3
Vragenuur

Vragenuur

Vragen Kathmann

Vragen van het lid Kathmann aan de staatssecretaris van Justitie en Veiligheid, bij afwezigheid van de minister van Justitie en Veiligheid, over **het bericht "Dag geen onderwijs op TU Eindhoven vanwege cyberaanval"**.

De **voorzitter**:
We gaan door met het volgende onderwerp. Daartoe heten wij de staatssecretaris van Justitie en Veiligheid van harte welkom; goed u weer te zien. Hij heeft een vraag van mevrouw Kathmann van de fractie van GroenLinks-PvdA. Ik geef graag het woord aan haar. Mevrouw Kathmann, ik heb u het woord gegeven. Als u er prijs op stelt, mag u bij de microfoon het een en ander zeggen. "Ik ga even hollen", hoor ik haar zeggen. Het woord is aan mevrouw Kathmann; wellicht buiten adem.

Mevrouw **Kathmann** (GroenLinks-PvdA):
Dank, voorzitter. "Get used to it." Dat was de boodschap van het kabinet bij het cyberincident afgelopen zomer. Dat klopt, want we zijn digitaal kwetsbaar. Maar dat betekent juist dat we niet achterover kunnen leunen, maar keihard aan de bak moeten. Vandaag is het de TU Eindhoven die getroffen wordt, maar morgen is het onze energievoorziening of zijn het onze operatiekamers.

Ik wil eerst even een hele dikke pluim geven aan iedereen, ICT'ers maar ook anderen, die nu keihard bezig is om het in Eindhoven op te lossen en vooral ook om erger te voorkomen. Dit roept wel een aantal vragen op.

Voorzitter. Het is heel belangrijk dat Nederland en vooral de vitale onderdelen van Nederland blijven doordraaien als er een storing is. Cyberexperts zeggen dat vooral de eerste 48 uur daarbij cruciaal zijn. 48 uur om je systeem weer aan de praat te krijgen of een back-up aan de praat te krijgen en 48 uur om analoog weer door te kunnen draaien, dus zonder al die digitale systemen. Denk bij het belang daarvan aan de haven van Rotterdam of aan onze operatiekamers. Is de staatssecretaris het met mij eens dat elke vitale sector zo'n 48 uursplan nodig heeft om het acute probleem op te lossen en systemen weer in de lucht te krijgen?

De **voorzitter**:
Het woord is aan de staatssecretaris, die de minister vervangt. Het woord is aan hem.

Staatssecretaris **Struycken**:
Voorzitter. Ik sta hier namens mijn collega Van Weel. De minister van Justitie en Veiligheid is de coördinerend bewindspersoon op het gebied van digitale weerbaarheid en vitale infrastructuur. Hij is daar uiteraard samen met het hele kabinet verantwoordelijk voor. Wij zijn allemaal verantwoordelijk voor de digitale weerbaarheid van de eigen sectoren in onze portefeuilles en in zijn totaliteit. Verder zijn organisaties in Nederland primair verantwoordelijk voor hun eigen beveiliging van de ICT-systemen.

De Technische Universiteit Eindhoven is zaterdagavond geraakt door een cyberaanval. Zij hebben die avond besloten preventief alle systemen offline te halen. Dit hebben ze zondag naar buiten gecommuniceerd. Zoals bekend kunnen medewerkers en studenten hierdoor tot op heden niet in hun systemen. De Technische Universiteit Eindhoven is een onderzoek gestart naar dit incident. Dit onderzoek loopt nog.

Voorzitter. Ik val mevrouw Kathmann gaarne bij daar waar zij een pluim uitdeelt aan de mensen die hard aan het werk zijn. Ik deel haar analyse dat het cruciaal is om snel en adequaat te acteren in de eerste uren en daar ook adequaat over te communiceren. Wat dat betreft is er een duidelijke verantwoordelijkheid die rust op iedereen.

Het incident past binnen het beeld van een toenemende cyberdreiging. Daarom neemt het kabinet meerdere maatregelen om de cyberweerbaarheid van Nederland te verhogen. Onderdeel van deze aanpak is de implementatie van de NIS2-richtlijn in de ontwerp-cyberbeveiligingswet. Met deze wet worden 10.000 entiteiten in Nederland in heel veel sectoren, zoals de zorg, de overheid en de voedselindustrie, verplicht tot het nemen van cyberbeveiligingsmaatregelen. Dat omvat dus mede maatregelen die zien op de eerste 48 uur waar mevrouw Kathmann over sprak.

Onder de Cyberbeveiligingswet is het ook mogelijk om een aanval op te nemen op de rijksoverheid en de decentrale overheid en overigens ook op hogeronderwijsinstellingen.

Mevrouw **Kathmann** (GroenLinks-PvdA):
Ik hoor eigenlijk niet een begin van een antwoord. Ik heb gewoon een hele duidelijke vraag gesteld, namelijk: vindt deze staatssecretaris dat wij voor alle vitale delen van onze samenleving een 48 uursplan moeten hebben? Specifiek 48 uur om de systemen weer op orde te krijgen of de back-up aan de praat te krijgen en 48 uur om analoog door te kunnen draaien. De vitale delen van onze samenleving dus. Ja of nee?

Staatssecretaris **Struycken**:
Ja. Mevrouw Chakor en mevrouw Kathmann hebben daar in hun motie van 11 december 2024 aandacht voor gevraagd. Zij hebben de regering verzocht om samen met overheden en vitale sectoren plannen te ontwikkelen om die essentiële dienstverleningen in geval van een grote storing zo veel mogelijk in stand te houden. Ik neem zo maar aan dat die juist ook zien op die 48 uur. Deze motie is door het kabinet overgenomen. Daarmee wordt dit zonder meer onderdeel van het kabinetsbeleid.

Mevrouw **Kathmann** (GroenLinks-PvdA):
Ik ben heel blij dat de staatssecretaris nu zelf even op die motie terugkomt, want ik was heel even bang dat ik het moest doen met zijn woorden "iedereen staat eigenlijk zelf aan de lat voor zijn veiligheid". Wij hier en dit kabinet staan ook aan de lat voor de vitale sectoren van Nederland, zodat die door kunnen draaien. Ik wil dit kabinet ook een compliment geven. Het heeft meer geld uitgetrokken voor cyber-

security. Maar daarmee zijn we er niet, want ondertussen zijn er ongelofelijk veel vitale sectoren, zoals de zorg en het onderwijs — dat valt trouwens niet eens onder die vitale sectoren; alleen het hoger onderwijs valt daaronder — die keihard getroffen worden door bezuinigingen, dus ook door bezuinigingen in die cybersecurity. Wat gaat dit kabinet hieraan doen? Dit is namelijk de vierde bewindspersoon waarmee ik het moet doen. Ik word van het kastje naar de muur gestuurd. Moet ik het wat betreft cyberveiligheid met JenV doen? Moet ik het met de staatssecretaris Digitalisering doen? Moet ik het nu met de minister van Onderwijs doen? Er is geen integraal plan. Wanneer gaat dat er wel komen? Ik zou heel graag van deze minister horen dat dat voor de zomer is.

Staatssecretaris **Struycken**:
Mevrouw Kathmann stelde: ik was bang dat de verplichting bij ons allemaal ligt. Maar ik moet u zeggen dat de verplichting bij ons allemaal rust, niet alleen bij bedrijven en instellingen in de vitale sector, maar werkelijk bij ons allemaal: bij burgers, bij bedrijven, bij instellingen. Wij hebben allemaal, ieder voor zich, een verantwoordelijkheid, een taak, om te zorgen voor onze cyberveiligheid. Dat geldt ook als ik thuis mijn password niet verander. Dat gaat weliswaar niet over een vitale sector, maar er is wel een verantwoordelijkheid, wel een taak. Als we ons daarvan bewust worden in Nederland — dat is het doel van dit kabinet — dan zijn wij allemaal zorgzamer en dan werkt dat vanzelf door in een algemeen veiliger beleid en kader voor onze cyberveiligheid. Ook voor instellingen in de vitale sector betekent dat wel dat er keuzes gemaakt moeten worden. Het doel van dit kabinet is mede om heel duidelijk te maken dat cyberveiligheid een verantwoordelijkheid is die een kernprioriteit is, niet een sluitpost. In het aanwenden van mensen en middelen zal die prioritering moeten doorklinken.

Mevrouw **Kathmann** (GroenLinks-PvdA):
Ik wil nog heel even een correctie maken. Ik zei namelijk juist dat ik bang was dat ik het met de woorden moest doen dat allemaal Nederlanders zelf aan de lat staan voor de cyberveiligheid van dit land. Dat is wat ik zei. Ik zei niet datgene wat de staatssecretaris net herhaalde: dat ik bang ben dat we hier in Den Haag verantwoordelijkheid moeten pakken. Dat is nou juist de reden waarom ik hier sta. Ik had weer een hele concrete vraag waarop ik nog geen begin van een antwoord heb gekregen. Die vraag is: ligt er een integraal plan waarmee we erop kunnen rekenen dat we in Nederland binnen 48 uur in de vitale sectoren a goed kunnen acteren op het weer aan de praat krijgen van de systemen of de back-ups en b analoog kunnen doordraaien? Denk aan de haven van Rotterdam, aan operatiekamers en aan onze energievoorziening. Dat zijn hele concrete vragen. Daar zou ik heel graag antwoord op willen hebben.

Staatssecretaris **Struycken**:
Nationaal zet het kabinet zich in met de Nederlandse Cybersecuritystrategie 2022-2028. Deze staat ook wel bekend als de NLCS. Daarnaast is er sprake van de implementatie van de Cyberbeveiligingswet op basis van de Europese richtlijn. Het conceptontwerp hiervan zal in de komende maanden naar uw Kamer worden gestuurd. Er wordt gewerkt aan één centrale cybersecurityorganisatie, die alle organisaties in Nederland informeert over dreigingen en beveiligingsmaatregelen. Er wordt ook gebouwd aan een cyberweerbaarheidsnetwerk met het doel om alle publieke en private organisaties in Nederland in staat te stellen om het cyberweerbaarheidsniveau te verhogen en gecoördineerd samen te werken. Dat zijn allemaal maatregelen die gaande zijn. Ik heb er geen twijfel over dat het kabinet uw Kamer nader zal informeren over de te nemen maatregelen in het commissiedebat op 5 februari aanstaande dat gaat over onlineveiligheid en cybersecurity.

Mevrouw **Kathmann** (GroenLinks-PvdA):
Dat is wéér geen antwoord op mijn vraag. Ik refereerde eerder ook al aan een aangenomen voorstel van GroenLinks-Partij van de Arbeid om ervoor te zorgen dat er in ieder geval analoge plannen liggen ten aanzien van de vitale sectoren. Cyberspecialisten zeggen dat die 48 uur cruciaal zijn. We moeten voor een deel gewoon kunnen doordraaien. De dreiging is heel realistisch. Kan de staatssecretaris toezeggen dat er voor de zomer een integraal plan ligt waarin die 48 uur worden ingevuld? Nogmaals, dan hebben we tijd om die systemen goed aan de praat te krijgen en kunnen we analoog doordraaien. Dat is gewoon een heel simpele vraag, en ik heb nog geen begin van een antwoord gehoord.

Staatssecretaris **Struycken**:
De minister van Justitie en Veiligheid zal daarop terugkomen in het commissiedebat van 5 februari aanstaande.

De heer **Six Dijkstra** (NSC):
Mijn vraag aan de staatssecretaris is de volgende. Die Cyberbeveiligingswet komt eraan. Het hoger onderwijs moet daardoor digitaal weerbaarder worden. Tegelijkertijd is het natuurlijk nog een grote opgave om daar te komen. Heeft hij of zijn collega inzichtelijk wat de huidige stand is van de cyberweerbaarheid van het hele hoger onderwijs? Want op papier helpt zo'n wet, maar in de praktijk moeten al die maatregelen wel getroffen worden.

Staatssecretaris **Struycken**:
Wat het onderwijs betreft is er een gesprek gaande tussen het ministerie van Justitie en Veiligheid en het ministerie van OCW. De essentie van dat gesprek is dat in kaart wordt gebracht wat thans allemaal al gebeurt en eventueel welke additionele maatregelen nodig zijn, mede in verband met de te maken keuze of het onderwijs komt te vallen onder de cyberveiligheidswet. Die inventarisatie wordt gemaakt. Ik kan niet bevestigen of ontkennen dat er op dit moment voldoende maatregelen zijn getroffen.

De heer **Ceder** (ChristenUnie):
Dit is niet de eerste keer dat er een cyberaanval plaatsvindt op een universiteit. In 2019 hebben we bijvoorbeeld de aanval op de universiteit van Maastricht gehad. Daarna heeft de onderwijsinspectie daar onderzoek naar gedaan, maar die heeft met name onderzoek gedaan naar het wanbeheer van het bestuur van de universiteit en niet per se naar het veiligheidsvraagstuk. Mijn vragen zijn als volgt. Welke instantie of bevoegdheid gaat onderzoek doen naar hoe dit heeft kunnen gebeuren? Wat is de veiligheidsimpact? Hoe kunnen we zien of de aanbevelingen van toen nu opgevolgd zijn door de universiteit van Eindhoven?

Staatssecretaris **Struycken**:
Voor zover ik weet, is in het geheel nog niet duidelijk wat er precies aan de hand is in Eindhoven. Dat onderzoek loopt nog en daarmee ook de vaststelling of er tekortgeschoten is door deze of gene. Ik kan wel in algemene zin zeggen dat met het van kracht worden van de Cyberbeveiligingswet ter uitvoering van de NIS2 er ook een duidelijke rol komt te liggen voor bestuurders. Bestuurders worden zelf medeverantwoordelijk voor het nemen van maatregelen op het vlak van cyberweerbaarheid. Zij moeten er toezicht op houden en zij moeten een opleiding volgen om dat toezicht adequaat te kunnen uitvoeren.

De **voorzitter**:
Heel goed. Tot zover dit onderwerp. Dank aan de staatssecretaris. Wij zijn in afwachting van de minister van Onderwijs, Cultuur en Wetenschap. Ik schors een enkel ogenblik totdat hij zijn opwachting maakt.

De vergadering wordt enkele ogenblikken geschorst.