Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2012–2013

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 253

VERSLAG VAN EEN SCHRIFTELIJK OVERLEG

Vastgesteld 24 september 2012

De vaste commissie voor Veiligheid en Justitie heeft een aantal vragen voorgelegd aan de minister van Veiligheid en Justitie over de brief inzake het Dorifelvirus bij (overheids)instellingen (Kamerstuk 26 643, nr. 251). Bij brief van 21 september 2012
heeft de minister deze vragen beantwoord. Vragen en antwoorden zijn hierna afgedrukt.

De fungerend voorzitter van de commissie,
De Roon

Adjunct-griffier van de commissie,
Hessing-Puts

kst-26643-253
ISSN 0921 - 7371
's-Gravenhage 2012

Inhoudsopgave

I. Vragen en opmerkingen vanuit de fracties

1. Vragen en opmerkingen vanuit de VVD-fractie

De leden van de VVD-fractie hebben met belangstelling kennisgenomen van de brief van de minister van Veiligheid en Justitie (hierna: de minister) over het Dorifelvirus (Kamerstuk 26 643, nr. 251). Zij hebben hierover enige vragen. Doet de minister al het nodige om het Dorifelvirus te bestrijden en wat doet hij om de kans op een toekomstig uitbreken van een virus, vergelijkbaar met het Dorifelvirus, tot een minimum te beperken?

Deze leden merken op dat in de onderhavige brief staat dat er geen aanwijzingen zijn dat persoonsgegevens van burgers zijn gelekt. Is hier nu meer zekerheid over? Kan de minister inderdaad garanderen dat er geen persoonsgegevens zijn gelekt? Het virus lijkt zich pas te manifesteren bij het opstarten van systemen. Het is dus mogelijk dat het virus in de komende weken, als mensen terugkomen van vakantie, weer de kop zal opsteken. Wat is de inzet van de minister om een eventuele tweede uitbraak van het Dorifelvirus voor te zijn? Kan de minister tevens nader ingaan op de samenwerking met private partijen en gemeenten?

De aan het woord zijnde leden merken op dat de minister aangeeft dat hij nieuwe wetgeving wil introduceren voor ruimere strafrechtelijke opsporingsbevoegdheden op het internet. Doel hiervan is om te voldoen aan de gesignaleerde behoeften van de diensten die zijn belast met opsporing en vervolging van cybercrime. Kan de minister allereerst concreet uiteenzetten wat de gesignaleerde behoeften zijn in relatie tot het Dorifelvirus en vergelijkbare virussen? Wat is de stand van zaken als het gaat om de aanpak van het onderliggende probleem, namelijk wereldwijde botnets?

2. Vragen en opmerkingen vanuit de PvdA-fractie

De leden van de PvdA-fractie hebben kennisgenomen van de brief van de minister inzake het Dorifelvirus. Zij vragen hoe kan het dat vooral infecties bij overheden aan het licht kwamen. Was de overheid een gericht doelwit dan wel extra kwetsbaar voor dit virus? Hoeveel infecties van computersystemen in het bedrijfsleven zijn er bekend en wat is de schade die de besmettingen hier veroorzaakt hebben? Heeft de minister de indruk dat bedrijven besmettingen open gedeeld hebben of zijn bedrijven terughoudend met het melden van inbreuken in hun computersysteem? Kan een ruimere meldplicht de aanpak van computercriminaliteit verbeteren? Betekent de infectie van computers bij overheidsinstellingen door het Dorifelvirus ook dat deze systemen al langer deel uitmaakten van het Citadel-botnet? Zo ja, hoe kan het dat deze eerdere infecties onopgemerkt zijn gebleven en hoe kunnen deze besmettingen alsnog opgeschoond worden om nieuwe activiteit van dit botnet te voorkomen? Tonen de latent

aanwezige botnet-besmettingen aan dat er tekortkomingen zijn in de beveiliging van overheidsnetwerken? Wat wordt er gedaan om deze beveiliging te verbeteren? Hoe effectief is de bestrijding van het Citadel-botnet door de toegang tot de bekende C&C-servers te blokkeren? Werken alle Internet Serviceproviders (ISP's) hier aan mee, of wordt er ook gebruik gemaakt van blokkering op een hoger niveau? Zijn alle servers bekend, of verandert het botnet snel van servers?

De leden van de PvdA-fractie vragen voorts of er al zicht is op de personen en organisaties die achter het Citadel-botnet en het Dorifelvirus zitten. Hoe verloopt hierin de samenwerking met buitenlandse opsporingsdiensten? Is er hierin behoefte aan meer en passender opsporingsmiddelen? Hoe verhoudt de diefstal van bankgegevens, die aan het licht kwam na de Dorifeluitbraak, zich tot het Citadel-botnet en Dorifel? Wat is het risico van deze inbreuk?

Ten slotte vragen deze leden hoe de bestrijding van met botnets geïnfecteerde computersystemen vordert bij particulieren? Worden deze computereigenaren door hun ISP's al geïnformeerd over geconstateerde besmettingen?

3. Vragen en opmerkingen vanuit de PVV-fractie

De leden van de PVV-fractie merken op dat in de onderhavige brief staat dat het Dorifelvirus zich in eerste instantie heeft verspreid via systemen die al met het Citadelvirus waren besmet. Waren het overheidscomputers die met dit Citadelvirus waren besmet? Zo ja, is er nader onderzoek gedaan naar eventuele andere virussen die deze (of andere) overheidscomputers tegelijkertijd besmet kunnen hebben? Waren de besmette computers op het moment van besmetting allemaal up-to-date waar het beveiligingsupdates, softwareversies en antivirusprogramma's betreft? Denkt u dat deze besmetting te voorkomen was geweest? Zo ja, op welke wijze en waarom is daar niet voor gekozen? Zo nee, waarom is dan slechts een beperkt aantal computers besmet?

De aan het woord zijnde leden vragen wat de minister gaat doen om in de toekomst te voorkomen dat virussen of wellicht cyberaanvallen (delen van) de overheid plat leggen. Ziet hij hierbij een grotere taak voor de Rijksoverheid of blijft het aan gemeenten zelf om individueel voorbereidingen te treffen?

Voornoemde leden vragen of er tijdens het onderzoeken en bestrijden van het Dorifelvirus gebleken is dat er momenteel strafrechtelijke opsporingsbevoegdheden werden gemist waarmee -indien deze er wel waren geweest- effectiever optreden mogelijk was geweest? De Zo ja, kunt u dan aangeven welke strafrechtelijke bevoegdheden dit zijn of diende deze passage in de brief alleen om een beeld van de ontwikkelingen aan de kant van het ministerie te schetsen? De leden van de PVV-fractie vragen dit gezien de aandacht die hier aan wordt besteed in de slotpassage van de onderhavige brief.

4. Vragen en opmerkingen vanuit de CDA-fractie

De leden van de CDA-fractie hebben naar aanleiding van de brief van de minister nog aan aantal vragen die hieronder aan bod zullen komen.

Deze leden vragen welke risico's er op dit moment nog zijn. Hoe kunnen bedrijven, overheidsinstellingen en burgers zich hiertegen wapenen, naast het uitvoeren van virusscans en het updaten van antivirusprogramma's? Heeft het Nationaal Cyber Security Centrum (NCSC) daarover informatie

beschikbaar? Zo ja, hoe wordt die gedeeld met overheidsinstellingen en met het bedrijfsleven?

Voornoemde leden vragen of het Dorifelvirus alleen in Nederland actief (is geweest), of dat dit virus ook buiten Nederland is verspreid?

De leden van de CDA-fractie brengen in herinnering dat de Landelijk Officier van Justitie Cybercrime enkele maanden geleden een oproep heeft gedaan. De Nederlandse recherche blijkt bij de opsporing van cybercriminelen soms de soevereiniteit van andere landen te schenden door buitenlandse computers te kraken. Dat is verboden, maar de Landelijk Officier verklaarde dat het in de opsporing van cybercrime soms onvermijdelijk is. Volgens hem schiet de wet tekort als het gaat om de online jacht op bijvoorbeeld pedofielen. Kan de minister hier nader op ingaan? Ook de Nationale Recherche heeft gepleit voor meer specifieke, juridische kaders voor online opsporing. Wat is de reactie hierop van de Minister? Heeft hij hierover contact met andere landen in de EU? Graag ontvangen deze leden een reactie op dit punt. Is de minister er gerust op dat in de opsporing de snelheid van de digitale ontwikkelingen bijgehouden kunnen worden? Kan hij voorts reageren op de stelling van de Nationale Recherche dat er behoefte is aan wetgeving die de snelheid van deze ontwikkelingen kan bijhouden, omdat er anders constant als opsporingsdiensten achteraan wordt gejaagd?

De aan het woord zijnde leden merken op dat de beveiligingsproblemen van vorig jaar bij de certificeringsonderneming DigiNotar al bekend waren ver voordat dit bedrijf aan de bel trok. Hoe lang speelde het probleem met het Dorifelvirus al voordat het in het nieuws kwam? Zijn alle betrokken (publieke en private) partijen voldoende op de hoogte over waar zij terecht kunnen met probleemmeldingen?

De leden van de CDA-fractie merken op dat het Dorifelvirus kennelijk al een tijd op de getroffen computersystemen aanwezig was voordat het actief werd. Richt het onderzoek van NCSC bij de door het Dorifelvirus getroffen bedrijven zich ook op eventuele andere, op dit moment nog verborgen virussen die op een later moment actief kunnen worden?

Deze leden vragen of het Dorifelvirus ook in andere landen is aangetroffen? Zo ja, hoe is de aanpak daar geweest en is er vanuit Nederland contact geweest met het desbetreffende land?

Voornoemde leden lezen in de brief dat het Dorifelvirus de inhoud van originele bestanden heeft gewijzigd waardoor deze bestanden niet meer leesbaar zijn. Hebben publieke of private instellingen te maken gehad met wijziging door het virus van bepaalde vitale bestanden? Kan de minister meer zeggen over de door het virus veroorzaakte schade?

Ten slotte merken deze leden op dat het Openbaar Ministerie is begonnen met een strafrechtelijk onderzoek naar de dader(s) achter het Dorifelvirus en het Citadel-botnet. Kan de minister informatie verstrekken over de vorderingen van dit onderzoek? Klopt het dat het virus zijn oorsprong heeft bij servers in Oekraïne? Welke verwachtingen heeft de minister van strafrechtelijke aanpak van de mogelijke dader(s)? Is hierover contact met de betreffende autoriteiten?

5. Vragen en opmerkingen vanuit de SP-fractie

De leden van de SP-fractie hebben met interesse kennisgenomen van de brief van de minister over het Dorifelvirus bij (overheids)instellingen. Graag complimenteren zij de minister voor het keurig op tijd versturen

van de brief. De leden vinden de reactie van de minister echter te summier. Graag stellen zij hier dan ook een aantal vragen over.

Het verbaast deze leden dat de brief geen duidelijkheid geeft over de zaken die burgers, bedrijven en instellingen op het moment van uitbreken van het virus dienen te doen dan wel moeten verwachten. De leden zijn van mening dat de minister iedere gelegenheid die zich voordoet om burgers, bedrijven en instellingen te kunnen informeren over de te nemen stappen met beide handen moet aanpakken. Op de website van het NCSC is een duidelijke handleiding te vinden over hoe om te gaan met het Dorifelvirus. Op welke wijze is aan burgers, bedrijven en instellingen gecommuniceerd dat deze handleiding beschikbaar is? Heeft de minister een persbericht uit laten gaan om aandacht te vragen voor de beschikbare handleiding op de website van het NCSC? Is de minister van mening dat bij een volgende cyberaanval van dergelijk formaat er op een actievere wijze gecommuniceerd dient te worden over de stappen die ondernomen dienen te worden?

Deze leden vragen voorts of de minister kan aangeven hoe het kan dat een vermoedelijk in april opgelopen besmetting pas in augustus aan het licht kwam. Wat zegt dit over de mogelijkheden van Nederlandse overheidsdiensten om besmettingen op overheidscomputers te ontdekken? Betekent dit dat de minister niet kan uitsluiten dat er ook op dit moment mogelijk geheel andere virussen en malware aanwezig zijn op computers binnen de overheid? Wat is de minister van plan te doen om hierover duidelijkheid te verkrijgen? Wanneer kan hij de Kamer daarover informeren? Wanneer verwacht de minister te kunnen zeggen dat het virus zich niet via de websites van de betroffen organisaties verder heeft verspreid en dat er geen persoonsgegevens van burgers zijn gelekt? Ook willen deze leden graag vernemen welke risico's er op dit moment nog zijn. Zijn er sinds 10 augustus 2012 nog nieuwe meldingen van besmetting bij het NCSC binnengekomen? Heeft het Dorifelvirus zich de afgelopen weken nog ergens gemanifesteerd? Zo ja, kunt u de Tweede Kamer op de hoogte brengen om hoeveel gevallen dit gaat?

Tot slot vragen deze leden wanneer zij de uitkomst van de inventarisatie naar noodzakelijke nieuwe strafrechtelijke opsporingsbevoegdheden op het internet kunnen verwachten, gelet op de urgentie van de problemen rond cyberaanvallen. Is de minister van mening dat de Nederlandse overheid voldoende kennis, capaciteit en middelen beschikbaar stelt om dergelijke aanvallen in de toekomst eerder op te merken en te voorkomen?

6. Vragen en opmerkingen vanuit de D66-fractie

De leden van de D66-fractie hebben naar aanleiding de brief van de minister een aantal vragen.

Deze leden vragen of de minister bekend is met het weblog van Rickey Gevers?[1] Is de minister van mening dat het hacken van de server door een veroordeelde hacker uiteindelijk ergere problemen heeft voorkomen nu door het hacken van de server de hacker er achter kwam dat het virus uiteindelijk bankaccounts zou aanvallen?

Kent de minister het radio-interview met de staatssecretaris van Veiligheid en Justitie, waarin hij aangaf dat het Dorifelvirus maar een komkommerverhaal was?[2] Hoe kan het dat het politieke bewustzijn ten aanzien van de gevaren van ICT na alle incidenten nog steeds lijkt te ontbreken?

[1] http://rickey-g.blogspot.nl/2012/08/more-details-of-dorifel-servers.html
[2] www.bnr.nl/?player=archief&fragment=20120810170200600

Deze leden vragen of het waar is dat het ministerie van OCW getroffen is door het Dorifelvirus? Zo ja, was dit op het netwerk van de Haagse Ring of op een apart netwerk van het ministerie. De leden van de D66-fractie merken op dat het Dorifelvirus is geïnstalleerd door computers die onderdeel waren van het Citadel-botnet. Hoe lang zijn de computers van het ministerie van OCW onderdeel geweest van dat botnetwerk? Is de minister mening dat de beveiliging van het ministerie van OCW adequaat was? Draait er op het interne netwerk van de Haagse Ring een zogenaamd Intrusion Detection System? Zo ja, is dit in eigen beheer en intern ontwikkeld of van een derde partij?

Voornoemde leden vragen of de minister van mening is dat bij de uitbraak van een virus dat gebruik maakt van «zero day» lekken, de overheid voldoende kennis in huis heeft om de uitbraak te neutraliseren en de digitale samenleving voldoende te ondersteunen om de impact minimaal te houden?

Deze leden vragen tot welke gegevens/systemen dit virus toegang heeft gehad. Wat is de maximale schade die het virus aan had kunnen richten vanuit de systemen waar het toegang toe had? Hoe beoordeelt u de «Incident response» van overheidsinstellingen? Welke verbeterpunten ziet u? Zijn alle systemen inmiddels schoon?

II. Reactie van de minister

De leden van de CDA fractie vragen of het NCSC informatie beschikbaar heeft gesteld over hoe overheidsinstellingen, bedrijven en burgers zich kunnen wapenen tegen de risico's en hoe deze informatie wordt gedeeld. Verder vragen deze leden of partijen voldoende op de hoogte zijn waar zij terecht kunnen met probleemmeldingen? De leden van de SP fractie refereren hier ook aan.

In antwoord op vragen van de SP en CDA-fractie kan ik aangeven dat er op actieve wijze gecommuniceerd is. Naar aanleiding van de eerste meldingen van het Dorifel virus heeft het NCSC op dezelfde dag een waarschuwing uitgestuurd binnen de overheid en richting de vitale sectoren. Daarnaast zijn ook de aangesloten partijen binnen het NCSC geïnformeerd. Toen verdere verspreiding zichtbaar werd is vervolgens ook actief via de media gecommuniceerd.
Getroffen partijen zijn gedurende het onderzoek actief geïnformeerd en het NCSC heeft op de website handelingsperspectieven gepubliceerd. Tevens is een lijst met veelgestelde vragen gepubliceerd. Uiteindelijk heeft dit onderzoek geresulteerd in de factsheet: «Verlos me van een botnet». Dit factsheet is actief verspreid en gepubliceerd op de website www.ncsc.nl. Tevens is in samenwerking met de industrie gewerkt aan het bieden van handelingperspectief voor getroffen organisaties. Tenslotte zijn alle communicatie-uitingen over het Dorifel-virus geplaatst op de website van het NCSC onder vermelding van dossier Dorifel-virus.

De leden van de VVD-fractie vragen of de Minister al het nodige doet om het Dorifelvirus te bestrijden en wat doet hij om de kans op een toekomstig uitbreken van een virus, vergelijkbaar met het Dorifelvirus te beperken. Tevens vragen de leden van de VVD-fractie Wat de inzet van de minister is om een eventuele tweede uitbraak van het Dorifelvirus voor te zijn. Ook de leden van de CDA-fractie stellen vragen over het onderzoek naar het Dorifel virus en of andere virussen hierdoor later actief kunnen worden. De VVD-fractie vraagt ook of de Minister nader in kan gaan op de samenwerking met private partijen en gemeenten. De PVDA-fractie vraagt zich in relatie tot samenwerking af of de Internet Service Providers (ISP's) meewerken.

De verdere aanpak van het NCSC heeft zich gericht op het verstoren van de botnet-infrastructuur en het informeren van slachtoffers. Het NCSC heeft hierbij effectief samengewerkt met een groot aantal partijen uit de community. In het totaal zijn tot dit moment circa 60 domeinnamen die het botnet gebruikt aangepakt. Er zijn verder 10 Notice and TakeDown (NTD)- verzoeken uitgegaan naar servers in Oostenrijk, VS, Vietnam en Rusland. Daarbij is samengewerkt met publieke en private organisaties om analyses en zijn NTD's uit te voeren. Daarnaast zijn slachtoffers binnen en buiten Nederland via het netwerk van het NCSC geïnformeerd om opvolging en schoning te realiseren. De meeste Internet Service Providers (ISP's) hebben de door NCSC gecommuniceerde gegevens overgenomen en de IP-adressen vanuit hun netwerken onbereikbaar gemaakt, later zijn ook de NTD-verzoeken uitgevoerd.

De verwachting is dat het Dorifel virus de komende weken nog hier en daar zal worden gevonden. De partijen achter het Citadel botnet zijn nog steeds bezig met pogingen om de infrastructuur opnieuw beschikbaar te maken. Het NCSC blijft dit in de gaten houden en, zo mogelijk, verstoren. Dit gaat waarschijnlijk door totdat het opsporingsonderzoek van de politie naar daders resulteert in arrestaties of de middelen van de criminelen op zijn.

De leden van de PVV-fractie vragen om een inschatting of de besmetting te voorkomen was geweest en zo ja, waarom daar niet voor gekozen is. Zo nee wil de PVV-fractie weten waarom slechts een beperkt aantal computers besmet is. De CDA-fractie wil weten hoe bedrijven, overheidsinstellingen en burgers zich kunnen wapenen tegen virussen, naast het uitvoeren van van en updaten van antivirusprogramma's.

Besmetting was met alleen het gebruik van een virusscanner en een firewall niet te voorkomen geweest. De malware, zowel Dorifel als de Citadel variant, werden op dat moment door anti-virus scanners niet herkend. Door de sterk wisselende verschijningsvormen van deze malware is het lastig om nieuwe besmettingsvormen nu en in de nabije toekomst snel te herkennen. Het nemen van aanvullende beveiligingsmaatregelen kan het risico op besmetting wel verder beperken. Om de besmetting met Dorifel tegen te gaan zijn Internet Protocol (IP) adressen en domeinnamen met partners en doelgroepen gedeeld en is op een Amerikaans IP-adres een Notice and Take Down (NTD) verzoek gedaan in de VS. Daarnaast zijn enkele domeinnamen die zijn gevonden door het analyseren van de malware door het NCSC geregistreerd en omgeleid.

Om meerdere redenen heeft het Dorifel virus zich vaak niet over alle computers in het netwerk weten te verspreiden. De initiële verspreiding van Dorifel vond plaats doordat één of meerdere computers in het netwerk van een organisatie al enige tijd besmet waren met het Citadel virus. Van hieruit kon het virus vervolgens bestanden op het netwerk besmetten. Vervolgens kan een andere computer met het virus besmet worden doordat het in contact is gekomen met door Dorifel besmette bestanden. Bijvoorbeeld doordat een besmet office-bestand wordt geopend via het netwerk of per e-mail. Omdat in de meeste gevallen het er op lijkt dat niet alle pc's binnen organisaties besmet waren met het Citadel virus, kende de initiële verspreiding een beperkte omvang. Daarnaast hebben tijdige updates van antivirus software om Dorifel, en met Dorifel besmette bestanden, te herkennen, alsook verdere maatregelen die zijn genomen om de verspreiding tegen te gaan, ervoor gezorgd dat men het totaal aantal besmettingen heeft weten te beperken.

Om zich in de algemene zin te wapenen tegen virussen is het uitvoeren en updaten van de virusdefinities van antivirusprogramma's van groot belang. Ook is het belangrijk om patches voor kwetsbaarheden in software direct te installeren. Daarnaast worden op de website van het NCSC dagelijks beveiligingsadviezen gegeven. Naar aanleiding van het Dorifel virus is de factsheet «Verlos me van een botnet» gepubliceerd.

De leden van de VVD en de SP fractie vragen of de minister kan garanderen dat er geen persoonsgegevens zijn gelekt?

In de brief d.d. 14 augustus jl. is reeds aangegeven dat er geen aanwijzingen zijn dat het virus zich via de websites van betroffen organisaties verder heeft verspreid en dat er
persoonsgegevens van burgers zijn gelekt. Dit is echter niet te garanderen.

De leden van de Pvda en de CDA fractie vragen wat de schade is die besmettingen hebben veroorzaakt?

In antwoord op de schriftelijke vragen van het lid Heijnen heeft de Minister van BZK reeds aangegeven dat voor zover bekend de kosten zitten in het de doen van onderzoek naar de besmetting, het blokkeren van de bronservers en het herstellen van de besmette bestanden. Dit maakt deel uit van reguliere bedrijfsvoering. Directe kosten zijn daarmee niet te kwantificeren. Vanuit de contacten met gemeenten is duidelijk geworden dat de kosten sterk samenhangen met hoe zwaar de gemeente is getroffen en welke maatregelen men heeft kunnen nemen. Enkele eerste schattingen lagen tussen de 10 000 en 50 000 euro per organisatie.

De leden van de D66 fractie vragen tot welke gegevens en/of systemen dit virus toegang heeft gehad en wat de maximale schade is die het virus aan had kunnen richten vanuit de systemen waar het toegang toe had?

In de brief d.d. 14 augustus is reeds aangegeven dat aan de RijksCIO is gerapporteerd dat besmetting is opgetreden bij het Rijksinstituut voor Volksgezondheid en Milieu
(RIVM, twee PC's), het Koninklijk Meteorologisch Instituut (KNMI, 3 PC's), het
ministerie van Onderwijs, Cultuur en Wetenschappen (OCW, 6 PC's), het ministerie van Economische Zaken, Landbouw en Innovatie (EL&I, 10 PC's en
twee servers) en op één PC op het separate studentennetwerk van de Nederlandse Defensie Academie (NLDA). Genoemde organisaties geven aan dat
de besmetting is bestreden, dat besmette bestanden zijn geïsoleerd en worden
geschoond en dat bedrijfscontinuïteit van de organisaties niet in het geding is
geweest. Medusoft, SurfRight en QuarantaineNet hebben op donderdag en vrijdag (9 en 10 augustus) tools beschikbaar gesteld om het virus te herkennen en de schade ongedaan te maken. Een inventarisatie bij reeds getroffen organisaties laat zien dat voor zover bekend binnen deze organisaties geen bedrijfsprocessen meer worden gehinderd.

De leden van de CDA fractie vragen of publieke of private instellingen te maken hebben gehad met wijziging door het virus van bepaalde vitale bestanden?

De inhoud van de originele bestanden wordt door het virus versleuteld, maar niet vernietigd. Van definitieve wijziging, zowel bij publieke als bij private partijen, is dus geen sprake.

De leden van de PVDA-fractie vragen of de overheid een gericht doelwit was dan wel extra kwetsbaar. Tevens vragen de leden van de PVDA-fractie hoeveel infecties van computersystemen in het bedrijfsleven er bekend zijn.

Uit logdata is zichtbaar geweest hoeveel besmettingen hebben plaatsgevonden. Op basis hiervan is het uiteindelijke aantal besmettingen van Dorifel rond de 3 500 geschat, waarvan ca. 90 % in Nederland. De besmettingen hebben zowel overheid als bedrijfsleven getroffen, vermoedelijk evenredig. Er is op basis van de huidige informatie en signalen uit de community geen indicatie dat het aantal publieke partijen zwaarder zijn getroffen dan private partijen of andersom.

De leden van de SP-fractie vragen welke risico's er op dit moment nog zijn. De leden van de CDA-fractie vragen of het virus alleen in Nederland verspreid is of ook in het buitenland. Tevens vragen de leden van de CDA-fractie naar de eventuele aanpak in het buitenland en de contacten hiermee.

De verwachting is dat het Dorifel virus de komende weken nog hier en daar zal worden gevonden. De partijen achter het Citadel botnet zijn nog steeds bezig met pogingen om de infrastructuur opnieuw beschikbaar te maken. Het NCSC blijft dit in de gaten houden en, zo mogelijk, verstoren. Dit gaat waarschijnlijk door totdat het opsporingsonderzoek van de politie naar daders resulteert in arrestaties of de middelen van de criminelen op zijn.

Het Dorifel virus is ook buiten Nederland verspreid. Ten tijde van de initiële incident response vond verreweg het grootste percentage besmettingen met het Dorifelvirus in Nederland plaats. Vanuit andere getroffen landen is er vervolgens met name naar Nederland gekeken met betrekking tot de aanpak. Wel is er informatie over mogelijk gecompromitteerde ip-adressen uitgewisseld en zijn er internationale NTD-verzoeken uitgegaan om command & control servers onschadelijk te maken.

De leden van de SP-fractie vragen of er sinds 10 augustus 2012 nog nieuwe meldingen van besmettingen bij het NCSC binnnengekomen, of het virus zich de afgelopen weken nog ergens heeft gemanifesteerd en zo ja, of de TK kan worden geïnformeerd over hoeveel gevallen het gaat. De leden van de PvdA fractie vragen of de minister de indruk heeft dat bedrijven besmettingen open gedeeld hebben of zijn bedrijven terughoudend met het melden van inbreuken in hun computersysteem?

Bij het NCSC en via de media hebben 19 organisaties gemeld dat zij geïnfecteerd zijn met het Dorifel virus. Via particuliere IT-security organisaties vernamen wij dat nog meer organisaties waren getroffen. Daarmee is de schatting op 30 organisaties uitgekomen. Het getal van 30 organisaties is gebaseerd op wat het NCSC heeft kunnen waarnemen door meldingen en andere contacten. Waarschijnlijk is dit aantal fors groter omdat veel organisaties geen melding hebben gedaan of ruchtbaarheid aan de besmetting gegeven hebben, maar met de verspreidde informatie en tools zelf aan de slag zijn gegaan om de besmettingen aan te pakken.

De leden van de PVDA fractie vragen of een ruimere meldplicht de aanpak van computercriminaliteit kan verbeteren.

Wat betreft de meldplicht «security breach notification», is de Tweede Kamer d.d. 6 juli jl. geïnformeerd over de uitwerking van de in de motie Hennis-Plasschaert voorgestelde security breach notification. Deze uitwerking is een evenwichtig voorstel en draagt bij aan de verbetering van de aanpak van computercriminaliteit.

De leden van de SP fractie vragen of de minister kan aangeven hoe het kan dat een vermoedelijk in april opgelopen besmetting pas in augustus aan het licht kwam en vragen wat dit zegt over de mogelijkheden van Nederlandse overheidsdiensten om besmettingen op overheidscomputers te ontdekken? De leden van de CDA fractie vragen hoe lang Dorifel al speelde voordat het in het nieuws kwam?

Het Dorifel virus blijkt initieel verspreid te zijn via een uitvoering van het Citadel botnet. Dit botnet is al zeker sinds april 2012 actief. (Dit betreft dus het botnet en niet het Dorifel virus) De malware, zowel Dorifel als de Citadel variant, werden door anti-virus scanners niet herkend. Door de sterk wisselende verschijningsvormen van deze malware is het lastig om nieuwe besmettingsvormen nu en in de nabije toekomst snel te herkennen.

De leden van de D66 fractie vragen of de minister van mening is dat bij de uitbraak van een virus dat gebruik maakt van zero day lekken, de overheid voldoende kennis in huis heeft om de uitbraak te neutraliseren en de digitale samenleving voldoende te ondersteunen om de impact minimaal te houden? De leden van de SP fractie vragen of de minister van mening is dat de Nederlandse overheid voldoende kennis, capaciteit en middelen beschikbaar stelt om dergelijke aanvallen in de toekomst eerder op te merken en te voorkomen?

De overheid heeft voldoende kennis en capaciteit beschikbaar. Daarnaast heeft de overheid geïnvesteerd. Zo is sinds januari 2012 het NCSC operationeel. Tevens heeft het Kabinet in de brief d.d. 6 juli jl. reeds aangegeven dat het fundament gelegd is voor een integrale Nederlandse cyber security aanpak. Nu is het zaak voort te bouwen op dit fundament, om in publiek-private, civiel-militaire en (inter)nationale samenwerking te komen tot integraal cyber security management, waarin verantwoordelijkheden helder zijn benoemd en intensievere samenwerking leidt tot synergie. Een belangrijke stap hiertoe is blijven investeren in mogelijkheden om digitale aanvallen te detecteren die gericht zijn op de Rijksoverheid en vitale infrastructuren. Ook het vergroten van de weerbaarheid en het versterken van het herstelvermogen zal hier onderdeel uit van moeten maken.

De leden van de D'66 fractie vragen of de minister het radio interview kent met de staatssecretaris van VenJ waarin hij aangaf dat het Dorifelvirus een komkommerverhaal was? Verder vragen de leden zich af hoe het kan het dat het politieke bewustzijn ten aanzien van de gevaren van ICT na alle incidenten nog steeds lijkt te ontbreken.

Nee, het radio interview is mij niet bekend. Het politieke bewustzijn ten aanzien van de risico's die ict-gebruik met zich mee kan brengen is van groot belang. De Staatssecretaris van Veiligheid en Justitie onderschrijft dit belang en heeft hierom onder andere het initiatief genomen tot een meldplicht datalekken.

De leden van de VVD fractie vragen om een concrete uiteenzetting van door opsporingsdiensten gesignaleerde behoeften aan ruimere bevoegdheden, in relatie tot het Dorifelvirus en vergelijkbare virussen. Ook de leden van de PVDA fractie refereren aan een behoefte aan meer en

passende opsporingsmiddelen en brengen dit vooral in verband met de samenwerking met buitenlandse opsporingsdiensten. De leden van de PVV fractie vragen naar de effectiviteit van strafrechtelijke opsporingsmiddelen ter zake, gezien de aandacht hiervoor in de Dorifelbrief van 14 augustus jl. De leden van de CDA fractie verwijzen in dit verband naar een oproep van de landelijk Officier van Justitie Cybercrime voor specifieke juridische kaders over online opsporing.

Het incident met het Dorifelvirus toont onze kwetsbaarheid aan voor computercriminaliteit die buiten Nederland zijn oorsprong vindt. Dit incident onderstreept het belang van passende wetgeving om deze vorm van criminaliteit aan te pakken. Op grond van de praktijkervaringen en wensen, zoals die ook blijken uit de recente cybersecuritybeelden uit 2011 en 2012 en mijn brief aan uw Kamer van 23 december 2011 over het juridisch kader voor cybersecurity, heb ik een inventarisatie van uit te werken wetgevingsvoorstellen nagenoeg afgerond. Op korte termijn stuur ik u deze inventarisatie toe. Bij cybercriminaliteit zoals in de Dorifel casus, gaat het om het gebruik van zogenoemde Botnets om kwaadaardige virussen te verspreiden die het mogelijk maken op afstand en zonder instemming of zelfs tegen de wil van gebruikers veranderingen in geautomatiseerde werken aan te brengen. Deze Botnets bestaan uit groepen – van wisselende omvang – van computers die via het internet aan elkaar zijn verbonden en die via zogenoemde command en control servers door cybercriminelen worden aangestuurd. Technologische ontwikkelingen leiden er toe dat het zeer gecompliceerd is geworden om criminele activiteiten op het internet te traceren. Deze command en control servers bevinden zich namelijk vaak in een ander land, dan wel worden veelvuldig binnen een zeer kort tijdsbestek (internationaal) verplaatst. In de praktijk betekent dit dat het vaak moeilijk is om de command en control server te lokaliseren en er tegen op te treden voordat de server is verplaatst. Zoals ik in de antwoorden op de Kamervragen van de leden Hachchi en Schouw heb geschreven is er een internationaal gevoelde behoefte aan nieuwe regels voor grensoverschrijdende bestrijding en voorkoming van cybercrime. Het op afstand betreden van computers, dat sommigen als terughacken aanduiden, maakt ook onderdeel uit van die internationaal – en dus ook met andere EU landen – gevoerde discussie.

De leden van de PVDA fractie, en ook de leden van de CDA fractie, vragen naar de stand van zaken van het opsporingsonderzoek naar personen achter het Citadel-botnet en het Dorifelvirus. Daarbij vragen zij ook naar de samenwerking met buitenlandse opsporingsdiensten. De leden van de PVDA fractie vragen naar de verhouding van de recent bekend geworden diefstal van bankgegevens tot het Citadel botnet en het Dorifelvirus.

Het strafrechtelijk onderzoek richt zich op de identificatie, opsporing en aanhouding van personen en/of organisaties achter het Dorifel virus en het Cidatel botnet. Voor zover daarbij de hulp van buitenlandse opsporingsautoriteiten nodig is, zullen daartoe rechtshulpverzoeken worden gedaan. Het strafrechtelijk onderzoek is nog in volle gang. Het is niet in het belang van dat onderzoek om nu reeds prijs te geven of zicht bestaat op betrokken personen en/of organisaties. Het is ook niet in het belang van het opsporingsonderzoek om nu uitspraken te doen met welke landen wordt samengewerkt. Het opsporingsonderzoek richt zich niet op de vraag of sprake is van een rechtstreeks verband tussen de diefstal van bankgegevens die plaatsvond na de Dorifeluitbraak en het Citadel-botnet. Ten slotte merk ik op dat in deze fase van het onderzoek zijn (nog) geen uitspraken te doen zijn over de effectiviteit van de ingezette opsporingsmiddelen.

De leden van de D'66 fractie vragen naar mijn mening over het weblog van een veroordeelde hacker . Daarop is diens «hack» van een bepaalde server beschreven. De leden van de D'66 lijken de mening te zijn toegedaan dat door het publiceren van deze «hack» mogelijk uiteindelijk ergere problemen zijn voorkomen, nu door het hacken van de server de hacker er achter kwam dat het virus uiteindelijk bankaccounts zou aanvallen.

Ik ben bekend met het weblog van Rickey Gevers. De impact van de handelingen die hij heeft verricht ter onderzoek van dit incident is op dit moment onduidelijk. In zijn algemeenheid ben ik een voorstander van burgerparticipatie bij de bestrijding van criminaliteit. Burgers die de overheid bij haar taken behulpzaam zijn, dienen zich daarbij echter te allen tijde te onthouden van het plegen van strafbare feiten. Indien zou blijken dat door burgers verzamelde informatie is verkregen door het plegen van strafbare feiten, dient de overheid zich terughoudend op te stellen met betrekking tot het gebruik van die informatie.

De leden van de SP fractie vragen of de minister niet kan uitsluiten dat er ook op dit moment mogelijk geheel andere virussen en malware aanwezig zijn op computers binnen de overheid, wat de minister van plan is te doen om hierover duidelijkheid te verkrijgen en wanneer hij de Kamer hierover kan informeren?

Mede namens de minister van BZK geef ik hierbij aan dat binnen de overheid er alles aan gedaan wordt om dergelijke besmettingen te voorkomen. Binnen de Rijksdienst is het aantal besmettingen daardoor relatief laag gebleven. Ik kan echter nooit uitsluiten dat er malware actief is waarvan het bestaan onbekend is. Daarom kan ik evenmin de Kamer hierover rapporteren.

De leden van de PVDA fractie vragen of de infectie van computers bij overheidsinstellingen door het Dorifel virus ook betekent dat deze systemen al langer deel uitmaakten van het Citadel botnet en zo ja, hoe kan het dat deze eerdere infecties onopgemerkt zijn gebleven en hoe kunnen deze besmettingen alsnog opgeschoond worden om nieuwe activiteit van dit botnet te voorkomen?

Mede namens de minister van BZK geef ik hierbij aan dat een infectie met het Dorifel virus niet automatisch betekent dat er een besmetting met het Citadel virus aanwezig was. Dit is voor enkele systemen wel het geval geweest. Deze systemen maakten derhalve deel uit van het gebruikte Citadel botnet. De malware, zowel Dorifel als de Citadel variant, werden door virusscanners initieel niet herkend. Door de sterk wisselende verschijningsvormen van deze malware is het lastig om nieuwe besmettingsvormen nu en in de nabije toekomst te voorkomen, Virusmakers worden immers ook steeds slimmer in het maskeren van hun producten. Het is dan ook zaak om zowel te blijven werken aan het voorkomen van virussen, maar ook aan de snelle opsporing en verwijdering ervan. Het NCSC heeft een factsheet gepubliceerd waarin wordt aangegeven hoe de besmetting kan worden geschoond.

De leden van de PVDA fractie vragen of de latent aanwezige botnet-besmettingen aantonen dat er tekortkomingen zijn in de beveiliging van overheidsnetwerken en vragen wat er wordt gedaan om deze beveiliging te verbeteren. Ook de leden van de PVV fractie refereren hieraan.

Mede namens de Minister van BZK geef ik hierbij aan dat digitale informatie-uitwisseling een essentieel onderdeel is geworden voor het functioneren van de Nederlandse samenleving. Het gaat hierbij zowel om het economische verkeer als om het functioneren van de overheid.

Gegeven het feit dat internet per definitie niet als volledig veilig te beschouwen is alsmede internationaal bepaald wordt, kunnen inbreuken op die veiligheid nooit geheel worden uitgesloten. Iedereen dient zijn eigen verantwoordelijkheid te nemen. Daarbij dient aandacht te zijn voor het vergroten van de weerbaarheid en het vergroten van het herstelvermogen. Een goede beveiliging bestaat uit het zoveel mogelijk voorkomen van incidenten en een vermogen tot herstel indien zich toch een incident voordoet. In dit geval, waarbij de aard van het virus detectie veelal pas mogelijk maakt op het moment dat het virus zich manifesteert, is echter wel gebleken dat de ICT-gemeenschap zich meteen informeert en gezamenlijk werkt aan de oplossing van deze problemen.

In het kader van het programma compacte rijksdienst en de i-strategie van de Rijksdienst is reeds een aantal acties in het gang gezet die een bijdrage leveren aan de versterking van de bestaande maatregelen op het gebied van informatiebeveiliging. Door de consolidatie van data-centers, het terugdringen van het aantal interne aanbieders van ICT-diensten en de rijksinternet koppeling wordt versnippering tegen gegaan, hetgeen de kwaliteit van de beveiliging verder verbetert.

Het is de verantwoordelijkheid van medeoverheden om zelf voorzieningen te treffen voor een adequate informatiebeveiliging. Het Nationale Cyber Security Centre vervult een belangrijke taak bij waarschuwing en ondersteuning van verschillende organisaties, met name binnen de overheid. daar waar het gaat om (potentiële) verstoringen van de informatie-infrastructuur van Nederland .

VNG is in samenwerking met KING overgegaan tot het uitwerken van een propositie om te komen tot een informatiebeveiligingsdienst ter ondersteuning van gemeenten. Deze zogenaamde IBD komt op 12 oktober a.s. aan de orde op de ALV van de VNG.
Het Uitvoeringsinstituut Werknemersverzekeringen (UWV) heeft samen met ketenpartners het Centrum Informatiebeveiliging en Privacybescherming (CIP) opgezet. Doel van dit centrum is het weerbaarheids-, herstel- en leervermogen van zelfstandige bestuursorganen (zbo's en uitvoeringsinstellingen van het Rijk) rond cybercrime te versterken. IBD en CIP stemmen hun activiteiten af met NCSC, teneinde overlap te voorkomen en kennis te delen.

In reactie op het rapport van de Onderzoeksraad voor Veiligheid «Het DigiNotar incident, waarom digitale veiligheid de bestuurstafel te weinig bereikt» zal het kabinet in het najaar met een nadere reactie komen, waarbij mede ingegaan zal worden op het versterken van de bewustwording van bestuurders en hoger management, daar waar het gaat om nut en noodzaak van informatiebeveiliging.

De leden van de PVV fractie vragen of er nader onderzoek gedaan is naar eventuele andere virussen die deze (of andere) overheidscomputers tegelijkertijd besmet kunnen hebben en vragen of de besmette computers op het moment van besmetting allemaal up-to-date waren waar het beveiligingsupdates, softwareversies en antivirusprogramma's betreft?

Mede namens de minister van BZK geeft ik hierbij aan dat ministeries met grote regelmaat computers toetsen op malware, trojans en virussen met behulp van de laatste updates van virusdefinities. De malware, zowel

Dorifel als de Citadel variant, werden door antivirus scanners niet herkend. Organisaties die zijn getroffen, hebben in nauw contact met NCSC het virus bestreden en nader onderzoek gedaan. Organisaties die niet zijn getroffen, hebben bekeken of extra onderzoek noodzakelijk was. Door de sterk wisselende verschijningsvormen van deze malware is het lastig om nieuwe besmettingsvormen nu en in de nabije toekomst snel te herkennen. Een besmetting als deze lijkt dus niet altijd te voorkomen. Zie daarvoor ook de recente besmetting die via een «betrouwbare» sites als NU.nl heeft plaatsgevonden. Dit onderschrijft het belang van zowel risico-voorkoming alsook het belang van risico-opvolging in geval van voorkomende besmettingen.

De leden van de D66 fractie vragen of het waar is dat het ministerie van OCW getroffen is door het Dorifelvirus? Zo ja, was dit op het netwerk van de Haagse Ring of op een apart netwerk van het ministerie. De leden van de D66-fractie merken op dat het Dorifelvirus is geïnstalleerd door computers die onderdeel waren van het Citadel-botnet. Hoe lang zijn de computers van het ministerie van OCW onderdeel geweest van dat botnetwerk? Is de minister mening dat de beveiliging van het ministerie van OCW adequaat was? Draait er op het interne netwerk van de Haagse Ring een zogenaamd Intrusion Detection System? Zo ja, is dit in eigen beheer en intern ontwikkeld of van een derde partij?

Zoals reeds in de brief van 14 augustus (KST 26 643 nr 251) is gemeld, is het Ministerie van OCW inderdaad door dit virus getroffen geweest. De dienst DUO is echter niet getroffen door het virus. De besmetting betrof uitsluitend een beperkt deel van het interne deel van het eigen netwerk. Er zijn sporen aangetroffen die erop wijzen dat zes computers vanaf eind mei 2012 geïnfecteerd zijn geraakt. De beveiliging van het netwerk van het ministerie wordt dagelijks gecontroleerd. Naast periodieke updates worden als daar aanleiding toe bestaat additionele maatregelen getroffen om kwaadaardige software tegen te gaan. Momenteel wordt onderzoek gedaan naar de wijze waarop het virus zich heeft kunnen installeren. Indien de uitkomsten van dat onderzoek daar aanleiding toe geven worden aanvullende maatregelen genomen.

Aangezien noch de Minister van BZK, noch de minister van V&J toezicht uitoefent op andere ministeries, hebben zij geen oordeel over de beveiliging van het ministerie van OCW.

Het vrijgeven van details over de beveiliging van de Haagse Ring zou potentiële aanvallers ongewenst informatie kunnen verschaffen.