/beleid-omgang-met-onbekende-kwetsbaarheden/Beleid+AIVD+en+MIVD+over+onbekende+kwetsbaarheden.pdf

2.2 Risico's Zerodays en het belang van digitalisering

Zerodays maken gebruikers van het apparaat of de software waar de softwarefout zich in bevind kwetsbaar voor hackaanvallen, totdat er een «patch» beschikbaar is die het «gat» dicht. Apparaten waarop die software draait kunnen bijvoorbeeld gemanipuleerd worden of er kan data gelekt worden. Neem bijvoorbeeld een fout in de software van een slimme thermostaat. Die kan een hacker in staat stellen om de temperatuur op afstand te manipuleren of gegevens te downloaden over het gebruik van de thermostaat en daarmee te bepalen of iemand thuis is. Dat is nuttige informatie voor inbrekers. Ook kan het apparaat gebruikt worden om DDoS-aanvallen mee te plegen, bijvoorbeeld om het bankverkeer stil te leggen.

Het belang van digitalisering neemt steeds verder toe. We gebruiken steeds vaker digitale technologieën in ons dagelijks leven, de overheid digitaliseert steeds meer en bedrijven en bedrijfsprocessen worden steeds meer digitaal. Hetzelfde geldt voor onze vitale infrastructuur, zoals energienetwerken, waterkeringen, sluizen en communicatienetwerken.

De Wetenschappelijke Raad voor Regeringsbeleid zegt over digitalisering: «*Het internet is niet meer weg te denken uit ons dagelijks leven. Het is vervlochten met ons sociale leven, consumptie, werk en relatie met de overheid, en in toenemende ook met steeds meer objecten die we dagelijks gebruiken, van de slimme meter tot de auto waarin we rijden en de ophaalbrug die we onderweg tegenkomen.*»[4]

Ook het Rathenau Instituut ziet deze ontwikkeling:
«*Het verschil tussen online en offline vervaagt. Zonder te weten wat het precies betekent, leven we daardoor steeds meer in een digitale samenleving. Digitale technologieën veranderen de manier waarop docenten lesgeven, hoe dokters en patiënten met elkaar praten, waar politici over debatteren en hoe mensen nieuws delen. Achter de schermen werken algoritmen en kunstmatige intelligentie op manieren die we vaak niet eens herkennen. Onze samenleving wordt op deze manier compleet anders ingericht.*»[5]

De Nederlandse Digitaliseringsstrategie van het kabinet benadrukt ook de economische kansen die digitalisering biedt[6]: «*Digitalisering transformeert onze economie en maatschappij in een razendsnel tempo. Dit is een wereldwijde ontwikkeling, waarbij digitale technologieën op steeds meer plekken worden ingezet. Het gaat bijvoorbeeld om big data analyse, kunstmatige intelligentie, blockchain, 3D printen, cloudstorage en -computing en het internet der dingen. Digitalisering is de belangrijkste bron van groei, innovatie en nieuwe bedrijvigheid. En digitalisering is noodzakelijk als we de maatschappelijke uitdagingen van onze tijd willen oplossen, zoals de stijgende zorgkosten, de groeiende filedruk of het zorgen voor voldoende, gezond en duurzaam geproduceerd voedsel.*

Digitalisering transformeert ook ons dagelijks leven. We kunnen online winkelen, zaken doen met de overheid, op afstand werken, internetbankieren en onze belastingaangifte doen. Internetplatforms, zoals Google, Bol.com, Booking.com en Marktplaats, bieden grote voordelen zoals betere toegang tot kennis, makkelijkere en snellere communicatie, en

---

[4] WRR, De publieke kern van het internet. Naar een buitenlands internetbeleid (2015)
[5] https://www.rathenau.nl/nl/privacy-en-cyberveiligheid-een-digitale-samenleving
[6] https://www.rijksoverheid.nl/documenten/rapporten/2018/06/01/nederlandse-digitaliseringsstrategie

nieuwe mogelijkheden voor ondernemers en consumenten om producten en diensten aan te bieden in Nederland en daarbuiten.

Nederland heeft een goede uitgangspositie om de economische en maatschappelijke kansen van digitalisering te verzilveren. We hebben een digitale infrastructuur van wereldklasse. Wifi en bluetooth zijn uitvindingen van Nederlandse bodem. De AMS-IX, een van de belangrijkste internetknooppunten ter wereld, bevindt zich in ons land. Nederland heeft internationaal gezien een hoog opgeleide beroepsbevolking en consumenten lopen hier vaak voorop in het omarmen van nieuwe digitale toepassingen. Ook hebben we in Nederland toonaangevende bedrijven als Booking.com, TomTom, Adyen, NXP, Coolblue en WeTransfer.»

Ook de Cybersecurity Raad benadrukt het grote belang van digitalisering voor Nederland[7]:
«*Nederland heeft zich ontwikkeld tot één van de meest ICT-intensieve economieën van Europa, dankzij onze uitstekende digitale infrastructuur. Denk aan het Amsterdam Internet Exchange (AMS-IX), het grootste internetknooppunt ter wereld, en onze razendsnelle, breedbandige telecomnetwerken. Dat brengt ons veel goeds. Zo is Nederland een aantrekkelijk vestigingsland voor ICT-bedrijven en multinationals. E-commerce genereert nieuwe economische activiteiten en werkgelegenheid. Slimme digitale toepassingen dragen bij aan innovatie en vooruitgang in tal van sectoren. Burgers communiceren steeds vaker digitaal met de overheid en krijgen steeds meer slimme meters en apparatuur in huis.*

De afgelopen 25 jaar zorgde digitale bedrijvigheid voor ruim een derde van alle economische groei. Ruim 5 procent van ons BNP wordt inmiddels verdiend met ICT. De digitale economie vormt inmiddels een derde mainport, naast Schiphol en de Rotterdamse haven. Een mainport die bovendien sneller groeit dan andere economische sectoren.

Digitalisering biedt dus enorme kansen voor de samenleving en economie van de 21e eeuw.
Maar dan is het wel zaak te zorgen dat de digitale wereld veilig en vertrouwd blijft. Of het nu gaat om innovatie, de bescherming van bedrijfsgevoelige informatie, privacy of onze nationale veiligheid: cybersecurity is een basisvoorwaarde voor een welvarende en veilige samenleving in de 21e eeuw. Net zoals we ons land beschermen tegen overstromingen, zullen we ook in de digitale wereld onze dijkbewaking op orde moeten brengen. Alleen zo houden we digitaal droge voeten en kunnen we alle kansen die digitalisering ons land biedt, volop benutten.»

Het beeld dat deze organisaties schetsen is duidelijk. Digitalisering is van groot belang voor onze samenleving, onze economie en onze vrijheden. Bovendien zal dat belang in de toekomst alleen maar toenemen. We gebruiken digitale technologieën steeds vaker in onze vitale infrastructuur, in de zorg, op het werk, in onze vrije tijd en op het gebied van mobiliteit. De nieuwe «kampioenen» van het bedrijfsleven zijn veelal digitale bedrijven als Adyen, Elastic, Booking en Wetransfer. Het wordt tijd dat ook de overheid het belang van digitalisering goed op waarde schat.

2.3 Groeiend belang cybersecurity

Gelijk met het belang van digitalisering groeit ook het belang van cybersecurity in onze samenleving. Voor mensen is het belangrijk dat producten en apparaten veilig zijn. Onveilige apparaten zorgen er nu

[7] Cybersecurity Raad, Nederland Droge Voeten (2016)

bijvoorbeeld voor dat persoonlijke gegevens van mensen lekken of dat kinderen benaderd en gechanteerd worden door pedofielen. Voor bedrijven groeit het belang van het beveiligen van bedrijfsgeheimen. We zien namelijk steeds vaker cyberaanvallen uit andere landen bedoeld om technologie te stelen. Tegelijkertijd zien we steeds meer cyberaanvallen op vitale infrastructuur, zoals energienetwerken, communicatienetwerken, democratische instituties, banken en zorginstellingen.

Ook binnen de vitale sectoren zijn processen steeds meer gedigitaliseerd en dus kwetsbaar voor cyberaanvallen. De Algemene Inlichtingen- en Veiligheidsdienst (AIVD) zegt in het meest recente jaarverslag steeds vaker activiteiten te signaleren die erop zijn gericht digitale sabotage van vitale infrastructuur mogelijk te maken. Ook volgens het Nationaal Cyber Security Centrum (NCSC) neemt deze dreiging toe; de aanvallen zijn bovendien steeds geavanceerder en complexer. Het NCSC ziet sabotage en verstoring door statelijke actoren als de grootste dreiging voor de nationale veiligheid.

De Cybersecurity Raad benadrukt de grote maatschappelijke kosten die gemoeid gaan met slechte cyberveiligheid: «*... cyberdreigingen nemen fors toe. Kwetsbaarheden in ICT-systemen, zoals een tekortschietende beveiliging of verouderde software, vormen de achilleshiel van onze digitale veiligheid. Cybercrime vormt in Nederland nu al een schadepost van 10 miljard euro. Het Cyber Security Beeld Nederland 2016 (CSBN 2016) schetst een zorgelijk beeld van de veiligheidssituatie in het digitale domein. De dreigingen zijn gericht op diefstal van geld en kostbaar intellectueel kapitaal. Ook het verstoren en saboteren van diensten en processen bij overheden en cruciale maatschappelijke organisaties komt voor. Grootschalige maatschappelijke ontwrichting kan het gevolg zijn, bijvoorbeeld als energiecentrales, transportsystemen of waterkeringen aangevallen worden.*»[8]

Maar ook de veiligheid van onze vitale infrastructuur is in het geding. De Algemene Rekenkamer zegt in een rapport over de cyberveiligheid van onze vitale waterwerken: «*Vitale waterwerken maken voor het aansturen van processen gebruik van automatiseringssystemen die veelal stammen uit de jaren '80 en '90 van de 20e eeuw. Toen was het woord cybersecurity nog geen gemeengoed. Deze systemen functioneerden oorspronkelijk stand alone (losstaand) maar zijn in de loop der jaren gekoppeld aan grotere computernetwerken, bijvoorbeeld om bediening op afstand mogelijk te maken. Daardoor is de kwetsbaarheid ervan voor cyberdreigingen toegenomen.*»[9]

Uit het Cybersecuritybeeld 2018 blijkt dat volgens de NCTV en het NCSC sabotage en verstoring door staten de grootste dreiging vormt voor de nationale veiligheid. «*Staten voeren vanuit geopolitieke motieven steeds meer digitale aanvallen uit op andere landen, organisaties of individuen. Zij hebben als doel verwerving van strategische informatie via spionage, beïnvloeding van de publieke opinie of democratische processen en verstoring of zelfs sabotage van vitale systemen. Digitale aanvallen door staten zijn het afgelopen jaar concreet waargenomen. Opvallend is dat eenvoudige aanvalstechnieken succesvol worden ingezet en dat de Nederlandse ict-infrastructuur wordt misbruikt om aanvallen op andere landen uit te voeren. Grote incidenten laten zien dat actoren het risico van nevenschade niet voorzien of mogelijk zelfs accepteren. In het buitenland heeft nevenschade geleid tot maatschappelijke verstoring, in Nederland tot economische schade. Door de afhankelijkheid van (buitenlandse)*

[8] Cybersecurity Raad, Nederland Droge Voeten (2016).
[9] Algemene Rekenkamer, Digitale dijkverzwaring: cybersecurity en vitale waterwerken (2019).

partijen groeit de kwetsbaarheid voor spionage, verstoring en sabotage. Buitenlandse partijen kunnen in specifieke landen wettelijk verplicht worden mee te werken aan het ondersteunen van operaties zoals spionage of voorbereidingen voor sabotage.»[10]

In het meest recente cybersecuritybeeld blijkt dat deze dreiging permanent is en dat zelfs maatschappelijke ontwrichting op de loer ligt. Het NCTV zegt: «*Vrijwel alle vitale processen en diensten zijn volledig afhankelijk van ict. Door het bijna volledig verdwijnen van analoge alternatieven en de afwezigheid van terugvalopties is de afhankelijkheid van gedigitaliseerde processen en systemen zo groot geworden dat aantasting hiervan kan leiden tot maatschappij-ontwrichtende schade. Vitale processen zijn in hoge mate afhankelijk van elektriciteitsvoorziening en datacommunicatie. Uitval en verstoring hiervan hebben zeer snel, binnen enkele uren, impact op een aantal vitale processen. Vanwege de omvang van de dreiging en het achterblijven van de weerbaarheid, ontstaan risico's voor de nationale veiligheid.*»

Ook de AIVD wijst op de kwetsbaarheden van digitale systemen in het jaarverslag 2018: «*Activiteiten van andere landen waarmee zij op heimelijke wijze informatie verzamelen in en over Nederland en daarmee onze belangen schaden, noemen wij spionage. Spionage kan digitaal plaatsvinden, bijvoorbeeld door het inbreken in een systeem, of fysiek via personen. Het kan gaan om belangrijke politieke inlichtingen, bijvoorbeeld ten aanzien van besluitvormingsprocessen en standpunten van de regering. Ook kan een ander land proberen via spionage (bedrijfs)geheimen te stelen om daarmee de eigen economie een impuls te geven.*

Uit onze onderzoeken is verder gebleken dat digitale spionage steeds complexer wordt. Statelijke actoren maken in toenemende mate gebruik van vaker gebruikte methoden en technieken, waardoor het vaststellen van de herkomst van een aanval (attributie) wordt bemoeilijkt. Daarnaast gebruiken statelijke actoren in toenemende mate internetserviceproviders en managed service providers als springplank om binnen te dringen bij een doelwit. Deze dienstverleners hebben uit hoofde van hun dienstverlening vaak diepgravende, omvangrijke en structurele toegang tot informatie van organisaties of personen. Zulke methoden bemoeilijken detectie, analyse en attributie van digitale aanvallen.

Staten kunnen ook een dreiging vormen voor de onafhankelijkheid en zelfstandigheid van Nederland doordat zij digitale sabotage van vitale infrastructuur mogelijk maken. Dit doen zij door zich toegang te verschaffen en zich vervolgens in te nestelen in ICT-systemen van vitale processen. De AIVD heeft gezien dat hiertoe pogingen zijn gedaan.»[11]

Uit deze rapporten komt een duidelijk beeld naar voren: hoe meer onze samenleving digitaliseert hoe belangrijker goede cybersecurity wordt. Mensen, bedrijven, vitale infrastructuur en overheden gebruiken allemaal steeds meer digitale technologie. Dat biedt veel kansen, maar vergt ook meer aandacht voor de veiligheid van die digitale technologie. Uit publicaties van de meest toonaangevende instanties in Nederland op het gebied van cyberveiligheid blijkt de potentiële maatschappelijke en economische schade van slechte cyberveiligheid. Ondanks de vele hackaanvallen, datalekken en rapporten die waarschuwen voor de grote gevolgen van slechte cyberveiligheid wordt het belang ervan nog onvoldoende erkend.

---

[10] NCTV, Cybersecuritybeeld Nederland (CSBN) 2018 (2018)
[11] Algemene Inlichtingen- en Veiligheidsdienst, jaarverslag 2018 (2019)

2.4 Hackaanvallen in de praktijk

Dat het belang van cybersecurity is toegenomen door de digitalisering van onze samenleving is geen theoretische constatering. De afgelopen jaren zijn er tal van cyberaanvallen geweest die dit belang concreet hebben aangetoond. De AIVD zegt in haar jaarverslag 2017 al dat zij «*...digitale spionage [heeft] vastgesteld bij diverse Europese multinationals en onderzoeksinstellingen in de energie-, hightech-, en chemische sector. Hieronder bevinden zich diverse organisaties die intensieve samenwerkingsrelaties hebben met Nederland of vestigingen hebben in Nederland. Bij deze digitale inbraken zijn terabytes aan vertrouwelijke gegevens gestolen die een substantiële economische waarde vertegenwoordigen. Dergelijke hardnekkige digitale aanvallen vormen een bedreiging van het economisch verdienvermogen van Nederland.*»[12]

De bekendste cyberaanvallen van de afgelopen jaren zijn waarschijnlijk Wannacry en NotPetya. Wannacry heeft waarschijnlijk tussen de 4 en 8 miljard dollar schade veroorzaakt en NotPetya zelfs tot 10 miljard dollar wereldwijd. Wannacry was een ransomware aanval in mei 2017. Deze cryptoworm gebruikte een kwetsbaarheid in Microsoft Windows (EternalBlue) om systemen binnen te dringen. Deze kwetsbaarheid was bekend geworden doordat een hackersgroep genaamd Shadow Brokers een server van de NSA had gehackt en de daarop gevonden hacktools openbaar had gemaakt. De EternalBlue kwetsbaarheid was een zeroday die door de NSA geheim was gehouden zodat het gebruikt kon worden door de NSA om hackaanvallen te plegen.

De Wannacry aanval bereikte meer dan 200.000 computers in meer dan 150 landen. Een van de grootste slachtoffers van de Brits «National Health Service». De ransomware besmette computers, MRI scanners, bloedopslag systemen en andere apparatuur, waardoor zelfs kankerpatiënten tijdelijk niet geholpen konden worden. Ook legde de aanval fabrieken van Nissan en Renault stil en werd het treinverkeer in Duitsland ontregeld.

NotPetya had in Nederland een nog grotere impact. De cyberaanval trof onder andere de Rotterdamse haven, een van de Nederlandse economische mainports. Twee grote container terminals werden platgelegd door NotPetya, dat waarschijnlijk door Rusland is gemaakt. Waarschijnlijk heeft dit tientallen miljoenen schade veroorzaakt in Nederland.

Een van de grootste slachtoffers van de cyberaanval was Maersk, het Deense logistiek bedrijf. NotPetya legde de complete digitale infrastructuur van Maersk plat. Twee weken lang kon het bedrijf computersystemen niet gebruiken om containers te verschepen. Bij havens over de hele wereld ontstonden kilometerslange files van vrachtwagens met containers die Maersk niet kon verwerken. Medewerkers begonnen bestellingen met de hand, via WhatsApp, met persoonlijke Gmail accounts en met excelsheets bij te houden. Uiteindelijk kon Maersk zijn backups herstellen doordat een server in Ghana tijdens de aanval uit was gevallen door een stroomaanval en daardoor niet was besmet. Een van de medewerkers van het bedrijf is naar Ghana gevlogen en met de backup op een fysieke harde schijf terug gevlogen naar het crisiscentrum in Engeland. Uiteindelijk moest het bedrijf de complete digitale infrastructuur opnieuw opbouwen, waaronder 4000 servers en 45 000 computers. De aanval kostte het Deense bedrijf tussen de 250 en 300 miljoen dollar.

---

[12] Algemene Inlichtingen- en Veiligheidsdienst, jaarverslag 2017 (2018)

De meeste bekende cyberaanval door een statelijke actor was de Stuxnet aanval. Deze digitale aanval, waarschijnlijk uitgevoerd door Israël en de Verenigde Staten, maakte gebruik van verschillende zerodays en had als doel het verstoren van het Iraanse atoomprogramma. De Stuxnet-worm beïnvloedde de werking van zogeheten SCADA-systemen die aanwezig waren in nucleaire centrales van Iran en zorgde ervoor dat ongeveer een vijfde van Irans nucleaire centrifuges zichzelf vernietigden.

Meer recent werd bekend dat het Amerikaanse Cyber Command Iraanse raketsystemen onklaar heeft gemaakt.[13] Details ontbreken, maar het toont wel aan dat offensieve cybercapaciteiten steeds meer een «regulier» onderdeel uitmaken van krijgsmachten.

Daarnaast zien we ook steeds vaker dat statelijke actoren ingekochte kant en klare hacksoftware gebruiken voor inlichtingendoelen. Het meest bekende voorbeeld is het gebruik door Saoedi-Arabië van hacksoftware van het Israëlische bedrijf NSO Group om de vermoorde Saudische journalist Khashoggi te volgen.[14] Maar dezelfde software wordt ook gebruikt door Mexico en de Verenigde Arabische Emiraten om journalisten en dissidenten te volgen.[15] Ook hacksoftware van Europese bedrijven als HacktingTeam en Gamma International wordt gebruikt door repressieve regimes in Sudan, Ethiopië, Bahrein, Egypte en Kazachstan.

Naast deze cyberaanvallen zijn er veel meer voorbeelden van hackaanvallen met grote maatschappelijke gevolgen. Enkele voorbeelden hiervan zijn:
- In 1998 slaagde een tiener erin om de communicatie tussen inkomende vliegtuigen en de luchtverkeersleiding in Worcester, Massachusetts af te snijden.
- In 2001 kreeg een criminele hacker toegang tot een rioolwaterzuiveringsinstallatie in Maroochy Shire, Queensland, Australië en liet miljoenen liters rioolwater lekken, met enorme schade aan de plaatselijke natuur en potentiële gezondheidsrisico's voor inwoners tot gevolg.
- Tussen 2005 en 2007 was er sprake van een golf van cyberaanvallen vlakbij Rio de Janeiro. Dat leidde er onder andere toe dat meer dan 3 miljoen mensen en bedrijven zonder stroom zaten, met grote economische schade tot gevolg.
- In 2009 berichtte de Wall Street Journal dat staatshackers van China, Rusland en andere landen Amerikaanse energienetwerken waren binnengedrongen. Vooralsnog zijn de aanvallen vooral gericht op het in kaart brengen van de energienetwerken en op het inbouwen van mogelijkheden om in oorlogstijd de netwerken plat te kunnen leggen.
- In 2011 slaagden hackers erin een waterzuiveringsinstallatie in South Houston, Texas te hacken en een pomp te beschadigen door het snel achter elkaar aan en uit te schakelen.
- In 2013 zei de Amerikaanse overheid dat China achter een serie cyberaanvallen zat die gericht was op het achterhalen van informatie over de nieuwe F-35 straaljager en andere technologische kennis over een nieuwe raketsysteem, de F/A 18 straaljager, de V-22 Ospreys helikopter en nieuwe marineschepen.
- In 2015 werd bekend dat Chinese hackers toegang hadden verkregen tot systemen van ASML en mogelijk technologische kennis hebben gestolen. Achteraf bleek dat de hackers via een zeroday toegang

[13] https://tweakers.net/nieuws/154348/amerikaanse-staatshackers-hebben-iraanse-raketsystemen-onklaar-gemaakt.html
[14] https://www.nytimes.com/2018/12/02/world/middleeast/saudi-khashoggi-spyware-israel.html
[15] https://www.nytimes.com/2019/05/13/technology/nso-group-whatsapp-spying.html

hadden gekregen tot een VPN-verbinding die gebruikt werd door een dochterbedrijf van ASML.
– In 2017 berichtte het bekende technologie tijdschrift *Wired* dat Rusland Oekraïne gebruikt als een «cyber test lab». De aanvallen die Rusland in Oekraïne uitvoert zouden een soort blauwdruk zijn voor wat Rusland wereldwijd aan cyberaanvallen zou kunnen uitvoeren. Een leger van hackers zou systematisch vrijwel elke sector in het land aanvallen. Van energienetwerken tot banken en van mediabedrijven tot openbaar vervoer. Informatie wordt gestolen, computers platgelegd en systemen gemanipuleerd.

De dreiging van hackaanvallen is geen theoretisch probleem. Er zijn tal van voorbeelden van hackaanvallen die grote gevolgen hadden voor onze economie, onze vrijheid en onze veiligheid. Dergelijke aanvallen zullen in de toekomst alleen maar toenemen als gevolg van onze steeds verder digitaliserende samenleving. De enige manier om dit te voorkomen is om het belang van cyberveiligheid te erkennen en concrete stappen te nemen om onze cyberveiligheid te vergroten. Initiatiefnemer is van mening dat deze initiatiefwet daaraan een concrete en belangrijke bijdrage kan leveren.

2.5 Actoren

Een breed scala aan actoren zoekt actief naar en/of gebruikt zerodays. Statelijke actoren, criminelen, terroristische groeperingen, bedrijven, ethisch hackers, wetenschappelijk onderzoekers enzovoort. Sommigen zoeken naar zerodays om ervoor te zorgen dat ze gedicht worden, zoals ethisch hackers, onderzoekers en bedrijven. Anderen hebben als doel zerodays te gebruiken om te hacken. Zo gebruiken statelijke actoren steeds vaker digitale middelen om nationale belangen na te streven. Of het nou gaat om het stelen van technologische informatie, het verdedigen van nationale veiligheidsbelangen of offensieve cybercapaciteiten.

Statelijke actoren gebruiken zerodays voor het vergaren van informatie voor opsporings- of inlichtingendoeleinden of om computersystemen en de apparaten die door die systemen aangestuurd worden te verstoren. Een goed voorbeeld van het laatste is de eerdergenoemde Stuxnet aanval, waarmee nucleaire centrifuges gesaboteerd werden. Meer recent werd bekend dat Amerikaanse staatshackers Iraanse raketsystemen onklaar zouden hebben gemaakt.[16]

Een ander voorbeeld van het gebruik van zerodays door inlichtingendiensten zijn de Snowden-onthullingen. Snowden maakte bekend dat Amerikaanse inlichtingendiensten op grote schaal hacktools gebruikten om mensen af te kunnen luisteren. Deze hacktools maakten veelal gebruik van zerodays om apparaten binnen te dringen.

Ook criminelen maken veelvuldig gebruik van cyberaanvallen, vooral om geld buit te maken. De pakkans is immers klein en de winsten groot. Traditionele criminele organisaties als de Italiaanse Maffia, de Japanse Yakuza en andere georganiseerde misdaadorganisaties hebben de afgelopen decennia ook een cybercrime-tak opgezet. Vaak gaat het om afpersing via ransomware, het verspreiden van kinderporno of creditcard-fraude. Er zijn zelfs criminelen die «cybercrime as a service» aanbieden. Criminelen kopen hier kant en klare software om ransomware te verspreiden of om DDoS-aanvallen uit te voeren.

[16] https://tweakers.net/nieuws/154348/amerikaanse-staatshackers-hebben-iraanse-raketsystemen-onklaar-gemaakt.html

Bovenstaande actoren zijn op zoek naar zerodays om ze te gebruiken om te hacken. Daarnaast zijn er ook actoren op zoeken naar zerodays om ze kunnen dichten en zo software, apparaten en uiteindelijk de mensen die ze gebruiken veiliger te maken. Ethische hackers en wetenschappelijke onderzoekers zijn de meest belangrijke voorbeelden van actoren die streven naar het vinden en dichten van zerodays. Overheden en bedrijven hebben bovendien beleid ontwikkeld om ethisch hackers en onderzoekers te ondersteunen. Zo heeft Nederland een zogeheten Responsible Disclosure richtlijn[17] ontwikkeld en hebben veel bedrijven en overheden «bug-bounty»-programma's om ethisch hackers te belonen en te stimuleren. Er zijn zelfs bedrijven die hierop inspelen en ethische hackers en bedrijven en overheden met bug-bounty programma's met elkaar in contact brengen, zoals de Groningse Startup HackerOne.

2.6 Nut en Noodzaak

2.6.1 Waarom is een afwegingskader nodig?
De gevolgen van hackaanvallen worden steeds groter. Onze samenleving digitaliseert steeds verder en we sluiten steeds meer aan op het internet. Tegenwoordig zijn niet alleen PCs, laptops en mobiele telefoons aangesloten op het internet, maar ook onderdelen van onze vitale infrastructuur, hele fabrieken, systemen in het openbaar vervoer, medische apparaten en energienetwerken. Het aantal apparaten groeit naar verwachting snel van 9 miljard in 2017 naar 55 miljard in 2025.[18] Nederland is dankzij de digitale mainport, het snelle internet en de digitaal vaardige bevolking koploper in digitalisering.

Dat biedt tal van kansen. Bijvoorbeeld op het gebied van economische groei, betere dienstverlening, meer gemak, betere zorg en veiligere communicatie. Het is belangrijk om deze kansen goed op waarde te schatten omdat het geheimhouden van zerodays negatieve gevolgen kan hebben voor deze belangen. Opengehouden zerodays kunnen namelijk ook door andere actoren gevonden en gebruikt worden, met mogelijke schade als gevolg op het gebied van economie, (cyber)veiligheid en vrijheid. Meer digitalisering betekent namelijk ook meer kwetsbaarheid voor hackaanvallen en dus moet er meer aandacht zijn voor cybersecurity. Het openhouden van zerodays heeft per definitie een negatief effect op de cybersecurity van onze samenleving.

Neem een aanval als Wannacry. De kwetsbaarheid die werd gebruikt tijdens deze cyberaanval was oorspronkelijk een zeroday die door de NSA geheim werd gehouden om zelf te kunnen hacken. De NSA werd echter zelf gehacked door de hackgroep ShadowBrokers, die vervolgens de kennis over de zeroday publiceerde. Vervolgens konden criminelen en statelijke actoren die kennis gebruiken om hun eigen cyberaanvallen te lanceren, zoals de Wannacry aanval. Deze aanval is volgens onderzoekers waarschijnlijk door Noord Korea geïnitieerd. Het gevolg was miljarden aan economische schade, ziekenhuizen in het VK konden kankerpatiënten niet behandelen en meerdere fabrieken in Europa lagen plat.

Internationaal zijn er meerdere voorbeelden van de enorme maatschappelijke en economische schade die het openhouden van zerodays met zich mee kan brengen. De genoemde voorbeelden zijn bovendien slechts van zerodays die eerst geheimgehouden zijn door overheden om te kunnen hacken en onbedoeld publiek bekend zijn geworden. Het is zeer aanne-

[17] https://www.ncsc.nl/actueel/nieuwsberichten/leidraad-responsible-disclosure.html, geraadpleegd op 6 mei 2019
[18] https://www.businessinsider.com/intelligence/bi-intelligence-iot-research-bundle-reports-store?international=true&r=US&IR=T

melijk dat overheden momenteel kennis over zerodays geheimhouden, terwijl statelijke actoren, criminelen, terroristen of andere kwaadwillenden diezelfde zeroday gebruiken voor minder goede bedoelingen.

Dit soort voorbeelden tonen de kwetsbaarheid van de steeds verdergaande digitalisering van onze samenleving en de noodzaak van een goed afwegingskader voor het gebruik van zerodays door overheden. Daarmee kunnen dit soort situaties in de toekomst worden voorkomen. Met een goed afwegingskader kunnen namelijk betere beslissingen genomen worden over het openhouden, dan wel het laten dichten, van zerodays.

2.6.2 Verschillende belangen

Het openlaten en gebruiken van zerodays om te hacken leidt tot een dilemma. Het openlaten van een zeroday kan een bepaald inlichtingen of opsporingsbelang dienen. Deze belangen zijn uitgebreid omschreven in de wet computercriminaliteit 3 (CC3), de wet op de inlichtingen en veiligheidsdiensten (WIV) en de Defensie cyberstrategie. In essentie komen deze belangen neer op de waarde van het inwinnen van informatie over verdachten en het inwinnen van informatie die voor inlichtingendiensten van belang is voor de nationale veiligheid door middel van het binnendringen van apparaten. Het belang van defensie gaat verder dan het inwinnen van informatie en kan ook het beïnvloeden of platleggen van de werking van apparaten omvatten, zoals het platleggen van een radarinstallatie of een (deel van een) elektriciteitsnetwerk.

In de memorie van toelichting van de Wet Computercriminaliteit 3 wordt het belang volgt omschreven: «*Het doel van de bevoegdheid van onderzoek in een geautomatiseerd werk is om toegang te verkrijgen tot de gegevens die in een geautomatiseerd werk zijn of worden verwerkt ten behoeve van de opsporing van ernstige vormen van computercriminaliteit of andere ernstige misdrijven.*»[19]

De memorie van toelichting van de Wet op de Inlichtingen en Veiligheidsdiensten 2017 zegt het volgende hierover: «*De bevoegdheid van de diensten tot het kunnen binnendringen in een geautomatiseerd werk en het kunnen overnemen van gegevens, zoals deze thans in artikel 24 van de Wiv 2002 is geregeld, is in de afgelopen jaren van groot belang gebleken. Met het oog op het huidige dreigingsbeeld en het gegeven dat wij leven in een digitale wereld, is het voor diensten noodzakelijk om deze bijzondere bevoegdheid te kunnen uitoefenen. Het gebruik van digitale apparatuur zoals pc's, smartphones, laptops, tablets, maar ook de opslag in de cloud, is onmiskenbaar in alle facetten van het maatschappelijk leven (bij burgers, bedrijven en overheden) doorgedrongen en heeft daar een niet meer weg te denken positie verworven. Voeg daarbij de ontwikkeling van de Internet of Things(waarbij apparaten, zoals koelkasten, auto's, horloges e.d. in toenemende mate worden gecomputeriseerd), waardoor onmiskenbaar blijkt hoe groot de impact van de digitalisering op de samenleving is. Bij targets van de diensten is toegang tot de smartphone of tablet tegenwoordig vaak relevanter dan bijvoorbeeld het binnentreden in een woning of het inzetten van een telefoontap. Bij onderzoek naar cyberaanvallen gericht op de Nederlandse infrastructuur of specifiek op de vitale sectoren is het belang om hetzelfde gereedschap te hebben als de digitale aanvaller. Zonder dit gereedschap, zijn de diensten niet staat om deze aanvallen (tijdig) te onderkennen.*»

Tegelijkertijd kan het openlaten van een zeroday andere belangen schaden. Zo kan de cyberveiligheid van de vitale infrastructuur negatief beïnvloed worden door het openlaten van een zeroday in systemen die in

[19] Kamerstuk 34 372 nr. 3

de vitale infrastructuur gebruikt worden, bijvoorbeeld in onze vitale waterinfrastructuur of energienetwerken. Onveilige consumentenapparaten kunnen bovendien gebruikt worden door criminelen om (vaak jonge) mensen af te persen. Er zijn tal van voorbeelden van jonge meisjes die door pedofielen zijn afgeperst om naaktfoto's en andere beelden te delen naar zij hun onveilige webcams hadden gehackt. Ook zijn er tal van voorbeelden van hackaanvallen die zorgapparatuur onklaar maken en daarmee adequate zorgverlening belemmeren, waarmee de fysieke gezondheid van mensen aangetast kan worden.

Daarnaast kan het openlaten van een zeroday negatieve economische gevolgen hebben, zoals we bij de Wannacry en NotPetya aanvallen hebben gezien. Deze aanvallen veroorzaakten vele honderden miljoenen euro's aan schade. Ook hebben kleine bedrijven en zzp'ers steeds vaker te maken met hackaanvallen als ransomware die in sommige gevallen zelfs tot faillissement en persoonlijke drama's kunnen leiden. Een door een overheid opengelaten zeroday in de software van apparaten van een Nederland bedrijf kan bovendien de reputatie van het bedrijf aantasten en daarmee de economische belangen van Nederland raken.

Tot slot kunnen door de overheid opengelaten zerodays de individuele vrijheid van individuen en de rechten van de mens aantasten. Onveilige apparaten of verbindingen kunnen gevoelige data lekken, zoals privéinformatie, zorgdata en andere gevoelige gegevens. Onveilige apparaten tasten het vertrouwen van mensen in technologie aan, waardoor zij zich minder vrij voelen. Ook kan het leiden tot een gevoel van surveillance waardoor mensen hun gedrag aanpassen.

2.6.3 Afwegingskader voor de hele overheid

In 2017 constateerde de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) het volgende: «*Tekortkomingen bestaan ook in de omgang met onbekende kwetsbaarheden, zogenaamde «zerodays». 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.*»[20]

De CTIVD constateerde kortom dat er een afwegingskader nodig is voor de omgang met zerodays. In mei 2018 is uiteindelijk beleid vastgelegd voor de AIVD en MIVD waarin uiteen wordt gezet hoe de diensten om moeten gaan met ontdekte zerodays. De kern van het beleid wordt gevormd door het uitgangspunt: «melden, tenzij...». De diensten hebben immers een veiligheidsbevorderende taak om de veiligheid van informatie en systemen te verbeteren. De diensten kunnen echter een uitzondering op de regel maken als zij van mening zijn dat het niet melden van de zeroday in het belang is van de nationale veiligheid.

Het beleid zegt het volgende over het afwegingsproces: «*Aan de hand van het afwegingskader wordt gekeken naar de wettelijke bepalingen, operationele overwegingen en belangen die door het melden kunnen worden behartigd. Dit afwegingskader is niet absoluut. De antwoorden op de vragen worden per casus gewogen. Ook wordt er periodiek (in ieder geval jaarlijks) gekeken of de niet gemelde kwetsbaarheid alsnog kan worden gemeld.*»[21] Het Amerikaanse afwegingsproces voor zerodays (het zogeheten VEP proces) is als model gebruikt als het gaat om de criteria en

[20] https://www.ctivd.nl/actueel/nieuws/2017/04/25/index

[21] https://www.aivd.nl/binaries/aivd_nl/documenten/publicaties/2018/05/01/beleid-omgang-met-onbekende-kwetsbaarheden/Beleid+AIVD+en+MIVD+over+onbekende+kwetsbaarheden.pdf

vragen die worden gehanteerd bij de afweging een zeroday al dan niet te melden.

Om de beste beslissingen te nemen wat betreft het openlaten, dan wel melden of openbaar maken van zerodays moeten deze belangen goed tegen elkaar afgewogen worden. Het Nederlands belang is niet gediend bij het openlaten van zerodays die slechts een beperkte operationele waarde hebben voor politie of AIVD, maar die wel een grote negatieve impact hebben op onze economie, op de cyberveiligheid van onze vitale infrastructuur of de vrijheid van mensen. Tegelijkertijd is onze nationale veiligheid niet gediend bij het verplicht moeten melden van zerodays in software dat vooral door criminelen of buitenlandse mogendheden wordt gebruikt. Een goede afweging, op basis van zoveel mogelijk informatie en met een degelijke weging van verschillende belangen is daarom van groot belang voor onze cyberveiligheid.

Daar hoort een afwegingskader bij dat voor de hele overheid geldt en niet alleen voor de AIVD en MIVD. Momenteel bestaat er geen formeel vastgelegd afwegingskader voor de Politie, Marechaussee, FIOD en Defensie. Terwijl de beslissingen die deze organisaties nemen met betrekking tot het al dan niet melden van zerodays de werkwijze van onze inlichtingen- en veiligheidsdiensten, economische belangen, (cyber)veiligheids- en vrijheidsbelangen of zelfs de veiligheid van onze vitale infrastructuur kunnen schaden.

Een wettelijk vastgelegd afwegingskader zorgt er kortom voor dat:
A) De verschillende veiligheidsbelangen van de Politie, Marechaussee, Defensie, FIOD en AIVD en MIVD elkaar niet onnodig schade berokkenen, en
B) Dat alle relevante belangen (economie, cyberveiligheid, vrijheid, etc.) meegewogen worden in de afweging om een zeroday al dan niet te melden.

Dit afwegingskader moet leiden tot betere afwegingen over het al dan niet melden van zerodays, wat beter is voor onze nationale veiligheid, onze cyberveiligheid, onze economie, onze privacy en de veiligheid van onze vitale infrastructuur.

Bovendien kan Nederland, door het opstellen van een wettelijk geborgd afwegingskader, bijdragen aan het vormgeven van een internationale norm van goede belangenafweging voor het openhouden en gebruiken van zerodays. Dit kan ook wereldwijd leiden tot meer cyberveiligheid en een betere borging van belangen die geschaad (kunnen) worden door het openlaten van zerodays. Dit is voor een land als Nederland dat sterk gedigitaliseerd is van groot belang.

2.6.4 Voorbeelden van afwegingsprocessen in andere landen en belangwekkende rapporten
Voor zover bekend hebben alleen de Verenigde Staten en het Verenigd Koninkrijk momenteel een afwegingskader voor zerodays dat geldt voor de gehele overheid.[22] Dit zijn in ieder geval de enige landen die documentatie hebben gepubliceerd over hun afwegingsproces. Daarnaast bespreken we een belangwekkend rapport van de *Stiftung Neue Verantwortung* genaamd «Governmental Vulnerability Assessment and Management» waarin belangrijke inzichten zijn geformuleerd over de vormgeving van een afwegingsproces voor zerodays.

[22] In Nederland bestaat tevens een afwegingskader voor zerodays, maar deze is alleen van toepassing op de AIVD en MIVD.

2.6.4.1 Verenigde Staten

In 2015/2016 is een aantal documenten over het afwegingsproces, oftewel het: «Vulnerability Equities Process» (VEP), in de Verenigde Staten openbaar gemaakt. Als reden voor het opstellen van het VEP wordt het volgende gezegd over het vinden van zerodays door overheden: «[this] may present competing equities for offensive and defensive mission interests». Daarom stelt het document dat: «actions taken in response to knowledge of a specific vulnerability must be coordinated to ensure the needs of each of these «equities» are addressed». Kortom: het vinden en openhouden van zerodays leidt tot spanning tussen offensieve en defensieve belangen en alle verschillende belangen moeten goed afgewogen worden.

Het doel van het Amerikaanse VEP is «*het prioriteren van het publieke belang op het gebied van cybersecurity en het beschermen van de vitale kern internet infrastructuur, informatie systemen, vitale infrastructuur systemen en de Amerikaanse economie door middel van het openbaar maken van (onbekende) kwetsbaarheden die gevonden worden door de Amerikaanse overheid, tenzij er een aantoonbaar, doorslaggevend belang is bij het gebruik van de kwetsbaarheid voor wettige inlichtingen, wetshandhaving of nationale veiligheidsdoeleinden.*»[23]

Om het VEP uit te voeren is een zogeheten «Equities Review Board» (ERB) opgericht, oftewel een orgaan dat een afweging moet maken tussen verschillende belangen. Het secretariaat wordt gevormd door het «National Security Agency» (NSA). Het ERB komt elke maand samen en bestaat uit tal van overheidsinstanties, namelijk:
- Office of Management and Budget
- Office of the Director of National Intelligence (to include Intelligence Community-Security
- Coordination Center (IC-SCC))
- Department of the Treasury
- Department of State
- Department of Justice (to include the Federal Bureau of Investigation and the National Cyber
- Investigative Joint Task Force (NCIJTF))
- Department of Homeland Security (to include the National Cybersecurity Communications and
- Integration Center (NCCIC) and the United States Secret Service (USSS))
- Department of Energy
- Department of Defense (including the National Security Agency (NSA) (including Information
- Assurance and Signals Intelligence elements)), United States Cyber Command, and DoD Cyber
- Crime Center (DC3)
- Department of Commerce
- Central Intelligence Agency

Bij de afweging om een zeroday geheim te houden of openbaar te maken wordt in ieder geval een aantal categorieën overwegingen meegenomen, namelijk:
- «Defensive Equity Considerations»
- «Intelligence, Law enforcement, and Operational Equity Considerations»
- «Commercial Equity Considerations»

[23] https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF

– «International Partnership Equity Considerations»

2.6.4.2 Verenigd Koninkrijk

Eind 2018 heeft ook het Verenigde Koninkrijk informatie gepubliceerd over het «Equities Process» met betrekking tot zerodays. Ook in het VK is het uitgangspunt dat het openbaar maken of melden van zerodays in het nationaal belang is. De inrichting van het proces verschilt echter met de manier waarop het proces in de VS is ingericht. Naast een «Equities Board», is er een ook een «Equities Technical Panel» en een «Equities Oversight Committee». Naast een orgaan dat afwegingen maakt over het al dan niet geheimhouden van zerodays is er dus ook een technisch orgaan dat een eerste schifting maakt en een commissie dat toezicht houdt op het goed verlopen van het proces.

Het «Equities Board» wordt in het VK voorgezeten door een hoge ambtenaar, vaak afkomstig uit het Engelse National CyberSecurity Centre (NCSC) en bestaat tevens uit vertegenwoordigers van verschillende ministeries en overheidsinstanties. Bij het Engelse afwegingsproces worden soortgelijke overwegingen gebruikt als in het Amerikaanse VEP; aanvullend wordt ook het gebruik van de zogeheten «Common Vulnerability Scoring System» genoemd als standaard om de «zwaarte» van zerodays een bepaalde waarde te geven.

2.6.4.3 Rapport: Governmental Vulnerability Assessment and Management

In augustus 2018 publiceerde de denktank *Stiftung Neue Verantwortung* (SNV) een rapport samen met de Transatlantic Cyber Forum genaamd: Governmental Vulnerability Assessment and Management.[24] Het rapport beschrijft het belang van goede afwegingsprocessen voor zerodays en zet een kader neer voor de mogelijke inrichting van dergelijke afwegingsprocessen.

Het rapport stelt een aantal uitgangspunten op voor afwegingsprocessen voor zerodays:
– Elke overheid die zerodays wil gebruiken voor wetshandhaving, inlichtingendiensten of militaire operaties moet een open en transparant afwegingskader opstellen.
– Het proces moet wettelijke verankerd worden, met een evaluatie gericht op effectiviteit en proportionaliteit binnen vijf jaar.
– Het afwegingsproces voor zerodays moet worden toegepast op alle zerodays die door de overheden zijn verworven, inclusief hacktools en -diensten die gebruik maken van zerodays.
– Kwetsbaarheden worden nooit permanent bewaard.
– Het principe dat openbaarmaking van kwetsbaarheden in het beste belang is van handel, burgerlijke vrijheden, openbare veiligheid en IT veiligheid moet voorop staan.
– Een overheid die kwetsbaarheden wil behouden, moet een kritieke behoefte aantonen die opweegt tegen de beveiligingsvoordelen van openbaarmaking van de zeroday en een plan opstellen om schade te minimaliseren, inclusief adequate beveiligingen om te zorgen voor een veilige bewaring van zerodays door deze op de juiste manier te beschermen tegen ongeautoriseerde toegang gedurende de periode voorafgaand aan de bekendmaking. Deze beveiliging moet een mechanisme bevatten om de openbaarmaking te versnellen in het licht van een gebeurtenis die aangeeft dat het bestaan van de zeroday bekend is bij derden.

[24] https://www.stiftung-nv.de/sites/default/files/vulnerability_management.pdf

– Regeringen die een dergelijk proces hebben uitgevoerd, moeten ernaar streven dit als een internationale norm te promoten via relevante internationale coördinatiemechanismen en samenwerkingsnetwerken.
– Onderzoek naar «collision rates» moet financieel worden gesteund door de overheid om het behouden en gebruiken van zerodays te rechtvaardigen, zonder tegelijkertijd de burgerlijke vrijheden, de handel, openbare veiligheid en IT-beveiliging in het geding te breng.
– Een beter begrip van acquisitie van zerodays (bijvoorbeeld transparantievereisten voor kwetsbaarheidsmarkten en handel) en openbaarmaking (bijvoorbeeld de implementatie van gecoördineerde openbaarmaking van kwetsbaarheden) moet worden ontwikkeld.

Daarnaast bevat het rapport adviezen met betrekking tot de reikwijdte, de organisatorische opzet, eventuele uitzonderingen, mitigatie maatregelen en overwegingen die belangrijk zijn voor de inrichting van zeroday afwegingskaders. Een aantal adviezen uit het rapport is relevant om te melden.

Allereerst over de reikwijdte. Het rapport stelt dat het afwegingskader voor alle zerodays zou moeten gelden en dat overheden geen geheimhoudingsverklaringen zouden mogen tekenen om te voorkomen dat zerodays door het afwegingsproces beoordeeld worden. Dit zou ook moeten gelden voor de zerodays waarvan ingekochte hacktools gebruik maken. Het toelaten van dit soort geheimhoudingsverklaringen en het aankopen van hacktools zou het afwegingsproces omzeilen en is uiteindelijk slecht voor de cyberveiligheid en daarmee het nationaal belang van Nederland. Ook benadrukt de denktank dat zerodays die door ethische hackers, onderzoekers of anderen gemeld worden aan de overheid direct aan de maker van de software gemeld moeten worden of openbaar gemaakt moeten worden. Dit is cruciaal voor het vertrouwen in de overheid om deze functie als «neutrale derde» te kunnen vervullen.

Ook op het gebied van de organisatorische opzet heeft de *Stiftung Neue Verantwortung* een aantal belangrijke aanbevelingen. Allereerst stelt de denktank dat er een centraal orgaan, een secretariaat, moet zijn waar de verschillende overheidsinstanties samen komen om afwegingen te maken en de verschillende belangen tegen elkaar af te wegen. Elke overheidsinstantie die betrokken wordt in het afwegingskader moet een «Point of Contact» (POC) aanwijzen die concreet zitting neemt in het afwegingsorgaan. Dit afwegingsorgaan is, zoals eerder beschreven, in de Verenigde Staten onder het NSA gehangen, maar het SNV geeft de aanbeveling om dit orgaan onder te brengen bij een overheidsinstantie die beter aansluit bij het kernprincipe van het afwegingskader, namelijk dat er een «bias towards disclosure» moet zijn. Bijvoorbeeld bij een instantie dat zich bezig houdt met cybersecurity. Verder adviseert de SNV om het principe «bias towards disclosure» vast te leggen in de stemverhoudingen, namelijk dat een zeroday openbaar gemaakt of gemeld wordt als een robuuste minderheid (15% of meer) van de POCs dat adviseert.

Met betrekking tot de afweging zelf stelt het SNV dat in ieder geval de volgende overwegingen meegenomen moeten worden:
– Het verspreidingsniveau van de zeroday;
– Waarschijnlijkheid van patch-voorziening;
– Waarschijnlijkheid van acceptatie van patches;
– Mogelijke mitigatiemaatregelen;
– Herkomst van de software;
– De mate van gebruik van het betreffende product;
– Waarschijnlijkheid van detectie;
– Ernst van de kwetsbaarheid;

– De kans dat andere actoren dezelfde zeroday vinden (Collision rate);
– De operationele waarde van de zeroday.

2.7 Moet de overheid überhaupt de bevoegdheid hebben om te hacken?

Sommigen zijn van mening dat de overheid überhaupt niet de bevoegdheid zou moeten hebben om te hacken, of alleen via bekende kwetsbaarheden. Initiatiefnemer is van mening dat dit standpunt, hoe begrijpelijk ook, te rigide is. De argumentatie achter dit standpunt is vergelijkbaar met die van de initiatiefnemer, namelijk dat het belang van cybersecurity, mede doordat zoveel onderdelen van onze samenleving digitaal zijn geworden (zorg, vitale infrastructuur, communicatie, bedrijfsprocessen, etc.), zo groot is geworden dat het openlaten van zerodays een niet toelaatbaar risico is geworden.

Initiatiefnemer is het eens dat, door de toegenomen digitalisering van onze samenleving en daarmee het gegroeide belang van cybersecurity, we zorgvuldiger om moeten gaan met het openlaten van zerodays. Dat is de reden waarom initiatiefnemer pleit voor een wettelijke geborgd afwegingskader met een «bias towards disclosure». Dat wil zeggen dat belangen als economie, privacy en cyberveiligheid van mensen zwaar moeten wegen in afwegingen om zerodays open te houden.

Dit zal in de meeste gevallen ertoe moeten leiden dat zerodays gemeld en gedicht worden. Tegelijkertijd moeten politie, inlichtingendiensten en defensie de mogelijkheid houden om te hacken via zerodays. Zeker als zij stuiten op zerodays in software die vooral door criminelen gebruikt wordt of software dat alleen zit in militaire systemen van niet-bevriende landen, dan moeten zij de mogelijkheid hebben om dergelijke zerodays open te houden voor offensieve doeleinden. Dit betekent echter niet dat de overheid ook consumentenauto's moet kunnen hacken. Het veiligheids-risico dat gepaard gaat met het openhouden van dergelijke zerodays is simpelweg te groot. Andere actoren kunnen immers dezelfde zeroday vinden en gebruiken om auto's te hacken en daarmee de fysieke veiligheid van miljoenen gezinnen op het spel zetten.

Initiatiefnemer is van mening dat een goede belangenafweging een betere manier is om recht te doen aan de analyse dat cyberveiligheid steeds belangrijker wordt als gevolg van de vergaande digitalisering dan een zwart/wit stelling dat een overheid überhaupt geen zerodays zou mogen gebruiken om te hacken. Dit laat namelijk geen ruimte voor de noodzakelijke nuance dat opsporings- en inlichtingendiensten effectief moeten kunnen opereren in een digitale wereld, zonder daarmee belangen op het gebied van economie, veiligheid en vrijheid onevenredig hard te raken. Uitgangspunt daarbij is dat de (cyber)veiligheid van onze samenleving voorop staat, maar dat in bepaalde afgekaderde uitzonderingen opsporings- en inlichtingendiensten de mogelijkheid moeten hebben om zerodays te gebruiken om inlichtingen te verzamelen of verdachten op te sporen.

3. Hoofdlijnen van het wetsvoorstel

3.1 Uitgangspunten

Initiatiefnemer is van mening dat het Nederlandse Zeroday Afwegings-Proces (ZAP) gebaseerd moet zijn op een aantal uitgangspunten:
– Alle door de overheid verworven (gevonden of gekochte) zerodays moeten onderworpen worden aan het ZAP en openbaar gemaakt kunnen worden of aan de maker van de software gemeld kunnen worden.

– Het proces is ingericht met een «bias towards disclosure». Het (cyber)veiligheidsbelang staat voorop, het openhouden van zerodays om te hacken is een uitzondering. Of zoals het huidige afwegingskader voor de AIVD en MIVD zegt: «melden, tenzij...».
– Tegelijkertijd is de realiteit dat de overheid afhankelijk is van door bedrijven ontwikkelde hacksoftware. De zerodays die door deze hacksoftware gebruikt worden om apparaten of software binnen te dringen kunnen niet gemeld worden. De aankoop van hacksoftware moet dus zoveel mogelijk vermeden worden (nee, tenzij). Daarom wordt de inkoop van hacksoftware aan eisen onderworpen en moet het goedgekeurd worden door het afwegingsorgaan.
– Zerodays worden nooit permanent bewaard; er moet altijd een periodieke heroverweging plaatsvinden.
– Alle relevante belangen bij het openhouden, dan wel melden, van zerodays (opsporing, inlichtingen, economie, privacy, cyberveiligheid, etc.) worden vertegenwoordigd in het afwegingsorgaan.
– Het ZAP wordt een wettelijke geborgd proces.
– Er is onafhankelijk toezicht op het ZAP en er wordt jaarlijks gerapporteerd over gemaakte beslissingen.

3.1.1 Alle zerodays worden onderworpen aan het ZAP
Voor een goed functionerend ZAP is het belangrijk dat alle door de overheid verworven zerodays het afwegingsproces doorlopen. De overheid kan zerodays «verwerven» door zelf zerodays te vinden, door zerodays aan te kopen of doordat derden – vaak ethisch hackers – zerodays melden aan de overheid.

Als zerodays niet onderworpen worden aan het afwegingsproces vindt er geen, of een te beperkte, afweging plaats tussen aan de ene kant het operationeel belang en aan de andere kant de mogelijke schadelijke gevolgen van het openlaten van de zeroday op het gebied van economie, (cyber)veiligheid of burgerrechten. De CTIVD wees in rapport 53 tevens op deze problematiek.

Bovendien bestaat het risico dat de overheid zichzelf in de voet schiet. Belangen van de ene overheidsorganisatie (bijvoorbeeld de politie) kunnen de belangen van andere overheidsorganisaties, zoals de AIVD en MIVD, ondermijnen. Op dat moment vindt er namelijk geen afweging plaats tussen het belang van het openhouden van een zeroday en het belang van het dichten van een zeroday. Zo is het mogelijk dat een zeroday die opengehouden wordt vanwege de opsporingsbelangen van de politie belangen van de AIVD of MIVD op het gebied van nationale veiligheid, economie of vitale infrastructuur schaadt.

Zerodays die door derden aan de overheid worden gemeld met de intentie of verwachting dat de kwetsbaarheid wordt gedicht, bijvoorbeeld aan het NCSC of via Responsible Disclosure procedures, worden altijd aan de maker van de software gemeld.

3.1.2 Het proces is ingericht met een «bias towards disclosure»
Nederland is een van de meest gedigitaliseerde landen ter wereld. We hebben het grootste internet knooppunt ter wereld, we behoren tot de top 10 landen met het snelste internet en Nederland heeft het op 1 na hoogste percentage internetgebruikers (82,9%). We hebben veel grote bedrijven en startups die actief zijn in de «digitale economie», zoals ASML, Philips, Adyen en Elastic, en Nederlanders gebruiken snel nieuwe internet diensten. Tot slot heeft Nederland bovendien veel internationale instituties, waardoor het een aantrekkelijk doelwit is voor statelijke actoren.

Bovendien sluiten we steeds meer aan op het internet. Niet alleen computers, tablets en smartphones zijn aangesloten op het internet, maar ook hele fabrieken, openbaar vervoerssystemen, watermanagement systemen, sluizen, elektriciteitsnetwerken, zorgapparaten, webcams, enzovoorts. Dat biedt kansen, maar vergroot ook het risico op verstoring of manipulatie van deze apparaten. Wat er kan gebeuren hebben we gezien bij cyberaanvallen als Wannacry, Stuxnet en NotPetya. Tientallen miljoenen schade in de haven van Rotterdam, openbaar vervoer dat platgelegd wordt, zorginstellingen die kankerpatiënten niet kunnen helpen, storingen in elektriciteitsnetwerken met dodelijke gevolgen, mensen en bedrijven die geen betalingen meer kunnen doen.

Zeker voor een klein land als Nederland, dat heel erg afhankelijk is van handel en internationale samenwerking is het belangrijk om de risico's van de vergaande digitalisering van onze samenleving op waarde te schatten. Dat betekent dat Nederland veel aandacht moet besteden aan goede cybersecurity. Dit wetsvoorstel is een belangrijk onderdeel in een bredere cybersecurity agenda met aandacht op het gebied van bewustwording van cyberhygiëne en het menselijke aspect van cybersecurity, het delen van informatie (via het NCSC) en het stimuleren van veiligere apparaten.

Initiatiefnemer is van mening dat, door de vergaande digitalisering van de Nederlandse economie en samenleving en de risico's en kwetsbaarheden op het gebied van cyberveiligheid die daarmee gepaard gaan, het in het belang is van Nederland om het Zeroday AfwegingsProces in te richten met een «bias towards disclosure», oftewel een voorkeur voor het openbaar maken van zerodays of het melden van zerodays bij de maker van de software. Zo kunnen potentieel gevaarlijke zerodays gedicht worden en kunnen criminelen en statelijke actoren deze zerodays niet meer gebruiken voor cyberaanvallen op Nederlandse doelwitten. Dat vergroot uiteindelijk de cyberveiligheid van Nederland. Dit betekent concreet dat een zeroday openbaar wordt gemaakt of gemeld wordt aan de maker van de software als een meerderheid van de POC's in het afwegingsorgaan pleit voor bekendmaking.

De afwegingskaders in de VS en het VK zijn tevens ingericht met een «bias towards disclosure», daardoor sluit dit principe ook aan op de internationale praktijk van afwegingskaders van zerodays. Bovendien is het huidige afwegingskader van de inlichtingendiensten ingericht vanuit het uitgangspunt «melden, tenzij». Bovendien geldt voor Nederland dat wij nog kwetsbaarder zijn dan de VS en het VK voor cyberaanvallen en daardoor nog voorzichtiger moeten zijn met het openhouden van zerodays. Iniatiefnemer is van mening dat het in het belang is van een klein land als Nederland als wereldwijd de standaard wordt dat overheden zerodays in principe melden of openbaar maken in plaats van openhouden. Nederland kan met dit wetsvoorstel een rol spelen om die standaard te zetten.

3.1.3 Ook hacksoftware moet door het afwegingskader
Bij het inkopen van hacking tools die gebruik maken van zerodays ontstaat een ander dilemma. Bedrijven die hacking tools aanbieden schrijven kant-en-klare software (exploits) om apparaten of software binnen te dringen, vaak in de vorm van een makkelijk te gebruiken programma's die iedereen kan gebruiken. De koper van de hacking tool gebruikt dus feitelijk de zeroday om te kunnen hacken, maar krijgt geen specifieke kennis over de zeroday of is gehouden aan een geheimhoudingsverklaring. Kennis over de zeroday is immers het verdienmodel van het bedrijf. Veel van de informatie die nodig is om een goede afweging te maken over de zeroday is daarom niet voorhanden en het resultaat van

het afwegingsproces kan nooit het openbaar maken van de zeroday zijn. Toch is het wenselijk om eisen te stellen aan de inkoop van hacksoftware waarvan aannemelijk is dat het gebruik maakt van een zeroday[25] en om de afweging ook via het afwegingsorgaan te laten verlopen.

De hacksoftware-markt heeft namelijk een aantal zeer onwenselijke aspecten. Allereerst kopen dit soort bedrijven zerodays, inclusief kant en klare exploits, van (black hat) hackers. Deze hackers worden hierdoor gestimuleerd om gevonden zerodays niet aan de maker van de software (Apple, Google, Microsoft, etc.) te melden en daarmee mensen veilig te houden, maar aan dit soort bedrijven die het verwerken in hun hacksoftware. Dit kan namelijk gaan om bedragen van boven de miljoen euro per zeroday, meer dan bedrijven als Google en Apple bieden om zerodays te melden. Zo stimuleren deze bedrijven, en indirect ook overheden die klant zijn van deze bedrijven, een markt die als gevolg heeft dat mensen onveiliger zijn; evenals onze economie en onze samenleving.

Daarnaast leveren dit soort bedrijven vaak aan schimmige regimes die de hacksoftware inzetten tegen dissidenten, mensenrechtenactivisten en journalisten. Soms met mensenrechtenschendingen tot gevolg. Zakendoen met dit soort bedrijven is wat de initiatiefnemer betreft uitgesloten. Ook in het Regeerakkoord is afgesproken dat de AIVD leveranciers screent en dat geen hacksoftware gekocht wordt van bedrijven die zakendoen met «dubieuze regimes», oftewel regimes waartegen vanuit de EU of de VN repressieve sancties bestaan.

Tot slot is het op de lange termijn onwenselijk om voor onze offensieve cybercapaciteiten afhankelijk te zijn van dergelijke private aanbieders die aan tal van statelijke actoren dezelfde hacksoftware verkopen. Andere staten kunnen dezelfde hacksoftware inkopen en daarmee belangrijke kennis vergaren over onze offensieve capaciteiten. Landen kunnen de hacksoftware «reverse engineeren» en defensieve maatregelen treffen of in hun aankoopbeleid rekening houden met de mogelijkheden van commercieel beschikbare hacksoftware.

Deze negatieve aspecten moeten meegewogen worden bij een beslissing als overheid om dergelijke hacksoftware in te kopen. Initiatiefnemer meent dat het uitgangspunt moet zijn dat de Nederlandse overheid in principe geen hacksoftware koopt, tenzij er geen andere mogelijkheid is om zwaarwegende offensieve belangen te verdedigen. Het geniet de voorkeur dat de overheid zelf mogelijkheden ontwikkelt om offensieve cyberactiviteiten te kunnen ontplooien in plaats van afhankelijk te zijn van de inkoop van hacksoftware. Tegelijkertijd beseft initiatiefnemer zich dat de Nederlandse overheid op dit moment afhankelijk is van dergelijke hacksoftware en een verbod op het gebruik een te grote inbreuk zou doen op de offensieve cybercapaciteiten van Nederland. Toch is het belangrijk dat de Nederlandse overheid deze markt zo weinig mogelijk stimuleert en een aantal eisen stelt aan de inkoop van hacksoftware. Maar bovenal dat het principe «nee, tenzij...» ten opzichte van de inkoop van hacksoftware ingebed wordt in het overheidsbeleid.

Ook de inkoop van hacksoftware moet daarom door het afwegingsorgaan goedgekeurd worden. Als de inkoop van hacksoftware buiten het kader gehouden zou worden dan zou dat een incentive kunnen creëren om juist vaker hacksoftware in te kopen en zo buiten de controle van het afwegingskader om te kunnen werken. De uitkomst van de afweging over

[25] Het is onder andere aannemelijk dat hacksoftware gebruik maakt van zerodays als met de hacksoftware de laatste versie van een bepaald softwareproduct gehackt kan worden, zoals de laatste versie van iOS, Google Android of Windows.

het al dan niet inkopen van hacksoftware kan niet zijn dat de zeroday gemeld wordt aan de maker van de software, maar alleen of de software wel of niet gekocht wordt. Tegelijkertijd kan er wel een afweging gemaakt worden over het offensieve belang van de hacksoftware versus de schade op het gebied van algemene cyberveiligheid door deze markt te stimuleren en de eventuele beschikbaarheid van alternatieven. Dat is immers het principe van het afwegingskader: weegt het offensieve belang op tegen de negatieve defensieve gevolgen?

- Het afwegingsorgaan moet handelen vanuit het principe: «nee, tenzij...»
- Om afhankelijkheid op de lange termijn te voorkomen is het beter om zelf offensieve cybercapaciteiten te ontwikkelen, dan hacksoftware in te kopen.
- Dit betekent dat de organisatie die hacksoftware wil inkopen in het afwegingsorgaan moet aantonen dat het offensieve belang zwaarder weegt dan de negatieve (defensieve) gevolgen, zoals het stimuleren van deze schimmige markt, en dat er geen redelijke alternatieven zijn. Is de inkoop van hacksoftware onvermijdelijk om bepaalde offensieve belangen te behartigen?
- Voortaan geldt dat bedrijven waarvan de Nederlandse overheid hacksoftware inkoopt geen zaken mogen doen met landen die op EU of VN sanctielijsten staan.

3.1.4 Zerodays worden nooit permanent bewaard

De afweging over het al dan niet geheimhouden van zerodays moet onderworpen worden aan een periodieke heroverweging. Verschillende afwegingsfactoren kunnen door de tijd heen veranderen. Apparaten die kwetsbaar zijn voor hackaanvallen via een betreffende zeroday kunnen in maatschappelijk belang toenemen. De kans dat andere actoren de zeroday ook ontdekken kan na verloop van tijd toenemen. Zo zijn er nog tal van factoren die kunnen veranderen en daarmee de afweging om een zeroday geheim te houden kunnen veranderen. Daarom wordt als uitgangspunt opgenomen in de wet dat een besluit om een zeroday geheim te houden altijd gebonden is aan een heroverwegingstermijn van maximaal een jaar. Deze termijn is, onder andere, gebaseerd op het feit dat volgens beschikbare studies de «collission rate» van een zeroday al binnen 1 jaar op een significant niveau ligt. Er is een kans van 1 op 20 dat een zeroday binnen een jaar door een andere actor gevonden wordt. Daarnaast is een termijn van een jaar een redelijk termijn om te verwachten dat er ook op het gebied van andere afwegingsfactoren veranderingen te verwachten zijn. Bijvoorbeeld toename van het gebruik van de betreffende software waar de zeroday zich in bevind in onderdelen van de vitale infrastructuur. Maar er kan ook sprake zijn van een toegenomen economisch of privacy belang.

Daarnaast kan het afwegingsorgaan ertoe besluiten om een kortere heroverwegingstermijn te hanteren in het geval van zerodays waarvan men op kortere termijn verwacht dat er zich veranderingen in de afwegingsfactoren zullen voordoen.

3.1.5 Alle relevante belangen bij het openhouden, dan wel melden, van zerodays (opsporing, inlichtingen, economie, privacy, cyberveiligheid, etc.) worden vertegenwoordigd in het afwegingsorgaan

Er zijn veel verschillende belangen die geraakt worden door een beslissing om een zeroday open te houden, dan wel te melden of openbaar te maken. Concreet gaat het met name om: opsporings- en inlichtingen belangen enerzijds en belangen op het gebied van economie, (cyber)veiligheid, privacy en vrijheid anderzijds. Deze belangen worden vertegenwoordigd in het afwegingsorgaan door verschillende delen van

de overheid, zoals het Ministerie van Economische zaken, de Autoriteit Persoonsgegevens en het Ministerie van Infrastructuur en Waterstaat.

3.1.6 Het ZAP wordt een wettelijke geborgd proces
Om te borgen dat alle overheidsinstanties in Nederland zich aan het afwegingskader voor zerodays moeten houden is het van belang het proces wettelijk te borgen. Bovendien wordt Nederland daarmee het eerste land ter wereld met een wettelijk geborgd zeroday afwegingsproces. Daarmee kan Nederland binnen Europa en internationaal de standaard zetten voor zeroday afwegingsprocessen. Voor een klein en zeer gedigitaliseerd land als Nederland is dat van groot belang. De risico's van het openlaten van zerodays voor de veiligheid van onze vitale infrastructuur, onze economie en onze privacy zijn immers groot. Het ontwikkelen van internationale aandacht voor cybersecurity, inclusief een internationale standaard wat betreft een afwegingskader voor zerodays met een «bias towards disclosure», is daarmee in het Nederlands belang.

Daarnaast is het wettelijk borgen van een afwegingskader ook van belang om ervoor te zorgen dat er een zo zorgvuldig mogelijke afweging plaatsvindt waar alle verschillende overheidsorganen bij betrokken zijn die de bevoegdheid hebben om te hacken of geraakt kunnen worden door beslissingen om zerodays open te houden. Uit consultaties met verschillende stakeholders uit het bedrijfsleven, vitale infrastructuur en wetenschap is naar voren gekomen dat het cruciaal is voor het slagen van een goed afwegingskader voor zerodays dat de verschillende overheidsorganen die deelnemen aan het afwegingsorgaan ook daadwerkelijk informatie delen om tot een goede afweging te komen. Daarom is het belangrijk dat het afwegingskader een wettelijke verplichting wordt, waardoor de verschillende partijen gedwongen worden om informatie te delen. Daarnaast is het belangrijk dat het «clearance»-niveau van de POCs in het afwegingsorgaan van het hoogste niveau is zodat er vertrouwen is dat gedeelde informatie niet lekt of anderszins doorsijpelt binnen de organisaties die de verschillende POC's, bijvoorbeeld van het Ministerie van economische zaken of het Ministerie van infrastructuur en milieu, vertegenwoordigen.

3.1.7 Er is onafhankelijk toezicht op het ZAP en er wordt jaarlijks gerapporteerd over gemaakte beslissingen
Het openhouden van zerodays heeft een potentieel groot effect op de (online) veiligheid van mensen, op de economie, op burgerlijke vrijheden en onze vitale infrastructuur. Initiatiefnemer is daarom van mening dat het van groot belang is dat er goed, onafhankelijk toezicht wordt gehouden op het Zeroday AfwegingsProces om de goede werking van het afwegingsproces te borgen.

Daarom wordt de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) belast met het toezicht op het goed functioneren van het ZAP. De CTIVD publiceert jaarlijks informatie over het afwegingskader met in ieder geval:
– Een analyse over het goed functioneren van het kader;
– Het aantal geheimgehouden zerodays en het aantal vrijgegeven zerodays;
– De gemiddelde periode van geheimhouding.

3.1.8 Organisatorische inrichting
Het afwegingsproces zal bestaan uit een afwegingsorgaan waarin verschillende overheidsinstanties in vertegenwoordigd zijn die verschillende maatschappelijke belangen vertegenwoordigen. Daarnaast wordt er een adviserend orgaan ingesteld met vertegenwoordigers van private

partijen uit de vitale infrastructuur dat aanvullende, en voor de afweging relevante, informatie kan aanleveren over de vitale infrastructuur.

Het afwegingsorgaan wordt ondergebracht bij het Nationaal Cyber Security Centrum (NCSC). Het NCSC heeft als doel het bevorderen van de cyberveiligheid in Nederland door het vergroten van de weerbaarheid in het digitale domein. In de praktijk betekent dat onder andere het delen van informatie over cyberaanvallen tussen verschillende partijen binnen de vitale infrastructuur. Ook is het NCSC een aanspreekpunt voor ethisch hackers die kwetsbaarheden vinden en willen melden. Deze positie en ervaring van het NCSC maakt het bij uitstek een goede plek om het afwegingsorgaan onder te brengen.

De volgende overheidsinstanties zijn vertegenwoordigd in het afwegingsorgaan en wijzen een «Point of Contact» (PoC) aan die zitting neemt in het afwegingsorgaan:
– Nationaal Cyber Security Centrum (NCSC)
– AIVD/MIVD
– Politie & OM
– Het Ministerie van Defensie
– Het Ministerie van Economische Zaken & Klimaat (EZK)
– Het Ministerie van Infrastructuur & Waterstaat (I&W)
– De Autoriteit Persoonsgegevens (AP)

Daarmee is er een goede balans tussen belangen die gebaad zijn bij het openhouden van zerodays en belangen die gebaad zijn bij het dichten van zerodays. Daarnaast is het belangrijk dat het afwegingsorgaan over voldoende informatie beschikt over de vitale infrastructuur. In het cybersecuritybeeld 2019 waarschuwt de NCTV voor maatschappelijke ontwrichting als gevolg van digitale kwetsbaarheid van onze vitale infrastructuur. De NCTV zegt het volgende hierover om het belang van goede cyberveiligheid te onderstrepen: «*Vrijwel alle vitale processen en diensten zijn volledig afhankelijk van ict. Door het bijna volledig verdwijnen van analoge alternatieven en de afwezigheid van terugvalopties is de afhankelijkheid van gedigitaliseerde processen en systemen zo groot geworden dat aantasting hiervan kan leiden tot maatschappijontwrichtende schade. Vitale processen zijn in hoge mate afhankelijk van elektriciteitsvoorziening en datacommunicatie. Uitval en verstoring hiervan hebben zeer snel, binnen enkele uren, impact op een aantal vitale processen. Vanwege de omvang van de dreiging en het achterblijven van de weerbaarheid, ontstaan risico's voor de nationale veiligheid.*»[26] De Rekenkamer heeft daarnaast onderzoek gedaan naar de digitale weerbaarheid van onze vitale waterinfrastructuur en heeft cruciale tekortkomingen geconstateerd.

Daarom wordt er een adviesorgaan ingesteld, bestaande uit partijen uit de vitale infrastructuur, dat ervoor moet zorgen dat er voldoende relevante informatie beschikbaar is om zo goed mogelijke afwegingen te maken over het al dan niet openhouden van een voorliggende zeroday.
Het afwegingsorgaan kan tot drie verschillende besluiten komen:
1. De zeroday mag, voor een bepaalde termijn, geheim worden gehouden;
2. De zeroday mag, voor een bepaalde termijn, geheim gehouden worden, maar tegelijkertijd wordt informatie verstrekt aan belangrijke stakeholders, zoals partijen in de vitale infrastructuur, in verband met mogelijke mitigerende maatregelen;
3. De zeroday moet gemeld worden aan de maker van de software (of openbaar gemaakt moet worden).

[26] https://www.nctv.nl/binaries/CSBN2019_online_tcm31–392768.pdf

Het afwegingsorgaan moet per meerderheid beslissen dat de zeroday geheim gehouden moet worden, in alle andere gevallen moet de zeroday gemeld of openbaar gemaakt worden. Hiermee wordt het principe «bias towards disclosure» ingebakken in het afwegingsproces.

De enige uitzondering op het niet openbaar maken van de zeroday is als de zeroday gevonden wordt in closed-source software waarvan bekend is dat het niet langer ondersteund wordt door de maker van de software. In dat geval kan besloten worden om de zeroday geheim te houden in het belang van de algemene cyberveiligheid.

Wat betreft de afweging over het al dan niet mogen inkopen van hacksoftware kan het afwegingsorgaan tot dezelfde drie besluiten komen:
1. De hacksoftware mag ingekocht worden;
2. De hacksoftware mag ingekocht worden, maar gebruik ervan, inclusief relevante technische kennis moet gedeeld worden met belangrijke stakeholders, zoals partijen in de vitale infrastructuur, over mitigerende maatregelen;
3. De hacksoftware mag niet ingekocht worden.

Voordat een zeroday wordt beoordeeld in het afwegingsorgaan volgt eerst beoordeling door een technisch orgaan dat een eerste schifting maakt tussen open te maken en geheim te houden zerodays. Alleen zerodays waarvan het technisch orgaan zegt dat die geheim gehouden moeten worden gaan door naar het afwegingsorgaan om een belangenafweging te maken. Hiermee kan werklast tot een minimum gehouden worden en beslist het afwegingsorgaan alleen over zerodays waar een belangenafweging over gemaakt moet worden.

3.1.9 Afwegingsfactoren

Naast het vastleggen van de *governance* van het afwegingsproces acht de initiatiefnemer het ook van belang om de factoren vast te leggen die in ieder geval bij de afweging meegenomen moeten worden. De documentatie over het afwegingsproces in de VS[27] en het VK[28] noemt enkele belangrijke afwegingsfactoren, hetzelfde geldt voor het bestaande afwegingskader van de AIVD en MIVD[29] en voor Kamerbrieven over de hackbevoegdheid van de Politie, Marechaussee en FIOD.[30]

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. De categorieën van afwegingsfactoren zijn:
– Overwegingen met betrekking tot de operationele(/offensieve) noodzaak van de zeroday;
– Overwegingen met betrekking tot de negatieve (/defensieve) gevolgen voor de cyberveiligheid van de zeroday;
– Overwegingen met betrekking tot alternatieve belangen aangaande het gebruik van de zeroday, zoals economische, maatschappelijke, (cyber)veiligheids- of grondwettelijke belangen;
– Technische overwegingen aangaande het gebruik van de zeroday.

Binnen deze categorieën van afwegingsfactoren kunnen vragen aan bod komen als:

---

[27] https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF

[28] https://www.gchq.gov.uk/features/equities-process

[29] https://www.aivd.nl/binaries/aivd_nl/documenten/publicaties/2018/05/01/beleid-omgang-met-onbekende-kwetsbaarheden/Beleid+AIVD+en+MIVD+over+onbekende+kwetsbaarheden.pdf

[30] https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2018/05/04/tk-schriftelijk-overleg-over-ontwerpbesluit-onderzoek-in-een-geautomatiseerd-werk/tk-schriftelijk-overleg-over-ontwerpbesluit-onderzoek-in-een-geautomatiseerd-werk.pdf

– Hoe groot is de toegevoegde waarde van het gebruiken van de zeroday voor inlichtingen of opsporingsbelangen?
– Zijn er alternatieven beschikbaar voor het gebruik van de betreffende zeroday?
– In hoeveel (software) producten/apparaten zit de zeroday? Hoeveel gebruikers kunnen worden getroffen?
– Hoe groot is de kans dat andere actoren dezelfde zeroday kunnen ontdekken (de collision rate) en gebruiken?
– Bevindt de zeroday zich in producten/apparaten aanwezig in de vitale infrastructuur?
– Welke economische gevolgen heeft het openlaten van de zeroday? Bevindt de zeroday zich in apparaten/producten van Nederlandse, dan wel Europese, bedrijven?
– Wat zijn de mogelijke privacy gevolgen van het openlaten van de zeroday?
– Wat is de impact en «zwaarte» van de zeroday? Biedt de zeroday bijvoorbeeld de mogelijkheid tot externe toegang zonder «user interaction»?
– In wat voor apparaten/producten bevindt de zeroday zich? Betreft het bijvoorbeeld veelgebruikte consumentensoftware of software dat uitsluitend door criminelen/vijandige militaire wordt gebruikt?

4. Financiële paragraaf

In het initiatief wetsvoorstel zit een aantal aspecten die een beperkte financiële consequentie hebben. Allereerst wordt het afwegingsorgaan ondergebracht bij het NCSC, en moeten de leden van het afwegingsorgaan een *Point of Contact* aanwijzen. Hiervoor moet binnen deze organisaties budget vrijgemaakt worden. De verwachting is echter dat dit qua inzet per organisatie een beperkt financieel beslag zal leggen op deze organisaties. Daarnaast wordt het toezicht ondergebracht bij het CTIVD. Deze toezichthouder had al de taak om het afwegingskader van de diensten te controleren, dit toezicht wordt in feite verplaatst naar het afwegingsorgaan en zal naar verwachting een beperkte invloed hebben op de werklast van de CTIVD.

5. Consultatie en adviezen

Initiatiefnemer heeft een drietal rondetafelsessies georganiseerd met verschillende stakeholders uit het bedrijfsleven, de wetenschap, de vitale infrastructuur en NGOs. Het belang van een wettelijk geborgd afwegingskader werd breed gedeeld en gezien als belangrijk element in een bredere aanpak op het gebied van cybersecurity.

Daarnaast is een aantal thema's breed aan de orde gekomen tijdens de sessies. Allereerst de *governance*. Onder de geconsulteerde personen en organisaties leefde breed de voorkeur om het afwegingsorgaan onder te brengen bij het NCSC als organisatie dat het bevorderen van cybersecurity als voornaamste doel heeft. Hieraan is in het initiatiefvoorstel tegemoet gekomen. Daarnaast werd de noodzaak van goed toezicht op het proces breed gedeeld. Hieraan is tegemoet gekomen door de CTIVD verantwoordelijk te maken voor het toezicht op het proces.

Ook is tijdens de gesprekken het dilemma wat betreft de omgang met hacksoftware uitgebreid besproken. Tijdens de gesprekken werd duidelijk dat het buiten beschouwing laten van dit dilemma in deze initiatiefwet geen optie was omdat in dat geval er sprake zou kunnen zijn van een perverse prikkel om juist meer gebruik te maken van hacksoftware. Daarom is besloten om ook de aankoop van hacksoftware via het afwegingsorgaan te laten verlopen.

Tot slot hebben meerdere stakeholders hun zorgen geuit dat onderdelen van de overheid die offensieve cybercapaciteiten ontwikkelen het afwegingsproces zouden proberen te ontwijken. Dit is een reële zorg die initiatiefnemer deelt en een van de belangrijkste beweegredenen was om dit afwegingsproces middels een wettelijke verplichting vorm te geven. Doorgaans neigen overheden zich te houden aan de wet. Daarnaast is gekozen voor een sterke, bestaande toezichthouder die het goed functioneren van het afwegingsproces moet controleren.

II. ARTIKELSGEWIJS

In dit deel worden de artikelen toegelicht die een nadere uitleg behoeven.

Artikel 1

Dit artikel definieert de in dit wetsvoorstel gebruikte begrip van onbekende kwetsbaarheid.
Met een onbekende kwetsbaarheid wordt in dit wetsvoorstel een zeroday bedoeld. Kenmerkend van een zeroday is dat het moet gaan om een kwetsbaarheid die nog onbekend is bij de producent of de leverancier van het geautomatiseerde werk waar de kwetsbaarheid in is aangetroffen. Omdat het in de praktijk lastig kan zijn om met zekerheid vast te stellen of een zeroday daadwerkelijk nog niet bekend is bij een producent of leverancier, is er in deze definitie voor gekozen dat het aannemelijk moet zijn of verondersteld kan worden dat een zeroday nog niet bekend is bij de producent of leverancier. Om vast te stellen of hier sprake van is kan bijvoorbeeld worden afgegaan op gedragingen van de producent of leverancier of de aard van de kwetsbaarheid zelf.

Artikel 2

In artikel 2, eerste lid, is de hoofdregel neergelegd met betrekking tot de bekendmaking van een zeroday. In principe moet een zeroday altijd aan de producent of leverancier van het geautomatiseerde werk waarin de zeroday is ontdekt bekend worden gemaakt. Het tweede lid regelt vervolgens dat de Ministers die het aangaat (ofwel het afwegingsorgaan zoals toegelicht in het algemeen deel van deze toelichting) kunnen besluiten om een zeroday niet bekend te maken of alleen aan betrokkenen die vitale infrastructuur beheren. Hierbij worden een aantal belangen overwogen. Niet is bedoeld dat dit redenen kunnen zijn om de zeroday geheim te houden- economische belangen of veiligheidsbelangen kunnen immers juist nopen tot het zo spoedig mogelijk dichten van de bewuste zeroday. Dit is in het algemeen deel toegelicht. Deze opsomming is voorts niet limitatief, ook andere belangen die niet genoemd zijn in deze opsomming kunnen worden meegewogen.

Voor het besluit wordt genomen, wordt vanzelfsprekend ambtelijk geadviseerd, maar het derde lid legt wettelijk vast dat ook vertegenwoordigers van betrokkenen die vitale infrastructuur beheren hierin adviseren. Er wordt hier bewust gesproken van vertegenwoordigers, omdat anders de betrokkenen zelf direct de kennis zouden verwerven van de zeroday. Daar dit echter een expliciet besluit vergt, wordt dit wenselijk geacht. Het is evident dat het geheel van overwegingen alsmede de kennis van en over de zeroday als zeer vertrouwelijk wordt gerubriceerd.

Als wordt besloten een zeroday niet bekend te maken aan de producent of leverancier of aan betrokkenen die vitale infrastructuur beheren, dient uiterlijk na een jaar een heroverweging plaats te vinden. Dit is geregeld in het vierde lid.

Het vijfde lid geeft ten slotte de grondslag om een en ander conform het algemeen deel van de toelichting in te richten bij AmvB.

Artikel 3

In het eerste lid wordt geregeld dat de aankoop van een technisch hulpmiddel om binnen te dringen in een geautomatiseerd werk instemming behoeft indien aannemelijk is dat dit technisch hulpmiddel is gebaseerd op een zeroday. In het tweede lid wordt een grondslag gegeven om bij AMvB te regelen waaraan een dergelijke aankoop moet voldoen.

Artikel 4

Dit artikel regelt een voorhang op de AMvB's die conform deze wet moeten worden vastgesteld.

Artikel 5

Middels dit artikel wordt het toezicht op deze wet toegevoegd aan de taken van CTIVD. Dit is in het algemeen deel nader toegelicht.

Artikel 6

Een besluit over de bekendmaking van een zeroday of de aankoop van een technisch hulpmiddel zijn te kwalificeren als besluit in de zin van de Awb. Dit artikel regelt dat geen bezwaar en beroep mogelijk is bij de bestuursrechter over deze besluiten.

Artikel 7

Dit artikel regelt een evaluatie van deze wet na vijf jaar. Na die termijn is naar verwachting van de initiatiefnemer een goed beeld te verkrijgen van de werking van het afwegingskader.

Verhoeven