4
Vragenuur: Vragen Verhoeven

Vragen van het lid Verhoeven aan de minister van Justitie en Veiligheid over **het beveiligingslek in Citrixsoftware**.

De **voorzitter**:
Dan geef ik nu het woord aan de heer Verhoeven namens D66 voor zijn vraag over het beveiligingslek in Citrixsoftware. De vraag wordt gesteld aan de minister van Justitie en Veiligheid.

De heer **Verhoeven** (D66):
Voorzitter, dank u wel. Het decennium is weer digitaal begonnen, mag ik wel zeggen. Ik ben heel blij dat wij als Tweede Kamer een commissie Digitale toekomst hebben ingesteld.

Voorzitter. De universiteit van Maastricht werd getroffen door een ransomware-aanval. Studenten en docenten konden niet bij hun data. Een man werd opgepakt met 12 miljard inlognamen. Na het Medisch Centrum Leeuwarden en de gemeente Zutphen zijn er nu honderden bedrijven, instellingen en andere organisaties getroffen door de fout in de Citrixsoftware. Deze fout bleek al in december. Er was nog geen update, geen patch, geen "pleister", zoals dat heet, maar wel een tijdelijke oplossing. Die zou veilig zijn. Maar afgelopen vrijdag riep het Nationaal Cyber Security Centrum, het NCSC, op, op basis van informatie van de AIVD, om Citrix helemaal uit te zetten.

Dat klinkt eenvoudig en overzichtelijk, maar dat is het niet, want voor veel organisaties is Citrix helemaal niet probleemloos uit te zetten. Het hangt ook af van de specifieke versie die je hebt of er nu al een oplossing is. Medewerkers van bedrijven, ambtenaren van gemeenten en ministeries, Tweede Kamerleden en bewindspersonen kunnen allemaal niet op afstand inloggen. Ze kunnen niet via hun telefoon hun mailbox bekijken. Thuiswerken is niet mogelijk. Er zijn te weinig flexwerkplekken. Er is economische schade. Er staan zelfs Citrixfiles!

Enige maanden geleden stonden wij hier ook. Toen noemde de minister van Justitie en Veiligheid elk bedrijf dat zijn digitale beveiliging niet op orde heeft, een "ongelofelijke oliebol". Heeft de minister het allemaal zelf wel op orde, vraag ik me nu af. De eerste vraag die ik hem daarom stel is: is de minister van Justitie en Veiligheid nu zelf een ongelofelijke oliebol? En zo nee, waarom niet?

De **voorzitter**:
Nou.

De heer **Verhoeven** (D66):
Ja, voorzitter, het zijn zijn eigen woorden.

Minister **Grapperhaus**:
Voorzitter. Nou heb ik aangegeven dat het kabinet een grote stap gaat zetten op het vuurwerkdossier, maar nu begrijp ik dat de heer Verhoeven kennelijk ook de oliebollen wil aanpakken. Het wordt dus wel een steeds soberder jaarwisseling, als ik het goed begrijp.

Voorzitter. Als het gaat om het goed monitoren van wat er aan dingen gebeurt in de digitale wereld van de rijksoverheid en de vitale infrastructuur, hebben onze overheidsdiensten de afgelopen jaren zeer grote stappen gemaakt. Ik wil dat niet op mijzelf laten afstralen. Ik wil natuurlijk graag aan het eind van deze kabinetsrit ook niet als oliebol worden beoordeeld door de heer Verhoeven. Ik ga zo wat meer uitleggen over de afgelopen weken, maar het is wel saillant dat enkele overheden van grote bevriende naties het compliment hebben gemaakt dat het NCSC, de NCTV, maar ook de rijks-CIO, de Chief Information Officer voor het Rijk, in hun handelen aanzienlijk voorliepen op wat er in andere landen aan actie werd ondernomen.

Dan nog moeten we ons echt realiseren — de Wetenschappelijke Raad voor het Regeringsbeleid heeft daar in augustus een toch echt heel belangrijk advies over uitgebracht dat wij eerder ook in de vaste Kamercommissie bespraken — dat het er niet om gaat óf er iets in de digitale wereld zal leiden tot een maatschappelijke ontwrichting, maar dat dat gáát gebeuren, aldus de WRR, gezien de afhankelijkheid die we in onze samenleving in grote mate hebben van onze computersystemen en digitale technologie.

Hoe is het hier gegaan? Op 17 december vorig jaar, dus 17 december 2019, werd bekend dat er een zogenaamde kwetsbaarheid was in de Citrixsystemen. Zo snel mogelijk daarna heeft het NCSC een waarschuwing daarover uit doen gaan. Vanaf het begin was duidelijk dat Citrix nog geen sluitende oplossing kon aanbieden. Die sluitende oplossing is wat de heer Verhoeven de patch noemt. Er werden wel tussentijdse veiligheidsmaatregelen door Citrix aangeboden. Maar op 24 september constateerde het NCSC (Nationaal Cyber Security Centrum) dat het nodig was om de waarschuwing te verhogen naar high-high — dat is echt de hoogste waarschuwingsgraad — op basis van technische analyses. Ik benadruk dat het NCSC daarbij aan de ene kant voortdurend heeft gekeken naar wat er uit internationaal overleg met experts naar voren kwam en aan de andere kant adviezen heeft gegeven over wat rijksoverheid en vitale partijen konden doen. Die situatie is voortdurend gemonitord. Er is steeds gekeken of de mitigerende tussentijdse maatregelen van Citrix afdoende waren en of er op dat moment niet meer nodig was.

Op 9 januari jongstleden kwam er een zogeheten exploit uit, niet te verwarren met het exploot, dat een deurwaarder uitbrengt. Een exploit is een Engelse term. Dat is eigenlijk een programma waarmee het lek kan worden misbruikt en dat in kringen van verkeerde hackers wordt bekendgemaakt. Die volgen de diensten. Toen dat duidelijk werd, heeft het NCSC het advies geactualiseerd en is men organisaties binnen Rijk en Vitaal actief gaan adviseren. Nog steeds blijven ze bezien of de maatregelen die zijn getroffen afdoende zijn.

Op 16 januari —- dat was afgelopen donderdag — was er nog steeds geen sluitende oplossing van Citrix, geen patch dus. Daarnaast ontstond er ook nog eens twijfel onder de experts over de houdbaarheid van de tussentijdse mitigerende maatregelen van Citrix, want inmiddels waren we twee weken verder. Dat is aanleiding geweest voor het NCSC om donderdagavond jongstleden te adviseren: overweeg uw Citrixservers uit te zetten. Dat was voor de NCTV (Nationaal Coördinator Terrorismebestrijding en Veiligheid) aanleiding om interdepartementaal op te schalen.

Vervolgens is er op vrijdag 17 januari nog een beveiligingsadvies van de AIVD gekomen voor de rijksoverheid. Diezelfde dag heb ik met mijn collega Knops van BZK namens het kabinet de zware afweging gemaakt: hoe verder? Want dat zou, zoals de heer Verhoeven zeer terecht zegt, echt een forse stap betekenen. Wij hebben besloten het advies te verzwaren en ook tot actie over te gaan. Onder coördinatie van de CIO Rijk en het NCSC is toen geadviseerd: zet uw Citrixservers uit, tenzij u laat zien en motiveert welke grondige extra maatregelen u …

De **voorzitter**:
Ja.

Minister **Grapperhaus**:
… en waarom die afdoende zijn. Ik ben er bijna, voorzitter. Het is toch goed om het even af te maken.

De **voorzitter**:
Jazeker.

Minister **Grapperhaus**:
De afgelopen dagen is daar voortdurend contact over geweest met alle betrokken organisaties bij Rijk en Vitaal, inclusief het gehele weekend. Het beeld is dat er inmiddels voor 50% van de gebruikers in Nederland patches vanuit Citrix beschikbaar zijn. Citrix heeft gezegd dat vrijdag deze week de resterende patches beschikbaar komen. Het NCSC onderzoekt en blijft onderzoeken wat de kwaliteit is van die patches, en blijft ook met de NCTV monitoren of er nog eventueel bijkomende problemen zouden zijn. Donderdag aanstaande, zo is door mij aangeboden, geven wij een briefing aan uw experts op Binnenlandse Zaken en op Justitie en Veiligheid. Daar heeft uw Kamer gelukkig gebruik van gemaakt.

Ik wil toch afsluiten met het volgende, voorzitter. Ik heb dit al vaak gezegd en ik geef het toe, de vraagsteller ook, dus daar vinden wij elkaar zonder meer in, al dan niet in de gebakkraam: onze digitale veiligheid staat voortdurend onder druk. De WRR zegt: het is niet een kwestie óf het gebeurt, maar je moet voorbereid zijn áls het gebeurt. We zullen natuurlijk ook gaan evalueren hoe het hier gegaan is: hebben we dat goed aangepakt? Ook zullen we kijken wat de implicaties zijn voor het cyberbeleid. Ik zeg nu vast toe dat ik dat meteen meeneem in de brief aan uw Kamer — die is aangekondigd voor maart — over de beleidsreactie op dat WRR-rapport.

De heer **Verhoeven** (D66):
Ik waardeer dit feitenrelaas en deze uitgebreide toelichting. Het is bijna een minicollege cybersecurity geworden. Dat waardeer ik ook. Ik heb nog een paar korte vragen over de situatie van nu. Ook daarna wil ik nog een paar algemenere vragen over cybersecurity stellen. Ik heb nu toch graag wat concrete antwoorden.

Wat zijn de geschatte kosten van dit incident? Kan de minister daar al iets over zeggen? Is de nationale veiligheid in gevaar geweest? Welke maatregelen zijn er nu getroffen? Daar heeft de minister het meeste al over gezegd, denk ik. Wanneer zijn alle mensen weer in de gelegenheid om Citrix te gebruiken? Dus wanneer komt de laatste patch van de versies die nu nog niet zijn gedekt? Die vragen zou ik toch nog willen stellen. En hoe voorkomen we in de tussentijd, de komende dagen, dat ministers, Kamerleden en ambtenaren gaan werken met een onveilig privémailadres, zoals in de vorige regeerperiode gedaan is door minister Kamp van Economische Zaken? Straks heb ik nog een paar algemene vragen, voorzitter.

De **voorzitter**:
Eerst de specifieke vragen.

Minister **Grapperhaus**:
Over de geschatte kosten kan en wil ik nu nog niets zeggen. Het moge duidelijk zijn dat dit inderdaad een schadepost oplevert; daar moeten we heel duidelijk over zijn. Maar het allerbelangrijkste is — dat moet de Kamer ook van mij verwachten — dat de onder mij ressorterende diensten samen met de onder BZK ressorterende diensten alert en actief in zo'n crisis optreden en natuurlijk geen maatregelen nemen die onnodig schade en kosten opleveren. Dat is ook de reden geweest — dat mag u best weten — dat Knops en ik vrijdag een echt uitgebreid overleg hebben gehad, dat zich tot het begin van de avond uitstrekte, om die zeer ingrijpende stap te zetten.

De nationale veiligheid kan altijd in dit soort situaties een keer in het geding komen, maar het is natuurlijk wel zo dat wij daar ook, samen met de diensten, proactief zo veel mogelijk op handelen. Meer kan ik daar in dit stadium niet over zeggen. Ik wil daar best nog wel iets meer over zeggen, maar niet in dit gremium.

Dan is er gevraagd welke maatregelen er zijn genomen. De heer Verhoeven heeft gezegd dat ik daar al iets over had gezegd. Ik wil het ietwat expliciteren. Wij hebben de Engelse uitdrukking "comply or explain" gebruikt. Dat betekent: zet al je apparatuur van Citrix uit, tenzij je overtuigend aan de rijks-CIO dan wel het NCSC dan wel het daartoe bevoegde sectorale Computer Emergency Response Team, dat we allemaal hebben ingesteld, laat zien dat je extra veiligheidsmaatregelen hebt getroffen en dat je ook niet in de contaminatie zit.

De laatste versie van die patch heeft Citrix voor eind van de week aangekondigd, maar daarvoor moet ik dus even afgaan op wat Citrix daarvan zegt.

Hoe voorkomen we in de tussentijd onveilig privé mailen? Bij de afweging die organisaties maken, hoort uiteraard ook dat men een afweging maakt omtrent de vraag hoe

men met het eigen verkeer verdergaat. Er zijn organisaties die vooral getroffen zijn op het gebied van thuiswerken en, zoals u in de krant heeft kunnen lezen, zeggen: mensen moeten gewoon naar kantoor komen, met alle fricties die dat met zich meebrengt.

Dit waren de bijzondere vragen.

De heer **Verhoeven** (D66):
Tot slot, want dit geval staat niet op zichzelf. Ik noemde net al een aantal andere problemen. Want er zijn natuurlijk ook wel een aantal andere stappen nodig, waar ik al vaker vragen over heb gesteld aan de minister. Het Nationaal Cyber Security Centrum zou meer moeten kunnen doen in dit soort situaties. Een oproep en breed gesteund voorstel van D66 is de mogelijkheid tot het scannen van de vitale infrastructuur. Wanneer gaat de minister daar nu werk van maken? Het breder delen van informatie door het Nationaal Cyber Security Centrum — een oproep van het bedrijfsleven — is nog niet geregeld. Ook voor een stevige doorzettingsmacht tegen alle onderdelen van de vitale infrastructuur — dan heb ik het over de banken, elektriciteit, telecom — zou het Nationaal Cyber Security Centrum meer geld en meer bevoegdheden moeten krijgen. Wanneer gaat de minister daar werk van maken?

De tweede vraag is wanneer we een wettelijke verplichting voor het doorvoeren van dit soort updates gaan organiseren. De minister heeft daar al eens over gesproken, maar ik heb nog geen concrete voorstellen gezien.

En wanneer gaat de overheid serieus investeren in cybersecurity? De minister heeft toegezegd dat er een onderzoek komt naar wat nodig is om Nederland digitaal veilig te maken. Ik ben heel benieuwd wat daar de bevindingen van zijn en wanneer we daar resultaat van kunnen verwachten. Ik hoor het graag. Het zijn serieuze en prangende vragen.

De minister zei het al: de nieuwjaarsrecepties lopen nu zo langzamerhand op een einde. Ik ga graag een keer met de minister naar een gebakskraam, maar het laatste waar Nederland op zit te wachten is een ongelofelijke oliebol op het ministerie van Justitie en Veiligheid. Dus ik hoop dat de minister mij gerust kan stellen.

Dank u wel.

Minister **Grapperhaus**:
Ik heb de nieuwjaarsrecepties volledig gemist, zowel in mijn betoog als vorige week, want toen was ik aan het werk op de eilanden.

De heer **Verhoeven** (D66):
Ik zei: in het land.

Minister **Grapperhaus**:
Ah, ja. Maar voor alle duidelijkheid: deze punten hebben wij in ieder geval in het algemeen overleg van begin november aan de orde gehad. Ik heb toen ook aangegeven dat ik daar in de beleidsreactie op het WRR-rapport uitvoerig op wil terugkomen, op alle drie de punten. Het is natuurlijk heel triest, maar deze gang van zaken, maar ook het incident in Maastricht, geeft heel duidelijk aan dat dit iets is waar we als samenleving, parlement en kabinet nu echt heel erg iets mee moeten. Maar ik kom op die punten terug in mijn beleidsreactiebrief. Dan heb ik, denk ik, al die punten behandeld.

De heer **Verhoeven** (D66):
Dank u wel.

De **voorzitter**:
Ik ben benieuwd waar de commissie digitalisering mee komt, meneer Verhoeven. Dank u wel. Dan ga ik naar de heer Van Dam namens het CDA.

De heer **Van Dam** (CDA):
Met alle waardering voor alle mensen die zich hier achter de schermen al weken mee bezighouden, maar toch snap ik het niet helemaal. Op 17 december zou bekend zijn geworden dat er een Citrixprobleem was. Ik heb nog eens gekeken, maar dat was al op 6 december bekend. Dan duurt het per saldo tot 17 januari tot de overheid Citrix uitzet, hoewel er in de tussentijd op 24 december nog een kwalificatie van een high-highrisico is gegeven. Dat betekent dat op z'n minst in de periode van 17 december tot 17 januari de deur open heeft gestaan. Daar maak ik mij zorgen over. Want wie is er door die deur binnengekomen zonder dat we dat zien? Ik hoef de minister niet uit te leggen — dat legt hij normaal aan ons uit — welke risico's daaraan verbonden zijn. Zou de minister nog eens in kunnen gaan op de vraag waarom het zo lang heeft moeten duren voordat die forse maatregelen genomen zijn?

Minister **Grapperhaus**:
In de eerste plaats is het niet zo dat de deur vanaf enig moment heeft opengestaan. Daar zijn nou juist die zogenoemde mitigerende maatregelen voor geadviseerd. Daar is ook heel duidelijk contact over geweest met de instanties en diensten die het betrof. Ik heb ook al aangegeven dat het niet zo is dat men tussen 24 december en 9 januari stil heeft gezeten. Integendeel, er is toen aan de ene kant voortdurend geüpdatet om te kijken of de mitigerende maatregelen nog steeds voldoende leken. Aan de andere kant is natuurlijk ook gekeken wat er vanuit Citrix aan patches kon worden waargemaakt. Ik zou verder willen verwijzen naar de technische briefing. Voordat we nou tot de conclusies gaan springen, zoals hier toch een beetje gebeurt, denk ik namelijk dat het het beste is dat uw Kamer daar en detail van de zaken kennisneemt.

Mevrouw **Buitenweg** (GroenLinks):
Ik zou het fijn vinden om voorafgaand aan die technische briefing al een feitenrelaas te hebben. De minister noemt al heel veel zaken, maar ik wil daar bijvoorbeeld ook bij hebben vanaf wanneer Citrix het al zelf wist, voordat het verder vermeld werd? Ik begrijp zelf het volgende niet, en sluit me wat dat betreft aan bij onder anderen de heer Van Dam. Het Nationaal Cyber Security Centrum heeft ten minste al op 14 januari gezegd dat de dreiging 9,8 is op een schaal van 10. 9,8 op een schaal van 10! Dat is inderdaad high-high. Ik bedoel, je kan er bijna niet meer overheen.

Dat was dus drie dagen voordat de minister het advies gaf om de systemen uit te zetten, en dat baart me zorgen. Want als het zo hoog is — 9,8 op een schaal van 10 — waarom is daartoe dan niet eerder besloten? Was dat misschien omdat we toch geen terugvalopties hadden? De minister zegt wel steeds dat het WRR-rapport hartstikke belangrijk is, maar dat betekent dat we voorbereid moeten zijn. Waarom is niet gelijk toen het 9,8 was, gezegd dat de systemen uitgeschakeld moesten worden?

Minister **Grapperhaus**:
Het Nationaal Cyber Security Centrum monitort en heeft op 16 januari het advies gegeven dat organisaties moesten overwegen om af te koppelen. Daar ben ik uiteindelijk verantwoordelijk voor, maar dat dat is in de handen gelegd van het Nationaal Cyber Security Centrum. Ik vind het prima om daarover nog voor donderdag een feitenrelaas op een rij te zetten. Overigens zit dat in grote lijnen ook al in de brief die gisteren naar uw Kamer is gestuurd.

De **voorzitter**:
Goed, dan ga ik naar de heer Middendorp. Nee, sorry, de heer Van der Staaij, namens de SGP.

De heer **Van der Staaij** (SGP):
Tegen het eind van het jaar pleeg ik behalve oliebollen ook appelflappen te kopen, want dan heb je, als die oliebollen tegenvallen, nog iets anders in handen. Toegepast op waar we het vandaag over hebben, vraag ik me af of er wel voldoende geïnvesteerd wordt in werkbare terugvalopties. Dat is toch wel een vraag die bij mij steeds boven komt drijven bij alle digitale kwetsbaarheid. Bij elektriciteit hadden we op een gegeven moment een systeem van noodaggregaten. Hier is het een slagje ingewikkelder, maar wordt daar voldoende werk van gemaakt?

Minister **Grapperhaus**:
Zeker omdat het woord "voldoende" in deze vraag staat, vind het wat vergaand om daarover hier een oordeel uit te spreken. Maar ik wil best toezeggen om daarop terug te komen als we die evaluatie gedaan hebben. Waar de WRR en overigens ook de NCTV regelmatig voor heeft gewaarschuwd, is het feit dat we hoe dan ook, dus ook in onze terugvalopties, te afhankelijk zijn van alle digitale technologie, om het zo maar te zeggen. Vaak zijn er geen analoge terugvalopties. Dit is echt iets voor de technische briefing, maar dit is ook iets wat speelt als bijvoorbeeld een instantie die ermee geconfronteerd wordt dat er iemand in de systemen is gekomen, merkt dat niet alleen die systemen zelf maar ook de back-ups daarvan besmet zijn. Dan is je terugvaloptie geen terugvaloptie meer. Maar ik wil hierbij toch echt verwijzen naar de technische briefing, met de toezegging dat ik daarop terugkom in het kader van de evaluatie, waarin we natuurlijk ook naar dit aspect gaan kijken.

De heer **Middendorp** (VVD):
Er is net gesproken over pleisters. Ik heb ook veel gehoord over monitoren en adviseren. Ik denk dat daar goed werk wordt gedaan, maar de minister heeft rond de zomer ook gezegd: eigenlijk zou ik het liefst zelf gaan kijken bij die bedrijven die de informatieveiligheid niet op orde hebben. Daar gaat mijn vraag over. Wordt er gekeken op al die verschillende ministeries die hiermee geconfronteerd zijn? Is de minister dat van plan, of wordt dat nu al gedaan? En ten tweede: is het niet ook zaak om te gaan kijken in Amerika, waar de leverancier van deze software zit? Er zijn voorbeelden waarin de Staat zich vrij stevig heeft opgesteld richting leveranciers. Daar is misschien ook een rol weggelegd voor deze daadkrachtige minister.

Minister **Grapperhaus**:
Naar aanleiding van een incident zoals het zich hier afspeelt, zal het NCSC zeker ook, als er een sluitende oplossing is gevonden, in het kader van de evaluatie ter plekke in gesprek moeten gaan met de leverancier. Daar heeft de heer Middendorp zonder meer een zeer terecht punt. Ik heb dit van de zomer inderdaad aangegeven in een debat dat we hierover hadden. Het lastige is dat daarbij natuurlijk het probleem speelt dat we het er maatschappelijk met elkaar over eens moeten zijn dat instanties als het NCSC daartoe de bevoegdheid moeten hebben; u heeft er immers niks aan als ik zelf ga kijken. Dat is het punt dat de heer Verhoeven terecht maakt en waar ik in de beleidsreactie op terugkom. Moeten we hier in het kader van wetgeving niet op enig moment gewoon verplichtingen opleggen? Tot nu toe was de maatschappelijke opvatting niet zo.

De **voorzitter**:
De heer Middendorp, tweede vraag.

De heer **Middendorp** (VVD):
Ja, dat begrijp ik, maar een daadkrachtige minister gaat helpen op de ministeries, want er is een heel groot verschil tussen de bedrijven waar het toen, rond de zomer, over ging en onze eigen infrastructuur, namelijk die van de rijksoverheid en dit huis. Ik ben blij dat de minister naar Amerika gaat, maar ik hoor alleen maar "monitoren" en "adviseren". Ik ben ook op zoek naar wat er gedaan wordt om de verschillende rijksoverheidsinstellingen — dat zijn onze eigen systemen — te helpen om dit snel te verhelpen en veilig te maken. Misschien zit daar ook nog iets in wat in de toekomst beter kan. Dat zou zomaar kunnen.

Minister **Grapperhaus**:
Daar hebben wij uitvoerig over gesproken met elkaar in een algemeen overleg. Het punt is dat mijn bevoegdheden en die van mijn diensten niet zover strekken dat die kunnen voorschrijven wat er op onderscheiden departementen moet gebeuren. Gelukkig hebben we een rijks-CIO om aanwijzingen te geven, maar uiteindelijk hebben alle departementen hun eigenlijk verantwoordelijkheid daarin en moeten ze die oppakken. Vandaar dat ik een brief heb gestuurd naar alle departementen en hen daar nog eens op heb gewezen. We zullen er met elkaar over moeten debatteren als u vindt dat deze minister, respectievelijk zijn ministerie, een soort superbevoegdheid moet krijgen op het gebied van ICT-systemen. Ik ben daar eerlijk gezegd nog niet van overtuigd, maar laten we daar een debat over aangaan.

De heer **Van Raak** (SP):
Dit ding, de mobiele telefoon, is helaas onontbeerlijk geworden voor ons werk hier in de Tweede Kamer. Dit ding doet het eigenlijk al maanden niet. Eerst hadden we de fouten van Vodafone. Toen hadden we de fouten van Microsoft. Nu hebben we het gat in de beveiliging van Citrix. Deelt de minister mijn grote zorgen dat onze nationale democratie zo afhankelijk is geworden van buitenlandse bedrijven? Deelt hij mijn zorg dat deze bedrijven ontzettend veel invloed hebben op de gang zaken hier en dat wij eigenlijk nauwelijks invloed hebben op de gang van zaken bij deze multinationals?

Minister **Grapperhaus**:
Even vooraf, de Tweede Kamer is een Hoog College van Staat. Dat zeg ik met een lichte buiging. Ik ga zeker niet over, en hoop ook in de toekomst niet te gaan, over de beslissing van de Tweede Kamer op het gebied van ICT. Dat zou volgens mij geen van uw 150 leden willen. Ik vind dat zelf ook niet goed verenigbaar met de democratie, de machtenscheiding enzovoort. Dat neemt overigens niet weg dat het NCSC en de cyberexperts van de Kamer op dit moment erg goed samenwerken om de problemen te verhelpen. Althans, dat is mijn indruk. Maar voor de Hoge Colleges van Staat is en blijft dat een eigen verantwoordelijkheid.

De vraag of wij vinden dat we inmiddels niet te veel afhankelijk zijn geworden van derden is zeker een vraag die we moeten beantwoorden. In mijn cybersecurity agenda van vorig jaar heb ik dit punt ook aan de orde gesteld. Maar wat de samenleving vindt dat we daar moeten doen, moeten we volgens mij in een debat bespreken.

Mevrouw **Kuiken** (PvdA):
Ik weet in ieder geval dat ik te afhankelijk ben van mijn telefoon, maar dat is nu niet zo relevant.

Voorzitter, ik zou via u aan de minister willen vragen of we morgen in de technische briefing specifiek in kunnen gaan op de 158 landen en 80.000 bedrijven die ook Citrix gebruiken. Het lijkt net of zij minder ernstige last ondervinden of minder in de high-high sferen zitten, terwijl zij toch ook grote problemen moeten hebben. Ik vind een vergelijking daarmee relevant en nuttig.

Minister **Grapperhaus**:
Ik zeg onmiddellijk toe dat we daarop zullen ingaan. Dat was eigenlijk al de bedoeling. Het woord "vergelijking" is wat lastig. Het punt is dat in Nederland in veel gevallen voor Citrix is gekozen. Dat verschilt per land. Ik kan overigens wel zeggen dat in enkele landen inmiddels het — laat ik het zo zeggen — proces van maatregelen op gang begint te komen, terwijl intussen ook daar de datum van 17 december geldt, want toen werd het bekend.

De **voorzitter**:
De vraag was of deze vragen meegenomen kunnen worden.

Minister **Grapperhaus**:
Dat heb ik al gezegd, voorzitter.

De **voorzitter**:
Prima, dan komt dat goed. Dank u wel.