Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2015–2016

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 420

BRIEF VAN DE STAATSSECRETARIS VAN VEILIGHEID EN JUSTITIE

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 5 september 2016

Hierbij bied ik uw Kamer, vanuit mijn coördinerende verantwoordelijkheid voor cybersecurity het, onder verantwoordelijkheid van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) in samenwerking met de publieke en private sector tot stand gekomen, Cybersecuritybeeld Nederland 2016 (CSBN 2016) aan[1].

Dit zesde opeenvolgende jaarlijkse beeld schetst de zorgelijke ontwikkeling in de periode van mei 2015 tot en met april 2016 van een toenemende en reële dreiging in het digitale domein. Deze ontwikkeling vraagt om blijvende investeringen in cybersecurity en een doorontwikkeling van de Nederlandse cybersecurityaanpak. Met deze brief informeer ik u tevens over de afronding van het actieprogramma bij de tweede Nationale Cyber Security Strategie (NCSS 2) en de vervolgstappen die worden gezet. Uiteraard zijn deze resultaten geen eindpunt, derhalve informeer ik u tevens over de eerste vervolgacties in het licht van de genoemde zorgelijke ontwikkeling. De kernbevindingen, conclusies en beleidsopvolging worden onderschreven door de Cyber Security Raad.

CSBN 2016

Het CSBN 2016 schetst een zorgelijk beeld van de veiligheidssituatie in het digitale domein. Waar in 2015 sprake was van het doorzetten van zorgelijke trends, kan nu gesproken worden van toenemende en reële cyberdreigingen. Deze dreigingen zijn gericht op diefstal van geld en kostbare commerciële informatie maar richten zich ook op de ondermijning van politiek en bestuur en het verstoren of saboteren van diensten en processen waar overheden en de samenleving van afhankelijk zijn voor hun functioneren.

[1] Raadpleegbaar via www.tweedekamer.nl.

kst-26643-420
ISSN 0921 - 7371
's-Gravenhage 2016

Cybercriminelen hebben zich ontwikkeld tot zeer geavanceerde actoren wier capaciteiten in een aantal gevallen gelijk staan met die van staten. Deze capaciteiten worden bovendien verkocht of verspreid waardoor kennis, kunde en tools om geavanceerde of grootschalige digitale aanvallen uit te voeren in handen komen van technisch minder vaardige partijen zoals cybervandalen en scriptkiddies. Cybercrime is daarmee zowel kwantitatief als kwalitatief een groeiend probleem voor de Nederlandse samenleving.

Statelijke actoren zetten steeds meer digitale middelen in voor spionage-, beïnvloedings- en sabotagedoeleinden als integraal onderdeel van hun machtsinstrumentarium. Op dit moment is digitale spionage gericht op economische en politieke informatie een grote bedreiging voor Nederland. Door diefstal van intellectueel eigendom of andere kostbare informatie worden Nederlandse bedrijven benadeeld en wordt het verdienmodel van de Nederlandse economie ondermijnd.

Internationaal is er een trend waarneembaar dat digitale capaciteiten worden ingezet in conflictsituaties, al dan niet als onderdeel van hybride oorlogsvoering. De meest voorkomende verschijningsvormen zijn de zogenaamde informatie operaties, die als doel hebben de publieke opinie te beïnvloeden. Ook is er een trend waarneembaar dat (militaire)inlichtingendiensten zich in toenemende mate specialiseren in het binnendringen van zogenaamde Industriële Controle Systemen of SCADA systemen. Deze systemen worden onder andere gebruikt voor vitale onderdelen van de economie. Manipulatie, ontzegging van- of schade aan dergelijk systemen kunnen zowel militair als civiel een belangrijke rol gaan spelen in toekomstige conflicten. Geopolitieke ontwikkelingen hebben een belangrijke invloed op de ontwikkeling van de dreiging. Steeds meer staten ontwikkelen (militaire) cybercapaciteiten en het is voorstelbaar dat wanneer Nederland betrokken raakt bij oplopende geopolitieke spanningen of een internationaal conflict, zij doelwit kan worden van digitale sabotage of andere ernstige cyberaanvallen.

De kernbevindingen uit het CSBN 2016 worden hieronder genoemd en dienen in samenhang te worden bezien met de kernbevindingen uit de voorgaande cybersecuritybeelden:

- *Beroepscriminelen hebben zich ontwikkeld tot geavanceerde actoren en voeren langdurige en hoogwaardige operaties uit*
  Campagnes van beroepscriminelen worden steeds geavanceerder. In het verleden waren de digitale aanvallen en bijbehorende campagnes van criminelen vaak van korte duur en gericht op snel geld verdienen door veel partijen te benadelen. Criminelen hebben het afgelopen jaar een aantal campagnes uitgevoerd waarvoor hoge investeringen zijn gedaan en waaruit een hoge organisatiegraad blijkt. Bovendien wordt spearphishing door criminelen steeds verfijnder en daarmee geloofwaardiger. Spearphishing is zo steeds lastiger te bestrijden met beveiligingsbewustzijn. Langdurige campagnes met grote investeringen en geavanceerde spearphishing waren in het verleden het terrein van statelijke actoren.
- *Digitale economische spionage door buitenlandse inlichtingendiensten zet de concurrentiepositie van Nederland onder druk*
  Het afgelopen jaar zijn veel digitale aanvallen waargenomen op bedrijven in Nederland, waarbij het motief economische spionage was. Spionage met een economisch oogmerk is schadelijk voor de concurrentiepositie van Nederland. Deze aanvallen richtten zich op het verkrijgen van technologie die zijn marktwaarde soms nog moet bewijzen. Twee derde van de getroffen bedrijven had deze aanvallen niet zelf waargenomen.

- *Ransomware is gemeengoed en is nog geavanceerder geworden*
  Het gebruik van ransomware door criminelen is het afgelopen jaar gemeengoed geworden. Besmettingen zijn aan de orde van de dag en raken de gehele samenleving. Waar in het verleden dezelfde prijs betaald moest worden per besmetting, wordt nu een prijs bepaald aan de hand van het type getroffen organisatie. Bovendien is de malware zelf verfijnder: naast bestanden op de lokale schijf worden tegenwoordig ook databases, back-ups en bestanden op netwerkschijven versleuteld.
- *Advertentienetwerken zijn nog niet in staat gebleken malvertising het hoofd te bieden*
  Het verspreiden van malware via advertenties op grote websites is een probleem. De advertentienetwerken zijn nog niet in staat gebleken dit probleem het hoofd te bieden. Het brede bereik van advertentienetwerken zorgt, samen met het grote aantal systemen waarop de laatste updates ontbreken, voor een groot aanvalsoppervlak. Beheerders van deze websites en de advertentienetwerken zelf hebben geen volledige controle over de advertenties. Dit zorgt ervoor dat malware zich kan verspreiden. Het volledig blokkeren van advertenties in de browser raakt aan het verdienmodel van website-eigenaren. Om gebruikers te beschermen tegen malvertising zonder alle advertenties te blokkeren zijn fundamentele wijzigingen nodig in de manier waarop deze netwerken werken.

Ontwikkeling cybersecuritylandschap

Digitalisering wordt meer en meer gezien als de vierde industriële revolutie die de werking van onze samenleving en economie fundamenteel verandert. Deze mondiale ontwikkeling voltrekt zich in een steeds hoger tempo en dringt al maar verder door in de haarvaten van onze samenleving. De vraag hoe Nederland optimaal kan profiteren van deze ontwikkeling is afhankelijk van de mate en snelheid waarmee Nederland in staat is nieuwe technologie op een veilige en kwalitatieve wijze in te zetten en door te ontwikkelen. Hierover heeft de Minister van Economische Zaken uw Kamer op 5 juli 2016 middels «de Digitale agenda»[2] geïnformeerd.

Cybersecurity is zowel randvoorwaardelijk voor het veilig functioneren van onze samenleving, als een fundament van vertrouwen onder onze economie. Veiligheid is daarbij geen absoluut goed maar wordt bereikt in een dynamische balans waarbij vrijheid, veiligheid en maatschappelijke groei soms harmonieus samengaan en soms op gespannen voet staan.

De inspanningen die onder andere in het kader van de NCSS 2 hebben plaatsgevonden hebben Nederland de kennis, kunde en capaciteiten gegeven om op dit moment nog in de voorhoede van het digitale domein te kunnen acteren. Het inzicht van de aard en omvang van de dreiging in het digitale domein laat een zorgelijk beeld zien dat nauw samenhangt met geopolitieke ontwikkelingen en de verslechterde internationale veiligheidssituatie. Er is sprake van een reële en steeds toenemende dreiging in het digitale domein tegen Nederlandse (inter)nationale belangen. Digitale spionage en cybercrime vormen de grootste maar zeker niet de enige dreigingen. Nederlandse overheidsinstellingen en bedrijven zijn in toenemende mate doelwit van steeds complexere cyberaanvallen met een steeds verder toenemende impact. Kwaadwillende partijen, waaronder ook potentiele militaire tegenstanders, ontwikkelen hun digitale capaciteiten door en gebruiken cyberaanvallen als integraal onderdeel van hun instrumentarium. De kwantitatief en

[2] Kamerstuk 29 515, nr. 390.

kwalitatief toenemende dreiging in combinatie met een toenemende afhankelijkheid van inherent kwetsbare ICT in Nederland maken dat een doorontwikkeling van de Nederlandse cybersecurity noodzakelijk is. Zowel om op topniveau in het cybersecuritydomein te kunnen acteren als om de omvangrijke cyberdreiging te adresseren en het Nederlandse vestigingsklimaat zo op peil te houden. Zonder deze doorontwikkeling komt de Nederlandse cybersecurity en daarmee onze digitale samenleving en economie in toenemende mate onder druk te staan.

Resultaten NCSS 2

Het actieprogramma van de NCSS 2 bevat een breed scala aan activiteiten die de Nederlandse cybersecurity over de volle breedte moet versterken. De geboekte resultaten zijn significant en hebben Nederland een belangrijke voorsprong gegeven ten opzichte van veel andere vergelijkbare landen. Onderstaande hoogtepunten en de uitgebreide beschrijving in bijlage 1[3] dienen echter bezien te worden in de context van het zorgelijke beeld dat door het CSBN 2016 geschetst wordt.

- Er is in de afgelopen kabinetsperiode geïnvesteerd in innovatie en onderwijsinitiatieven om de Nederlandse kennis en kunde op het gebied van cybersecurity te vergroten. Zo is bijvoorbeeld tijdens de NCSC One conference in april 2016, het startschot gegeven voor het Dutch cybersecurity platform for higher education and research (Dcypher)[4]. Dcypher zorgt voor agendering en coördinatie van (wetenschappelijk en praktijkgericht) cybersecurity onderzoek en -hoger onderwijs. Met Dcypher wordt beoogd te bereiken dat het aantal cybersecurity specialisten groeit en dat meer studenten in het hoger onderwijs zich voor relevante curricula inschrijven en deze succesvol afronden.
- Het wetsvoorstel Computer Criminaliteit III is bij uw Kamer ingediend en moet de politie de bevoegdheden geven die zij nodig heeft om cybercrime effectief aan te pakken. Daarnaast is het wetsvoorstel gegevensverwerking en meldplicht cybersecurity[5] bij uw Kamer ingediend. Zoals aangegeven door de Minister van Defensie tijdens het algemeen overleg over de MIVD d.d. 29 juni 2016, zal het aangepaste wetsvoorstel ten aanzien van de Wet op de Inlichtingen en Veiligheidsdiensten na behandeling door de Raad van State aan uw Kamer worden aangeboden.
- Cybersecurity is van nature grensoverschrijdend en vraagt daarom ook om een internationale aanpak. Nederland heeft in de afgelopen kabinetsperiode het voortouw genomen om tijdens de Global Conference on Cyberspace 2015 (GCCS 2015) en het Nederlandse EU voorzitterschap cybersecurity internationaal op de agenda te zetten.
- Nederland bedrijft actieve cyberdiplomatie op het gebied van mensenrechten online, internet governance, het bewerkstelligen van een normatief kader voor de regulering van cyberoperaties tussen staten en capaciteitsopbouw. Tijdens de GCCS 2015 is het, in Den Haag gevestigde, Global Forum on Cyber Expertise (GFCE) opgericht dat internationale kennisontwikkeling en capaciteitsopbouw op het gebied van cybersecurity en de bestrijding van cybercrime stimuleert en faciliteert. Op advies van Nederland heeft het GFCE een civil society advisory board opgericht. Hiermee wordt ook binnen het GFCE gehoor gegeven aan de noodzaak om het maatschappelijk middenveld middels het multistakeholdermodel te betrekken bij internationale

[3] Raadpleegbaar via www.tweedekamer.nl.
[4] Dcypher is geïnitieerd door het Ministerie van Veiligheid en Justitie, het Ministerie van Economische Zaken, het Ministerie van Onderwijs, Cultuur en Wetenschap en de Nederlandse Organisatie voor Wetenschappelijk Onderzoek, gebied Exacte Wetenschappen.
[5] Kamerstuk 34 388, nr. 2.

cybercapaciteitsopbouw. Nederland levert daarmee een significante bijdrage aan meer veiligheid in een domein waarin interne en externe veiligheid bij uitstek met elkaar verbonden zijn.

Doorontwikkeling Nederlandse cybersecurityaanpak en maatregelen

Met de doorontwikkeling van de cybersecurityaanpak moet Nederland de volgende stap zetten om in het digitale tijdperk mee te blijven komen. Overheid en bedrijfsleven moeten hierbij elk hun verantwoordelijkheid pakken. Uitgaande van de huidige aanpak wordt daarom bezien waar actualiseringen en intensiveringen nodig zijn. Publieke en private partijen zijn daarom in kaart aan het brengen welke maatregelen nodig zijn om de cybersecurity van Nederland te borgen. Met name de overheid moet hierin het goede voorbeeld geven, de samenleving verwacht dat ook. Publieke en private inspanningen zijn daarbij in het digitale domein niet los van elkaar te zien.

Gezien de ernst van de dreiging zijn er reeds een aantal concrete acties die het kabinet samen met een initiële groep private partijen inzet om de Nederlandse cybersecurity te versterken:

- Het kabinet zal, in het licht van de toenemende dreiging, de inzet op het verder versterken en uitbouwen van het Nationaal Detectie Netwerk (NDN) blijven continueren. In het NDN werken het NCSC, de AIVD en MIVD samen om cyberaanvallen op rijksoverheid en vitale infrastructuur te onderkennen, zodat deze aanvallen sneller aangepakt kunnen worden en de effecten ervan beheersbaar worden gemaakt. Ook worden gegevens uitgewisseld met private partijen.
- De twee belangrijke Nederlandse mainports, de luchthaven Schiphol en de haven Rotterdam, erkennen het belang van een goed functionerend cybersecurity ecosysteem. Daarom werken zij aan het versterken van de gehele keten, bestaande uit de aan deze mainports verbonden bedrijven en organisaties, op het gebied van digitale veiligheid. Deze initiatieven zijn publiek-private pilots die samen met de NCTV/NCSC worden uitgevoerd.
- KPN werkt in een publiek-privaat samenwerkingsverband samen met de NCTV, aan een inventarisatie van de belangrijkste ICT kwetsbaarheden van dit moment. De geïdentificeerde kwetsbaarheden worden voorzien van voorgestelde oplossingsrichtingen, zodat de kwetsbaarheden sneller opgeheven kunnen worden en daarmee de periode dat misbruik van deze kwetsbaarheden gemaakt kan worden wordt gereduceerd.
- VNO-NCW, MKB-Nederland en het Ministerie van Economische Zaken zijn het initiatief gestart om in een publiek-privaat verband te hoe een sectorgerichte (keten)aanpak voor cybersecurity, gericht op het verspreiden van kennis en daaraan gekoppeld handelingsperspectief, kan worden ontwikkeld en geïmplementeerd.
- Ook werken VNO-NCW, MKB-Nederland en het Ministerie van Economische Zaken aan een plan ter versterking van cybersecurity voor het MKB. Er wordt een branchegerichte cybersecurityaanpak ontwikkeld die het MKB in staat moet stellen haar cybersecurity te versterken. In het algemeen is het MKB beperkt in wat het kan investeren in cybersecurity en heeft het daarom sterke behoefte aan «hapklare brokken».
- Om meer aandacht te genereren voor cybersecurity onderwijs en training, zet de Rabobank samen met de NCTV in op het bundelen van lopende activiteiten die in dit kader gebundeld worden om zo een grotere impact te hebben.
- Defensie investeert een deel van haar extra beschikbaar gestelde budget in de versterking van cybercapaciteiten. De gelden uit de

intensivering[6] zullen worden ingezet om Defensie op een aantal kerngebieden te versterken, te weten: de ontwikkeling van operationele cybermiddelen, de doorontwikkeling van het inlichtingenvermogen, de versterking van de digitale weerbaarheid en de ontwikkeling van cybercapaciteit bij de Koninklijke Marechaussee.
- Om de internationale rechtsorde verder te versterken heeft het Ministerie van Buitenlandse Zaken samen met het NATO Cooperative Cyber Defence Centre of Excellence het «The Hague Process» gestart om aan de hand van de *Tallinn Manual on the International Law Applicable to Cyber Operations* te verhelderen hoe het internationaal recht van toepassing is op cyberoperaties.
- Nederland heeft belang bij een geïntegreerde afweging van Nederlandse belangen op het gebied van het internet en een daarop gebaseerde internationale strategie die recht doet aan de verschillende belangen. In de kabinetsreactie op het AIV advies «Het internet, een wereldwijde vrije ruimte met begrensde staatsmacht» en WRR advies «De publieke kern van het internet: naar een buitenlands internetbeleid» is dan ook weergegeven dat het kabinet een geïntegreerde internationale cyberstrategie zal formuleren.
- Nederland vaardigt op uitnodiging van het United Nations Office on Disarmament Affairs een vertegenwoordiger af naar de UN Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security en bepaalt daar mede hoe het normatieve kader voor de regulering van cyberoperaties tussen staten verder vormgegeven kan worden.

2017 en verder

Zoals de acties benadrukken, neemt het kabinet de verantwoordelijkheid om, gegeven het zorgelijke dreigingsbeeld, gepaste acties te initiëren om Nederland nu en in de toekomst digitaal veilig te houden. Dit op basis van het fundament van de eerste en tweede Nationale Cyber Security Strategie en het bijbehorende actieprogramma. Digitale aanvallen zijn in het informatietijdperk helaas een gegeven. De geïnitieerde acties betreffen publiek-private samenwerking en de detectie van de dreigingen aangezien de combinatie van deze elementen resulteert in het noodzakelijke volledige beeld om ons publieke en private beleid op te bepalen. Daarnaast wordt bezien hoe de respons op cyberincidenten verder kan worden versterkt.

Op basis van de resultaten en de lessen die geleerd zijn uit de implementatie van het actieprogramma 2014–2016 kan ook na 2016 onverwijld worden gewerkt aan een eerste doorontwikkeling van de Nederlandse cybersecurityaanpak voor de periode na 2016. Tevens zal dan worden bezien of de huidige strategie, de NCSS 2 nog volstaat.

De Cyber Security Raad heeft mevr. Verhagen, als vooraanstaande Nederlandse CEO, bereid gevonden om een publiek-privaat advies met betrekking tot het belang van cybersecurity voor de Nederlandse economie en maatschappij op te stellen. Dit advies zal begin oktober 2016 verschijnen. Mede op basis van dit advies zullen activiteiten voor 2017 en verder worden vormgegeven.

De Staatssecretaris van Veiligheid en Justitie,
K.H.D.M. Dijkhoff

---

[6] Kamerstuk 34 000, nr. 23.