6
Vragenuur: Vragen Schouw

Vragen van het lid Schouw aan de minister van Defensie over **het bericht dat e-mailadressen van het ministerie van Defensie zijn gehackt**.

☐

De heer **Schouw** (D66):
Mevrouw de voorzitter. In augustus werd Nederland slachtoffer van de grootste hack in de geschiedenis. Ook het ministerie van Defensie werd aangevallen, wat natuurlijk zeer ernstig is omdat Defensie zich wereldwijd inzet voor het bestrijden van brandhaarden, voor het brengen van vrede en voor het bijdragen aan de veiligheid. Nu wisten we al uit de debatten van mei dat ICT zo ongeveer de zwakste schakel van het ministerie van Defensie is. Deze minister zei dat ze er alles aan moet doen om in control te komen. Mijn fractie is echt geschrokken van de hack. Daaruit zou je namelijk kunnen afleiden dat het ministerie van Defensie en de aanpalende organisaties op ICT-gebied zo lek zijn als een mandje.

Op papier gebeurt er ontzettend veel. Een maand geleden werd nog het Defensie Cyber Commando opgericht en ook er is een Joint Sigint Cyber Unit. Er worden tientallen miljoenen geïnvesteerd in ICT en er is bij Defensie zelfs een heuse honeypot om hackers te onderscheppen. Hoe geloofwaardig is echter die papieren werkelijkheid als je aan de andere kant ziet dat Defensie gevoelig is voor dit soort ICT-hacks?

Ik heb dan ook de volgende vragen. De eerste vraag is natuurlijk wanneer de minister dit wist. De tweede is hoe dit heeft kunnen gebeuren. De derde vraag is wie daarvoor verantwoordelijk is, en of er nog een aantal goede gesprekken met die mensen gaat plaatsvinden. De vierde vraag is wat de risico's voor de veiligheid zijn, hier in Nederland, maar met name voor de operaties in het buitenland.

Minister **Hennis-Plasschaert**:
Voorzitter. Dank voor de gestelde vragen. Deze zomer werd inderdaad bekendgemaakt dat wereldwijd 1,2 miljard inloggegevens zijn verkregen. Het Nationaal Cyber Security Centrum heeft vervolgens van het Amerikaanse bedrijf Hold Security de beschikking gekregen over de domeinnamen en e-mailadressen met een .nl-extensie. Het gaat om ongeveer 5600 kwetsbare websites en ongeveer 1,3 miljoen e-mailadressen en inlognamen die eindigen op .nl. Er staan inderdaad ook adressen van het ministerie van Defensie op die lijst. Het gaat daarbij om ongeveer 380 e-mailadressen. Een hoeveelheid daarvan is niet meer in gebruik. Een aantal is nog valide. Het gaat dan om medewerkers die, zoals wij dat intern zeggen, contact hebben met de buitenwereld, bijvoorbeeld omdat ze zich registreren voor een congres. Ze zijn dan op een kwetsbare site geweest. Ook kan het zijn dat ze zich aanmelden voor een nieuwsbrief.

Het Defensie Computer Emergency Response Team, DefCERT, en de Beveiligingsautoriteit zijn in een heel vroeg stadium geïnformeerd door de NCSC. De dataset is vervolgens geanalyseerd. Ik herhaal dat het gaat om ongeveer 380 e-mailadressen, waarvan het merendeel niet meer in gebruik is. Omdat defensiemedewerkers sowieso heel regelmatig hun wachtwoord moeten wijzigen, is er geen gevaar geweest van ongeautoriseerde toegang tot MULAN. MULAN is het interne departementale vertrouwelijke netwerk. Op afstand dat systeem binnenkomen is niet mogelijk als je niet beschikt over nog een hoeveelheid gegevens en een bepaalde pas. Om operationele redenen ga ik daar nu niet verder op in. Het is dus niet mogelijk geweest om het systeem van Defensie binnen te komen. De digitale infrastructuur van Defensie is derhalve niet geraakt. Ik kan dus geruststellende woorden uitspreken aan het adres van de heer Schouw.

De heer **Schouw** (D66):
Ik ben blij met deze beantwoording van de minister. Je moet er natuurlijk niet aan denken dat binnen die heel gevoelige organisatie, die bezig is met de veiligheid in binnen- en buitenland, hackers zomaar direct toegang kunnen krijgen tot gevoelige informatie. Aan de andere kant heb ik het idee dat de minister een uiterste poging doet om het heel klein te maken. Het gaat om een nieuwsbrief en ze zegt dat je op afstand niet zou kunnen binnendringen in de systemen van Defensie. Ik wil toch graag van de minister weten wanneer zij voor het eerst hoorde dat het mogelijk was om binnen te dringen. Er is namelijk gewoon gehackt. Dat betrof weliswaar een beperkt aantal gevallen, maar het is gebeurd. Wanneer hoorde zij dat voor het eerst en waarom heeft ze de Kamer daar niet onmiddellijk over geïnformeerd? Daarnaast vraag ik welke garanties deze minister kan geven dat het hacken in operationele situaties niet kan voorkomen.

☐

Minister **Hennis-Plasschaert**:
Ik heb de precieze datum van het informeren niet op mijn netvlies staan, maar het zal in de zogenoemde dagrapporten van deze zomer hebben gezeten. Als het gaat om het hacken zeg ik dat Defensie niet gehackt is. Er zijn kwetsbare sites gehackt waarop Defensiemedewerkers inlognamen hebben gecreëerd of zich hebben geregistreerd. Dat is een groot verschil. Hackers kunnen niet zomaar toegang krijgen tot het MULAN-netwerk van Defensie. Daarvoor heb je echt een hoeveelheid van gegevens nodig, alsmede een pas; laat dat voor alles duidelijk zijn. Ik maak deze zaak helemaal niet onnodig kleiner. Dat is ook overbodig, want het gaat hier om een serieuze zaak. In het geval van Defensie kan ik echter slechts benadrukken dat de digitale infrastructuur niet is geraakt. Dat zou de heer Schouw toch goed moeten doen.

De heer **Schouw** (D66):
Nee. Het doet mij heel goed, zoals heel veel andere dingen mij goed doen, maar de minister moet het mij niet kwalijk nemen dat ik toch een beetje scherp probeer te zijn op wat hier is gebeurd. De minister spreekt geruststellende woorden en zegt dat het niet om de vitale infrastructuur gaat, maar eigenlijk om randapparatuur en nieuwsbrieven. Er is toch een verbinding tussen het een en het ander? Ik herhaal mijn vraag uit het vorige blokje. Kan de minister een 100%-garantie geven dat hackers geen toegang hebben tot de vitale ICT-infrastructuur van Defensie, waarvan wij met zijn allen weten dat het vooralsnog een houtje-touwtjeomgeving

is? Dat heeft de Kamer in mei van dit jaar namelijk vastgesteld.

Minister **Hennis-Plasschaert**:
Ik neem de woorden houtje-touwtje niet voor mijn rekening. Die doen ook echt geen recht aan de realiteit. Natuurlijk is het het goed recht van de heer Schouw om op scherp te staan. Daar houd ik ook van. Tegelijkertijd benadruk ik nogmaals dat het hier gaat om kwetsbare websites, niet zijnde die van Defensie, waarop een e-mailadres van een defensiemedewerker is geregistreerd, bijvoorbeeld — ik gaf een voorbeeld — ten behoeve van het aanmelden voor een nieuwsbrief, ten behoeve van het aanmelden voor een congres of ten behoeve van internationale samenwerking en afspraken die je over en weer maakt. Van houtje-touwtje is geen sprake. Onze beveiliging is op orde. 100% garantie is er niet in het leven. Ik kan de heer Schouw wel één ding zeggen, namelijk dat de beveiliging ingrijpt als dat nodig is. Als er sprake is van een hack, spreekt het voor zich dat Defensie altijd een target is van buitenlandse diensten.

Mevrouw **Hachchi** (D66):
Begrijp ik de minister goed dat zij uitsluit dat er informatie dan wel gevoelige informatie buit is gemaakt? Mijn tweede vraag is of de minister ons een brief kan sturen voor het debat van 5 november over ICT bij Defensie.

Minister **Hennis-Plasschaert**:
Ik stuur graag brieven. Ik zou graag willen weten waaraan mevrouw Hachchi behoefte heeft en wat er in die brief zou moeten komen te staan, want volgens mij ben ik duidelijk geweest. Het gaat hier om 380 e-mailadressen. Een veelvoud daarvan is niet meer in gebruik. Andere zijn geregistreerd geweest en zijn nog steeds valide. Tegelijkertijd worden wachtwoorden met enige regelmaat gewijzigd en is er geen inbreuk geweest op de digitale infrastructuur van Defensie. Ik heb er niets meer aan toe te voegen.

De **voorzitter**:
Dank u wel voor uw antwoorden en dank voor uw komst naar de Kamer. Ik hoop dat u nog even wilt blijven voor de stemmingen. Ik zie dat dit zo is; fijn dat u dat wilt!