2
Vragenuur: Vragen Van Raak

Aan de orde is **het mondelinge vragenuur**, overeenkomstig artikel 136 van het Reglement van Orde.

Vragen van het lid Van Raak aan de minister van Justitie en Veiligheid over **het interne netwerk van honderden bedrijven en ministeries dat maandenlang wagenwijd openlag**.

De **voorzitter**:
Zoals elke dinsdag beginnen we met het mondelinge vragenuur. Vandaag beginnen we met de vraag van de heer Van Raak van de SP-fractie aan de minister van Justitie en Veiligheid, die ik ook van harte welkom heet. De vraag gaat over het interne netwerk van honderden bedrijven en ministeries dat maandenlang wagenwijd openlag. Het woord is aan de heer Van Raak namens de SP.

☐

De heer **Van Raak** (SP):
De voorzitter zegt het terecht: maandenlang stond de deur wagenwijd open bij belangrijke, vitale infrastructuur, omdat er een beveiligingslek was. Dat was zo bij Shell, bij Boskalis, bij defensiebedrijven, bij krantenbedrijven en bij luchtverkeersleiders. Je kon zó naar binnen. Je kon bestanden, wachtwoorden en gebruikersnamen gebruiken. Je kon je voordoen als een werknemer. Je kon gegevens manipuleren. Je kon bespioneren. Bij al dit soort bedrijven konden China, Rusland, Iran en Amerika zo naar binnen om hun spionagesoftware te plaatsen. Dat konden ze maandenlang, terwijl deze bedrijven daarvoor gewaarschuwd waren. Het enige wat ze hadden moeten doen, was het uitvoeren van een update om de beveiliging weer op orde te maken. Maar dat is niet gedaan. We kregen dat te horen via de Volkskrant. Later in het weekend kregen we via Reporter te horen dat er nog veel meer gevallen waren, waaronder scholen en zorginstellingen.

De eerste reactie van de minister, bij de NOS, was: als je als bedrijf of instelling niet in staat bent om een beveiligingsupdate te doen, dan ben je — ik citeer de minister — een ongelofelijke oliebol. Klopt het dat, zoals de Volkskrant schrijft, er ook op het ministerie van Justitie en Veiligheid maandenlang een lek is geweest, omdat het maandenlang de update niet heeft gedaan? Ik vraag de minister: vindt hij zichzelf ook een ongelofelijke oliebol? En hoe gaat hij ervoor zorgen dat organisaties bij dit soort vitale infrastructuur wél een update doen? Hoe kunnen we dat organiseren? Hoe kunnen we dat verzekeren in het kader van de nationale veiligheid?

De **voorzitter**:
Het woord is aan de minister van Justitie en Veiligheid.

☐

Minister **Grapperhaus**:
Voorzitter. Ik stel het zeer op prijs dat uw Kamer dit, via de heer Van Raak, aan de orde stelt. En daarmee bedoel ik de kwestie van de cybersecurity en niet zozeer, in de aanloop naar de jaarwisseling, de gebakskwestie. Maar daar kom ik ook op terug.

Het is juist dat, zoals de Volkskrant meldt, het interne netwerk van honderden organisaties in Nederland een aantal maanden een kwetsbaarheid had. Die kwetsbaarheid kwam voort uit het niet tijdig uitvoeren van beveiligingsupdates voor de zogenoemde virtual private network software van het bedrijf Pulse Secure. Ik leg heel kort uit wat virtual private network software is. Dat is eigenlijk software waarmee je geanonimiseerd verbinding kan maken met wifi. Het NCSC, het Nationaal Cyber Security Centrum, dat onder mijn verantwoordelijkheid valt, heeft op 15 april een advies uitgebracht waarin het heeft gewezen op die kwetsbaarheid. Het heeft ook de doelgroepen rijksoverheid en vitale-infrastructuurbedrijven actief daarover geïnformeerd. Op basis daarvan hebben organisaties updates kunnen uitvoeren. Op 21 augustus is dat eerste advies door het NCSC omgezet in het hoogste beveiligingsadvies. Daarna is dat ook door vrijwel alle JenV-organisaties opgepakt, maar ook bij JenV was er sprake van dat men achterliep op die beveiligingsupdate. Het advies van het NCSC heeft ertoe geleid dat alle instanties bij JenV uiteindelijk ook die updates hebben doorgevoerd.

Ik probeer het onderwerp cybersecurity zeer nadrukkelijk onder de aandacht te brengen. Daarom is het ook echt goed dat we hierover spreken. Dit onderwerp wordt onderschat. Het rapport van de WRR, de Wetenschappelijke Raad voor het Regeringsbeleid, zegt: er kan nu gewoon zonder meer iets gebeuren in de computersystemen waardoor er een duurzame maatschappelijke ontwrichting ontstaat. Het blijkt heel moeilijk om dat zodanig voor het voetlicht te brengen dat er een volledige alertheid bestaat op dit punt. En ik heb inderdaad aangegeven dat je, als je als reden opgeeft "we kunnen nu even geen update uitvoeren, want dan staat de productie stil", wat mij betreft een ongelofelijke oliebol bent. Je moet inderdaad aan de slag zo gauw als je die updates krijgt. Zeker als het NCSC je waarschuwt, moet je dat onmiddellijk oppakken.

Voorzitter, ten slotte. Ik heb vandaag gesproken met de CEO's, de hoogste bazen, van een aantal bedrijven, waaronder Schiphol en de Rabobank, om ook deze problematiek aan te horen. Daar kwam in ieder geval een aanvullend idee uit naar voren, namelijk om te kijken of we niet een soort ketenverantwoordelijkheid moeten maken, zoals nu al in de financiële sector geldt. Als je de eindgebruiker bent van een heel groot systeem, dan ben je er verantwoordelijk voor dat het goed werkt voor degenen die delen daarvan onder hun verantwoordelijkheid hebben. Terecht vraagt de heer Van Raak hier vandaag aandacht voor.

De heer **Van Raak** (SP):
We hebben het over energiebedrijven, we hebben het over defensiebedrijven en we hebben het over mediabedrijven, die dus maandenlang hun beveiliging niet op orde hadden en gewoon de deur open hadden staan voor spionage, kwaadwillendheid en manipulatie. Dat geldt dus ook voor het ministerie van Justitie en Veiligheid. Hoelang is het ministerie onderwerp geweest van oliebollerij? Hoelang heeft het geduurd voordat het gat gedicht is? We hebben iemand die waarschuwt, namelijk het Nationaal Cyber Security Centrum. Dat heeft in maart al gewaarschuwd. Alleen overheden en bedrijven hebben niets gedaan en zijn oliebollen geweest.

En dan is er ook een nationaal belang. Hoe komt het dat we deze beveiliging van vitale infrastructuur overlaten aan publieke belangen of ambtenaren die niet willen optreden? Waarom is het niet mogelijk om ervoor te zorgen dat het Nationaal Cyber Security Centrum bindend kan adviseren en dat er veel meer controle plaatsvindt? Waarom heeft de overheid bijvoorbeeld geen hackers in dienst om dit soort gaten op te sporen? Nu zijn we afhankelijk geweest van Matthijs Koot, die in zijn eigen tijd als beveiligingsexpert naar dit soort zaken heeft gezocht. Waarom worden er geen boetes uitgedeeld? Waarom hebben we geen toezichthouder die hier zelf naar op zoek kan gaan, vraag ik de minister.

Minister **Grapperhaus**:
Voordat ik daarop antwoord geef, wil ik toch enige nuance aanbrengen. Het is zo dat op 21 augustus dat hoogste beveiligingsadvies is afgekomen, want toen werd duidelijk dat de zogenaamde uitbuitingscode van die systemen openbaar beschikbaar zou komen. Toen is gezegd: nu moet men bij de bedrijven echt in de hoogste versnelling komen om dit aan te passen. Nu is het zo dat op dit moment de situatie is volgens de wet die we in deze Kamer een paar jaar geleden hebben aangenomen, namelijk de Wet beveiliging netwerken en informatiesystemen, de Wbni. In beginsel zet het NCSC als twee waarschuwingen niet helpen dit door naar het betrokken of verantwoordelijke ministerie en dat kan zogenaamde bestuursdwang opleggen.

Ik heb in de cybersecuritybrief van afgelopen zomer aan uw Kamer aangekondigd dat ik een studie doe naar de vraag of er geen centraal toezicht moet komen bij een aparte autoriteit. Eigenlijk is dat min of meer wat de heer Van Raak zegt: een soort autoriteit cyber security die voortaan doorzettingsmacht moet krijgen. Ik heb daar vandaag in een publicatie in een van de kranten over gezegd dat we er wel voor moeten oppassen dat het niet een soort A-Team wordt, want het moet nog wel binnen de verhoudingen van onze maatschappij. Ik deel dus het punt van de heer Van Raak dat we moeten gaan kijken naar een centrale autoriteit die op enig moment wel kan zeggen: nu gaan wij het zelf uitvoeren.

De heer **Van Raak** (SP):
Daar ben ik blij mee. De minister neemt het serieus en zegt sorry voor wat er gebeurd is op het ministerie. Ik ben blij dat er iemand komt die doorzettingsmacht heeft. Komt er ook iemand die onderzoek gaat doen naar die lekken? Anders blijft de nationale veiligheid in gevaar. Ik denk niet dat dat een zaak is die we aan bedrijven kunnen overlaten. Reporter heeft ook aangetoond dat op dit moment nog honderden bedrijven een beveiligingslek hebben, dus ondanks de waarschuwingen. In maart is het begonnen. In augustus is er alarm geslagen. Het geldt voor deze VPN-aanbieder. Het geldt ook voor andere. Honderden bedrijven hebben het lek nog niet op orde. Kan de minister aangeven welke bedrijven dat zijn en hoeveel bedrijven het zijn, of heeft hij dat helemaal niet in beeld?

Minister **Grapperhaus**:
Het NCSC, het Nationaal Cyber Security Centrum, heeft wel degelijk de mogelijkheid, verschillende vormen zelfs, om het internet te scannen op bepaalde kwetsbaarheden die zich voordoen. Die bevoegdheid en capaciteit heeft het NCSC. Daar moeten we zeker mee doorgaan. Dat zouden we moeten koppelen aan zo'n autoriteit die ik net beschreef. Volgens mij denkt de heer Van Raak daar zelf ook aan. U zult begrijpen dat ik om vertrouwelijkheidsredenen niet aan u kan melden welke concrete bedrijven met dit probleem hebben gekampt. Maar weet dat het NCSC daar juist bovenop zit. Dat heb ik net geschetst.

De **voorzitter**:
Dank u wel, meneer Van Raak.

De heer **Van Dam** (CDA):
Laat ik eerst eens doen wat de geachte collega Van Raak kennelijk niet over zijn lippen krijgt, namelijk de minister complimenteren omdat hij substantiële actie onderneemt op dit probleem. Dat is heel goed. Ik zou wel nog iets meer invulling willen krijgen van het volgende. Daarmee sluit ik graag aan bij collega Van Raak. Dit is enorm urgente problematiek. In de plannen van de minister lees ik dat het nog wel even gaat duren voordat er iets gebeurt. Welke mogelijkheden ziet hij om echt op heel korte termijn al maatregelen te nemen om dit soort dingen te voorkomen?

Minister **Grapperhaus**:
We hebben die Wbni. Voor de kijkers thuis: hij heette oorspronkelijk de cybersecuritywet. Maar deze wet is uiteindelijk omgedoopt tot Wbni. Die wet geeft juist mogelijkheden aan overheden, met name aan ministeries, om echt met zogenaamde bestuursdwang een bedrijf te dwingen om bepaalde ingrepen te doen. Ik constateer nu dat we hier heel eerlijk over moeten zijn. Als we cybersecurity echt serieus willen nemen en goed op orde willen krijgen, moeten we dit centraal gaan inregelen. In vervolg op de brief die ik van de zomer heb gestuurd, zal ik spoedig bij de Kamer terugkomen met een nader uitgewerkt plan. Dan kom ik ook terug op de gedachte, de vraag, die vanuit de bedrijven zelf komt, namelijk: waarom doet u niet iets met een soort ketenaansprakelijkheid?

Mevrouw **Özütok** (GroenLinks):
De vitale infrastructuur lag wagenwijd open. Er was geen whizzkid nodig om gebruik te maken van informatie en die in verkeerde handen te spelen. Het is wel belangrijk om na te gaan welke risico's er hier zijn gelopen en waarom er in april-mei geen actie is ondernomen.

Minister **Grapperhaus**:
De actie is ondernomen. Dat heb ik net beschreven in de eerste termijn van mijn beantwoording aan de heer Van Raak. Dat is ook de actie die we hebben beschreven in de wetgeving, de Wet bni. Dat proces moeten we met elkaar doorlopen. Ik zeg hier heel duidelijk: ik constateer dat er nog een ontbrekend element is. Dat is dat een onafhankelijke autoriteit op enig moment, na waarschuwingen, zou moeten kunnen zeggen: er gebeurt niets; wij zullen hierop door moeten pakken.

De heer **Verhoeven** (D66):
Ik ben blij dat de minister heel serieus is over dit onderwerp en spreekt over een centrale autoriteit. Maar het roept bij

mij toch ook wel een vraag op. We hebben namelijk het Nationaal Cyber Security Centrum. Dat is er om dit soort problemen tijdig op te sporen en bedrijven en overheidsorganisaties te waarschuwen. Dat heeft het ook gedaan. Alleen, heeft het voldoende mogelijkheden om die coördinerende rol te spelen? Je kunt de stap zetten naar een nieuwe autoriteit, maar we hebben een Nationaal Cyber Security Centrum. Dat moet dan misschien wat meer bevoegdheden krijgen, maar dat is misschien wel een veel logischere weg. Ik ben dus even op zoek naar waar de minister nu aan denkt.

Minister **Grapperhaus**:
Het is heel goed dat de heer Verhoeven dat punt hier echt even expliciet benoemt. Het gaat mij er niet om om weer een nieuw loket of iets dergelijks te maken. Waar het mij om gaat, is dat het NCSC geen doorzettingsmacht heeft. Dus ze kunnen niet tegen bedrijf X, een heel groot bedrijf dat een rol speelt in de vitale infrastructuur, zeggen: en nu gaat u het doen, u krijgt een aanzegging en anders komen we het over een maand voor u doen. Die bevoegdheid moet er komen. Ik wil er graag zeker ook met de heer Verhoeven als specialist over in gesprek of dat het NCSC zou moeten worden of dat we het elders moeten beleggen. In ieder geval moeten we dat goed gaan inrichten.

De **voorzitter**:
Tweede vraag van de heer Verhoeven.

De heer **Verhoeven** (D66):
Het is fijn dat we inderdaad kunnen gaan kijken naar hoe we dat precies gaan organiseren, op een manier die aansluit bij wat we al hebben in plaats van dat er weer iets nieuws komt.

Overigens, er is nog een andere suggestie die ik de minister zou willen doen. D66 en de VVD hebben een halfjaar geleden, denk ik, een motie ingediend met als oproep om de vitale infrastructuur in zijn volledigheid te scannen en de gaten snel te dichten. Ik krijg zo hier en daar het gevoel dat de minister daar nog niet zo heel veel prioriteit aan geeft. Ik zou hem nooit een oliebol noemen, maar ik zou het wel oliedom vinden als we daar niet werk van zouden maken. Het is gewoon een aangenomen Kamermotie die naadloos aansluit op hetgeen er afgelopen zaterdag in de Volkskrant stond.

Minister **Grapperhaus**:
Er ligt al een dergelijke scan van belangrijke delen van de vitale infrastructuur. Pijnlijk genoeg. Dat is het rapport van de Algemene Rekenkamer van maart over dit onderwerp. Naar aanleiding daarvan heb ik in mijn brief van deze zomer aan uw Kamer gezegd: ik denk dat de beste weg voorwaarts is dat die doorzettingsmacht er is. Die scan kan ik natuurlijk elke keer periodiek doen, maar het gaat erom — dat zegt het woord update al — dat die vitale systemen voortdurend bij de les blijven.

Mevrouw **Yeşilgöz-Zegerius** (VVD):
De minister gaf als antwoord op de vraag van de heer Van Raak aan dat het klopt dat er organisaties zijn geweest die achterliepen met de update. Dat vind ik een iets te vriendelijke formulering voor wat er echt aan de hand is, dat is namelijk dat systemen en netwerken wagenwijd openlagen voor kwaadwillenden. De minister zegt: als ze het dan zelf niet regelen, komen wij het wel doen. Daarbij wil ik de minister vragen of hij dan ook aandacht wil hebben voor bedrijven en mkb'ers die daarbij ondersteuning nodig hebben. Mag ik die opmerking van deze minister op deze manier verstaan en bedoelt hij dat ook zo? Ik zou ook heel graag een analyse willen — ik begrijp dat dit nu niet kan — van de risico's die we de afgelopen tijd hebben gelopen, onder andere bijvoorbeeld doordat het ministerie van Justitie en Veiligheid hiermee ook te maken had.

Minister **Grapperhaus**:
Een echte doorwrochte analyse, laat ik die toezeggen, want dan gaan we, denk ik, het beknopte gedeelte van dit debat nu te buiten. Ik denk wel dat het NCSC — dat is in ieder geval de opzet van de wet geweest — dit op tijd heeft gesignaleerd en ook tijdig dat hoogstebeveiligingsadvies heeft gegeven. Ik heb hier, voorzitter, juist om tegemoet te komen aan die kleine bedrijven, het cybersecurity woordenboek dat ik u graag zo dadelijk namens het NCSC en mijzelf zou willen overhandigen. Dat is vandaag uitgekomen en is een eerste stap op weg naar het voor iedereen toegankelijk maken van wat cybersecurity is, want alleen dán kunnen we iedereen die cybersecurity aanbieden.

De **voorzitter**:
Dank u wel.