Commissie BiZa

Aan de minister van
Binnenlandse Zaken en Koninkrijksrelaties
Mr. J.P.H. Donner

Plaats en datum: Den Haag, 1 april 2011
Betreft: Op afstand afluisteren van mobiele telefoons bij de overheid
Ons kenmerk: 32500-VII-91/2011D16997

Geachte heer Donner,

In de procedurevergadering van de vaste commissie voor Binnenlandse Zaken van 31 maart 2011 is gesproken over uw brief inzake het op afstand afluisteren van mobiele telefoons bij de overheid.
De commissie heeft besloten u te verzoeken de Kamer zo spoedig mogelijk te informeren over de resultaten van het onderzoek dat in gang is gezet, en over de maatregelen die reeds genomen zijn of waartoe de onderzoeksresultaten aanleiding geven.
De commissie ontvangt voorts graag een overzicht van de huidige maatregelen met betrekking tot de beveiliging van data bij de overheid (bijv. e-mailverkeer, data-opslag etc.).

Naar aanleiding van uw brief zijn in de commissie de volgende vraagpunten aan de orde gesteld.
- Monitoring van ICT-systemen binnen de overheid is van groot belang. Heeft de overheid zicht op wat er gebeurt op haar netwerken, waaronder mailsystemen, en kan ze tijdig ingrijpen als er sprake is van een onbewuste hiaat in de beveiliging of een doelbewuste inbreuk op de beveiliging ?
- Goed opdrachtgeverschap. In hoeverre vormt (informatie-)beveiliging een expliciet aandachtspunt bij een aanbesteding? Het grootste risico is dat in een aanbesteding beveiliging niet in de eisen wordt meegenomen. Bij wie is belegd dat (informatie)beveiliging standaard in aanbestedingen wordt meegenomen?
- Het wordt steeds gebruikelijker om eigen apparatuur te mogen gebruiken op het zakelijke netwerk (‘bring your own device’ beleid). Dit vergt een goede en veilige infrastructuur. Hoe is dit geregeld bij de overheid en hoe verhoudt dit beleid zich tot het initiatief van enkele ministers om eigen toestellen te gebruiken tegen het advies van de departementale ICT-afdeling in?
- Om succesvol het nieuwe werken te kunnen invoeren in een organisatie is goede en veilige infrastructuur nodig. Hoe is dit geregeld bij de overheid?
- Eigen verantwoordelijkheid. Gebruikers hebben een eigen verantwoordelijkheid bij het veilig gebruiken van communicatiemiddelen en ICT. Hoe wordt dit veilige gebruik binnen de overheid gestimuleerd?
- Het GovCERT en het NBV hebben een taak om de overheid te adviseren en waarschuwen als er mogelijke beveiligingsrisico’s zijn. Hebben zij ook een signalerende rol naar de leverancier van producten en diensten, waarin zij dit risico signaleren?

Tweede Kamer der Staten-Generaal
Postbus 20018
2500 EA Den Haag

T. 070-3182211
E. cie.biza@tweedekamer.nl

Bij deze breng ik u het verzoek en de vragen van de commissie over.

Hoogachtend,
de griffier van de vaste commissie
voor Binnenlandse Zaken,

drs. M.J. van der Leeden

Tweede Kamer der Staten-Generaal
Postbus 20018
2500 EA Den Haag

T. 070-3182211
E. cie.biza@tweedekamer.nl