5
Vragenuur

Vragen van het lid Gesthuizen aan de minister van Veiligheid en Justitie over **spyware waarmee een toeleverancier van het leger blijkt te zijn bespioneerd**.

☐

Mevrouw **Gesthuizen** (SP):
Voorzitter. Het was weer zo ver. Een trojan bleek misbruik te maken van een tot dusver onbekend lek in software, namelijk in het Windows besturingssysteem. Bij een eerder lek werd nota bene een leverancier van het Nederlandse leger getroffen. De principiële vraag die zich de afgelopen tijd bij dit soort zaken steeds weer opdringt, is of het terecht is dat zo veel vertrouwen wordt geschonken aan een steeds verdergaande digitalisering van de samenleving. Gaan wij niet te snel? Is de overheid wel veilig bezig en zich bewust van risico's, ook bij toeleveranciers van belangrijke instituten zoals het Nederlandse leger?

Welke organisaties in Nederland houden zich bezig met de mogelijke implicaties van verspreiding van en besmetting door zeer complexe spionage malware van het type stuxnet en duqu, en virussen zoals conficker? Wat kunnen burgers en bedrijven verwachten van deze organisaties? Ik vraag de minister om de Kamer hierover uitgebreid te informeren. Is er reeds informatie beschikbaar over de organisaties of personen die verantwoordelijk zijn of kunnen zijn voor de verspreiding van dergelijke malware? Heeft het kabinet een inventarisatie gemaakt van mogelijk voor aanvallers relevante, interessante of ten minste voor de overheid gevoelige doelwitten van cybercriminelen of -organisaties, dan wel van landen die spionageactiviteiten in Nederland willen verrichten? Zo ja, neemt de overheid dan maatregelen om schade zo veel mogelijk te voorkomen? Acht het kabinet het uitgesloten dat niet alleen informatie wordt ontvreemd van partijen die zorgdragen voor kritieke infrastructuren, maar dat langs deze weg ook toegang wordt verkregen tot fysieke infrastructuren, mogelijk met daadwerkelijk gevaar voor mensenlevens. Hoewel ik begrijp – het is ook mensenwerk – dat er altijd fouten in systemen kunnen sluipen, vraag ik het kabinet toch om producenten zoals Microsoft in dezen aan te spreken. Als wij met hen niet tot richtlijnen kunnen komen, laten wij dan in ieder geval zorgen dat er regels zijn om mogelijke schade te kunnen verhalen.

☐

Minister **Opstelten**:
Voorzitter. Ik dank mevrouw Gesthuizen voor haar vragen. In antwoord op de eerste vraag kan ik zeggen dat de Nederlandse diensten AIVD, MIVD en Govcert dit proces goed in de gaten houden. Zij spelen de betrokken organisaties alle informatie toe, zoals in dit verband ook is gebeurd door Govcert op 19 oktober. Zijn wij op de hoogte van gevoelige doelwitten? Natuurlijk zijn onze diensten dat. Zij geven de informatie door aan de NCTB, de nationale coördinator, die een en ander natuurlijk weer op de juiste plaatsen doorpgeeft en ons op de bekende terreinen informeert. Op 1 januari hebben wij de Cyber Security Council en de National Cyber Security Office waar alle krachten bij elkaar komen. Wij hebben er geen indicatie van, maar er is een risico dat dit soort fouten in de programmatuur gemaakt worden. Wij hebben de indicatie dat er in Nederland één besmetting is. Wij weten niet waar het om gaat. De geruchten over Defensie kunnen door ons niet bevestigd worden. Via onze internationale netwerken en kanalen houden wij contact met Microsoft en andere bedrijven die hierbij betrokken zijn.

Mevrouw **Gesthuizen** (SP):
Ik zou het zeer op prijs stellen als de Kamer uitgebreid wordt geïnformeerd over de wijze waarop de communicatie naar aanleiding van dit laatste voorval precies is verlopen. Hoe is precies gecommuniceerd met Govcert, met de AIVD, met de MIVD? Ik wil dat graag inzichtelijk krijgen. Ik ben ook benieuwd naar wat de minister zich voorstelt van een screening van leveranciers. De minister zegt dat hem niets bekend is over de toeleverancier van het leger. De afgelopen weken heeft mij informatie bereikt waaruit blijkt dat dit wel het geval is geweest. Het bedrijf Acal BFI, een grote Europese toeleverancier van het leger, is getroffen door een cyberattack. Het zou mij dus hooglijk verbazen als de minister daar nog helemaal niet van op de hoogte is. Hoe gaat hij leveranciers van dergelijke belangrijke infrastructuren screenen?

Minister **Opstelten**:
Ik geef even aan hoe dit concreet is gegaan. De Amerikaanse antivirusleverancier Symantec heeft op 19 oktober het duquvirus waar het hier over gaat, kenbaar gemaakt op zijn website. Govcert.nl en de inlichtingendiensten hebben vervolgens contact gelegd binnen hun internationale netwerk om meer informatie te achterhalen. Op 19 oktober heeft govcert.nl een bulletin uitgestuurd naar zijn publieke partners en de relevante vitale sectoren om ze te informeren. Op dit moment lijkt de impact van het duquvirus beperkt. Wereldwijd gaat het over tien à twintig besmettingen. In Nederland gaat het om één geval. Doordat het bij spionage gaat om het heimelijk verkrijgen van informatie, is het moeilijk een exact beeld te verkrijgen. Dat is er niet. De MIVD doet momenteel onderzoek en zal via de geëigende kanalen op korte termijn informatie geven over de uitkomsten.

Dan kom ik op de laatste vraag. Ik heb al in eerdere debatten, over DigiNotar bijvoorbeeld, aangekondigd dat er een cyberbeeld Nederland aankomt. Dat is zeer nabij. Het komt nog dit jaar. Daarin zal inzicht worden gegeven in dreigingen en dreigers op dit gebied. Dat gaat naar de Kamer zoals wij hebben afgesproken.

Mevrouw **Gesthuizen** (SP):
Dat laatste is heel belangrijk. Die toezegging is gedaan. Ik ben echter niet volledig gerust op wat ik als Kamerlid voor ogen heb, namelijk de manier waarop er gecommuniceerd wordt tussen de diverse inlichtingendiensten, mede aangezien wat wij daar in de Kamer van meekrijgen. Daar vertrouw ik nog niet blind op. Ik apprecieer het zeer als de minister dit voor ons op papier zet en ons daarover informeert, met name omdat er in beide debatten over DigiNotar, waar de minister zelf ook naar verwees, nogal wat vraagtekens zijn gezet bij het opereren van bijvoorbeeld govcert.nl en de snelheid waarmee dergelijke diensten kunnen ingrijpen als er problemen zijn.

Minister **Opstelten**:
Ik heb heel concreet en precies aangegeven wat er is gebeurd. Het kost mij geen moeite om binnen de mogelijk-

heden de Kamer adequaat te voorzien van de informatie die wij van de diensten krijgen rond dit proces, dat belangrijk is. Uiteraard.

De heer **El Fassed** (GroenLinks):
De grote ontbrekende in dit verhaal is DefCERT, de digitale veiligheidsdienst van Defensie. Wat zijn precies de afspraken tussen govcert.nl en DefCERT over toeleveranciers van Defensie? Als DefCERT nog niet voldoende is toegerust, zoals wij vanuit Defensie begrijpen, wanneer wordt die dan wel voldoende toegerust? Is 2012 niet een wat laat tijdstip daarvoor?

Minister **Opstelten**:
Hier geldt voor mij precies hetzelfde antwoord. Govcert.nl heeft de informatie gekregen van de diensten. Die is daarvoor. Die heeft de collega's allemaal geïnformeerd. Er is geen bevestiging van het bericht dat dit een Defensiegerelateerde besmetting is, zo zeg ik nu. Dat staat in allerlei stukken. Ik heb dat een- en andermaal gevraagd. De diensten gaan verder. Ik houd mij bij wat ik net ook tegen mevrouw Gesthuizen zei: ik zal de Kamer informeren binnen de bestaande verantwoordelijkheden en de Kamer kent de gremia waar de informatie naartoe gaat.

De **voorzitter**:
Ik dank de minister voor de beantwoording.