Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2012–2013

27 529 Informatie- en Communicatietechnologie (ICT) in de Zorg

Nr. 117 **BRIEF VAN DE MINISTER VAN VEILIGHEID EN JUSTITIE**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 5 december 2012

Op donderdag 29 november 2012 (Handelingen II 2012/13, nr. 29, behandeling begroting Veiligheid en Justitie) heb ik tijdens het begrotingsdebat met uw Kamer toegezegd om samen met de Minister van VWS u uiterlijk 5 december 2012 te informeren over de situatie ten aanzien van de hacker van het Groene Hart Ziekenhuis. Met deze brief mede namens mijn ambtgenote van VWS voldoe ik aan mijn toezegging.

Gezien het feit dat het strafrechtelijk onderzoek nog loopt beperk ik mij tot de volgende feiten.

Op 7 oktober jl. is het NCSC geïnformeerd door de media dat het Groene Hart Ziekenhuis zojuist door hen in kennis is gesteld van een beveiligingsincident. Hierop is gelijk contact opgenomen door het NCSC met het Groene Hart Ziekenhuis. Daarop is aangegeven dat het Groene Hart een technisch onderzoek liet uitvoeren.

Indien er sprake is of lijkt te zijn van een grote hoeveelheid ontvreemde bestanden uit databases dan is het inderdaad het advies van het NCSC aan betrokken partij om te overwegen om aangifte te doen. Middels een strafrechtelijk onderzoek kan dan onderzocht worden of er inderdaad sprake is van een strafbaar feit. Hierbij heeft het OM, gegeven de omstandigheden in de zaak, de mogelijkheid om vervolging in te stellen. Het is uiteindelijk aan de rechter om te beslissen of er daadwerkelijk sprake is van een strafbaar feit.

Bij het melden van kwetsbaarheden in ICT is «responsible disclosure», het op verantwoorde wijze melden van incidenten, van het grootste belang. Centraal bij het werken met responsible disclosure staat het verhelpen van de kwetsbaarheid en het verhogen van de veiligheid van informatiesystemen. Daarbij gelden een aantal algemene uitgangspunten, zo is het bijvoorbeeld niet gepast om onnodige schade aan te richten of verder te

kst-27529-117
ISSN 0921 - 7371
's-Gravenhage 2012

gaan dan het aantonen van de kwetsbaarheid. In een dergelijk geval is het niet gepast om onnodig grote databestanden te ontvreemden als al is aangetoond dat het databestand benaderbaar is. Tot slot speelt ook de proportionaliteit van de ingezette middelen een belangrijke rol, denk hierbij bijvoorbeeld aan het plaatsen van een eigen backdoor in een informatiesysteem om vervolgens daarmee de kwetsbaarheid aan te tonen. Ik zal de TK nog voor het einde van 2012 een kader voor responsible disclosure doen toekomen.

Toen er uit onderzoek in het Groene Hart Ziekenhuis bleek dat er meerdere hacks hadden plaatsgevonden heeft het ziekenhuis mede op advies van Fox-IT, politie, justitie en het Nationaal Cyber Security Centrum (NCSC)aangifte gedaan. In het belang van het onderzoek is dat toen niet naar buiten gebracht.

Op 27 november 2012 heeft de Nationale Recherche in Amsterdam een 26-jarige man aangehouden die vermoedelijk betrokken is geweest bij de digitale inbraak in het computersysteem van het Groene Hart Ziekenhuis in Gouda. De woning van de verdachte in Nieuwerkerk aan den IJssel is doorzocht. Daarbij heeft de Nationale Recherche beslag gelegd op computers en digitale gegevensdragers.

Op 30 november 2012 meldt het Openbaar Ministerie dat de 26-jarige man tegenover de Nationale Recherche een bekentenis heeft afgelegd.
De verdachte is aan het einde van de middag in vrijheid gesteld, in afwachting van het verdere verloop van het onderzoek.
Het OM meldt verder dat de man na de inbraak bij het Groene Hart Ziekenhuis kwaadaardige software heeft achtergelaten op het computersysteem. Na de eerste inbraak is een grote hoeveelheid medische gegevens gedownload.
Het onderzoek, dat wordt uitgevoerd door het Team High Tech Crime, wordt voortgezet en richt zich ook op mogelijk andere verdachten.

De minister van Veiligheid en Justitie,
I.W. Opstelten