Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2014–2015

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 337

BRIEF VAN DE MINISTER VAN VEILIGHEID EN JUSTITIE

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 24 november 2014

In het actieplan bij de Tweede Nationale Cybersecurity Strategie (NCSS-2) is toegezegd een verkenning uit te voeren naar de haalbaarheid en wenselijkheid van een gescheiden ICT-netwerk voor (publieke en private) vitale processen, waaronder clouddiensten. Deze verkenning treft u bijgevoegd aan.

Naar aanleiding van vragen van leden van de VVD-fractie in de Eerste Kamer heb ik bij brief d.d. 4 augustus 2014 toegezegd het vraagstuk van haalbaarheid en wenselijkheid van het scheiden van ICT-netwerken en de toepassing van de Amerikaanse Patriot Act in onderling verband te bezien. Met deze brief aan beide Kamers der Staten-Generaal en de opgestelde verkenning in de bijlage wordt aan deze toezegging gevolg gegeven.

Proces

Om tot een gedegen eerste verkenning naar dit onderwerp te komen zijn door de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) diverse publiek-private dialoogsessies georganiseerd. Op basis van eigen onderzoek en de dialoog tussen deze verscheidenheid aan publieke en private partijen, waarbij zowel leveranciers als afnemers van ICT-producten en diensten vertegenwoordigd waren, is, op mijn verzoek door een externe partij (PwC) de bijgevoegde verkenning opgesteld[1].

Hoofdlijnen verkenning

In de verkenning is ingegaan op de vraag: «*zijn gescheiden ICT-netwerken in Nederland haalbaar en wenselijk*? » Hierbij wordt het volgende beeld geschetst:

– Bij geen van de voorbeelden van bestaande (deels) gescheiden netwerken is in brede zin sprake van een *volledige* scheiding op alle in

[1] Raadpleegbaar via www.tweedekamer.nl

kst-26643-337
ISSN 0921 - 7371
's-Gravenhage 2014

de verkenning gebruikte aspecten: productieketen, netwerkhiërarchie en fysieke dan wel virtuele scheiding.
– In de voorbeelden is wel sprake van het gebruik van gescheiden netwerkvoorzieningen, voorbeelden hiervan bevinden zich binnen de rijksoverheid en vitale sectoren. De haalbaarheid van een in algemene zin volledige scheiding van netwerken wordt twijfelachtig geacht.
– De wenselijkheid van een volledig gescheiden nationaal netwerk ter vervanging van (delen van) het open internet, moet vanuit de verkenning worden bezien in het licht van de volgende feiten: een gescheiden netwerk zal kostbaar zijn, het open internet beperken in haar functionaliteit en een schijnveiligheid creëren doordat het idee bestaat dat het netwerk per definitie dan veiliger zal zijn. Dit terwijl het na volledige scheiding mogelijk juist een aantrekkelijker doelwit zal vormen voor gerichte cyberaanvallen.
– Concluderend geeft de verkenning aan dat zowel de haalbaarheid als wenselijkheid van een volledig gescheiden netwerk (mede als alternatief voor het open internet) op basis van de genoemde aspecten twijfelachtig zijn. Het aanleggen of gebruiken van deels gescheiden netwerkvoorzieningen is één van de varianten die, zo laat de verkenning ook zien, reeds veelvuldig toegepast worden in bestaande netwerken. Deze oplossingen maken communicatie zonder gebruik van het open internet mogelijk.
– Er zijn hiervoor reeds uiteenlopende en afhankelijk van de omstandigheden, deels eenvoudigere en minder kostbare maatregelen te nemen die een bijdrage kunnen leveren aan het verbeteren van de cybersecurity in algemene zin. Gesuggereerde maatregelen zouden bijvoorbeeld kunnen zijn: encryptie, verbeteren van toegangscontrole, training van gebruikers, detectie van incidenten bijvoorbeeld door de monitoring van koppelvlakken met het internet, certificering, accreditatie en audits of het introduceren van «digitale ophaalbruggen» om netwerkdelen in geval van nood af te koppelen.

Reactie op het rapport

De verkenning geeft inzicht in het feit dat een volledig gescheiden netwerk op zichzelf geen realistische optie is. Dit geldt eveneens voor het gesloten maken van delen van het internet. Dit onderschrijft het door het kabinet gehechte belang aan een open en vrij internet. Het open karakter is de intrinsieke waarde die het internet vertegenwoordigt. Vanuit mijn coördinerende rol ten aanzien van cybersecurity zet ik in op het zoeken naar een balans tussen veiligheid, vrijheid en maatschappelijke groei. Juist door de sterke verbondenheid van netwerken en diensten is in de afgelopen decennia aanzienlijke maatschappelijke groei gerealiseerd.

Dit laat onverlet dat de verkenning tevens laat zien dat het van belang is om de onderliggende belangen: beschikbaarheid, integriteit en vertrouwelijkheid blijvend te beschermen. Dit kan betekenen dat op basis van een uitvoerige risicoanalyse, in het kader waarvan kosten en baten in vergelijking met verschillende alternatieven en/of aanvullende maatregelen vergeleken kunnen worden, door eigenaren van informatiesystemen wordt besloten tot het creëren van een veilige omgeving middels bij de situatie passende (scheidings-)maatregelen, zoals o.a. ook plaatsvindt binnen de rijksoverheid door fysieke en/of virtuele scheiding van specifieke netwerkvoorzieningen.

Ingezette en ondernomen acties

In de verkenning worden enige aanbevelingen gedaan in de vorm van andere maatregelen die mogelijk getroffen kunnen worden. Deze maatregelen die zien op het beschermen van de belangen veiligheid,

beschikbaarheid en integriteit zijn grotendeels reeds voorzien in staand beleid op het gebied van informatiebeveiliging en/of in de Tweede Nationale Cyber Security Strategie. Over de voortgang van deze strategie zal nog voor het eind van het jaar aan de Tweede Kamer gerapporteerd worden.

De belangrijkste ingezette en ondernomen acties die aansluiten bij de in de verkenning aanbevolen maatregelen zien er als volgt uit.

– Voor de ontwikkeling van een Rijksnetwerkinfrastructuur wordt door het Rijk gestreefd naar het creëren van een veilige omgeving waarmee naast de interne communicatie ook digitale communicatie met burgers en bedrijven kan worden geborgd in termen van veiligheid, beschikbaarheid en integriteit. Essentieel daarin is de opslag van de data en de bediening van kritische ICT.
– Deze veilige omgeving kan worden gecreëerd met gebruik van de vier Overheidsdatacenters, gevormd op basis van de aanpak in het programma «consolidatie datacenters compacte Rijksdienst». De onderlinge verbinding tussen deze datacenters wordt gerealiseerd via bestaande eigen fysieke en/of virtueel gescheiden netwerken en, afhankelijk van het vereiste beveiligingsniveau, aanvullende maatregelen zoals encryptie.
– Middels beveiligde koppelvlakken wordt de connectie met overheidspartijen en samenwerkingspartners in de publieke en/of private sector met het internet beveiligd en kan bij afschakeling van het internet de overheid onderling blijven communiceren. Dat draagt bij aan de borging van het vitale belang van de beschikbaarheid van deze netwerken voor de bedrijfsvoering van het Rijk.
– De verkenning gaat beknopt in op het introduceren van digitale ophaalbruggen in het geval van nood. Inmiddels wordt door diverse marktpartijen gewerkt aan het zogeheten Trusted Networks Initiative om te bepalen op welke wijze bij grootschalige aanvallen op de beschikbaarheid van netwerken en diensten internetverkeer tijdelijk op alternatieve wijze gerouteerd kan worden tussen Nederlandse partners. De overheid neemt bij dit initiatief en andere initiatieven daar waar mogelijk en noodzakelijk een faciliterende rol op zich.
– In de publiek-private dialoogsessies is reeds geconstateerd dat in Nederland in de breedte diverse business cases zijn ontstaan en afgenomen worden door overheid, vitale sectoren en bedrijfsleven om risicogestuurd, vertrouwde netwerken op basis van bijvoorbeeld eigen of dedicated afgenomen glasvezelkabels te realiseren. De beschreven ontwikkelingen bij het Rijk onderschrijven dit.
– De verkenning laat zien dat het internet als digitaal ecosysteem van nature grensoverschrijdend en open van karakter is. Nederland is in het licht van maatschappelijke groei gebaat bij een vrij en toegankelijk cyberdomein. Om vrijheid en veiligheid daarbij te borgen wordt internationaal ingezet op samenwerking. Onderdeel hiervan is de organisatie in 2015 van de Global Conference on Cyberspace. De uitkomsten van deze verkenning zullen hierbij betrokken worden.

Samenhang met toepassing Patriot Act

Naar aanleiding van vragen van leden van de VVD-fractie in de Eerste Kamer heb ik bij brief d.d. 4 augustus jl. toegezegd om het vraagstuk van haalbaarheid en wenselijkheid van het scheiden van ICT-netwerken en de toepassing van de Amerikaanse Patriot Act in onderling verband te bezien. De Patriot Act vergt medewerking van onder Amerikaanse rechtsmacht vallende bedrijven om in bepaalde omstandigheden door hen verwerkte persoonsgegevens over te dragen aan Amerikaanse autoriteiten ten behoeve van terrorismebestrijding. Deze Amerikaanse wetgeving kan door extraterritoriale effecten in de uitvoering spanning

opleveren met EU-wetgeving die in Nederland is geïmplementeerd in de Wet bescherming persoonsgegevens. Deze wetgeving stelt eisen aan internationale doorgifte van persoonsgegevens vanuit Nederland door diezelfde bedrijven. De samenhang met de hier besproken thematiek is dat ook aanbieders van software en hardware ten behoeve van ICT-netwerken, of bedrijven die worden ingeschakeld om deze netwerken te bouwen of onderhouden, gezien de marktsituatie, vaak directe of indirecte banden kunnen hebben met de Verenigde Staten. De conclusie uit de verkenning dat dit ook kan spelen bij gescheiden netwerken kan worden onderschreven.

Het kabinet geeft zich hiervan rekenschap, maar heeft gelijktijdig te maken met de realiteit van de markt en de vereisten van het in Europees verband geharmoniseerd aanbestedingsrecht. Niettemin vindt het kabinet de mogelijkheid dat bedrijven met conflicterende plichten te maken kunnen krijgen onwenselijk. Het zet daarom ten eerste in op het zoveel als mogelijk beperken van nadelige gevolgen door afspraken in contracten. Het kabinet voelt zich in deze aanpak gesteund door een recente rechterlijke uitspraak.[2] De contractuele voorwaarden moeten overigens telkens ook worden gelezen in het licht van nieuwe aanscherpingen van het gegevensbeschermingsrecht door de Europese rechter, zoals de verplichting tot opslag van persoonsgegevens op EU-grondgebied.[3] Daarbij zet het kabinet zich ook bij de onderhandelingen over de algemene verordening gegevensbescherming in voor het verkleinen van het risico op conflicterende plichten.[4] Het kabinet is zich er echter van bewust dat het moeilijk, zo niet onmogelijk zal zijn om hier een volledig sluitende oplossing te bereiken, gegeven de aard van de problematiek. De weg die we via Europa bewandelen om de dialoog te zoeken met de Verenigde Staten om over verschillende onderwerpen te onderhandelen is de enige manier waarop we met respect voor elkaars rechtsstelsel tot oplossingen kunnen komen.

Relatie met specifiek de ontwikkeling van de Rijkscloud

De realisatie van de in de verkenning beschreven Rijkscloud door de Minister voor Wonen en Rijksdienst gaat uit van het via bestaande fysieke en/of virtueel gescheiden netwerken, zoals die thans binnen de rijksoverheid in gebruik zijn, koppelen van de vier Overheidsdatacentervoorzieningen. De huidige eigendomssituatie en volledig gebruiksrecht van de rijksoverheid van dit netwerk maakt dat het ten behoeve van die voorziening een fysiek gescheiden netwerk betreft. De feitelijke aansluiting tussen deze datacenters en het bestaande netwerk verloopt deels via eigen verbindingen van het Rijk dan via bij gecontracteerde marktpartijen gereserveerde verbindingen. De toegang vanuit de diverse Rijksdiensten tot deze Rijkscloud verloopt via hoofdnetwerken die grotendeels uit de markt worden afgenomen. Ter beveiliging hiervan wordt gebruik gemaakt van aanvullende maatregelen die aansluiten bij het passende beveiligingsniveau, zoals onder meer encryptie.

---

[2] Zie Rechtbank Midden-Nederland, Vereniging Praktijkhoudende Huisartsen [VPH] v. Vereniging van Zorgaanbieders voor zorgcommunicatie [VZVH], 23 juli 2014, ECLI:NL:RBMNE:2014:3097 (uitspraak electronisch patiëntendossier), r.o. 5.40.

[3] Zie de uitspraak van het Hof van Justitie van 8 april 2014 jl. in Digital Rights Ireland en Seitlinger, C-293/12 en C294/12, waarin expliciet wordt verduidelijkt dat uit het vereiste van onafhankelijk toezicht door een gegevensbeschermingsautoriteit op bescherming en beveiliging van persoonsgegevens voortvloeit dat deze gegevens op EU-grondgebied moeten worden bewaard (r.o. 68).

[4] Kamerstuk 22 112, nr. 1372, blz. 7

Slot

Na het uitvoeren van de verkenning kan geconcludeerd worden dat het creëren van een volledig gescheiden netwerk voor vitale processen als een onhaalbare mogelijkheid dient te worden beschouwd, maar dat het desalniettemin van belang is om aanvullende acties te blijven ondernemen om de onderliggende belangen: beschikbaarheid, integriteit en vertrouwelijkheid te borgen. Dit sluit ook aan bij de kabinetsinzet om de gevolgen van toepasselijkheid van extraterritoriale wetgeving zoals de USA Patriot Act zoveel als mogelijk te blijven beperken, en in EU-verband, een bestendige oplossing te vinden voor het probleem van conflicterende plichten. De genoemde acties in samenhang met de maatregelen uit o.a. de Tweede Nationale Cyber Security Strategie zijn hierop gericht ten einde te voorzien in veiligheid, vrijheid en maatschappelijke groei in het cyberdomein.

De Minister van Veiligheid en Justitie,
I.W. Opstelten