Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2010–2011

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

1252

Vragen van het lid **Schaart** (VVD) aan de minister van Economische Zaken, Landbouw en Innovatie inzake *cybercrime aanvallen op Nederlandse bedrijven* (ingezonden 7 januari 2011).

Antwoord van minister **Verhagen** (Economische Zaken, Landbouw en Innovatie) (ontvangen 31 januari 2011).

Vraag 1
Bent u bekend met het artikel «Nederlandse bedrijven vaak doelwit cyberaanval»?[1]

Antwoord 1
Ja.

Vraag 2
Bent u er van op de hoogte dat Nederland een van de landen is met de meeste ICT-beveiligingsincidenten binnen de Europese Unie en dat vooral Nederlandse bedrijven hier vaak de dupe van zijn?

Antwoord 2
Ja. Hier past wel enige nuancering. Het valt namelijk op dat een aantal landen met een vergelijkbaar relatief veel en geavanceerd ICT-gebruik zoals Finland, Noorwegen en Denemarken, ook minder goed scoren. Veel gebruik leidt klaarblijkelijk ook sneller tot de kans op meer incidenten.

Vraag 3
Deelt u de mening dat dit een zeer onwenselijke situatie is, die tot grote economische schade leidt en dat hier snel verandering in moet komen? Zo nee, waarom niet?

Antwoord 3
Ja. Een slechte score in de EU ten aanzien van ICT-incidenten is ongewenst. Los van het directe ongemak en schade, heeft dit mogelijk een negatieve impact op het vertrouwen in de ICT-dienstverlening en het vestigingsklimaat. Ondanks dat Nederland het over het algemeen (zeer) goed doet in de internationale benchmarks, zijn dit ontwikkelingen die mogelijk inbreuk hebben op dat beeld en derhalve de aandacht vragen.

[1] Nu.nl, 5 januari 2011.

ah-tk-20102011-1252
ISSN 0921 - 7398
's-Gravenhage 2011

Vraag 4
Welk beleid voert u met betrekking tot het voorkomen van cyberaanvallen op bedrijven in Nederland?

Antwoord 4
Netwerk- en informatiebeveiliging is in de eerste plaats een verantwoordelijkheid van de bedrijven zelf. De concrete maatregelen dienen dan ook door de bedrijven zelf te worden genomen. Dat neemt niet weg dat de overheid het van belang vindt om bedrijven te wijzen op de mogelijke risico's. Het voorkomen van cyberaanvallen begint namelijk bij bewustwording met betrekking tot de risico's en kennis van mogelijke oplossingen. Daarom is de afgelopen jaren veel geïnvesteerd in bewustwording en voorlichting via programma's als Digivaardig en Digibewust. Ook vanuit de private sector zijn initiatieven ondernomen zoals de campagne «3 x kloppen» en het recente vervolg erop van de bancaire sector.
Ook informatie-uitwisseling is van belang ter voorkoming van incidenten. Zo is al enige jaren het InformatieKnooppunt Cybercrime actief. Binnen dit knooppunt wordt tussen enerzijds GOVCERT, AIVD en KLPD en anderzijds marktpartijen, gevoelige en vertrouwelijke informatie over dreigingen en best practices uitgewisseld.

Vraag 5
Zijn de feiten uit dit artikel voor u aanleiding om verdere actie te ondernemen? Zo nee, waarom niet?

Antwoord 5
De feiten uit dit artikel zullen naast de inzichten worden gelegd die nu worden verzameld ten behoeve van de aan uw Kamer toegezegde nota Digitale Agenda.nl.
In de Digitale Agenda.nl zal ook worden ingegaan op de veiligheid van ICT netwerken en het vertrouwen dat de eindgebruiker in ICT moet ervaren. In maart 2011 zal de Nationale Cybersecurity Strategie aan de Tweede Kamer worden toegestuurd met daarin ondermeer het beleid rond de aanpak van cybercrime.
Beide documenten spelen daarmee in op de noodzaak om ICT incidenten te beperken.