26643 Informatie- en communicatietechnologie (ICT)

Nr. 1227 **VERSLAG VAN EEN COMMISSIEDEBAT**
Vastgesteld 24 oktober 2024

De vaste commissie voor Digitale Zaken heeft op 12 september 2024 overleg gevoerd met de heer Szabó, staatssecretaris Koninkrijksrelaties en Digitalisering, over:

**- de brief van de staatssecretaris Koninkrijksrelaties en Digitalisering d.d. 17 april 2023 inzake uitvoering van de motie van de leden Rajkowski en Van Weerdenburg over een scan van apparatuur of programmatuur van organisaties uit landen met een tegen Nederland gerichte offensieve cyberagenda (Kamerstuk 26643-830) en motie van het lid Rajkowski c.s. over een richtlijn om producten of diensten van organisaties en bedrijven uit landen met een offensieve cyberagenda uit bepaalde aanbestedingen te kunnen weren (Kamerstuk 26643-874) (Kamerstuk 26643, nr. 1007);**

**- de brief van de minister van Justitie en Veiligheid d.d. 20 april 2023 inzake stand van zaken Google Workspace (Kamerstuk 26643, nr. 1013);**

**- de brief van de staatssecretaris Koninkrijksrelaties en Digitalisering d.d. 29 juni 2023 inzake onderzoek nationale belangen (Kamerstuk 26643, nr. 1044);**

**- de brief van de staatssecretaris Koninkrijksrelaties en Digitalisering d.d. 12 januari 2024 inzake waarborgen ten behoeve van privacy en informatiebeveiliging en aanbestedingsregels (Kamerstuk 26643, nr. 1116);**

**- de brief van de staatssecretaris Koninkrijksrelaties en Digitalisering d.d. 14 mei 2024 inzake broncode DigiD-software openbaar gemaakt (Kamerstuk 26643, nr. 1159);**

**- de brief van de staatssecretaris Koninkrijksrelaties en Digitalisering d.d. 5 juni 2024 inzake gemelde kwetsbaarheid Cisco Webex-vergadervoorziening (Kamerstuk 26643, nr. 1181);**

**- de brief van de staatssecretaris Koninkrijksrelaties en Digitalisering d.d. 7 juni 2024 inzake update gemelde kwetsbaarheid Cisco Webex (Kamerstuk 26643, nr. 1182);**

**- de brief van de minister van Justitie en Veiligheid d.d. 25 juni 2024 inzake stand van zaken Google Workspace (Kamerstuk 26643, nr. 1201);**

**- de brief van de staatssecretaris Koninkrijksrelaties en Digitalisering d.d. 10 september 2024 inzake recente incidenten - Webex, CrowdStrike, NAFIN (Kamerstuk 26643, nr. 1218).**

Van dit overleg brengt de commissie bijgaand geredigeerd woordelijk verslag uit.

De voorzitter van de commissie,

Palmen

De griffier van de commissie,

Boeve

**Voorzitter: Kathmann**

**Griffier: Boeve**

Aanwezig zijn vier leden der Kamer, te weten: Buijsse, Kathmann, Six Dijkstra en Valize,

en de heer Szabó, staatssecretaris Koninkrijksrelaties en Digitalisering.

Aanvang 13.04 uur.

De **voorzitter**:

Welkom bij dit heugelijke feit: het commissiedebat van de Kamercommissie voor Digitale Zaken. Het is het eerste debat met onze kersverse staatssecretaris en daar zijn we ongelofelijk blij mee. Welkom! Ook welkom aan mijn collega's. We spreken vandaag over informatiebeveiliging bij de overheid. De spreektijd per fractie vandaag is maximaal vier minuten. Ik denk dat we gelijk van start kunnen gaan met de bijdrage van de heer Six Dijkstra van NSC.

De heer **Six Dijkstra** (NSC):

Hartelijk dank, voorzitter. Ook vanuit mij uiteraard van harte welkom aan de nieuwe staatssecretaris.

Voorzitter. De digitale incidenten van afgelopen zomer hebben duidelijk gemaakt dat onze afhankelijkheid van digitale processen groot is, dat de samenhang van systemen complex is en dat storingen een behoorlijk grote impact op de samenleving kunnen hebben. Daar zullen we de komende tijd nog wel vaker het debat over voeren.

De vorige staatssecretaris heeft in juni vorig jaar een rapport gedeeld met de Kamer over de beveiliging van gegevens, documenten en registraties van nationaal belang. Dit rapport bevat best een hoop nuttige en haalbare aanbevelingen waarvan het mij verstandig lijkt als daar nu op doorgepakt wordt. Mijn eerste vraag aan de staatssecretaris is dus: wat is er tot nu toe met dat rapport gedaan en wat zal er in de toekomst mee gebeuren? Het zou natuurlijk zonde zijn als het ergens in een lade verdwijnt. Is de staatssecretaris bereid om de aanbevelingen in het rapport op te volgen en over de voortgang daarvan aan de Kamer terug te rapporteren?

Ik wil één specifieke aanbeveling uit het rapport uitlichten. Dat is de volgende. "Voor toezicht op gegevens, documenten en registraties van nationaal belang zou het toezicht kunnen worden ingericht vergelijkbaar met het toezicht op de beveiliging van gerubriceerde informatie van de EU en NAVO." Dat lijkt mij een hele goede aanbeveling. We wijken af van ongeveer heel Europa in het feit dat we dit niet al ingeregeld hebben met nationaal toezicht. En het gaat hier nogal ergens om, zeker in het licht van de staatsgeheime informatie die bij de NCTV gestolen is. Ik ben mij ervan bewust dat er momenteel ook twee onderzoeken hiernaar lopen, maar hoe kijkt de staatssecretaris in zijn algemeenheid aan tegen hoe deze zogeheten NSA-taak invulling krijgt?

Kan de staatssecretaris verder toelichten hoe hij zijn mandaat wil oppakken wat betreft het grote, veelomvattende en helaas vaak ook knellende vraagstuk van overheidsdigitalisering in den brede, waar informatiebeveiliging een belangrijk onderdeel van is? Is hij bereid om in zijn termijn prioriteit te geven aan de aanbevelingen van de Algemene Rekenkamer en ervoor te zorgen, ten eerste, dat hij zijn mandaat inzet om overheidsbrede standaarden te zetten en dat hij die ruimer pakt dan zijn voorganger, en ten tweede, dat er duidelijk inzicht verkregen wordt in welke systemen binnen de hele overheid gebruikt worden en hoe deze onderling van elkaar afhankelijk zijn?

Dan het laatste punt. Eerder dit jaar is het NCSC door een Duitse journalist op de hoogte gebracht van softwarekwetsbaarheden die gevonden zijn in de Cisco Webex-dienst, waarmee metagegevens van vergaderingen van de Nederlandse rijksoverheid konden worden achterhaald. De rijksoverheid is niet rechtstreeks door de leverancier geïnformeerd over de kwetsbaarheden; dat moest via die journalist. Deze week zijn de antwoorden op de Kamervragen van de heer Valize van de PVV en van mijzelf naar de Kamer toegestuurd. Ik heb over de beantwoording van die vragen nog enkele vervolgvragen.

Ten eerste. De staatssecretaris geeft aan dat er meerdere checks zijn uitgevoerd naar dit product. Begrijp ik uit de beantwoording goed dat de voorspelbare logische volgordelijkheid in de internetadressen uit die checks niet naar voren is gekomen? Zo ja, kwam dat doordat deze kwetsbaarheid überhaupt niet aanwezig was in de specifieke versie van de Webex die de rijksoverheid het meest gebruikt? Of komt het doordat er niet wordt gekeken naar dit soort kwetsbaarheden?

Ten tweede. In welke mate heeft de staatssecretaris er zicht op of in de praktijk enkel informatie via Webex tot en met rubricering departementaal vertrouwelijk besproken wordt? Is weleens onderzocht hoe het veiligheidsbewustzijn van ambtenaren is, specifiek wat betreft het gebruik van communicatieproducten?

Bij de laatste twee vragen valt de staatssecretaris in zijn beantwoording specifiek terug op de aanbestedingsregels en de behoefte van individuele

departementen, maar als vragenstellers zouden wij eigenlijk het volgende willen weten. In welke mate zouden volgens de staatssecretaris het belang van de Nederlandse digitale autonomie en het borgen van de status van Nederland als cryptoproducerend land mee moeten wegen in de aanschaf van communicatieproducten over het hele Rijk heen?

Dank u wel, voorzitter.

De **voorzitter**:

Dank u wel. Dat is mooi binnen de tijd. U had nog twee seconden. Ik zie geen interrupties. Dan is het woord aan de heer Valize van de PVV.

De heer **Valize** (PVV):

Voorzitter, dank voor het woord. Een heel hartelijk welkom aan de staatssecretaris. Uw eerste debat in onze commissie! Welkom in ons gezellige clubje. We gaan er samen wat moois van maken. Vier minuten is kort, maar ik doe mijn best.

Voorzitter. Er zijn de afgelopen drie maanden wat incidenten geweest die tot de nodige onrust hebben geleid. De gemelde kwetsbaarheden van de Cisco Webex-vergadervoorziening, het debacle rondom CrowdStrike en de NAFIN-storing. CrowdStrike betekende geen goed begin van de vakantie voor vele miljoenen mensen wereldwijd. In dit geval werd het veroorzaakt door menselijk falen. Daar heeft de overheid niet direct invloed op, maar we kunnen er wel van leren. Ik noem een papieren back-up of een standalonesysteem. Maar je kunt als organisatie of bedrijf ook heroverwegen of outsourcing wel zo verstandig is. Maar dat is weer een andere discussie, in een andere setting. Dat gaat dan ook aan bod komen bij het commissiedebat Online veiligheid en cybersecurity direct na het kerstreces. NAFIN zal vanzelfsprekend terugkeren bij het debat over digitale infrastructuur in december. Het punt dat ik wilde maken is: we zijn gewoon ongelofelijk afhankelijk geworden van IT.

Voorzitter. Dan nu de informatiebeveiliging bij de overheid. Er zijn negen brieven. Ik zal enkele zaken belichten. Eerst ga ik het hebben over de offensieve cyberagenda en de moties van de leden Rajkowski van de VVD en Van Weerdenburg van de PVV. De PVV wil graag weten wat de grootste obstakels zijn bij het weren van technologie uit landen met een offensieve cyberagenda en of daar een plan voor uiteengezet is. Vanuit de Vereniging van Nederlandse Gemeenten komt het sterke signaal dat er op het ogenblik een scala aan handreikingen en eisensets bestaat, maar dat er geen eenduidig beleid en geen regie is. Daar kom ik aan het einde van mijn betoog nog op even op terug.

Ook hebben we nog de brief over de aanbestedingsregels, waarin onder andere wordt verwezen naar Baseline Informatiebeveiliging Overheid en de Inkoopeisen Cybersecurity Overheid als standaarden en instrumenten om informatiebeveiliging te borgen in aanbestedingen. Hoe wordt geborgd dat deze standaarden en instrumenten adequaat worden opgevolgd? Welke consequenties hangen eraan vast indien dat niet het geval is?

Voorzitter. Google Workspace. We lezen dat overheidsorganisaties dit kunnen gebruiken, mits ze specifieke aanvullende maatregelen afwegen, afhankelijk van hun situatie. De PVV wil graag weten welke risico's er nog steeds bestaan, om welke maatregelen het gaat en of dit voor alle overheidsorganisaties gelijk is.

De openbaarmaking van de broncode van DigiD. Hierbij is een zorgvuldige procedure gevolgd, waarbij een extern onderzoek is uitgevoerd naar de beveiligingsaspecten van de meest kritieke onderdelen van de broncode. Fragmenten die een beveiligingsrisico vormen, zijn aangepast in de gepubliceerde versie. De PVV wil graag weten waarom er gekozen is voor deze oplossing? Kan de inzet van AI niet alsnog de gewijzigde code corrigeren? En vormt dat dan geen risico?

Dan de brieven inzake de softwarekwetsbaarheden in Cisco Webex. Gisteren hebben we eindelijk antwoord mogen ontvangen op vragen van NSC, VVD en PVV. Het valt op dat er geen SLA's met Cisco zijn, maar met BIS. BIS draagt hier dus de verantwoordelijkheid. Waarom deze constructie? Verder sluit ik me aan bij de vragen van de heer Six Dijkstra.

Voorzitter. Dan nog een algemene vraag ...

De **voorzitter**:

Meneer Valize, ik waardeer uw technische vragen en uw oprechtheid. Daarom wil ik u 30 seconden meer geven. Dan heeft u, denk ik, het gevoel dat u uw bijdrage af kan maken. Dan kunt u met minder haast gewoon uw vragen stellen.

De heer **Valize** (PVV):

Dank, voorzitter. Als het goed is, heb ik nog 24 seconden.

Ik heb een algemene vraag voor de staatssecretaris. Deze brieven, maar ook de hiervoor genoemde incidenten, wijzen allemaal in de richting van één conclusie: er is onvoldoende regie. Deelt de staatssecretaris deze opvattingen? Is hij voornemens om, gezien de achtergrond die hij heeft en gezien hij inmiddels de aangewezen persoon hiervoor is, de rol van kartrekker op zich te nemen en een verbindende factor te zijn die interdepartementaal voor elkaar gaat krijgen dat er meer regie komt? Ik zag

gisteren een post op LinkedIn voorbijkomen over het iBestuur Congres waar de staatssecretaris gesproken heeft. Daarmee is al een tipje van de sluier opgelicht. Maar kan en wil de staatssecretaris hier al iets over zeggen of moeten we het regeerakkoord afwachten? We zijn erg nieuwsgierig; dat begrijpt u.

Dan nog een laatste uitsmijter, binnen de tijd. De vorige staatssecretaris heeft de spreekwoordelijke stekker uit het platform TikTok getrokken, waardoor via dit platform geen burgers meer geïnformeerd worden door de Staat. Gaat u dit besluit heroverwegen? Er maken immers behoorlijk wat mensen gebruik van dit medium.

Dan sluit ik af, binnen de tijd, als het goed is. Dank u, voorzitter.

De **voorzitter**:

Meneer Valize, ik had mijn waardering al uitgesproken, maar u heeft inderdaad nog twee seconden, dus perfect. Ik zie geen interrupties. Dan is het woord aan de heer Buijsse van de VVD.

De heer **Buijsse** (VVD):

Dank u wel, voorzitter. Ook van mijn hand welkom aan de staatssecretaris. Fijn dat u erbij bent.

Voorzitter. Bij mijn maidenspeech vorige week heb ik uitgedragen dat ik zo veel mogelijk Nederlanders wil bereiken bij de keukentafel. Nederlanders wisselen namelijk aan de keukentafel hun zorgen uit. Enerzijds kunnen ze dan zelf handelen, maar anderzijds moet er een sterke overheid zijn, die vanuit haar rol zaken veilig moet stellen. Het gaat vaak over zorgen die voortkomen uit de wereld van bits en bytes. Die zorgen zijn zichtbaar, bijvoorbeeld onlangs nog toen er een storing was op Eindhoven Airport. Deze storing bleek niet het gevolg te zijn van een cyberaanval, maar toch legde die onze kwetsbaarheid bij een storing bloot.

Tegelijkertijd zijn er ook risico's die de keukentafel niet halen -- gelukkig maar. Zo onthulde de MIVD op 6 februari jongstleden een werkwijze voor Chinese spionage in Nederland. Ze troffen malware aan bij de krijgsmacht op een losstaand computernetwerk. We willen niet weten wat de gevolgen kunnen zijn. Ook in de agenda van deze commissievergadering kwamen kwetsbaarheden voor de informatiebeveiliging terug, zoals bij Cisco Webex en Google Workspace. Al deze voorbeelden lijken slechts het topje van de ijsberg van wat nog komen gaat. Het doel van de VVD is om te komen tot een breed gedragen bewustzijn over de risico's en potentiële impact van onze nationale veiligheid wanneer landen met een tegen Nederland gekeerde cyberagenda echt zouden doorpakken. We willen bijvoorbeeld, vanwege de toegenomen cyberdreiging vanuit Rusland en China, dat de overheid

scenario's voorbereidt zodat we beter voorbereid zijn bij grootschalige cyberaanvallen of storingen. Daarnaast willen we de aanwezigheid afbouwen van digitale apparatuur, programmatuur en cryptografie van organisaties uit landen met een tegen Nederland gerichte cyberagenda. We willen ook dat de overheid samenwerkt met ethische hackers binnen de bestaande juridische kaders om kwetsbaarheden eerder in beeld te krijgen.

Als het gaat over de afbakening van de hiervoor genoemde doelen, betreft dat de rijksoverheid, inclusief de vitale processen van de rijksoverheid, zoals telecommunicatie, transport, defensie en de openbare orde en veiligheid. De beantwoording van de staatssecretaris op de twee moties die Rajkowski in 2022 heeft ingediend, toont aan dat de rijksoverheid werkt aan dat bewustzijn en aan intensivering van haar processen en procedures. Zo is de aanbestedingsprocedure aangepast met het oog op het weren van apparatuur en programmatuur van organisaties uit landen met een tegen Nederland gerichte cyberagenda. Dat geeft vertrouwen, maar de moties zijn nog niet volledig uitgevoerd en zijn wat ons betreft nog niet afgedaan. Met de moties werd namelijk verwezen naar de risico's en de vitale processen van de rijksoverheid en het maken van een scan om daar een actueel beeld bij te hebben. De scan hebben we nog niet tot ons kunnen nemen, terwijl wij graag deze oefening zouden willen doen of er kennis van zouden willen nemen. We willen weten waar en in welke mate er risico's zijn voor het gebruik van de apparatuur, programmatuur en cryptografie die gebruikt worden voor onze vitale infrastructuur. Het voorbeeld van de bevinding van de MIVD en de storing bij Defensie laat al voldoende zien wat de maatschappelijke impact kan zijn.

Ik wil de staatssecretaris daarom de volgende vragen stellen. Klopt het dat de brieven over de moties van Rajkowski een update zijn, en dat de moties nog een gevolg krijgen? Heeft u momenteel een actueel en volledig zicht op de software, apparatuur en cryptografie die gebruikt wordt voor onze vitale processen? Heeft u bij dit overzicht ook inzicht in of er organisaties bij betrokken zijn uit landen die een tegen Nederland gekeerde cyberagenda voeren? Kan de Kamer kennisnemen van dit overzicht, eventueel onder geheimhouding? Is de staatssecretaris bereid om in de toekomst afspraken te maken met en tussen departementen die bijdragen aan het stapsgewijs wegnemen van cyberrisico's van de vitale processen?

Dank u wel.

De **voorzitter**:

Dank u wel. U heeft een interruptie van de heer Six Dijkstra van NSC.

De heer **Six Dijkstra** (NSC):

Ik dank de heer Buijsse voor zijn bijdrage. Ik heb eigenlijk niks gehoord waar ik het fundamenteel mee oneens ben. Ik heb wel een verduidelijkingsvraag. Op een gegeven moment vertelde hij dat de Defensiecasus van afgelopen februari, van de MIVD-systemen, aanleiding zou geven om nog even tegen het licht te houden of onze afhankelijkheid van cryptografie en systemen van landen met een offensief cyberprogramma -- ik neem aan dat u op China doelt -- afgebouwd moest worden. Maar ik meen dat die systemen uit Amerika kwamen. Hoe ziet hij de samenhang daartussen? Wat zou hij hierop willen voorstellen?

De heer **Buijsse** (VVD):

Ik doelde in dit voorbeeld niet specifiek op landen. Ik doel met name op de kwetsbaarheid die we hebben voor storingen en gerelateerde incidenten en bijvoorbeeld voor malware die door derden wordt geïnstalleerd. Ik wil niet vereisen ... Volgens mij deed ik dat ook niet. Er is een werkwijze voor Chinese spionage in Nederland. Dat haal ik wel uit dit bericht. Maar dat weten we niet 100% zeker.

De **voorzitter**:

De heer Six Dijkstra heeft nog een interruptie.

De heer **Six Dijkstra** (NSC):

Mijn vraag is specifiek ... Ik ben het ermee eens dat we ons beter moeten wapenen tegen landen als China. Wat zou de heer Buijsse in dit geval dan concreet voorstellen? Welke dingen zouden geëvalueerd moeten worden? Want bij dit soort casussen is gebruikgemaakt van apparatuur die niet uit China komt, maar wel kwetsbaar bleek en in dit geval binnen het aanvalsoppervlak van de Chinese actoren lag.

De heer **Buijsse** (VVD):

Ik vond het sowieso interessant om in uw beider inbreng mogelijkheden te horen. U zoekt beiden naar regie op afhankelijkheden, interdepartementaal, om de veiligheid te waarborgen. Blijkbaar lukt het ons op dit moment niet om risico's weg te nemen. In het geval van de twee voorbeelden die ik gaf, zou ik ernaar willen streven om juist wel naar regie te gaan. Die vraag hoor ik ook bij u terug: hoe kunnen we de staatssecretaris in de positie brengen om tot echte afspraken te komen, om incidenten zoals het plaatsen van malware die schade zou kunnen geven of situaties zoals Defensie en Eindhoven Airport te voorkomen? Om dat te voorkomen moeten we wat ons betreft de handen ineenslaan om tot interdepartementale afspraken te komen. Daarop

aanvullend: als het kan, zou ik ook graag -- daar opteerde ik al voor -- duidelijker in beeld willen hebben welke apparatuur, software en cryptografie er eigenlijk is. Aan onze kant van de tafel, aan de kant van de Kamerleden, weten wij namelijk op dit moment helemaal niks. We kunnen dus ook niet zeggen of en welke risico's er zijn. Ik wil graag in gesprek met de staatssecretaris om daarover het gezamenlijk bewustzijn te vergroten. Dat is het doel van onze fractie.

De **voorzitter**:

Er is een interruptie van de heer Valize van de PVV.

De heer **Valize** (PVV):

Dank voor uw inbreng. Ik zat al te denken aan het volgende. De storingen bij het vliegveld van Eindhoven en bij Defensie en dergelijke kwamen door de storing bij NAFIN. Dat valt onder de digitale infrastructuur waar we in december op terugkomen. Met betrekking tot malware en dergelijke: over veiligheid en cybersecurity hebben we ook nog een debat meteen na het kerstreces. Welke samenhang ziet u met de informatiebeveiliging bij de overheid, dat we nu op de agenda hebben staan?

De heer **Buijsse** (VVD):

De samenhang zit 'm in de moties van Rajkowski die in 2022 zijn aangenomen. Daar komt het wat ons betreft samen. Ik deel uw vraag: waarom moet dit hier én in latere debatten? Ik heb daar overigens ook een mening over. Ik vind het lastig om de staatssecretaris echt in een goede positie te brengen, omdat er eigenlijk ook nog fragmentatie is in de opzet van onze eigen commissiestructuur. Ik geef even een praktisch voorbeeld. Ik ben nu hier voor mijn eerste commissiedebat. Mijn voorgangster was Queeny Rajkowski. Toen zij voor de eerste keer sprak, was digitale zaken een heel klein onderdeeltje. Digitale zaken is in omvang gegroeid en we komen steeds meer te weten als Tweede Kamer over digitale zaken in de breedste zin des woords. Als ik dat vertaal, vanuit mijn behoefte om dat naar de keukentafel te vertalen, naar wat het voor inwoners voor relevantie heeft, dan vraag ik me af: is dat wel eerlijk toebedeeld binnen het geheel van de Tweede Kamer? Ik kan het antwoord nu niet geven. Ik weet het ook niet, maar ik wil het daar wel over hebben. Mijn gevoel zegt namelijk -- misschien kunt u daar ook een reflectie op geven -- dat digitale zaken te gefragmenteerd is over departementen en dat we daardoor risico's niet goed beethebben. Ik zou de staatssecretaris graag in de positie helpen dat we dat voor Nederland, in het nationaal belang, zeker voor onze vitale processen, juist goed gaan doen.

De **voorzitter**:

Dank u wel. Ik zie geen interrupties meer. Dan vraag ik de heer Six Dijkstra om even de voorzittersrol over te nemen, zodat het lid Kathmann van GroenLinks-Partij van de Arbeid haar bijdrage kan doen.

**Voorzitter: Six Dijkstra**

De **voorzitter**:

Dank. Ik geef het woord aan het lid Kathmann van de fractie van GroenLinks-Partij van de Arbeid.

Mevrouw **Kathmann** (GroenLinks-PvdA):

Dank u wel, voorzitter. Onze samenleving en overheid zijn verregaand gedigitaliseerd en afhankelijk van digitale processen: van DigiD tot e-mail, van videoconferenties tot de toetscijfers van mijn kinderen. We kunnen gewoon niet meer zonder digitale middelen. Dat wordt bij elke storing keer op keer pijnlijk duidelijk. Bij zowel de storing veroorzaakt door NAFIN als bij het CrowdStrike-incident lijkt het er gelukkig op dat er geen sprake was van een cyberaanval. Maar het moet wel onze ogen openen. De samenleving en de overheid zijn compleet afhankelijk van digitale processen.

Voorzitter. Ik wil de heer Szabó van harte welkom heten en hem ten eerste heel veel succes wensen met zijn komende periode als staatssecretaris voor Digitale Zaken, maar ik wil hem ook iets meegeven. Zijn collega, de minister van Justitie, sprak de inmiddels beruchte woorden: "Get used to it. Wen er maar aan dat er storingen en problemen zullen plaatsvinden bij digitale processen." Hij sprak ze uit op het moment dat zowel de oorzaak als de impact van de storing volstrekt onduidelijk was. Wel was duidelijk dat de kustwacht in de problemen zat en DigiD niet functioneerde. De uitspraak was dan ook geen steun in de rug -- dit zijn niet mijn woorden; dit heb ik vernomen -- maar een klap in het gezicht van alle cybersecurityspecialisten die keihard aan het werk waren om oorzaken te achterhalen, impact te minimaliseren en problemen op te lossen en dus om onze nationale weerbaarheid te vergroten. Ja, er zullen zeker cyberaanvallen en storingen gaan plaatsvinden. Honderd procent veilig en honderd procent uptime bestaat niet. Ik zal ook de allerlaatste zijn die dit kabinet, en deze staatssecretaris in het bijzonder, aan onmogelijke standaarden zal houden. Maar ik wil de staatssecretaris wel vragen om er niet met de pet naar te gooien en onze nationale weerbaarheid te vergroten. Ik verwacht van hem dat hij zijn uiterste best gaat doen om ons land zo cyberveilig mogelijk te houden, om plannen te ontwikkelen voor de momenten dat er digitale

incidenten optreden, om deze incidenten zo snel mogelijk te verhelpen en om de samenleving zo goed mogelijk draaiende te houden.

Voorzitter. Dat brengt mij tot de volgende vragen. Kan de staatssecretaris aangeven wat zijn visie is op het cyberveilig houden van Nederland? GroenLinks-Partij van de Arbeid wil eigenlijk het allerliefst dat de woorden "get used to it" worden teruggenomen, of minimaal worden vervangen door "get ready". Vindt de staatssecretaris dat ook? Honderd procent uptime en veiligheid bestaat niet. Incidenten zullen voorkomen. Wat is voor de staatssecretaris een acceptabele downtime ten aanzien van de digitale dienstverlening van de overheid? Welke response time van dienstverleners, zoals de partijen die betrokken zijn bij NAFIN, verwacht de staatssecretaris?

Voorzitter. Tijdens de CrowdStrikestoring waren er ziekenhuizen die alle operaties stil moesten leggen. Maar er waren ook ziekenhuizen die door konden draaien, terwijl zij ook last hadden van de storing. Dat betekent dus dat sommige vitale delen van onze infrastructuur beter voorbereid zijn dan andere. Is de staatssecretaris het met mij eens dat alle overheids- en vitale organisaties niet alleen plannen moeten hebben om storingen zo snel mogelijk te verhelpen, maar ook plannen moeten hebben om, ondanks uitgevallen systemen, de dienstverlening doorgang te laten vinden? Ziet de staatssecretaris mogelijkheden om dit soort plannen af te dwingen en te controleren of deze plannen voldoen?

Voorzitter. De incidenten met Webex, CrowdStrike en NAFIN staan los van elkaar, maar de problemen kunnen wel in samenhang worden bezien. Daarom wil ik het volgende van de staatssecretaris weten. Volstaat volgens de staatssecretaris de huidige Nederlandse Cybersecuritystrategie om dit soort incidenten bij de overheid te voorkomen? Welke wijzigingen gaat de staatssecretaris in de strategie aanbrengen om Nederland cyberweerbaarder te krijgen? Na elk incident wordt er onderzoek gedaan, waarvoor hulde. Toch ruikt het ook een beetje naar brandjes blussen. Kan de staatssecretaris aangeven of hij reden ziet om te onderzoeken of er diepere problemen zijn in de manier waarop we bij de overheid IT hebben ingericht, waardoor incidenten vaker dan nodig kunnen voorkomen? Is er volgens de staatssecretaris dus gewoon meer onderzoek nodig?

Nu ga ik afronden. We hebben hier te maken met de staatssecretaris van niet alleen Digitale Zaken, maar ook Koninkrijksrelaties. Mijn vraag gaat eigenlijk over deze combinatie. Kan de staatssecretaris aangeven of de nieuwe cybersecuritywet ook van toepassing is op Caribisch Nederland? Zo nee, wat vindt de staatssecretaris daar dan van? Wat is eigenlijk zijn visie op het cyberveilig houden van het hele Koninkrijk en hoe dat het beste bereikt kan worden?

Dank u wel.

De **voorzitter**:

Dank u wel, mevrouw Kathmann. Dan geef ik de voorzittershamer weer terug aan u.

**Voorzitter: Kathmann**

De **voorzitter**:

Dank u wel, meneer Six Dijkstra. Dan zijn alle bijdragen gedaan. Ik kijk even naar de staatssecretaris met de vraag hoeveel tijd hij nodig denkt te hebben voor de beantwoording. We schorsen 25 minuten en dan gaan we naar de beantwoording.

De vergadering wordt van 13.28 uur tot 13.54 uur geschorst.

De **voorzitter**:

We gaan verder met de vergadering van de commissie voor Digitale Zaken. Het woord is aan de staatssecretaris voor de beantwoording.

Staatssecretaris **Szabó**:

Voorzitter, dank u wel. Voordat ik kom bij de inhoud waar we vandaag over spreken, wil ik er ook even bij stilstaan dat dit voor mij de eerste keer is dat ik vanuit deze positie met de Tweede Kamer spreek. Dat is een hele eer. Vroeger zat ik aan de andere kant van deze tafel, maar dat is inmiddels zo'n achttien jaar geleden. We zitten inmiddels in een nieuw gebouw en in een nieuw opgezette commissie, waar ik echt ontzettend blij mee ben. We hebben het er vroeger in debatten ook al over gehad of het niet wat strakker kon worden aangestuurd. Dat gebeurt nu zeker. Ook vanuit de VVD heb ik begrepen dat dingen dusdanig snel gaan bij uw inbreng dat het goed is dat deze structuur er nu is. Ik kijk ernaar uit om met u samen te werken.

U weet net als ik dat digitalisering grote kansen biedt op het gebied van maatschappelijke vraagstukken, de arbeidsmarkt en de dienstverlening vanuit de overheid. Het mes snijdt aan twee kanten. Wat gebeurt er als onze systemen platliggen? Daar gaan we het vandaag ook over hebben. Onlangs hebben we nog voorbeelden gezien van grote storingen; ik zit hier tweeënhalve maand, maar ik heb er inmiddels drie meegemaakt. Hoe beschermen we onze persoonlijke gegevens en hoe zorgen we ervoor dat iedereen digitaal meekomt? Dat is ook een hele belangrijke vraag. Ik kijk ernaar uit om in deze functie aan de slag te gaan met deze uitdagende en

veelomvattende portefeuille. Dat kan ik niet alleen; daar heb ik uw hulp bij nodig. Ik heb met u allemaal kennisgemaakt. Ik was ook heel blij met die eerste gesprekken. Ik zie tegenover mij allemaal mensen die heel bevlogen zijn met dit dossier. Dat vind ik heel goed. Ik wil u echter wel vragen om kritisch te zijn op mij, mee te denken en oplossingen aan te bieden voor de verschillende vraagstukken waarover we de komende jaren met elkaar zullen spreken.

Ik geloof er heel sterk in dat gezamenlijk optrekken belangrijk is bij deze grote digitaliseringsopgave. Dat doe ik niet alleen met u, maar ook met gemeenten, provincies, waterschappen en uitvoerders. Ik spreek ook met het bedrijfsleven en met de wetenschap, want ik denk dat we alleen samen grote problemen kunnen oplossen. Laten we bouwen aan een stevig fundament van waaruit wij kunnen werken, uniform voor allen, waardoor de burger weet wat hij aan ons heeft en hoe hij ons kan vertrouwen in het kader van de dienstverlening van de overheid.

Voordat ik verderga met de beantwoording van de vragen: er is al een beetje ingegaan op dat ik aan het nadenken ben over hoe we met dit dossier verder moeten gaan. Ik kan u vertellen dat ik van plan ben om toch te kijken waar we moeten gaan prioriteren, omdat we eigenlijk heel veel onderwerpen behandelen. Dat is hier ook aan de orde gekomen vandaag. Ik denk dat in ieder geval het onderwerp van vandaag, de informatiebeveiliging bij de overheid, hoog op het lijstje zou moeten staan, ook als het gaat om hoe we dat beter gaan coördineren en regisseren in de toekomst. Zoals ik al aangaf, ga ik de komende tijd met u, met andere betrokkenen en met medeoverheden aan de slag om die prioriteiten samen op papier te zetten. Dat even als korte inleiding.

Dan de beantwoording van de vragen. Ik heb drie pakketjes die ik ga behandelen. Het eerste is informatiebeveiliging en digitale weerbaarheid. Het tweede is incidentele storingen, de incidenten. Het derde is overige. Als ik daarna nog zaken niet heb behandeld, dan hoor ik dat graag.

Dan gaan we eerst over op het eerste pakketje, informatiebeveiliging en digitale weerbaarheid. Er was een vraag vanuit de heer Six Dijkstra van NSC. Wat is er tot nu toe gebeurd met het rapport nationaal belang? Wat is daarmee gedaan? Welke aanbevelingen worden overgenomen? Ik ben op dit moment aan de slag met het rapport, bijvoorbeeld bij het vormen van de overheidsspecifieke regels onder de Cyberbeveiligingswet, die onder coördinatie van Justitie en Veiligheid door departementen worden uitgewerkt. Een aanzienlijk deel van de adviezen kan ik opvolgen, maar niet allemaal. Ik verken momenteel welke aanbevelingen ik kan overnemen. Dit vergt een zorgvuldige afweging met het oog op ongewenste neveneffecten. Er staan goede suggesties in het rapport, zoals het bezien van de basisregistraties, maar er staan ook aanbevelingen in die niet kunnen worden ingezet, zoals het gebruik van DigiD voor ambtenaren. Dat is niet wenselijk, omdat het

burgerservicenummer voor identificatie binnen de werksituatie niet wenselijk is.

De heer **Six Dijkstra** (NSC):

Dank aan de minister voor zijn beantwoording. Kunnen wij als Kamer op de hoogte gesteld worden van de aanbevelingen die de staatssecretaris wel gaat opvolgen? En als hij bepaalde aanbevelingen niet gaat opvolgen, kunnen wij daar dan ook argumentatie bij krijgen?

Staatssecretaris **Szabó**:

Het antwoord is ja. Ik zeg ook toe om in het tweede kwartaal van 2025 de Kamer te informeren over de verdere voortgang en de opvolging. Daar zal ook in staan welke aanbevelingen we wel en niet zullen oppakken. Dat is het antwoord.

Dan nog een vraag van NSC. Hoe kijkt de staatssecretaris aan tegen hoe deze NSA-taak invulling krijgt? Het is goed om te onderzoeken hoe de National Security Agency-taak, de NSA-taak dus, invulling krijgt en of er behoefte is aan doorontwikkeling. Daarover zal de minister van BZK graag met uw Kamer van gedachten wisselen. Er gaat in ieder geval toezicht komen op informatiebeveiliging bij de overheid, vanwege de komst van de Cyberbeveiligingswet waar ik het net over had. Dit toezicht gaat uitgevoerd worden door de Rijksinspectie Digitale Infrastructuur, de RDI.

Dan nog een vraag van NSC. Hoe kan het dat de overheid achterloopt met de implementatie van onder andere open veiligheidsstandaarden voor websites en e-mails. Het klopt dat nog niet alle overheden de open standaarden hebben toegepast op de voorgeschreven manier of adequaat uitleggen waarom zij dit achterwege laten. In het Overheidsbreed Beleidsoverleg Digitale Overheid, de OBDO, zijn afspraken gemaakt over de implementatie van deze informatieveiligheidsstandaarden met de mede-overheden die daarin vertegenwoordigd zijn. Dit is een continu proces. Overigens loopt de overheid niet achter met de implementatie als we dit vergelijken met andere branches of omliggende landen. Uit de meest recente meting, uit 2024, blijkt namelijk dat bij 64% van de gemeenten voor internetdomeinen van de overheid en de verplichte websites op het internet de veiligheidsstandaarden correct zijn toegepast.

Dan nog een vraag van de heer Six Dijkstra. Die ging over onderzoeken hoe het veiligheidsbewustzijn bij ambtenaren is. Vanuit mijn functie is dat natuurlijk een hele belangrijke vraag. Bewustwording, veilig gedrag en weerbare medewerkers zijn pijlers waarop informatiebeveiliging rust. Onlangs is rijksbreed beleid vastgesteld, waarin verplicht wordt dat alle medewerkers een training moeten doorlopen en dit jaarlijks zullen herhalen. De

rijksoverheid ontwikkelt naast de voorzieningen die departementen en organisaties zelf hebben een basisopleiding digitale weerbaarheid. Deze is gebaseerd op de verplichte gedragsregels voor de digitale werkomgeving. De planning is dat die eind dit jaar klaar zal zijn. Diverse departementen zijn al verder en hebben zelfs al een training op dit gebied. Ook besteden zij zelf op diverse manieren aandacht aan dit onderwerp. Hierin worden ze ook ondersteund door het NCC, het CIP, de VNG -- wat vreselijk dat ik dit zo moet oplezen -- de IBD, SURF en het NBV, dat materialen hiervoor maakt. Hierachter heb ik een afkortingenlijstje liggen. Die had eigenlijk hier moeten liggen. De volgende keer wil ik graag dat dit allemaal gewoon uitgeschreven is, maar dan gaat de vergadering wel wat langer duren.

De **voorzitter**:

Meneer Six Dijkstra, u weet dat we nu aan het maximumaantal afkortingen zitten, dus ...

De heer **Six Dijkstra** (NSC):

Ja, voorzitter, zeker. Ik zal het de staatssecretaris niet aanrekenen als zijn kennis van afkortingen enigszins in gebreke is. Ik kon ze ook niet allemaal volgen.

Dank voor de beantwoording. Met betrekking tot het veiligheidsbewustzijn van rijksambtenaren was ik nog benieuwd naar het volgende. Hier ging het om de Webex-casus. Laten we het breder trekken naar videobelverbindingen, of misschien belverbindingen in den brede. Ik kan me zo voorstellen dat het als ambtenaar soms onduidelijk is wat je al dan niet over welke verbinding mag zeggen, zeker omdat er best wel een grijs gebied is als het gaat om gerubriceerde informatie. Wat is nog departementaal vertrouwelijk? Wat is ongerubriceerd? Vanaf waar wordt het staatsgeheim? Als ambtenaren intern of extern met mensen bellen en gerubriceerd materiaal bespreken, komen de signalen daadwerkelijk binnen bij de minister en het departement als blijkt dat er toch dingen besproken zijn die niet aan het rubriceringsniveau voldoen? Is er dus, behalve de trainingen, ook een tussentijdse evaluatie? Worden die signalen serieus genomen?

Staatssecretaris **Szabó**:

Ik zit er net twee maanden. Ik heb ze nog niet binnengekregen, maar ik heb begrepen dat dat wel degelijk zo is. Zoals u weet kom ik uit het bedrijfsleven, waar we allemaal mandatory trainingen hadden. Ik heb er zelf ook heel veel gedaan. Daarnaast heb ik daar ook met mijn ambtenaren over gesproken. Ik heb ook binnen mijn eigen ministerie gekeken wat voor trainingen men krijgt. Ik heb aangegeven dat we hier disciplinair echt heel goed mee moeten

omgaan, want veel ongelukken die gebeuren op het gebied van digitalisering komen door menselijke fouten. Als je de software een keer niet de schuld kan geven, heeft de mens iets niet goed gedaan. Daar ga ik dus ook heel erg op letten. De tijd van vrijblijvendheid is voorbij.

De **voorzitter**:

U heeft nog een interruptie van de heer Buijsse.

De heer **Buijsse** (VVD):

Aanvullend op de vraag van de heer Six Dijkstra. In de afbakening hoeft het wat mij betreft niet alleen over de ambtenaren te gaan; het mag ook gaan over ons, de Tweede Kamerleden, en over de organisatie van de Tweede Kamer. Mijn pleidooi is dus om dat ook mee te nemen in de afbakening. Het is ook voor ons een verantwoordelijkheid als Tweede Kamerlid.

Staatssecretaris **Szabó**:

Als het goed is, heeft u uw eigen organisatieondersteuning, ook op het gebied van ICT. Ik denk dat u in eerste instantie met hen in gesprek moet gaan. Maar ik denk dat het heel goed is dat ook binnen dit gebouw dezelfde urgentie bestaat.

Dan het onderwerp inkoop en het weren van landen met een offensieve cyberagenda. Er werd gevraagd: wat zijn de grootste obstakels bij het weren van technologie uit landen met een offensieve cyberagenda door middel van het inkoop- en aanbestedingsbeleid? Is hiervoor een plan uitgezet? Volgens mij kwam deze vraag van de heer Valize. Dat stond hier niet bij, maar ik heb het goed onthouden. Door technologie afkomstig uit landen met een offensief cyberprogramma per definitie uit te sluiten, schieten we ons doel voorbij. Aan het gebruik van technologie zit altijd risico's, ongeacht de leverancier. Het huidige beleid gaat uit van het in kaart brengen van mogelijke risico's en hier proportionele en effectieve maatregelen voor treffen. In het uiterste geval kan weren of uitfaseren wel aan de orde komen. Of een opdracht een risico vormt voor de nationale veiligheid hangt sterk af van de sector, het type product of dienst die geleverd wordt, de opdrachtgever, de afnemer en het bedrijf dat de opdracht wordt gegund. Ter ondersteuning is instrumentarium ontwikkeld dat hierbij handvaten biedt. We moeten daarbij denken aan de Tvi, de Toolbox veilig inkopen. Daarnaast wordt er gewerkt aan de ontwikkeling van Algemene Beveiligingseisen Rijksoverheid Opdrachten, ABRO. Daarnaast wordt door mijn collega, de minister van EZ, in Europees verband ingezet op het aanpassen van de aanbestedingsrichtlijnen, zodat de regels makkelijker en beter inzetbaar zijn om de veiligheidsrisico's te beheersen.

Dan nog een vraag van de heer Valize. Hoe wordt geborgd dat standaarden en instrumenten zoals de Baseline Informatiebeveiliging Overheid, de BIO, en Inkoopeisen Cybersecurity Overheid, de ICO, worden gevolgd? En welke consequenties hangen eraan als dat niet gebeurd? Overheidsorganisaties hebben zichzelf via verplichtende zelfregulering de Baseline Informatiebeveiliging Overheid en de Inkoopeisen Cybersecurity Overheid opgelegd. In de nadere regelgeving van de Cyberbeveiligingswet -- daar hebben we het eerder over gehad -- voor de overheid worden de BIO en de ICO verplicht. De Rijksinspectie Digitale Infrastructuur, de RDI, ziet als systeemtoezichthouder toe op toepassing van de Cyberbeveiligingswet voor de overheid en daarmee op de verplichte BIO en ICO. De RDI kan ook gebruikmaken van verschillende handhavingsinstrumenten wanneer een overheidsorganisatie niet voldoet aan de standaarden voor instrumenten.

Even tussendoor. In de stukken die ik heb ontvangen zaten in totaal 70 afkortingen. Dat was ik even vergeten te melden.

Dan nog een vraag van de heer Valize. Het valt op dat er geen SLA's met Cisco zijn, maar met BIS, dus BIS draagt de verantwoordelijkheid. Waarom zijn ze er niet met Cisco? Deze constructie is direct afkomstig uit de aanbesteding audio en video van de Belastingdienst. Uit deze aanbesteding is BIS voortgekomen als leverancier en contractpartner voor de levering van de producten binnen de scope van de aanbesteding, dus inclusief die van Cisco.

Nog een vraag van de heer Valize. Deelt de staatssecretaris het beeld dat er onvoldoende regie is op de digitale weerbaarheid? En ziet hij zichzelf als de aangewezen persoon om te zorgen voor interdepartementale verbinding en regie? De digitale veiligheid is een aangelegenheid van ons allen. Dat betekent dat iedereen zijn rol daarin moet pakken. Als coördinerende staatssecretaris digitalisering en stelselverantwoordelijke voor de informatiebeveiliging bij de overheid werk ik vanuit het uitgangspunt dat we als één overheid moeten handelen. Onder regie van de minister van Justitie en Veiligheid wordt gewerkt aan de digitale weerbaarheid. Elk departement heeft op zijn beurt te maken met zijn eigen verantwoordelijkheid en organisaties, die soms ook om een andere aanpak vragen. Ik wil vanuit mijn verantwoordelijkheid samen met de rijksoverheid en medeoverheden, zoals gemeenten, waterschappen en provincies, bouwen aan een stevig fundament van waaruit we kunnen werken, uniform voor allen. Zo werken we aan een betrouwbare overheid waarvoor burger en samenleving centraal staan. Ik ben dus in principe formeel coördinerend op dit dossier voor het Rijk, maar ik pak ook de handschoen op om dit soort belangrijke onderwerpen met onze medeoverheden te bespreken.

Dan de vragen van de heer Buijsse van de VVD. Bent u het ermee eens dat de motie-Rajkowski/Van Weerdenburg en de motie-Rajkowski c.s. nog niet zijn afgedaan? De motie-Rajkowski/Van Weerdenburg vraagt om een scan op de aanwezigheid van apparatuur van organisaties met een tegen Nederland

gerichte offensieve cyberagenda in de vitale infrastructuur. Deze motie is op dit moment nog in behandeling door mijn collega, de minister van Justitie en Veiligheid. De gevraagde scan is zeer complex en omvangrijk en hiervoor is er in 2023 door TNO, in opdracht van de minister van JenV, een onderzoek gestart. De eerste bevindingen van dit onderzoek zijn onlangs opgeleverd. Momenteel wordt bezien hoe het onderzoek kan worden afgerond en hoe de inzichten kunnen worden meegenomen. De minister van JenV zal uw Kamer hierover begin 2025 informeren.

De tweede motie, de motie-Rajkowski c.s., vraagt om te onderzoeken hoe apparatuur en programmatuur van organisaties uit landen met een tegen Nederland gerichte offensieve cyberagenda geweerd kunnen worden uit aanbestedingen van de rijksoverheid. In de Kamerbrief is als reactie hierop aangegeven dat we, in tegenstelling tot waar de motie om vraagt, niet bij voorbaat categorisch partijen uitsluiten, maar altijd een risicoafweging maken. Er worden daarom verschillende initiatieven benoemd waaraan is en wordt gewerkt zodat er veilig wordt ingekocht door de rijksoverheid. Denk aan de Algemene Beveiligingseisen Rijksoverheid Opdrachten, de Toolbox veilig inkopen die eerder al is teruggekomen en Inkoopeisen Cybersecurity Overheid. Uw Kamer is over de aanpak en de voortgang ten aanzien van veilig inkopen bovendien geïnformeerd in de technische briefing over veilig inkopen die voor de zomer is gehouden.

De **voorzitter**:

U heeft een interruptie van de heer Six Dijkstra van NSC.

De heer **Six Dijkstra** (NSC):

Ik heb eigenlijk een vraag over de uitvoering van de eerste motie, over een scan van apparatuur binnen de overheid. De staatssecretaris geeft aan dat dat best een omvangrijke klus is, zo vat ik het even in mijn eigen woorden samen. Tegelijkertijd lopen wij als commissie Digitale Zaken er vaker tegen aan dat we überhaupt heel slecht inzicht hebben in de apparatuur die zich op verschillende plekken binnen de overheid bevindt. Dan hebben we het niet alleen over Chinese en Russische apparatuur, maar in zijn algemeenheid. Denkt de staatssecretaris dat het mogelijk is dat de methodiek die gebruikt wordt om een scan als deze uit te voeren, ook nog ten goede kan komen van het beeld dat wij als Tweede Kamer kunnen krijgen van programmatuur, apparatuur en systemen die überhaupt binnen de overheid gebruikt worden?

Staatssecretaris **Szabó**:

Kunt u die vraag nog één keer stellen. Ik zit even te kijken welk antwoord ik moet geven, met name op de laatste twee zinnen.

De heer **Six Dijkstra** (NSC):

U mag er ook in de tweede termijn op terugkomen, hoor. Mijn vraag is eigenlijk de volgende. Deze scan vraagt om in kaart te brengen welke software of hardware van landen met een offensief cyberprogramma binnen de rijksoverheid wordt gebruikt. Een groter probleem waar wij als commissie Digitale Zaken tegenaan lopen, is het feit dat er in het algemeen te weinig inzicht is over de software, hardware en andere systemen die binnen de overheid gebruikt worden. Mijn vraag is dus: als er scans uitgevoerd worden waarin er wordt geselecteerd op land van herkomst, kan diezelfde methodiek dan gebruikt worden om de Tweede Kamer een beter beeld te geven van wat er binnen de overheid allemaal aanwezig is?

Staatssecretaris **Szabó**:

Ik was even aan het overleggen. Dit is een dusdanig belangrijke vraag dat ik hier in tweede termijn op terugkom.

Dan ga ik door naar de volgende vraag; die is ook van de heer Buijsse van de VVD. Is de staatssecretaris bereid om in de toekomst afspraken te maken, met en tussen departementen, die bijdragen aan het stapsgewijs meenemen van cyberrisico's voor de vitale processen? Het antwoord is als volgt. Onder coördinatie van de minister van Justitie en Veiligheid is er binnen de Aanpak vitaal en de brede cybersecurityaanpak doorlopend contact tussen departementen, het Nationaal Cyber Security Centrum, de NCSC dus, en het bedrijfsleven. Er zijn al veel afspraken en initiatieven over het wegnemen van cyberrisico's in vitale processen. Veel vitale aanbieders zijn hier ook wettelijk toe verplicht op grond van de Wet beveiliging netwerk- en informatiesystemen, de Wbni. Ook overheden krijgen deze verplichting als gevolg van de Cyberbeveiligingswet die al een aantal malen is langsgekomen. Vanuit mijn verantwoordelijkheid kijk ik uit naar het wegnemen van risico's voor de vitale processen bij de digitale overheid. Zo worden via departementen regelmatig instrumenten en handreikingen onder de aandacht gebracht bij vitale aanbieders, zoals de Toolbox veilig inkopen van daarnet en de cybercheck voor supplychainrisico's.

Dan een vraag van mevrouw Kathmann van ... Er staat op mijn blaadje "PvdA-GroenLinks", maar volgens mij moet dat "GroenLinks-PvdA" zijn. Welke is het?

De **voorzitter**:

GroenLinks-Partij van de Arbeid.

Staatssecretaris **Szabó**:

Oké. Mevrouw Kathmann van GroenLinks-Partij van de Arbeid vroeg: Kan de staatssecretaris aangeven wat zijn visie is op het cyberveilig houden van Nederland? Wat is zijn afweging tussen zo hoog mogelijk inzetten op veiligheid versus het gegeven dat 100% veiligheid niet bestaat? Als staatssecretaris Koninkrijksrelaties en Digitalisering onderstreep ik dat een veilige overheid essentieel is voor de digitale veiligheid van de samenleving. Daarbij heb ik stelselverantwoordelijkheid voor de informatiebeveiliging van de overheid en is de minister van Justitie en Veiligheid, JenV, verantwoordelijk voor het brede cybersecuritystelsel van de Nederlandse samenleving. In lijn met de aanstaande Cyberbeveiligingswet moet de overheid nu al een risicogestuurde aanpak hanteren. Daarbij wordt steeds de balans gezocht in het streven naar de optimale veiligheid. Het gaat om de afweging welke risico's acceptabel zijn en welke maatregelen proportioneel en effectief zijn in het licht van die risico's. Dat kan je niet alleen. Onze overheid moet daarbij opereren als één overheid, waarbij de rijksoverheid, provincies, gemeenten en waterschappen moeten samenwerken om de digitale weerbaarheid te waarborgen.

Dan de volgende vraag van mevrouw Kathmann van ... Hier staat wel "GroenLinks-Partij van de Arbeid". Wat is voor de staatssecretaris een acceptabele downtime ten aanzien van de digitale dienstverlening van de overheid? Welke responstijd van dienstverleners, zoals de partijen die betrokken zijn bij de NAFIN, verwacht de staatssecretaris? Het is van groot belang dat er goed nagedacht wordt over wat een acceptabele downtime kan zijn, maar op die vraag is geen generiek antwoord te geven. Wat in dezen acceptabel is, zal per dienst verschillend zijn en is afhankelijk van de beschikbaarheidseisen die aan de dienst gesteld worden door de betrokken partijen. Aan een dienst als DigiD of communicatiesystemen in de veiligheidssector worden hoge eisen gesteld en daarvoor zijn de maatregelen om een zo hoog mogelijke beschikbaarheid te realiseren uitgebreid. Bij sommige cruciale diensten, bijvoorbeeld bij basisregistraties, is beschikbaarheid niet het grootste goed; daar is de integriteit van de gegevens weer veel belangrijker. Dit kan in de loop der tijd verschuiven, waardoor het ook van belang is dat de beschikbaarheidseisen, evenals overige eisen, regelmatig beoordeeld en aangepast worden als dat nodig is, zodat zeker gesteld kan worden dat deze actueel, volledig en juist zijn.

Mevrouw Kathmann van GroenLinks-PvdA vroeg: is de nieuwe Cyberbeveiligingswet ook van toepassing op Caribisch Nederland? Zo nee, wat vindt de staatssecretaris daarvan en wat is zijn visie over het cyberveiliger maken van het gehele Koninkrijk? De Cyberbeveiligingswet, de implementatie van de NIS2-richtlijn, is niet van toepassing op Caribisch Nederland, omdat de richtlijn alleen van toepassing is op het Europese deel van de Europese Unie. Niettemin vind ik het van groot belang om de digitale weerbaarheid van het gehele Koninkrijk te versterken. Om te verkennen welke stappen nodig zijn om digitale weerbaarheid van de vitale

infrastructuur van het Caribische deel van het Koninkrijk te verhogen, is er ook een actie in het actieplan van de Nederlandse Cybersecuritystrategie. Vanuit mijn verantwoordelijkheid zie ik het als een belangrijke opgave om de digitale samenleving in het Caribisch gebied van het Koninkrijk der Nederlanden, als volwaardig onderdeel van het gehele koninkrijk, te versterken. Vanuit de gedachte van één overheid moeten we gezamenlijk zorgen voor het verhogen van de digitale weerbaarheid in het Caribische deel van het Koninkrijk. Daarover kan ik het volgende melden. Ik heb mijn eerste bezoeken benedenwinds gepleegd. Ik ga over twee weken bovenwinds op bezoek. Mijn voorgangster had dit ook als een van haar prioriteiten. Die neem ik over. Ik heb veel vragen gehad over weerbaarheid, maar ook over de digitalisering van dienstverlening. Ze zijn zelf namelijk ook bezig met het verbeteren van uitvoeringsprocessen in het kader van dienstverlening naar burgers en bedrijven. Ik heb ook aangegeven dat ik de plannen die ik de komende maanden op tafel wil leggen -- daarmee begon ik bij mijn inleiding -- zeker ook ga delen met het Caribisch gebied, om hen verder te helpen om hun dienstverlening aan burgers en bedrijven te verbeteren. Die toezegging heb ik daar zeker gedaan.

Dan vroeg de VVD naar een actueel overzicht van de software. Heeft u momenteel een actueel en volledig zicht op de software, apparatuur en cryptografie die gebruikt wordt voor onze vitale processen? Heeft u bij dit overzicht ook inzichtelijk of daar organisaties bij betrokken zijn uit landen die een tegen Nederland gekeerde cyberagenda voeren? Kan de Kamer kennisnemen van dit overzicht, eventueel onder geheimhouding? Informatie over specifieke software, apparatuur en cryptografie binnen alle vitale processen wordt niet in één centraal overzicht bijgehouden. Het is de verantwoordelijkheid van de vitale aanbieder om zelf zicht te hebben op de apparatuur die wordt gebruikt en welke risico's daaraan kleven. Een vitale aanbieder moet op basis van de risicoanalyse zelf passende maatregelen treffen om ervoor te zorgen dat de continuïteit van de vitale processen zo goed mogelijk beschermd is. Daar horen ook eventuele risico's uit toeleveringsketens bij. Wel hecht het kabinet aan goede ondersteuning van vitale aanbieders door het verhogen van de bewustwording en door het toepassen van economische veiligheidsinstrumenten zoals inkoop- en aanbestedingstoolboxen. Er bestaat geen centraal overzicht van de herkomst van de software, apparatuur en cryptografie die gebruikt wordt in de verschillende vitale processen in Nederland.

Dat waren mijn antwoorden op de vragen, voorzitter. Ik hoop dat ik er geen gemist heb.

De **voorzitter**:

Zijn er nog leden die een vraag hebben gemist?

De heer **Six Dijkstra** (NSC):

Ik heb volgens mij op drie vragen nog geen antwoord gehad. Eentje ging over het mandaat dat de staatssecretaris in zijn termijn wil gaan oppakken, zeker als het gaat om het verkrijgen van inzicht in systemen binnen de hele overheid. Dat raakt ook aan de interruptie die ik net had. Ik had ook nog vervolgvragen over Cisco Webex, die volgens mij allemaal nog niet beantwoord zijn. Ik kan ze herhalen, maar als de staatssecretaris ze daar nog heeft, bespaart dat mij moeite.

De heer **Valize** (PVV):

Ik heb nog geen antwoord gehoord op de vraag inzake Google Workspace over welke risico's nog steeds ...

De **voorzitter**:

Eén moment, meneer Valize.

Staatssecretaris **Szabó**:

Sorry, voorzitter, ik ben hier nieuw. Ik heb twee mapjes even links laten liggen.

De **voorzitter**:

O, kijk. Dit was gewoon een cliffhanger! Geen zorgen, de staatssecretaris gaat verder met de beantwoording van de vragen.

Staatssecretaris **Szabó**:

Dan hoop ik wel dat alle antwoorden erin staan. Een vraag van GroenLinks-PvdA. Volstaat volgens de staatssecretaris de huidige Nederlandse Cybersecuritystrategie om incidenten als bij NAFIN en CrowdStrike te voorkomen? Zijn er wijzigingen in de strategie nodig vanwege actuele ontwikkelingen? Het antwoord daarop is als volgt. Dit kabinet zet de ambities uit de Nederlandse Cybersecuritystrategie onverminderd voort om Nederland weerbaar te maken en incidenten te voorkomen. Tegelijkertijd moeten we beseffen dat systemen alsnog kunnen uitvallen. Een dienst kan ontregeld worden door menselijke fouten of door andere oorzaken. Daarom is het van belang dat alle (rijks)overheidsorganisaties naast het nemen van maatregelen ook plannen maken voor wanneer systemen toch uitvallen. Overheidsorganisaties moeten voorbereid zijn op uitval en moeten veel

oefenen. De NLCS wordt elk jaar herijkt op nieuwe dreigingen en ontwikkelingen. De minister van Justitie en Veiligheid zal u dit najaar informeren over de voortgang van de Nederlandse Cybersecuritystrategie en zal daarbij ook ingaan op eventuele wijzigingen in het actieplan. Deze recente incidenten worden daar uiteraard bij betrokken.

Dan ga ik naar incidentele storingen. De vragen van NSC waren als volgt. De staatssecretaris geeft aan dat er meerdere checks zijn uitgevoerd op Webex. Begrijp ik dan ook goed dat de voorspelbare logische volgordelijkheid uit de checks niet naar voren is gekomen? Zo ja, kwam dat omdat deze kwetsbaarheid überhaupt niet aanwezig was in de specifieke versie van Webex die de rijksoverheid het meest gebruikt, of omdat naar dit soort kwetsbaarheden niet gekeken wordt? Ten tweede: in welke mate heeft de staatssecretaris er zicht op of in de praktijk via Webex enkel informatie besproken wordt tot en met de rubricering "departementaal vertrouwelijk"? Er wordt regelmatig getoetst of er kwetsbaarheden zijn ontstaan in de producten. Nu zijn die via die Duitse journalist van -- als ik het goed heb -- Die Zeit bij het NCSC aan het licht gekomen. Deze kwetsbaarheden zijn toen verholpen. Met Cisco is overeengekomen dat de rijksoverheid aanvullend onderzoek kan doen vanwege het belang van de eerder geconstateerde late signalering door Cisco zelf. Tijdens dit aanvullende diepgaande beveiligingsonderzoek zijn er extra kwetsbaarheden aan het licht gekomen. Ook deze kwetsbaarheden zijn inmiddels verholpen. Ambtenaren zijn er zelf verantwoordelijk voor om enkel informatie tot en met departementaal vertrouwelijk te bespreken middels Webex. Zij worden wel regelmatig gewezen op die verantwoordelijkheid.

De **voorzitter**:

U heeft een interruptie van de heer Six Dijkstra van NSC.

De heer **Six Dijkstra** (NSC):

Dank, voorzitter. Die gaat over mijn eerste vraag. Daarbij vroeg ik eigenlijk door op de beantwoording van de minister op de schriftelijke vragen van de heer Valize van de VVD en van mij. De minister gaf daarin aan dat er onder andere een BSPA en een DPIA uitgevoerd zijn voordat Webex in werking trad binnen de rijksoverheid. Mijn vraag was dit. Uit de beantwoording is mij onduidelijk of de kwetsbaarheid door de voorspelbare logische volgordelijkheid in de unieke internetadressen van websites, niet bij zo'n BSPA of DPIA naar boven had moeten komen voordat zo'n systeem in werking treedt, aangezien het natuurlijk gaat om webadressen die elkaar heel logisch opvolgen waardoor je als het ware kan voorspellen wat voor URL de volgende meeting zal hebben. Dat lijkt mij iets wat bij zo'n check wel naar boven had kunnen komen. Dus mijn vraag is: is dat naar boven gekomen? En zo nee,

had dat dan wél naar boven moeten komen? Of is er überhaupt niet naar gekeken?

Staatssecretaris **Szabó**:

Ik heb hier mijn ideeën over. Ik ga die in de tweede ronde nog even terugbrengen, oké?

Dan van GroenLinks-Partij van de Arbeid: is er reden om te zoeken naar patronen die wijzen op structurele digitale kwetsbaarheden bij de overheid? Ook ik ben erdoor verrast bij mijn aantreden in dit kabinet dat het lijkt alsof er iedere maand wel een incident opduikt. Ik heb al eerder aangegeven dat ik hier twee maanden zit, met tweeënhalf of drie incidenten, en ik hoop niet dat dit structureel is. Ik heb uw Kamer deze week -- maar dat was mogelijk wat te kort voor dit debat -- per brief geïnformeerd over de recente incidenten, waarin ik het volgende heb gesteld. Er is geen indicatie dat de incidenten van de afgelopen drie maanden op enigerlei wijze aan elkaar gerelateerd zijn. Wel maken de diverse incidenten de afhankelijkheid van de rijksoverheid van netwerken en informatiesystemen zichtbaar, evenals de impact op de dienstverlening van de rijksoverheid wanneer deze systemen tijdelijk uitvallen. Deze afhankelijkheid is onvermijdelijk. Daarom is het van belang dat alle rijksoverheidsorganisaties maatregelen nemen en deze testen, zoals bijvoorbeeld met de TIBER-Rijkmethode, maar ook plannen maken voor wanneer systemen toch uitvallen. Overheidsorganisaties moeten voorbereid zijn op uitval, en ook veel oefenen. Het kabinet blijft daarom inzetten op de Nederlandse Cybersecuritystrategie 2022-2028 en de acties uit het actieplan. TIBER-Rijk, voor de mensen die niet weten wat dat is, is de voor de rijksoverheid geschikt gemaakte aanpak die De Nederlandsche Bank ontwikkelde voor de financiële sector, onder de I-strategie Rijk. In de NLCS is deze uitgevoerd en bekostigd. Ik wil wel een extra opmerking maken bij deze vraag. Wat dit ook impliceert, is dat we best wel bezig zijn met een complexe infrastructuur binnen de overheid, zowel het Rijk als gerelateerd aan medeoverheden. Mijn mening is dat we de laatste 25 jaar iets meer hadden moeten kijken naar de kwetsbaarheden. Dat betekent wat mij betreft dat dit onderwerp ook hoog op de agenda komt te staan de komende jaren. En daar wil ik nog een laatste opmerking bij maken. Vaak wordt ICT of digitalisering ingezet in de zin van "hé, kijk, we kunnen besparen als we ICT inzetten", bijvoorbeeld door minder personeel of weet ik wat. Maar we moeten vanaf nu, als we het hebben over zaken als weerbaarheid en het aankopen van nieuwe technologieën die je wilt implementeren rond de cloud of AI, ook gaan nadenken over: wat gaat dat kosten? Omdat het laatste wat ik wil is dat we, als we met goede plannen komen samen, aan het eind van de dag pas over financiën gaan praten en er dan achter komen dat de plannen die we hebben niet gerealiseerd kunnen worden. Dat is mijn lijn.

Dan de volgende vraag van GroenLinks-Partij van de Arbeid: wat is de visie van de staatssecretaris op het hebben van plannen op het moment dat er

een digitaal incident plaatsvindt, plannen om de storing zo snel mogelijk te verhelpen, maar ook plannen om de dienstverlening doorgang te laten vinden als systemen nog uitgevallen zijn? Het hebben van crisisplannen is vanzelfsprekend van groot belang. De Nederlandse Cybersecuritystrategie benadrukt het belang van snel en adequaat reageren op cyberincidenten en -crises. Zo is het Landelijk Crisisplan Digitaal, dat de gezamenlijke aanpak beschrijft bij een grootschalige digitale crisis, aanwezig. Daarnaast is het conform de Baseline Informatiebeveiliging Overheid, BIO, voor individuele organisaties binnen de overheid van belang om te beschikken over redundante systemen ten behoeve van de continuïteit van hun systemen en procedures voor back-up and restore. De BIO gaat ervan uit dat de organisaties bedrijfscontinuïteitsrisico's beheersen. Voor vitale aanbieders is het tevens verplicht om de nodige maatregelen te treffen om de continuïteit van hun diensten zo veel mogelijk te waarborgen. Verschillende sectoren hebben daarnaast aanvullende verplichtingen om de continuïteit te waarborgen via bijvoorbeeld de Drinkwaterwet of de Telecommunicatiewet. Toezichthouders controleren of vitale aanbieders algemene en sectorale wetgeving naleven. Dat geldt dus zeker voor het kunnen waarborgen van de continuïteit. Het is belangrijk dat er ook goed geoefend wordt, om ervoor te zorgen dat men weet hoe te handelen in een crisissituatie. En als laatste: het Nationaal Cyber Security Centrum en de Nationaal Coördinator Terrorismebestrijding en Veiligheid organiseren bijvoorbeeld ook op nationaal niveau de cyberoefening ISIDOOR om het Landelijk Crisisplan Digitaal te beoefenen. Als ik het wel heb, heeft niet zo lang geleden de laatste ISIDOOR plaatsgevonden.

Dan een vraag van GroenLinks-Partij van de Arbeid over "get used to it".

De **voorzitter**:

Excuses, zeker als voorzitter mag ik niet buiten de microfoon praten. Ik zei: het klinkt bijna als een applicatie.

Staatssecretaris **Szabó**:

Ja. Over "get used to it" ga ik eerst oplezen wat hier staat. De boodschap die de minister van JenV tijdens het incident heeft gecommuniceerd, is dat het in het digitale tijdperk cruciaal is dat IT-systemen vaak kunnen uitvallen door storingen. Zo waren er dit jaar de verstoringen die 28 augustus plaatsgevonden in het NAFIN-netwerk, en ook de storing op 19 juli in de software van het bedrijf CrowdStrike, waardoor onder andere de luchthaven Schiphol werd ontregeld. Het is erg dat deze storingen plaatsvinden. Vanuit de overheid zetten we in op meer weerbaarheid en redundantie in processen. Dat doen we onder meer via wetgeving als de Cyberbeveiligingswet, door acties uit te voeren uit de Nederlandse Cybersecuritystrategie en met de

Aanpak vitaal. Deze initiatieven worden gecoördineerd vanuit de minister van JenV. Ik heb dat "get used to it" ook gehoord. Ik heb ook iemand in een lezing gehoord die aangaf: doe er wat aan. Voor mij betekent "get used to it" ook: "doe er wat aan". We moeten get used eraan -- als ik het goed zeg in het Engels -- en ik heb al eerder aangegeven dat ook mijn voorganger en de premier hebben gezegd dat incidenten altijd kunnen plaatsvinden. Volgens mij bent u het daar ook mee eens. Maar dat "doe er wat aan" is het belangrijkste, en ik denk dat deze incidenten, met name omdat het er tweeënhalf à drie waren in twee maanden, een wake-upcall zijn voor ons allen om ook dit dossier serieus aan te blijven vliegen. Dat was het tweede blokje.

De **voorzitter**:

De heer Six Dijkstra van NSC heeft een vraag.

De heer **Six Dijkstra** (NSC):

Dank voorzitter, en ook dank aan de staatssecretaris voor de uitgebreide toelichting op "get used to it" en alles wat daarbij komt kijken. Ik ben blij dat hij het ook als wake-upcall ziet. Waar ik zelf van opkeek tijdens het incident in kwestie, toen we het over CrowdStrike hadden, is dat het effect van een digitale storing breder is dan digitale systemen: de bussen vallen uit, de vliegtuigen vallen uit, kassa's doen het niet meer en spoedeisende hulpen vallen uit. Dit zijn zaken waarvan je zou zeggen: daar zou ook een back-up voor moeten zijn, zodat als de systemen het niet doen ze alsnog hun dienstverlening kunnen regelen. Is dat ook iets wat op het netvlies van de staatssecretaris staat en hoe ziet hij dit binnen de plannen van weerbaarheid en redundantie?

Staatssecretaris **Szabó**:

U komt eigenlijk een beetje terug op de opmerking die ik een paar minuten geleden op tafel heb gelegd, namelijk dat we echt heel goed moeten kijken naar hoe we onze infrastructuur hebben ingericht en alles wat daarmee samenhangt. Dat heeft te maken met het goed inrichten van die systemen en voldoende applicaties hebben, maar ook met voldoende menscapaciteit om dat allemaal te kunnen beheren. Wat de overheid betreft is e-vakmanschap een van de dingen waar ik serieuzer naar ga kijken: hebben wij de juiste mensen om in ieder geval onze IT te onderhouden, maar ook om goed te kunnen nadenken over dit soort vraagstukken? En als laatste wil ik in dat kader zeggen -- daarom ben ik wel blij dat u deze opmerking maakt -- dat ook dit geld gaat kosten. Daar waar IT in mijn tijd als Kamerlid, zo'n achttien jaar geleden, werd gezien als van "mijn Word doet het niet, dus ik bel de

systeembeheerder", zitten we nu in een hele andere tijd. Dat heeft ook zijn consequenties. Daar ga ik graag met u de komende tijd over in gesprek.

Dan het blokje overige. Hoe kijkt de staatssecretaris aan tegen het beperken van onze digitale strategische afhankelijkheid? Digitale afhankelijkheden zijn niet te voorkomen en horen bij het openbaar handelssysteem. Sommige strategische afhankelijkheden zijn echter ongewenst. Dit gebeurt als er risico's ontstaan voor de borging van onze publieke belangen en nationale veiligheid. Op 17 oktober 2023 is uw Kamer geïnformeerd over de Agenda Digitale Open Strategische Autonomie, de DOSA, waarin de kabinetsaanpak voor de omgang met strategische afhankelijkheid in het digitale domein is uitgewerkt. Hierachter staat het woord "najaar". Ik kijk even naar mijn ambtenaar. In het najaar komt er een voortgangsrapportage. Dat is een belangrijke toevoeging.

Dan een vraag over de broncode van DigiD. Fragmenten die een beveiligingsrisico vormen zijn aangepast in de gepubliceerde versie. Die vraag kwam van de heer Valize van de PVV. Hij wil graag weten waarom er gekozen is voor deze oplossing. Het antwoord is dat het uitgangspunt was dat de broncode zo transparant mogelijk zou worden gepubliceerd. Door alleen deze fragmenten te vervangen door een "s" van security en mogelijke privacygevoelige delen te vervangen door een "p" van privacy konden de overige broncodes integraal vrijgegeven worden.

Dan nog een vraag met betrekking tot DigiD. Fragmenten die een beveiligingsrisico vormen, zijn aangepast in de gepubliceerde versie. Kan de inzet van AI, artificial intelligence, niet alsnog de gewijzigde code corrigeren en vormt dit dan geen risico? Het antwoord hierop is dat de meeste fragmenten die zijn weggehaald geen broncode bevatten, maar data zoals sleutelmateriaal voor testomgevingen. Dit zijn unieke data die niet door AI kunnen worden gereconstrueerd. AI is alleen goed voor het corrigeren van code die min of meer logisch voorkomt in andere code die het model heeft gebruikt om te trainen. Dat is hier niet van toepassing, omdat de gegevens die in de gepubliceerde code zijn aangepast nergens anders voorkomen.

Nog een vraag van de heer Valize van de PVV met betrekking tot Google Workspace. Google Workspace, agendapunt 2 en 8 van vandaag, bleek niet in lijn met de AVG, maar er zijn maatregelen genomen om daar alsnog aan te voldoen. We lezen dat overheidsorganisaties Google Workspace kunnen gebruiken, mits ze specifiek aanvullende maatregelen afwegen, afhankelijk van de situatie. De PVV wil graag weten welke risico's er nog steeds bestaan, om welke maatregelen het gaat en of dit voor alle overheidsorganisaties gelijk is. Dat is de vraag. Dan is hier het antwoord. Naar aanleiding van het onderzoek door strategisch leveranciersmanagement, oftewel SLM Microsoft, Google Cloud en AWS, zijn er geen resterende AVG-risico's geïdentificeerd als de aanbevolen maatregelen in acht worden genomen. Echter, SLM kan niet in alle scenario's voorzien welke inhoudelijke data er met het gebruik van Google Workspace door rijksoverheidsorganisaties gemoeid zijn. Daarom

dient elke individuele overheidsorganisatie voor zijn specifieke gebruikerscontext af te wegen of het gebruik van Google Workspace verantwoord is. Eventuele aanvullende benodigde maatregelen hangen af van de specifieke context. Daarnaast geldt dat de overheidsorganisaties op grond van de wet zelf verantwoordelijk zijn voor het voldoen aan de AVG en daarom altijd zelf moeten vaststellen of er met het gebruik van Google Workspace aan kan worden voldaan. Uiteraard kan daarbij gesteund worden op de onderzoeken die SLM heeft uitgevoerd.

Dan nog een vraag van de heer Valize, over TikTok. Hij zegt: de vorige staatssecretaris heeft de stekker uit TikTok getrokken. Er staat op mijn blaadje "geen burgers informeren?" Gaat de staatssecretaris dit heroverwegen, vraagt hij. Er stond een vraagteken verkeerd. Het gebruik van TikTok wordt rijksambtenaren ontraden. Het gebruik daarvan op mobiele devices uitgegeven door de rijksoverheid is technisch onmogelijk gemaakt. Voor privédevices kunnen burgers en rijksambtenaren zelf afwegen of zij gebruik willen maken van dergelijke applicaties. Punt. Ik zit nog even na te denken, voorzitter, maar ik krijg al een vraag, zo te zien.

De heer **Valize** (PVV):

Dat betekent dat er dus geen informatievoorziening vanuit de overheid richting de gebruikers van TikTok gaat. Klopt dat?

Staatssecretaris **Szabó**:

Ja, vanuit het ministerie van Algemene Zaken is dat als advies meegegeven.

De **voorzitter**:

Er rest nog een vraag van de heer Six Dijkstra. Die komt in de tweede termijn. Zijn verder alle vragen van iedereen beantwoord? Ja, alles is beantwoord. Dank aan de staatssecretaris voor de beantwoording.

Dat brengt ons bij de tweede termijn. Is er behoefte aan een tweede termijn? Ja, dat is het geval. Daar staat volgens mij anderhalve minuut voor. Dan beginnen we bij de heer Six Dijkstra van NSC.

De heer **Six Dijkstra** (NSC):

Dank, voorzitter. Dank ook aan de staatssecretaris voor dit debat. Ik heb nog één vraag die de staatssecretaris wel even aanraakte, maar waar hij mijns inziens nog niet voldoende antwoord op heeft gegeven. Hoe gaat hij de komende tijd zijn mandaat verder invulling geven? Dat zit 'm niet alleen op

informatiebeveiliging, maar überhaupt op systemen. Als het gaat om digitale systemen, is het binnen de overheid vaak niet alleen zo dat de rechterhand niet weet wat de linkerhand doet, maar dat de linkerhand vaak ook niet weet wat de linkerhand doet. Wij als Kamer zijn vaak zeer beperkt geïnformeerd over de systemen die er draaien en over de licenties die worden afgenomen. Mevrouw Kathmann en ik zijn er in het clouddossier ook tegen aangelopen dat we werkelijk geen flauw idee hebben hoeveel overheidsinstanties zijn overgegaan op de cloud en welke providers ze hebben. Dat gaat eigenlijk om een breder probleem. Ik denk dat er een hoop nieuw inzicht nodig is in de systemen die de overheid gebruikt en hoe die samenhangen. Is de staatssecretaris dat met mij eens? Is hij voornemens om zijn termijn te gebruiken om daar een verbeterslag in aan te brengen, ook in lijn met de aanbevelingen van de Algemene Rekenkamer? Wat kunnen wij daarvan verwachten?

Tot slot zou ik graag een tweeminutendebat willen aanvragen voor eventuele moties.

Dank u wel.

De **voorzitter**:

Dank u wel. Dan gaan we naar de heer Valize van de PVV.

De heer **Valize** (PVV):

Dank, voorzitter, voor het woord. Dank allen, voor de uitgebreide vragen en dank aan de staatssecretaris voor de beantwoording daarvan. Ik had een vraag gesteld over een post die op LinkedIn voorbijkwam over het iBestuur Congres. Zou hij al een tipje van de sluier kunnen oplichten of moeten wij wachten tot het regeerakkoord? Ik denk wel dat we uit de beantwoording en reacties hebben kunnen vernemen dat de staatssecretaris van harte ondersteund wordt in wat wij allemaal vinden, namelijk dat er meer centrale regie moet komen.

Ik heb geen verdere vragen. Dank.

De **voorzitter**:

Dank u wel. Dan is de heer Buijsse van de VVD.

De heer **Buijsse** (VVD):

Dank je wel, voorzitter. Ik heb drie vragen, over de weerbaarheid, de scan en de regie. Ik heb vernomen dat er in het kader van de weerbaarheid

crisisoefeningen plaatsvinden. U verwees bijvoorbeeld naar de ISIDOOR-oefening. Ik was er onbekend mee dat dit soort oefeningen plaatsvindt. Ik ben blij dat dit gebeurt. Ook uit fysieke crisisoefeningen -- politici doen die weleens, ik als wethouder in ieder geval heel veel -- moet je proberen lessen te trekken. Ik wil de staatssecretaris vragen of de Kamer kennis kan nemen van de crisisoefeningen die plaatsvinden en de lessen die geleerd worden, zodat wij daar gezamenlijk, en niet alleen de oefenende instanties, lering uit kunnen halen, want ik wil graag meeleren als dat zou kunnen. Dus graag een reactie van de staatssecretaris daarop.

Als tweede punt de scan. U informeerde ons erover dat de scan in uitvoering is. Ik ben echt heel blij om dat te vernemen, dus dank. U zegt: we gaan de Kamer hierover begin 2025 informeren. Dat is ook goed om te vernemen. Maar ik vind wel dat wij als commissie voor Digitale Zaken toegang mogen hebben tot een gesprek met de uitvoerders van deze scan. Ik ben ontzettend nieuwsgierig hoe die scan gaat. De staatssecretaris informeert ons erover dat het moeilijk, lastig, omvangrijk en complex is. Alle begrip daarvoor. Ik zou daarover graag mondeling in gesprek willen in een technische briefing of een van de andere mogelijkheden die daarvoor bestaan. Dat wil ik ook weer gewoon puur om van te leren.

Het derde punt is de regie, ook aansluitend op de mandaatvraag van de voorgaande spreker, Six Dijkstra. Ik ben er uiteindelijk gewoon niet tevreden over dat we het accepteren ... Nee, we accepteren het niet -- daar zijn we het namelijk eigenlijk allemaal over eens -- maar het is nu zo dat heel veel departementen bevoegdheden hebben over hun eigen systemen en software, met de bijbehorende risico's. Ik zie daar uiteindelijk toch een kwetsbaarheid in. Ik wil de staatssecretaris echt helpen door hem in positie te brengen. Een instrument van een Tweede Kamerlid is bijvoorbeeld het gezamenlijk indienen van een motie. Dan zetten we het kabinet op die manier onder druk om de staatssecretaris meer mandaat te geven. Maar ik weet niet of dat een politiek wijze zet is. Ik vraag me dus ook af hoe we u het beste kunnen helpen om u beter in het zadel te krijgen. Zo kunt u de regie pakken, wat we eigenlijk allemaal wel willen. Dus graag een reactie van de staatssecretaris daarop.

Dank u wel.

De **voorzitter**:

Dank u wel, meneer Buijsse. Ik wil u even meegeven dat het niet aan de staatssecretaris is om uw vraag over een technische sessie te beantwoorden. Als u dat in een procedurevergadering voorlegt aan uw collega's -- uw voorzitter wordt er bijvoorbeeld heel enthousiast van -- en er een meerderheid voor is, wordt zo'n technische sessie ingepland met degenen die de scan uitvoeren.

De heer **Buijsse** (VVD):

Alle begrip daarvoor. Toch zou ik van de staatssecretaris willen weten of de mogelijkheid bestaat om de informatie voor zo'n technische briefing aan te bieden, als die geheim is. Ik zou de randvoorwaarden van het ministerie dus graag willen meenemen bij zo'n verzoek.

De **voorzitter**:

We kunnen ook een vertrouwelijke technische briefing inplannen. Wat dat betreft kunt u goed bediend worden, denk ik.

Ik vraag de heer Six Dijkstra om het voorzitterschap even over te nemen.

**Voorzitter: Six Dijkstra**

De **voorzitter**:

Zeker. Dan geef ik bij dezen het woord aan mevrouw Kathmann van de fractie van GroenLinks-PvdA.

Mevrouw **Kathmann** (GroenLinks-PvdA):

Dank u wel, voorzitter. Ik wil de staatssecretaris ook bedanken voor de heldere beantwoording van de vragen. Ik heb vandaag geprobeerd om hem woorden in de mond te leggen. Normaal gesproken zou ik daarvoor excuses aanbieden. Ik vind het ook helemaal niet prettig als mensen dat bij mij doen. Maar ik vind het toch jammer dat het niet is gelukt. Ik had graag gezien dat we na vandaag "get used to it" niet meer gebruiken en "get ready!" gaan hanteren in deze commissie.

Ik heb nog een vraag over de downtime. De staatssecretaris zei: eigenlijk ligt het er per dienst aan wat een acceptabele downtime is. Is er dan voor elke dienst zo'n downtime gedefinieerd? Als dat niet zo is, zou dat dan wel een goed plan zijn?

Ik heb ook nog een vraag over de weerbaarheid. Ik snap heel goed -- ik ben het daar helemaal mee eens -- dat we moeten trainen en van alles en nog wat moeten doen. We hebben handreikingen, zijn aan het verkennen en we zijn in gesprek. Maar ik heb ook heel concreet gevraagd wat nou de mogelijkheden zijn om bepaalde zaken af te gaan dwingen. De staatssecretaris zei zelf ook: de tijd van vrijblijvendheid is voorbij. Welke mogelijkheden zijn er in dit hele proces, van inkoop tot implementatie,

gebruik, updates en noem het maar op, om bepaalde dingen in vitale onderdelen van onze maatschappij af te dwingen?

De **voorzitter**:

Dank u wel, mevrouw Kathmann. Ik geef de voorzittershamer weer terug aan u.

**Voorzitter: Kathmann**

De **voorzitter**:

Dank u wel. Ik kijk even naar rechts. Hoeveel tijd denkt de staatssecretaris nodig te hebben voor de beantwoording van de vragen? 20 seconden? Nou, dan schorsen we voor 20 seconden en gaan we daarna naar de beantwoording.

De vergadering wordt enkele ogenblikken geschorst.

De **voorzitter**:

We gaan naar de beantwoording van de staatssecretaris.

Staatssecretaris **Szabó**:

Dank u wel, voorzitter. Allereerst de vraag van de heer Six Dijkstra over Webex. De kwetsbaarheid gaat over opeenvolgende meeting-ID's en niet over IP-adressen, heb ik doorgekregen. Dit is in een BSPA, een Baseline Security Product Assessment, of een DPIA niet aan de orde gekomen, maar bleek wel uit aanvullende securitytesten, die regelmatig gedaan worden. Mijn vraag blijft daarom waarom Cisco dit niet zelf geconstateerd heeft. Dit is ook onderwerp van het gesprek dat ik op dit moment voer met Cisco.

De heer **Six Dijkstra** (NSC):

Ik refereerde aan de tekst die in de brief stond. Daarin werd "internetadressen" gezegd, natuurlijk geen IP-adressen. In dit geval ging het om URL's. Oké, dan is in ieder geval duidelijk dat dit soort dingen niet geconstateerd worden in de checks die gedaan worden. Is de staatssecretaris het niet met mij eens dat dit soort quick wins eigenlijk wel aan de voorkant

gepakt zouden moeten worden? Als je in vertrouwelijke meetings metadata naar boven kunt halen omdat ze zo voorspelbaar zijn, is dat misschien wel zo basaal dat dit soort kwetsbaarheden in zo'n check überhaupt niet naar voren komen. Maar als de producent het zelf niet ziet, zou het eigenlijk wel door de afnemer geconstateerd moeten worden.

Staatssecretaris **Szabó**:

Het antwoord daarop is natuurlijk ja. We zijn ook verder gegaan met Cisco, zoals u weet. Ook hier leren we weer van met z'n allen als het gaat om dossieropbouw voor toekomstige mogelijke problemen, die er hopelijk niet komen.

Dan de vraag van de heer Six Dijkstra over systemen. Ik vind het iets te ingewikkeld om hier af te doen met een of twee zinnen. Ik wil hier echt even met mijn ambtenaren over verder praten. Ik beloof hierover binnenkort een brief naar u toe te zenden.

De heer **Six Dijkstra** (NSC):

Ik zie daarnaar uit. Kan de staatssecretaris ook een termijn geven voor de brief, zodat we dat kunnen vastleggen als officiële toezegging?

Staatssecretaris **Szabó**:

Vier weken. Mijn ambtenaren dachten eerst dat ik "één week" zei, dus ze schrokken al van mijn nieuwe aanpak, maar ik geef ze dus wat meer tijd.

Dan met betrekking tot ISIDOOR. Daarvan is inmiddels al een evaluatie gezonden naar de Kamer. Als het goed is, ligt die ook bij u ergens op het bureau.

Met betrekking tot de scan kunnen we altijd een technische briefing toezeggen, ook samen met JenV. We moeten even bekijken hoe we dat onderwerp verder oppakken.

Mij in positie brengen vind ik misschien wel de meest interessante vraag voor de komende vier jaar. Het liefst had ik mijzelf iets meer in positie gebracht zien worden tijdens de onderhandelingen en het verdelen van de posten, maar ik zit hier als staatssecretaris die formeel verantwoordelijk is voor coördinatie binnen het Rijk. U ziet, hoop ik ook in mijn optreden gisteren, dat ik toch wel probeer de grenzen op te zoeken. Dat doe ik niet voor de lol. Lagere overheden vragen ook aan mij: hoe staat het met de regie? Ik denk dat het, na 25 jaar praten over dit onderwerp, steeds meer tussen de oren van bestuurders komt te zitten dat de regiefunctie op het gebied van digitalisering belangrijk is, want digitalisering is niets anders dan het bloed

dat door onze aderen stroomt. Het is dus geen klein dingetje. Als je het niet hebt, houd je op te bestaan. We moeten dus even samen bekijken hoe we dit verder oppakken. Desondanks weet ik wat mijn mandaat is. Ik sta in ieder geval in de stand van verder kijken, misschien eigenlijk ook al voor mijn opvolger of opvolgsters, om te bezien hoe we dit allemaal beter kunnen inrichten. Daarbij komen allerlei onderwerpen aan de orde, waaronder ook de onderwerpen die we vandaag hebben besproken. Hoe moet ik het netjes zeggen? Laat ik het maar zo zeggen: ik ga er vol in om dit nog beter gestructureerd te krijgen.

Dan "get ready". Ik ben u al tegemoetgekomen, aan de hand van een lezing die ik heb gehoord, van een paar dagen geleden, en zeg: doe er wat aan. Ik houd het dus toch Nederlands. We hebben al zo veel afkortingen -- vandaag zijn het er 70 -- dus als we dan ook nog Engels gaan praten ... Ik hoop dus dat u een beetje met mij meebuigt en dat u "doe er wat aan" als de nieuwe uitspraak forceert.

Dan het afdwingen van bepaald softwaregebruik en dat soort zaken. We zijn aan de slag gegaan, ook kijkende naar hoe het nu allemaal loopt, met een IT-sourcingdocument. Dat heb ik gevraagd van mijn CIO Rijk. Ik denk dat we dat in 2025 gaan afscheiden, want we moeten dat echt heel goed gaan inkleuren. Het gaat ook over leveranciersmanagement en dat soort zaken. Ook dit onderwerp moeten we dus gewoon straktrekken met z'n allen. Dat komt er dus aan. Dat kan ik toezeggen.

Dat was 'm van mijn kant, voorzitter.

De **voorzitter**:

Dank u wel. Dan kijk ik even naar links of alle vragen zijn beantwoord. Dat is zo.

Dan gaan we naar de toezeggingen. Ik heb er als het goed is vier.

- In het tweede kwartaal van 2025 ontvangt de Kamer een brief over de opvolgingen van de aanbevelingen naar aanleiding van het rapport Digitale Kroonjuwelen. De aanleiding is een vraag van de heer Six Dijkstra.

- Begin 2025 wordt de Kamer nader geïnformeerd over de uitvoering van de motie-Rajkowski/Van Weerdenburg over de scan van de apparatuur van de overheid. De aanleiding was een vraag van de heer Buijsse.

- In het najaar van 2024 ontvangt de Kamer de voortgangsrapportage DOSA.

- Binnen vier weken krijgt de Kamer een brief naar aanleiding van de vraag van de heer Six Dijkstra met betrekking tot de methodiek voor de scan van alle systemen.

De heer Six Dijkstra heeft een tweeminutendebat aangevraagd, dat wordt ingepland.

Er is een verzoek gedaan voor een technische sessie. Dat moeten we via de procedurevergadering doen.

Ik sluit dit commissiedebat over informatievoorziening bij de overheid. Ik dank de staatssecretaris, die nog even zijn vinger heeft opgestoken.

Staatssecretaris **Szabó**:

Over DOSA zal door de minister van EZK gerapporteerd worden, begrijp ik. Wij noemen dit ministerie "EZ". Het is nog wennen.

De **voorzitter**:

Perfect. Dank aan de staatssecretaris voor deze toevoeging. Dank ook voor de beantwoording. Dank voor dit allereerste commissiedebat in uw functie van staatssecretaris. We gaan volgende keer een poging wagen om minder jargon en afkortingen te gebruiken. Ik verwijs iedereen ook naar het cyberwoordenboek, volgens mij gewoon te vinden op cyberwoordenboek.nl.

De heer Six Dijkstra wil ook nog iets zeggen ter afsluiting.

De heer **Six Dijkstra** (NSC):

Ik wil ook u bedanken, voorzitter. Klopt het dat dit het laatste commissiedebat is in uw rol van voorzitter?

De **voorzitter**:

Ik denk onofficieel wel. Maar officieel is het natuurlijk onze taak als Kamerleden om nog in te stemmen met de nieuwe voorzitter en ondervoorzitters. Het is volgens mij goed gebruik dat dit zonder problemen zal verlopen. Daar ga ik dan maar even van uit. Dan is dit inderdaad mijn laatste commissiedebat als voorzitter.

De heer **Six Dijkstra** (NSC):

Alle procedures ten spijt: dat laat onverlet dat ik u heel hartelijk wil bedanken voor het goede werk in de afgelopen maanden dat ik u heb meegemaakt.

Sluiting 15.00 uur.