19
Datalek bij de politie

Datalek bij de politie

Aan de orde is het **tweeminutendebat Datalek bij de politie (CD d.d. 27/11)**.

De **voorzitter**:
We gaan meteen door met het tweeminutendebat Datalek bij de politie. Het commissiedebat vond plaats op 27 november jongstleden. Wij hebben twee sprekers van de zijde van de Kamer. Ik geef graag als eerste het woord aan mevrouw Mutluer van de fractie GroenLinks-Partij van de Arbeid. Het woord is aan haar.

Mevrouw **Mutluer** (GroenLinks-PvdA):
Voorzitter. Ik heb één vraag en één motie. De politiehack heeft laten zien hoe kwetsbaar de organisaties in onze strafrechtketen kunnen zijn en hoe groot de gevolgen daarvan zijn. Je wil dat zo veel mogelijk voorkomen. Ik heb tijdens het debat van de minister een aantal goede zaken gehoord waarmee hij de risico's zo veel mogelijk wil verkleinen. Voordat ik mijn motie aankondig, heb ik nog een vraag. Die heeft met name te maken met hoe hij de digitale kwetsbaarheden zo veel mogelijk naar boven kan halen. Ik had in het debat gevraagd om een doorlichting. Ook de inzet van ethische hackers die in de huid van een cybercrimineel kruipen om dit soort digitale kwetsbaarheden te achterhalen, is natuurlijk een interessante. Het lijkt me goed om te horen of dat soort zaken in de praktijk meegenomen wordt.

Mijn motie gaat met name over de communicatie, want die liet behoorlijk wat te wensen over. Dat was in ieder geval wel het gevoel voor ons als Kamerleden, gelet op alle gesprekken die we met agenten hebben gevoerd en het meldpunt, dat op enig moment in het leven is geroepen. De motie luidt als volgt.

Motie

De Kamer,

gehoord de beraadslaging,

overwegende dat er rekening moet worden gehouden met ernstige onlinedreigingen van onder andere buitenlandse actoren die onze veiligheid kunnen raken;

overwegende dat dit uit de recente politiehack ook naar voren kwam en daar al lessen uit kunnen worden getrokken;

verzoekt de regering om in overleg met de politie, het Openbaar Ministerie, de rechtspraak en het gevangeniswezen draaiboeken op te stellen dan wel te optimaliseren over hoe bij de desbetreffende organisatie met onlineaanvallen wordt omgegaan en hoe daarover in- en extern gecommuniceerd dient te worden,

en gaat over tot de orde van de dag.

De **voorzitter**:
Deze motie is voorgesteld door het lid Mutluer.

Zij krijgt nr. 1238 (29628).

Dank u wel. De laatste spreker van de zijde van de Kamer is de heer Six Dijkstra van de fractie van Nieuw Sociaal Contract. Het woord is aan hem.

De heer **Six Dijkstra** (NSC):
Dank u wel, voorzitter. Wederom dank aan de minister voor het debat. Ik wil me aansluiten bij de woorden van mevrouw Mutluer. Bij dit incident had de communicatie richting de politie inderdaad beter gekund. Tegelijkertijd wil ik ook benoemen wat goed gaat. Uit de antwoorden van de minister is mij duidelijk geworden dat de logging, de detectie en de compartimentering van het netwerk er bij dit incident voor hebben gezorgd dat de schade uiteindelijk beperkt bleef tot de mailomgeving en dat er goed en gedegen cyberonderzoek gedaan kan worden. Dat onderzoek loopt natuurlijk nog, maar als ik de minister goed begrijp, dan zijn de eerste signalen positief. Bij veel cyberincidenten zijn deze zaken niet op orde. Dat weet de minister ook. Hier was dat duidelijk wel het geval.

Ik wil nog een paar algemene vragen stellen aan de minister. Wordt in zijn algemeenheid bijgehouden, bijvoorbeeld door incidentcoördinatieteams van het NCSC, wanneer basale zaken, zoals de logging en compartimentering van netwerken, niet op orde zijn bij incidenten van de overheid? En welke consequenties worden eraan verbonden als die zaken niet op orde zijn? We hebben geen nieuwe regelgeving nodig, want we hebben al de BIO-richtlijn en ook de NIS2 komt eraan. Maar ik ben wel benieuwd welke consequenties instellingen ondervinden wanneer uit incidenten blijkt dat ze hun basisbeveiliging niet op orde hebben. Op welke manier kan er afgerekend worden met kwesties van nalatigheid binnen de overheid?

Dat waren mijn vragen. Dit was het van mijn kant. Dank u wel.

De **voorzitter**:
Tot zover de termijn van de Kamer. Ik geef het woord aan de minister.

Minister **Van Weel**:
Dank, voorzitter. Wederom dank aan de leden voor hun vragen en de motie.

Mevrouw Mutluer vroeg hoe wij de digitale kwetsbaarheden in kaart brengen. Wij benutten alle mogelijkheden. Er wordt getest en er worden af en toe via een steekproef phishingmails verzonden. Natuurlijk wordt er ook op andere manieren gekeken naar de kwetsbaarheid van systemen. We maken gebruik van het volledige spectrum aan mogelijkheden dat we hebben.

Tegen de heer Six Dijkstra zeg ik dat er met de inwerkingtreding van de NIS2, de Cyberbeveiligingswet, een heel groot aantal verantwoordelijkheden bij komen, zowel voor

organisaties als voor het NCSC. Ik zou in de voortgangsrapportage daarover graag willen meenemen wat de verantwoordelijkheid van het NCSC is in die nieuwe situatie als het gaat om logging of adviezen aan andere overheidsorganisaties. Die toezegging doe ik bij dezen.

Dat brengt mij bij de motie van mevrouw Mutluer. Die wil ik graag oordeel Kamer geven, als ik die tenminste zo mag lezen dat ik de organisaties ga wijzen op het belang van het hebben van goede draaiboeken en het optimaliseren daarvan. Zij gaan daar in principe zelf over, maar ik denk dat het voor hen evident zal zijn dat er naar aanleiding van dit incident alle reden is om dat te doen. In die zin geef ik de motie oordeel Kamer.

De **voorzitter**:
Ik heb strak zitten kijken naar mevrouw Mutluer. Beaamt zij deze interpretatie? Dat is het geval. Dan krijgt de motie oordeel Kamer.

Tot zover dit debat. Dank aan de minister voor zijn aanwezigheid hier vandaag.

De beraadslaging wordt gesloten.

De **voorzitter**:
Dinsdag stemmen we over de moties. Het heerlijk avondje is gekomen. Ik sluit de vergadering van 5 december.