Bijdrage: Jan Middendorp, Tweede Kamerlid VVD

Datum: 18 juni 2020,

Activiteit: plenair debat, initiatiefwetsvoorstel Wet Zerodays Afwegingsproces

Bewindspersoon: Minister van Binnenlandse Zaken Ollongren

Er kunnen fouten in software zitten die niet bekend zijn bij de makers daarvan. Deze voor de cybersecurity industrie “onbekende kwetsbaarheden” ook wel “Zerodays” genoemd kunnen, als die door kwaadwillende ontdekt worden, gebruikt worden om in te breken in digitale netwerken en gebruikt worden om andere soorten cyberaanvallen mee uit te voeren.

Dat dit misbruik van digitale kwetsbaarheden wordt tegengegaan is van groot belang:

Want Voorzitter

Cyberaanvallen kunnen onze nationale veiligheid, economie en burgerrechten schaden. Mijn eerste interventie in dit parlement ging over de wereldwijde cyberaanval met de gijzelsoftware WannaCry. December vorig jaar hadden we Citrix, nu is door de coronacrisis iedereen digitaal en zijn de potentiele ontwrichtende effecten van cyberaanvallen nog eens enorm toegenomen. Cyberaanvallen - die regelmatig van vijandelijke staten komen - kunnen havens platleggen, verkiezingen verstoren en banken digitaal beroven. De gevolgen kunnen kortom enorm zijn.

In het Cyber Security Beeld Nederland is al jaren te lezen dat de hoeveelheid en geavanceerdheid van de aanvallen toeneemt. Dit alles betekent Voorzitter dat Nederland een offensieve en gedecideerde strategie om cybercriminaliteit, cyberspionage, cyber sabotage, te bestrijden moeten hebben. En daar gaat dit debat over Voorzitter.

Een door de opsporings-/inlichtingendiensten ontdekte kwetsbaarheid in soft of hardware moet in principe gemeld worden bij de leverancier zodat het risico van misbruik door kwaadwillende wordt weggenomen. In het kader van de nationale veiligheid kan het echter nodig zijn zon ontdekte kwetsbaarheid juist niet te melden. Dan kan een dienst de kwetsbaarheid zelf gebruiken Nederland cyber veilig te houden door terroristen te hacken of pogingen ons te hacken van buitenlandse spionagediensten tegen onze belangen te stoppen. De vraag wat er moet gebeuren als een nieuwe kwetsbaarheid ontdekt wordt, is dus een terechte.

En dat Voorzitter is ook de vraag die voorligt in de voorstellen die we vandaag bespreken. Voor de VVD staat bij het beantwoorden van die vraag voorop dat als het vanuit overwegingen in het belang van de nationale veiligheid nodig is de AIVD / MIVD en opsporingsdiensten, binnen hun mandaat kunnen blijven hacken.

Gezien het belang ervan – zoals ik zojuist beschreef - is het in de eerste plaats zeer te prijzen dat collega Verhoeven veel tijd en energie in dit initiatiefwetsvoorstel heeft gestoken.

Maar Voorzitter Ik heb veel vragen bij de nieuwe procedure, het overkoepelend afwegingskader en afwegingsorgaan dat hier wordt voorgesteld. Is de oplossing het afwegingsproces volledig uniform te maken en om een nieuw en breed afwegingsorgaan vooraf te laten bepalen of een zeroday wel of niet gebruikt mag worden door onze diensten of defensie?

Het afwegingsorgaan, dat moet bepalen of ontdekte zerodays geheim kunnen worden gehouden of niet, dat in het wetsvoorstel beschreven wordt bestaat uit NCSC, AIVD/MIVD, politie, OM, FIOD,

Defensie, EZK, I en W, AP. Dat klinkt als een grote club, zeker omdat alle zerodays waarvan wordt overwogen om ze geheim te houden eerst door dit orgaan beoordeeld moeten worden. Laten we de praktijk van inlichtingen operaties niet uit het oog verliezen. Het zal toch zo zijn Voorzitter dat een zeroday soms afgewogen moet worden in het kader van een gecompartimenteerde inlichtingen operatie? Een zeroday wordt dan afgewogen door de diensten tegenover de kennis over hun targets; dat is gecompartimenteerde informatie die onmogelijk evenwichtig afgewogen kan worden door een breed afwegingsorgaan. Wel kan op de afweging controle plaatsvinden door TIB en/of CTIVD. Doet het voorstel dus recht aan de aard van het opsporings- en inlichtingenwerk dat vaak gediend is bij geheimhouding en slagkracht?

Daarbij houdt Verhoeven het voor mogelijk dat het afwegingsorgaan een inlichtingendienst zou verplichten tot het melden van een zeroday, terwijl deze dienst het daar niet mee eens is. Dat mag volgens de VVD fractie niet de uitkomst zijn. Is het lid Verhoeven het met mij eens dat inlichtingendiensten binnen hun mandaat efficiënt moeten kunnen blijven handelen om cyberdreigingen te voorkomen?

De Raad van State stelt dat het bestaande kader op hoofdlijnen al uniform is en door sectorspecifieke uitwerkingen al in voldoende mate voorziet van normstelling. De discussie daarover lezende tussen RvS en initiatiefnemer wekt de indruk dat de initiatiefnemer dit grote verschil van inzicht verklaart door een misverstand? Maar is hier niet gewoon sprake van een inhoudelijk verschil van inzicht? Ik vraag ook aan de minister hoe zij de kritiek van de raad van state beoordeeld.

We moeten natuurlijk voorkomen dat diensten tegen elkaar inwerken maar er zijn andere stappen die minder ingrijpend zijn dan de voorliggende voorstellen. Om opsporingsdiensten en inlichtingendiensten meer te laten samenwerken is niet ook een one size fits all kader nodig. Ik verwijs daarbij naar deze week aangekondigde stap om inlichtingendiensten, justitie en anti-terrorisme organisaties fysiek met elkaar te laten samenwerken om beter informatie over dreigingen op internet met elkaar te delen in een Cyber Intel/Info Cel (CIIC). Voorzitter

Ten tweede wordt op dit moment de Wet op de inlichtingendiensten geëvalueerd door de commissie Jones. Kan die commissie ook mogelijke verbeteringen aan het bestaande kader voor zerodays in die evaluatie mee nemen? Dezelfde vraag aan de minister.

Voorzitter ik sluit af: De antwoorden van Verhoeven op de vragen van de VVD fractie en het regeringsstandpunt zijn belangrijk omdat het hier over een zeer belangrijke kwestie gaat. Cyber spionage en cybercriminaliteit zijn cruciaal voor de welvaart en veiligheid van de Nederlander. Het one size fits all uniforme kader met één toetsingsorgaan dat vooraf beslist lijkt echter niet de oplossing.