4
Vragenuur: Vragen Van Toorenburg

Vragen van het lid Van Toorenburg aan de staatssecretaris van Veiligheid en Justitie over **het bericht "Massale wereldwijde cyberaanval"**.

Mevrouw **Van Toorenburg** (CDA):
Voorzitter. Vanmorgen reed ik de parkeerplaats van Q-Park op. Zonder dat ik mijn abonnement hoefde te laten zien, ging de slagboom open. Dat is winst, dacht ik. Het was er wel voller dan normaal. Meerdere mensen zullen vanmorgen hebben ervaren dat Q-Park openstond.

Ik dacht: laat ik een keertje luchtig beginnen, want zo kent u mij niet. Maar die luchtigheid kan ik wel meteen achter me laten, want we hebben hier een serieus probleem bij de kop. Afgelopen vrijdag werden we opgeschrikt door een weergaloze aanval van gijzelingssoftware, die talloze computers en organisaties infecteerde in ruim 150 landen. En het was ontwrichtend, zeker in Groot-Brittannië, waar de ziekenhuizen het slachtoffer werden. Maar ook andere landen en bedrijven zijn getroffen.

Nou lijkt de schade in Nederland mee te vallen. Dat is goed nieuws, maar het neemt de zorgen niet weg. Het zou namelijk heel goed kunnen dat men ons simpelweg niet op de korrel nam. De vraag is dus allereerst: is Nederland voldoende beveiligd? En zijn we voldoende scherp of lopen we nog steeds serieuze risico's? Als we mevrouw Zorko, een soort directeur veiligheid in Nederland, kunnen geloven, dan is het allemaal goed op orde. Ze doet zelfs een beetje luchtig. Want als een bedrijf zijn software niet al op orde had, dan heeft het daar nou wel voor gezorgd, zegt ze. Maar volgens het rapport dat we vandaag hebben ontvangen, moeten we serieus aan de bak. Er zijn plannen genoeg, maar de middelen ontbreken. Zo vat ik het rapport maar even samen. Ik krijg daarop graag een reactie van de staatssecretaris.

Er is ook een gebrek aan sturing, aldus het rapport. Zorko zegt: dat is juist goed; we polderen ons de goede kant op. Ik ben benieuwd naar de reactie van de staatssecretaris hierop. Ook de informatie-uitwisseling tussen publiek en privaat schiet tekort, en er is te weinig deskundigheid. Kortom, er is sprake van grote dreigingen en grote zorgen. Wat heeft de staatssecretaris daarop te zeggen?

Staatssecretaris **Dijkhoff**:
Voorzitter. Mevrouw Van Toorenburg wijst er terecht op dat de schade in andere landen groter is. Zij stelt ook terecht de vraag: is dat omdat wij geluk hadden of omdat we zo veel beter zijn? Als de schade zich had voorgedaan in landen waar de cybersecurity op een laag niveau lag, dan zou je nog kunnen zeggen dat wij onze beveiliging beter op orde hebben. Maar bij de landen die zwaar geraakt zijn, zitten ook medekoplopers van Nederland op het gebied van cybersecurity. Ik denk dus inderdaad dat het ook met toeval te maken heeft. Het hangt af van wie er als eersten worden getarget en welke systemen zo in elkaar zitten dat het als een worm van het ene naar het andere door kan kruipen. In deze situatie is gebruik of misbruik gemaakt van een kwetsbaarheid in systemen die al langer bekend was, waarvoor ons NCSC in maart en april al gewaarschuwd was en waar ook al een patch voor was. Als mevrouw Van Toorenburg vraagt of Nederland voldoende beveiligd is, zou ik dus bijna willen zeggen: kennelijk niet. Er was immers sprake van een kwetsbaarheid die we kenden en die we ook konden repareren, maar niet iedereen die verantwoordelijk is voor cybersecurity in zijn of haar organisatie heeft die update gedraaid. Als die update is gedraaid of dat SMB-protocol is uitgezet, dan kom je niet binnen. Die bewustwording is nog niet ver genoeg gevorderd. We lopen daarin nog risico's. Het gaat om netwerken, dus de zwakste schakel kan een ingang zijn tot cruciale systemen. Dit bewijst maar weer dat de scherpte nog beter moet worden. Het is nooit af. Je kunt niet zeggen: ik heb nu updates gedraaid en ik kan nu weer een jaar vooruit. Je moet blijven opletten.

Ik denk dat de doorlichting die we hebben laten doen, accuraat is. Je kunt het op allerlei manieren bekijken, maar de doorlichting laat zien dat er nog heel veel te doen is, ook voor Nederland. Ten opzichte van andere landen kunnen we ook trots zijn, maar het probleem groeit sneller dan wij kunnen bijbenen. Het rapport geeft ook aan dat we het in Nederland heel knap doen met de middelen die we wel hebben. Ik zou bijna zeggen: als je erin investeert, zoals we bij de vorige begroting ook een stap hebben gezet, weet je in elk geval dat het geld goed besteed zal worden en dat ze er goed mee overweg kunnen. Ik denk dat ik door de spreektijd voor de eerste reactie heen ben.

Mevrouw **Van Toorenburg** (CDA):
We geven de staatssecretaris ruim de tijd voor zijn tweede reactie. Ik wil wel een aantal punten uitlichten. Kijk bijvoorbeeld naar de ziekenhuizen. Daar blijken we nog een heel serieuze slag te moeten maken. In Engeland zijn juist de ziekenhuizen heftig getroffen. We hebben daar begin dit jaar al een alarmerend bericht over gekregen. De minister van VWS heeft gezegd: inderdaad moeten we hier de komende vier jaar nog van alles doen. Serieus, voorzitter, de minister zei "de komende vier jaar". Ik denk dat we ons dat niet kunnen permitteren. Ik krijg daarop graag een reactie van de staatssecretaris.

Ik wil ook graag weten wat de stand van zaken is ten aanzien van het computer emergency response team voor de zorg, dat hiermee bezig zou zijn.

We weten dat 75% van de gemeenten te maken heeft gehad met datalekken. Ze zouden een aantal zaken op orde hebben gebracht. Ons is geworden dat dit nog niet is gebeurd. Sterker nog, ik kreeg vanmorgen nog het bericht dat er ambtenaren zijn die op verre afstand sluizen en bruggen bedienen met een digitale infrastructuur die niet meer is dan houtje-touwtje. Ik denk dat dit nu de belangrijkste punten zijn om aan te kaarten: gemeenten, ambtenaren en ziekenhuizen.

Ik wil er nog één ding bij halen. De staatssecretaris zegt terecht dat er wel wordt gekeken naar de mogelijkheden om het te verbeteren. Maar ik begrijp dat we nog niet eens scherp hebben wat daadwerkelijk onze vitale infrastructuur is. Ik begrijp dat ziekenhuizen er soms wel en soms niet toe behoren: academische ziekenhuizen wel en andere ziekenhuizen niet. Ook daarvan zouden we met elkaar moeten weten waar onze zwakke plekken zitten en wat we eraan doen als er een grote crisis is die Nederland raakt.

Staatssecretaris **Dijkhoff**:
Het liefste zou je zeggen: we wijzen één iemand aan in Nederland die ervoor zorgt dat alles veilig is. Maar zo werkt het dus niet. In die zin snap ik de opmerking van mevrouw Zorko over het polderen wel. Iedereen moet uiteindelijk zelf zijn zaken op orde hebben. Als een organisatie cruciaal is voor onze samenleving, moeten wij als overheid hogere eisen stellen aan die organisatie, zodat zij dat zelf doet.

Als het gaat om ziekenhuizen en vitale infrastructuur, is het juist nu cruciaal dat we die duidelijkheid bieden in de implementatie van de Netwerk- en informatiebeveiligingsrichtlijn. Daar zijn wij ook flink mee bezig. Binnenkort gaat de implementatie van de richtlijn in consultatie. Ook op andere terreinen, zoals de gegevensverwerking en de meldplicht cybersecurity zijn wij, vooruitlopend op Europese regelgeving, aan de slag gegaan. Deze Kamer heeft dat al behandeld; het ligt nu in de senaat. Wij zouden er graag verder mee gaan.

Wij sturen op de verantwoordelijkheden die iedereen heeft, maar uiteindelijk moet iedereen zijn eigen zaak op orde hebben. Er is echt nog veel te doen. Laat afgelopen weekend een wake-upcall zijn voor iedereen om de eigen verantwoordelijkheid hierin te nemen. Als je dat niet doet, kan ook een ander daar flink last van hebben.

Mevrouw **Van Toorenburg** (CDA):
Dan toch nog even over die ziekenhuizen. Voorlopig hebben ze nog steeds vier jaar om het op orde te krijgen. Ik denk dat dat onbestaanbaar is. Daar wil ik graag een concrete reactie op, is het niet hier, dan via de minister. Die datalekken bij de gemeenten zijn er nog steeds. Er is vier jaar geleden gesproken over mogelijke wetgeving om hier dwingender in te zijn. Wanneer is het moment om dat te doen? Kortom, ik begrijp dat er van alles gebeurt, maar ik heb nog niet helemaal helder wat wij daadwerkelijk gaan doen als er een grote crisis is.

Staatssecretaris **Dijkhoff**:
Al die maatregelen waar mevrouw Van Toorenburg terecht naar vraagt, zijn vooral bedoeld om zo'n crisis te voorkomen, om die kwetsbaarheden te verminderen. Als er zo'n crisis is, zie ik dat in Nederland alle schotten verdwijnen en dat iedereen heel hard op zoek gaat naar een oplossing, publiek en privaat bij elkaar. Ik zal mijn collega van VWS vragen of zij u kan informeren over de stand van zaken. Ik heb begrepen dat zij ook hierin aanleiding ziet om het belang van informatiebeveiliging in haar sector nogmaals onder de aandacht te brengen en daarbij tot spoed te manen.

Het is goed dat wij met die meldplicht die datalekken bij gemeenten naar boven krijgen. Zo zien wij hoe groot het probleem is en kunnen wij er gericht aan werken. Ze zijn niet allemaal hoogtechnologisch, het zijn ook weleens verkeerd meegestuurde bestanden. Als je merkt dat je een lek hebt gehad, moet je het repareren en daarna in overtreffende trap dwingen tot dichten van de gaten.

De heer **Verhoeven** (D66):
Het is natuurlijk wel saillant dat een partij als het CDA, die warm voorstander was van het openlaten van kwetsbaarheden in het internet voor het gebruik door inlichtingendiensten, nu vragen stelt over deze wereldwijde cyberaanval, zonder daar ook maar met één woord over te spreken. Daar wil ik graag nog een vraag over stellen.

We kunnen het hebben over veiligheid en investeren — dat is allemaal hartstikke goed — maar het gaat hier natuurlijk over de fundamentele keuze of wij kwetsbaarheden in het internet openlaten om ze te laten gebruiken door inlichtingendiensten, zodat die daarmee verdachten kunnen hacken. De NSA is hackingtools kwijtgeraakt aan criminelen. Deze aanval heeft laten zien dat dat heel gevaarlijk is. D66 heeft hier in de afgelopen maanden bij wetgeving die hierover ging herhaaldelijk op gewezen. Ik ben heel benieuwd of het kabinet tot inkeer komt en ziet dat dit serieuze risico's met zich meebrengt. De CTIVD heeft geadviseerd om duidelijk beleid te voeren voor het gebruik van kwetsbaarheden en er niet elke keer aan voorbij te gaan dat dat een reëel risico is. Zal het kabinet dat advies opvolgen?

De **voorzitter**:
Voordat ik de staatssecretaris het woord geef, zie ik dat mevrouw Van Toorenburg kort wil reageren op de opmerking van de heer Verhoeven over het CDA. Het telt dus niet als een vraag en mevrouw Van Toorenburg mag dus ook geen vraag stellen.

Mevrouw **Van Toorenburg** (CDA):
Ik zou eigenlijk alleen maar willen zeggen dat het een beetje sneu is dat de heer Verhoeven dit doet. Ik denk dat hij zich vreselijk gepasseerd voelt dat hij de vraag niet eerder heeft kunnen stellen. Ik denk dat hij daarom zo uithaalt. Laat het een compliment zijn dat wij die wetten hebben behandeld en dat ze in de Eerste Kamer liggen. Laat de Eerste Kamer ze gauw behandelen!

Staatssecretaris **Dijkhoff**:
De heer Verhoeven snijdt wat bochten af in zijn vraagstelling. Het kabinet heeft hier geen wet neergelegd zonder oog voor dit risico. De wet gaat uit van het melden van kwetsbaarheden en ze zo snel mogelijk verhelpen. Er zitten processen en procedures in om in uitzonderlijke gevallen melding van een kwetsbaarheid uit te stellen in verband met een opsporingsonderzoek. Deze casus toont aan waarom die balans in het wetsvoorstel zo goed is. Je wilt ten eerste voorkomen dat het nog een keer gebeurt. Ten tweede wil je het gat zo snel mogelijk dichten. Ten derde wil je degene die erachter zit oppakken. Om dat laatste te kunnen doen, heb je bepaalde bevoegdheden nodig.

Wat ook duidelijk is, is dat een kwetsbaarheid als deze, die al bekend en gemeld was en waarvoor al een reparatie bestond — het gaat niet om iets wat recentelijk nog is stilgehouden — nooit de toets van niet-melding van het wetsvoorstel had doorstaan. Deze kwetsbaarheid zit namelijk zo diep en wijdverbreid in belangrijke systemen dat het OM in dit geval niet eens zou hebben aangevraagd om haar in het opsporingsbelang open te mogen houden; dat hebben we nagevraagd. Deze zou sowieso gemeld zijn.

De heer **Hijink** (SP):
De staatssecretaris lijkt te vergeten dat deze aanval niet had kunnen plaatsvinden als de overheid, in dit geval de Amerikaanse overheid, de NSA, gewoon haar werk had gedaan, namelijk burgers, bedrijven en overheden beschermen. Dat heeft zij niet gedaan. Zij heeft doelbewust een bestaand lek in software opengehouden om daar dankbaar misbruik en gebruik van te kunnen maken. De staatssecretaris zegt dan dat mensen maar netjes hun updates moeten doen, en daar heeft hij ook wel gelijk in, maar dat helpt natuurlijk niet als de overheid tegelijkertijd zelf doelbewust misbruik en gebruik maakt van achterdeurtjes die in software bestaan. Mijn vraag is dan ook of de staatssecretaris bereid is om de hackwet die nu in de Eerste Kamer voorligt, nog te gaan aanpassen, zodat de overheid niet zelf medeverantwoordelijk wordt voor dit soort aanvallen, sterker nog, het internet uiteindelijk een stuk onveiliger maakt.

Staatssecretaris **Dijkhoff**:
Nee, die wet ga ik niet aanpassen, want daarin zitten nu net regelingen om per keer af te wegen welk belang prevaleert. In dit geval zou de kwetsbaarheid onder die wet zeker niet stiekem gebruikt en niet opengehouden zijn. De NSA heeft de kwetsbaarheid in dit geval inderdaad ooit niet gemeld. Daarna is ze wel aan het licht gekomen en daarom waren er al reparaties voor. Zelfs als een kwetsbaarheid algemeen bekend is en er ook een reparatie voor is, zie je dus dat je die kwetsbaarheid nog steeds kunt misbruiken. Het is dus niet zo dat alle systemen geüpdatet zijn zodra een kwetsbaarheid gemeld is. Ik denk dat ons wetsvoorstel een goede balans heeft. De hoofdregel daarbij is: een kwetsbaarheid die je ontdekt moet worden gemeld, onder strikte voorwaarden en met de uitzonderingen die we destijds bij de wetsbehandeling hebben besproken.

De **voorzitter**:
Dank u wel.