Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2007–2008

Aanhangsel van de Handelingen

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

508

Vragen van het lid **Van Velzen** (SP) aan de minister van Defensie over *verlies van gevoelige informatie zoals USB sticks.* (Ingezonden 4 oktober 2007)

1
Wat is uw reactie op het artikel «MIVD'er verliest topgeheimen VS»?[1] Is de berichtgeving waar? Zo neen, bent u bereid verslag te doen van de feiten?

2
Welk soort informatie stond globaal op deze USB-stick?

3
Heeft de betreffende ambtenaar van de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) zich gehouden aan de richtlijn die bepaalt dat vertrouwelijke informatie niet van de werkplek mag worden meegenomen zonder specifieke reden en zonder toestemming van daartoe bevoegde leidinggevende?[2] Zo neen, waarom niet? Zo ja, is de betreffende MIVD-ambtenaar wel of geen toestemming verleend? Zo ja, op welke gronden?

4
Stonden de gegevens versleuteld op de USB-stick? Zo neen, waarom waren aanbevelingen[3] in die richting niet opgevolgd? Is het nog steeds mogelijk om geclassificeerde informatie niet versleuteld op een informatiedrager mee naar buiten te nemen? Zo neen, sinds wanneer is dit onmogelijk? Zo ja, wanneer wordt dit onmogelijk? Worden inmiddels vercijferde USB-sticks gebruikt voor vertrouwelijke gegevens?

5
Is het waar dat Defensie het gebruik van USB-sticks heeft ontraden?[4] Zo ja, waarom worden ze dan nog wel gebruikt? Zo neen, welke concrete maatregelen heeft Defensie op dit gebied genomen om verlies van gevoelige informatie tegen te gaan?

6
Is aanbeveling acht van het rapport «Cultuur ondersteund door structuur, hét wapen tegen lekken van vertrouwelijke informatie,»[5] namelijk het komen tot een effectieve controle bij het verlaten van het ministerie of (militair dan wel burger) complex op het meenemen van vertrouwelijke of geheime informatie in de praktijk volledig van kracht?

7
Is het zich houden aan beveiligingsregels al een vast onderdeel van functionerings- en beoordelingstrajecten?[6] Welke sanctie is er getroffen tegen de persoon die de USB-stick «kwijtraakte»?

8
Bent u bereid een overzicht op te stellen met alle incidenten over de afgelopen 5 jaar waarbij informatiedragers kwijt zijn geraakt? Neemt het aantal incidenten toe dan wel af?

9
Is het waar dat de centralisering van taken en verantwoordelijkheden op centraal niveau, waarbij de beveiligingsautoriteit een centrale positie inneemt, de expertise op het gebied van informatiebeveiliging wel beter aanstuurbaar maakt, maar tevens minder betrouwbaar?

10
Kent u de uitspraak van de Commandant der Strijdkrachten Berlijn dat Nederland alleen moeilijke missies in het buitenland kan uitvoeren dankzij de inlichtingen van de bondgenoten en dat deze bron als gevolg van onzorgvuldigheid met informatie op kan drogen?[7]

11
Kunt u toezeggen dat dit de laatste keer is dat onversleutelde gevoelige informatie op straat komt te liggen?

[1] Telegraaf, 29 september 2007.
[2] Brief van de minister van Defensie, 2 februari 2006, Kamerstuk 30 300 X, nr. 71, vergaderjaar 2005–2006.
[3] Rapport van de door de minister van Defensie ingestelde commissie, belast met onderzoek naar oorzaken van het lekken van vertrouwelijke informatie en aanbevelingen voor risico-verminderende maatregelen 's-Gravenhage, 8 november 2005, p. 35.
[4] «USB-sticks ministerie op straat», de Volkskrant 23 januari 2007.
[5] Rapport van de door de minister van Defensie ingestelde commissie, belast met onderzoek naar oorzaken van het lekken van

KVR29976
2070801320
0708tkkvr508
ISSN 0921 - 7398
Sdu Uitgevers
's-Gravenhage 2007

vertrouwelijke informatie en aanbevelingen voor risico-verminderende maatregelen 's-Gravenhage, 8 november 2005, bijlage overzicht van maatregelen ...
[6] Idem aanbeveling 13.
[7] «Defensie checkt personeel op geheime informatie», Algemeen Dagblad, 9 februari 2006.

Antwoord

Antwoord van minister **Van Middelkoop** (Defensie). (Ontvangen 6 november 2007)

1
Een medewerker van de MIVD heeft in januari 2006 een USB-stick verloren met daarop gerubriceerde informatie. Betrokkene heeft het verlies van de gegevensdrager gemeld aan de dienstleiding van de MIVD. Defensie heeft onderzoek gedaan en naar aanleiding van de bevindingen aangifte gedaan bij het OM.
Onlangs heeft de rechter betrokkene veroordeeld tot een taakstraf van 120 uur. Uit veiligheidsoverwegingen en uit oogpunt van bescherming van de persoonlijke levenssfeer worden geen nadere mededelingen gedaan.

2
Uit veiligheidsoverwegingen worden geen mededelingen gedaan over de informatie op de USB-stick.

3
De betreffende ambtenaar van de MIVD had een specifieke reden de vertrouwelijke informatie van de werkplek mee te nemen, maar had geen schriftelijke verklaring van de daartoe bevoegde leidinggevende. Defensie heeft geoordeeld dat er voldoende reden was om aangifte te doen.

4
De informatie op USB stick was niet versleuteld. De bedoelde aanbeveling betreft het investeren in beveiligingstechnologie. In dat kader is in 2005 opdracht gegeven om beveiligde USB-sticks te ontwikkelen waarop informatie automatisch is versleuteld. Dergelijke USB-sticks dienen te voldoen aan de criteria opgelegd door het Nationale Bureau voor Verbindingsbeveiliging, en waren in die tijd nog niet op de markt verkrijgbaar. De ontwikkeling is pas onlangs afgerond.
Hoewel het in beginsel niet is toegestaan om gerubriceerde informatie onversleuteld op een informatiedrager mee te nemen, zijn er geen maatregelen te treffen waarmee dit volledig is af te dwingen. Met een beveiligde USB stick zal het eenvoudig worden om (gerubriceerde) informatie wél op een veilige manier mee te nemen. Waarschijnlijk komen de beveiligde USB-sticks in het voorjaar van 2008 beschikbaar voor medewerkers.

5
Met de invoering van een nieuwe automatiseringsstandaard is in 2006 onder meer gecontroleerd gebruik van verwijderbare gegevensdragers ingevoerd. Dit is niet specifiek bedoeld om het gebruik van USB sticks te voorkomen, maar omvat technische en organisatorische maatregelen om kaders te stellen aan het gebruik van draagbare opslagmedia. Defensie-informatie mag in beginsel niet op privé-middelen zijn opgeslagen. Uitzonderingen hierop moeten expliciet zijn geautoriseerd. Zo moet de data gedurende de opslag op het draagbare medium deugdelijk zijn vercijferd, ongeacht de merking of rubricering. Ook zijn beperkingen opgesteld ten aanzien van gemerkte en gerubriceerde informatie. In grote lijnen komt dit erop neer dat gemerkte informatie uitsluitend mag worden meegenomen indien dit voor een goede voortgang der werkzaamheden noodzakelijk is. Voor gerubriceerde informatie geldt daarnaast dat hiervoor schriftelijke toestemming nodig is. Bovendien geldt dat moet zijn voldaan aan de voorschriften ten aanzien van het verpakken, behandelen en opbergen van het document of de gegevensdrager.

6
Steekproefsgewijs worden controles uitgevoerd bij de in- en uitgangen van defensielocaties. Hierover heb ik de Kamer op 20 juni 2006 geïnformeerd. Deze controles omvatten ook informatiedragers.

7
In het kader van de invoering van het Flexibel Personeels Systeem (FPS) wordt onder meer de functionerings- en beoordelingssystematiek herzien. Het zich houden aan beveiligingsregels wordt bij deze herziening meegenomen.
Zie verder het antwoord op vraag 1.

8
Beveiligingsincidenten werden tot voor kort decentraal binnen de onderdelen afgehandeld en niet structureel gerapporteerd. Het gevraagde overzicht over de afgelopen vijf jaar is daarom niet beschikbaar. Sinds enige tijd worden alle meldingen van beveiligingsincidenten doorgegeven aan de Beveiligingsautoriteit die deze beoordeelt en indien nodige verdere vervolgacties initieert. Uit deze gegevens kan worden afgeleid dat sinds januari 2007 vijftien maal een incident is gemeld over vermiste dan wel gestolen informatiedragers. Daarbij was in vier gevallen sprake van gerubriceerde informatie. Of het aantal incidenten in de loop van de tijd toe- dan wel afneemt is nog niet goed te beoordelen. Een database waarmee dergelijke analyses mogelijk zijn, is momenteel in ontwikkeling.

9
Het beveiligingsbeleid is conform de aanbevelingen uit het rapport van de Commissie van der Aa gecentraliseerd.
De Beveiligingsautoriteit heeft hierin de taak om defensiebreed het beleid en de regelgeving op te stellen. Hiertoe worden defensiebreed dezelfde normeringen toegepast, hetgeen in de toekomst moet resulteren in uniforme beveiligingplannen die defensiebreed op dezelfde wijze tot stand zijn gekomen en worden uitgevoerd. Door ondersteuning van de defensieonderdelen met de expertise van de Beveiligingsautoriteit wordt de betrouwbaarheid juist verhoogd.

10
Ja. De Commandant der Strijdkrachten wees op het risico dat, indien bondgenoten de indruk krijgen dat de Nederlandse krijgsmacht niet zorgvuldig met informatie omgaat, zij minder geneigd zullen zijn om in de toekomst informatie te delen.

11
Het beveiligingsbeleid van Defensie is er op gericht het risico dat informatie onbedoeld buiten de organisatie bekend wordt, te minimaliseren, met een zo beperkt mogelijke inbreuk op de bedrijfsvoering. Dit risico is echter niet volledig uit te sluiten.