Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2001–2002

28 000 X Vaststelling van de begroting van de uitgaven en de ontvangsten van het Ministerie van Defensie (X) voor het jaar 2002

Nr. 6 **BRIEF VAN DE STAATSSECRETARIS VAN DEFENSIE**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

's-Gravenhage, 17 oktober 2001

Met deze brief wil ik u, zoals toegezegd in de antwoorden op de Kamervragen over de voorjaarsnota 2001, nader informeren over de vercijferkaart (V-kaart). Het project V-kaart maakt deel uit van een interdepartementaal informatiebeveiligingsconcept voor data- en communicatienetwerken. Door middel van de V-kaart zou gerubriceerde informatie in computers en netwerksystemen van de ministeries van Defensie, Buitenlandse Zaken, Binnenlandse Zaken en Justitie beveiligd worden. In de begroting 2001 was de Kamer al gemeld dat de V-kaart voor netwerkcomputers niet in serieproductie zou gaan. Thans heb ik besloten dat ook de V-kaart voor «stand alone»-computers niet in serieproductie zal gaan. In deze brief zet ik uiteen op welke gronden dit besluit, in overleg met de betrokken ministeries, is genomen.

Inleiding

In de jaren negentig heeft het gebruik van geautomatiseerde informatie- en communicatiesystemen binnen de Nederlandse overheid een hoge vlucht genomen. Aan de beveiliging van de informatie stelt de rijksoverheid hoge eisen. In 1994 werd het Voorschrift Informatiebeveiliging Rijksoverheid (VIR94) van kracht, waarin werd bepaald dat een goed stelsel van maatregelen de exclusiviteit en integriteit van de informatievoorziening moest waarborgen. Elk departement was daarbij zelf verantwoordelijk voor de invulling van deze maatregelen.

Als eerste stap in een reeks van maatregelen besloten de ministeries van Defensie, Binnenlandse Zaken, Buitenlandse Zaken, en Justitie, een vercijferkaart te laten ontwikkelen voor de bescherming van staatsgeheime en vertrouwelijke informatie. In samenwerking met het Nationaal Bureau voor Verbindingsbeveiliging (NBV) en Philips Crypto was hiernaar een haalbaarheidsstudie verricht. Een gezamenlijke aanpak met andere ministeries zou de mogelijkheden tot onderling uitwisselen van informatie verbeteren en schaalvoordelen bij een eventuele seriebestelling maximaal benutten. Uit veiligheidsoverwegingen werd besloten de V-kaart in natio-

KST56292
ISSN 0921 - 7371
Sdu Uitgevers
's-Gravenhage 2001

naal beheer te ontwikkelen, en niet bij een buitenlandse leverancier een order te plaatsen. Op 1 juli 1997 werd de Kamer over dit besluit geïnformeerd (Kamerstuk 25 000 X, nr. 93).

Op 2 juli 1997 sloten de betrokken ministeries, waarbij Defensie als opdrachtgever fungeerde, een contract met Philips Crypto. Het contract voorzag in de ontwikkeling van een V-kaart voor de beveiliging van informatie in «stand alone»-computers (versie 1) en in netwerk-computers (versie 2). De ontwikkelingskosten van de V-kaart zouden f 14,5 miljoen bedragen. Deze kosten zijn op basis van de in 1997 voorziene afname als volgt verdeeld: Defensie betaalt f 8,8 miljoen, Binnenlandse Zaken f 3,1 miljoen, Justitie f 2,1 miljoen en Buitenlandse Zaken f 0,5 miljoen. Tussentijds heeft Defensie nog een aanvullend contract van f 3 miljoen afgesloten voor de ontwikkeling van een V-kaart voor desktop computers (oorspronkelijk was de V-kaart alleen bedoeld voor laptop computers). De verwerkingssnelheid van gegevens zou hiermee in belangrijke mate worden verhoogd.

Verloop van het project

De ontwikkeling en beproeving van de V-kaart zouden ruim twee jaar in beslag nemen. Hierbij werden ook het NBV en TNO als onafhankelijke deskundigen ingeschakeld. Eind 1998 kondigde Philips Crypto echter een vertraging aan van een half jaar. Vooral de ontwikkeling van de software voor de V-kaart bleek meer tijd in beslag te nemen dan vooraf was geschat.

Tevens werd er een separaat onderzoek ingesteld naar de toepassing van de V-kaart in de nieuwe standaard-netwerkomgeving van Defensie, LAN-2000. Uit dit onderzoek bleek dat de beheersconcepten van LAN-2000 en de V-kaart niet bij elkaar pasten. Het technisch beheer op afstand, essentieel voor een doelmatig beheer van LAN-2000, zou aanpassingen vergen van de V-kaart die de beveiligingswaarde ervan ontoelaatbaar zouden aantasten. Uit een eerste operationele beproeving van de netwerkversie van de V-kaart bleek bovendien dat deze instabiel en gebruiksonvriendelijk was.

In overleg tussen de betrokken ministeries werd derhalve besloten de ontwikkeling van de netwerkversie stop te zetten en de aandacht te richten op het voltooien van de «stand alone»-versie van de V-kaart. Hierover werd de Kamer, zoals gezegd, geïnformeerd in de begroting 2001.

In de tweede helft van 2000 werd de «stand alone»-versie van de V-kaart onder diverse omstandigheden getest. Allereerst werd getest of de V-kaart deed wat hij moest doen, namelijk het vercijferen van bestanden. Deze zogenoemde «fabriekstesten» werden met succes afgelegd. Vervolgens evalueerde het NBV het functioneren van de cryptografische kern van de V-kaart en de aansturing daarvan door de beveiligingssoftware en testte TNO/FEL de betrouwbaarheid van een computer met V-kaart. Deze testen waren vooral gericht op de inbraakgevoeligheid van de kaart. Uit deze testen bleek dat er problemen waren met bepaalde beveiligingsaspecten en met de stabiliteit van de V-kaart. Praktijktesten met enkele tientallen V-kaarten bevestigden de bevinding van het NBV en TNO/FEL dat de V-kaart niet aan de verwachtingen voldeed.

Het besluit

Samen met de genoemde externe deskundigen en Philips Crypto is onderzocht of de V-kaart zodanig aangepast zou kunnen worden dat deze alsnog aan de gestelde eisen zou voldoen. Alle betrokkenen hebben daarbij te

kennen gegeven dat een dergelijke aanpassing een enorme inspanning zou vergen, waarbij succes niet was gegarandeerd. Bovendien zou de V-kaart dus alleen gebruikt kunnen worden in «stand alone»-computers, terwijl juist het gebruik van (onderling gekoppelde) netwerken de afgelopen jaren sterk is toegenomen.

Om deze redenen heb ik, in overleg met de ministeries van Buitenlandse Zaken, Binnenlandse Zaken en Justitie, besloten het project V-kaart te beëindigen. Daarbij heb ik de mogelijkheid bezien (een deel van) de betaalde gelden van Philips Crypto terug te vorderen. Het grootste probleem daarbij is de complexiteit van het project, *die* ook door de overheid, als opdrachtgever, is onderschat. Bovendien moet geconstateerd worden dat, anders dan bijvoorbeeld bij het project Nafin (brief M2001002333, 21 juni 2001), de snelle technologische ontwikkelingen op ICT-gebied in het nadeel werkten van het project V-kaart. Zo konden er in het oorspronkelijke contract met Philips Crypto niet op alle gebieden concrete toetsingscriteria worden vastgelegd, omdat die internationaal nog in ontwikkeling waren. Verder stelden de snelle ontwikkelingen steeds hogere eisen aan de beveiliging van computers en netwerken.

Kort samengevat heeft Philips Crypto, ook volgens het NBV en TNO/FEL, naar de letter aan het Programma van Eisen voldaan. Aanvullende testen wezen echter toen op bepaalde gebreken wat betreft inbraakgevoeligheid en stabiliteit van de V-kaart. Zoals gezegd konden in het oorspronkelijke contract niet op alle gebieden de concrete toetsingscriteria worden vastgelegd. Voor een terugvordering van gelden zou een gerechtelijke procedure respectievelijk een arbitrage door onafhankelijke deskundigen moeten worden gestart. Dit zal, mede vanwege het eerder geschetste complexe karakter van het project, een kostbare en langdurige aangelegenheid worden, waarbij de kans op succes gering is. Alles afwegend heb ik dan ook als opdrachtgever besloten af te zien van verdere (juridische) stappen richting Philips Crypto.

Oplossingen

Met dit besluit blijft de noodzaak bestaan om (gerubriceerde) informatie in computers en netwerksystemen van de rijksoverheid te beveiligen. De verdere digitalisering van de werkprocessen bij de rijksoverheid en het verouderen van de huidige informatiebeveiligingsapparatuur maakt die noodzaak zelfs groter. Binnen de rijksoverheid lopen initiatieven om te komen tot een gemeenschappelijke, interdepartementale aanpak van deze problematiek op (midden)lange termijn. Daarbij wordt gebruik gemaakt van de ervaringen en expertise die is opgedaan in het project V-kaart.

Elk ministerie is er zelf voor verantwoordelijk om op grond van een specifieke eigen analyse toereikende maatregelen voor de korte termijn te nemen. Ieder ministerie is thans doende deze oplossingen te realiseren. Zo heeft deze analyse bij Defensie medio 2000 plaatsgevonden. Inmiddels zijn twee commerciële producten voor Defensiegebruik geëvalueerd en geschikt voor gebruik bevonden. Introductie is vanaf heden voorzien, waarmee de richting voor de korte termijn is bepaald. Het eerste product slaat informatie op laptops vercijferd op zodat de informatie niet toegankelijk is voor ongeautoriseerde gebruikers. Het tweede product maakt werkplekken in de standaard ICT-omgeving van Defensie geschikt voor verwerking van stg Confidentiële informatie. Daarnaast blijven ICT-omgevingen waar hoger gerubriceerde staatsgeheimen en/of NL-EYES-ONLY informatie wordt verwerkt, vooralsnog strikt gescheiden van andere omgevingen. Bij die hogere rubricering wordt voor Navo-informatie zo veel mogelijk gebruik gemaakt van Navo-producten.

Ook de thans bij de overige ministeries beschikbare informatiebeveiligingsapparatuur is in het beste geval geschikt voor departementaal vertrouwelijke informatie en de rubricerings- categorie stg confidentieel. Wanneer hogere rubriceringscategorieën zijn vereist is maatwerk nodig.

Bij het ministerie van Buitenlandse Zaken is het belangrijkste probleem voor de korte termijn, dat de huidige cryptografische apparatuur voor de beveiliging van informatie die niet in afgescheiden netwerken kan worden uitgewisseld, sterk verouderd is en niet meer voldoende functioneert. Deze apparatuur wordt onder meer door hen gebruikt voor de uitwisseling van nationale informatie met de diplomatieke vertegenwoordigingen in het buitenland. Het ministerie van Buitenlandse zaken zoekt samen met het NBV naar een alternatief voor hun specifieke situatie.

De Staatssecretaris van Defensie,
H. A. L. van Hoof