Inbreng rondetafel cybersecurity Tweede Kamer 7 februari 2018

KPN is door zijn wijdvertakte digitale infrastructuur en dienstverlening aan miljoenen consumenten, tienduizenden bedrijven en vitale diensten, zoals 1-1-2, onderdeel van de Nederlandse vitale infrastructuur. Net als andere vitale infrastructuren moeten we continu alert zijn op hacks, cyberaanvallen en kwetsbaarheden in hard- en software die wij inzetten om onze diensten mogelijk te maken. Omdat de digitale wereld er de afgelopen jaren niet veiliger op is geworden, bevinden we ons continu in de digitale frontlinie.

Net als overheden, bedrijven en andere vitale infrastructuren is KPN voor zijn digitale veiligheid mede afhankelijk van de buitenwereld. In een veilige digitale omgeving is de kans op cybersecurity-incidenten kleiner. Beleid dat leidt tot meer digitale veiligheid is daarom in het algemeen belang. Daarbij is het ook nodig om voorbereid te zijn op grootschalige incidenten. De afgelopen jaren hebben geleerd dat er deze incidenten plaatsvinden, met honderden miljoenen euro's aan schade als gevolg. De vraag is dus niet of zulke incidenten zullen plaatsvinden, maar wanneer. Daar moeten we op voorbereid zijn door te zorgen dat de basis op orde is en te investeren in de cyberveiligheid van de toekomst. Onderstaand zullen we daarvoor twee concrete aandragen die hiervoor de aandacht verdienen.

Vitale infrastructuur: de basis op orde krijgen

Wanneer het functioneren van een vitale infrastructuur wordt verstoord, bijvoorbeeld door een cyberaanval, is er een kans dat deze verstoring leidt tot maatschappelijke ontwrichting. De digitale veiligheid van de vitale infrastructuren is daarom van essentieel belang. Deze veiligheid begint door te zorgen dat vitale infrastructuren hun basis op orde hebben en hun organisaties goed kunnen beveiligen. Daar moeten nog enkele noodzakelijke stappen in worden gezet:

- De basis moet op orde. Verschillende vitale infrastructuren bestaan (deels) uit verouderde ICT (legacy). Deze ICT is niet gemaakt met de veiligheidsstandaarden die in deze tijd nodig zijn, maar wel in het afgelopen decennium steeds meer aangesloten aan het internet. Bijvoorbeeld om beheer op afstand mogelijk te maken. Hierdoor is het risico op hacks en verstoringen door malware fors toegenomen. Er zijn verschillende voorbeelden die hebben geleid tot grote schade. Met name met industriële ICT (SCADA) dat aan internet wordt gekoppeld is kwetsbaar. Om Nederland veiliger te maken is het daarom nodig om te starten met een programma waarbij vitale infrastructuren worden gescand op cybersecuritykwetsbaarheden om deze vervolgens gestructureerd op te lossen;

- De overheid heeft de mogelijkheid om hacksoftware in te zetten door de Nationale Politie en veiligheidsdiensten. Hierbij wordt onder andere gebruik gemaakt van onbekende (zero-day) kwetsbaarheden. Dit zijn kwetsbaarheden die het mogelijk maken om via hard- of software te hacken of malware te installeren, maar die nog onbekend zijn bij de fabrikant. Wanneer de Nederlandse overheid deze informatie heeft, dan hebben andere overheden of hackers deze ook. Hierdoor zijn vitale infrastructuren mogelijk kwetsbaar voor digitale aanvallen. Het is daarom nodig dat de overheid informatie over (onbekende) kwetsbaarheden in hard- en

software ook met vitale infrastructuren deelt, zodat zij – waar nodig – mitigerende maatregelen kunnen nemen.

- Het Nationaal Cybersecuritycentrum (NCSC) heeft een belangrijke functie voor vitale infrastructuren. Het is een knooppunt van informatievoorziening en fungeert als crisiscentrum bij grote cybersecurityincidenten. Door de steeds grotere aandacht voor cybersecurity ontstaat er steeds meer aandacht vanuit de overheid voor cyberveiligheid. Dat is positief. Initiatieven kunnen wel tot versnippering leien waardoor (schaarse) mensen en middelen daartussen worden verspreid. Er moet worden gewaakt dat het NCSC dienstverlening op hoog niveau blijft leveren.

- Gegeven de aanname dat niet de vraag is of, maar meer wanneer er grootschalige incidenten plaatsvinden, zal Nederland een actief en nationaal cross-sectoraal oefenprogramma moeten opstellen. Bedrijven, overheden, burgers, veiligheids- en hulpdiensten zullen regelmatig moeten oefenen. Dit levert weerbaarheid op, ook het besef dat wij allen verantwoordelijkheden hebben, maar ook operationele vaardigheden die in noodsituaties onontbeerlijk zijn.

Kwantumcomputing en encryptie

Kwantumcomputing zal in de aankomende jaren doorbreken. Met deze techniek is het – simpel gezegd – mogelijk om berekeningen bij bepaalde toepassingen vele malen sneller uit te voeren dan computers gebaseerd op conventionele technieken. Kwantumtechnologie biedt daardoor nieuwe wetenschappelijke en economische kansen waar Nederland en Europa zich volop moeten inzetten.

Deze technologische ontwikkeling heeft ook een schaduwzijde. Bestaande vormen van encryptie – waarmee staatsgeheimen, intellectueel eigendom en privacygevoelige gegevens worden ‘versleuteld’ – zijn niet bestand tegen de rekenkracht van kwantumcomputers. Dat maakt het relatief simpel om encryptiemethodes gebaseerd op conventionele technologie te breken.

Nederlandse burgers, bedrijven en overheid moeten worden beschermd tegen de digitale spionage van de toekomst. Met name China en de VS lopen op dit vlak voor op Europese landen: in het huidige tempo is plausibel dat deze landen op afzienbare termijn de mogelijkheid hebben om bestaande encryptie te breken met behulp van kwantumtechnologie. China heeft al een omvangrijk kwantumnetwerk voltooid dat functioneert via duizenden kilometers glasvezelnetwerken en satellietverbindingen.

Een oplossing vinden is daarom essentieel en randvoorwaardelijk voor zowel de (digitale) veiligheid en de toekomstige economische groei van Nederland. Dit onderwerp is daarom urgent, omdat een oplossing zich niet vanzelfsprekend aandient. Het is daarom nodig om nu stappen te zetten door:

- Nu te investeren in onderzoek naar technieken zoals Quantum Key Distribution (QKD) en Post Quantum Cryptography (PQC) in samenwerking met de wetenschap en het bedrijfsleven op nationaal en Europees niveau;
- Een nationale strategie voor het veiligheidsvraagstuk dat ontstaat door kwantumcomputing, waarbij nationale en Europese initiatieven in kaart worden gebracht en waarbij zeker wordt gesteld dat investeringen ten goede komen van Nederland en de Europese Unie.