Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2005–2006

30 300 VII Vaststelling van de begrotingsstaten van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (VII) voor het jaar 2006

Nr. 70

BRIEF VAN DE MINISTER VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 29 juni 2006

Hierbij bied ik u, mede namens de Staatssecretaris van Defensie en de Minister voor Bestuurlijke Vernieuwing en Koninkrijksrelaties, de antwoorden aan op de vragen die het kamerlid Szabó (VVD) tijdens de regeling van werkzaamheden d.d. 4 april 2006 (Handelingen 2005–2006, nr. 66, Tweede Kamer, pag. 4179) heeft gesteld naar aanleiding van het lekken van informatie via het Limewire netwerk. Deze vragen hebben betrekking op maatregelen en regels met betrekking tot internetgebruik door ambtenaren.

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,
J. W. Remkes

KST99482
0506tkkst30300VII-70
ISSN 0921 - 7371
Sdu Uitgevers
's-Gravenhage 2006

1
Ik wil vragen of genoemde bewindspersonen in het kader van het beleid met betrekking tot het gebruik van Internet bereid zijn om de ambtenaren mee te delen dat geen privé-gebruik meer mag worden gemaakt van pc's en informatiedragers van de overheid.

De Regering acht een dergelijk verbod mede in het licht van de rechtspraak van het Europees Hof voor de Rechten van de Mens op basis van artikel 8 EVRM onwenselijk.

Ten aanzien van privé-gebruik van zakelijke middelen gelden algemene normen die bijvoorbeeld ook voor telefonie van toepassing zijn en aansluiten op de integriteit die een ambtenaar heeft te betrachten. In de recent uitgebrachte Modelgedragscode integriteit voor de sector Rijk zijn de basisvoorwaarden voor computergebruik en omgang met informatie en geheimhouding vastgelegd. De modelcode geeft het verplichte basisniveau voor alle ministeries. Het uitgangspunt bij de code is dat overheidsmedewerkers gebruik maken van e-mail en internetvoorzieningen. Deze voorzieningen zijn voor zakelijk gebruik aan de werknemer ter beschikking gesteld. Beperkt persoonlijk gebruik van deze voorzieningen is toegestaan, mits dit niet schadelijk is voor de functievervulling en geen verboden gebruik oplevert zoals: pornografische, racistische, discriminerende, beledigende, aanstootgevende of (seksueel) intimiderende uitingen. Daarnaast hebben veel ministeries aanvullende op de eigen situatie toegespitste gedragscodes die vaak verder gaan dan de modelcode.

Verder kunnen binnen de Rijksdienst, daar waar informatiebeveiliging een belangrijk aspect is, specifieke regels met betrekking tot computergebruik gesteld worden. Voor bijzondere informatie, ten slotte, zijn specifieke regels van het Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere Informatie (VIR-BI) van toepassing.

2
Dat thuiswerk alleen is toegestaan met pc's en informatiedragers van de overheid.

De praktijk verschilt per departement (zie ook het laatste deel van vraag 1), afhankelijk van departementsspecifieke afwegingen. Bij Defensie bijvoorbeeld, is thuiswerken op privé-pc's niet toegestaan. Defensie werkt met dienstlaptops in combinatie met een (beveiligde) inbelverbinding.

Bij andere departementen is een andere veilige oplossing gekozen. Daar is thuiswerken op privé-pc's toegestaan mits de werkomgeving van de privéomgeving gescheiden is. Deze scheiding is daar niet gerealiseerd door scheiding van middelen. Immers, ook op privé-pc's kan een thuiswerkomgeving worden gecreëerd die uit oogpunt van beveiliging goed gescheiden is.

Het uitsluitend toestaan van thuiswerken op zakelijke middelen is in het algemeen niet nodig en zou aanzienlijke kosten met zich meebrengen, in de orde van, naar schatting, enkele honderden miljoenen euro's. Het zou bovendien een extra (formele) drempel opwerpen om thuis te werken. De bestaande en toekomstige technische oplossingen hebben het voordeel dat ambtenaren, die vanwege hun betrokkenheid en professionaliteit bereid zijn buiten werktijd door te werken, gemakkelijker thuis veilig kunnen werken zonder gebruik te hoeven maken van een potentieel onveilige privé-omgeving.

Naast het nemen van technische maatregelen hebben de meeste departementen ook gedragsregels – zoals bij vraag 1 al aan de orde kwam. Hierbij zijn bewustzijn en naleving van groot belang. Omdat alle departementen hiermee te maken hebben, beziet het ministerie van Binnenlandse Zaken en Koninkrijksrelaties of het mogelijk is om rijksbrede instrumenten hiervoor in zetten. Hierbij valt te denken aan instrumenten die ook worden gebruikt om het bewustzijn rond het thema integriteit te bevorderen, aangezien er raakvlakken zijn met het informatiebeveiligingsthema.

3
Om een inventarisatie te maken van de software op alle overheids-pc's en -informatiedragers en om daarna te verwijderen die bestanden die niet door de overheid geautoriseerd zijn.

Bij elk departement is het installeren van niet geautoriseerde software verboden en zijn technische maatregelen genomen die het installeren ervan zoveel mogelijk verhinderen.

Het is eveneens de praktijk dat in het kader van het departementaal beheer van pc's en netwerken regelmatig scans worden uitgevoerd ter voorkoming van virussen en spyware. Daarnaast zijn op departementaal niveau overzichten van geautoriseerde software beschikbaar.