Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2012–2013

Aanhangsel van de Handelingen

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

2470

Vragen van het lid **Krol** (50PLUS) aan de minister van Veiligheid en Justitie over *de hack op het Groene Hart Ziekenhuis* (ingezonden 6 maart 2013).

Antwoord van minister **Opstelten** (Veiligheid en Justitie) mede namens de minister van Volksgezondheid, Welzijn en Sport (ontvangen 4 juni 2013). Zie ook Aanhangsel Handelingen, vergaderjaar 2012–2013, nr. 1825.

Vraag 1
Bent u bekend met het nieuwsbericht dat journalist Brenno de Winter gevraagd is te getuigen over de hack op Groene Hart Ziekenhuis, waar documenten op een publiek toegankelijke internetserver stonden? Kunt u dit uitleggen hoe dit mogelijk is?[1]

Antwoord 1
De heer de Winter is door de politie uitgenodigd als getuige om in het kader van een strafrechtelijk onderzoek naar een hack bij het Groene Hart Ziekenhuis een aantal vragen van de politie te beantwoorden.
Een ieder waarvan wordt vermoed dat diens getuigenverklaringen kunnen bijdragen aan het oplossen van (ernstige) strafbare feiten, kan worden uitgenodigd voor een getuigenverhoor bij de politie. Zo'n getuigenis in de opsporingsfase gebeurt op basis van vrijwilligheid. Daarnaast geldt voor journalisten onverminderd het recht op bronbescherming waar zij zich op kunnen beroepen.

Vraag 2
Bent u bekent met de uitspraak van het Europese Hof voor de Rechten van de Mens van 2007 over de zaak Koen Voskuil?

Antwoord 2
Ja. In deze zaak werd een journalist tijdens de behandeling van een strafzaak in hoger beroep op vordering van de verdediging gegijzeld door het Hof Amsterdam omdat hij zijn bron niet bekend wilde maken. Het Hof in Straatsburg oordeelde dat de gijzeling een disproportionele schending had opgeleverd van het recht op bronbescherming van de journalist.
Ik zie geen samenhang met de kwestie waarop deze Kamervragen betrekking hebben, namelijk de uitnodiging aan de journalist Brenno de Winter om

[1] http://www.geenstijl.nl/mt/archieven/2013/03/groene_hart_hack.html

ah-tk-20122013-2470
ISSN 0921 - 7398
's-Gravenhage 2013

vragen van de politie te beantwoorden in een lopend strafrechtelijk onderzoek. Van inbreuk op de bronbescherming van de journalist is in dit geval geen sprake. Dit geldt in het bijzonder nu de aangehouden hacker zichzelf reeds aan de politie kenbaar had gemaakt als bron van de journalist.

Vraag 3
Hoe staat het in Nederland met het verschoningsrecht van journalisten als gevolg van onder andere deze uitspraak? In hoeverre is de betreffende uitspraak in wetgeving omgezet?

Antwoord 3
De diverse uitspraken van het EHRM over de bronbescherming en het verschoningsrecht van journalisten worden als leidend beschouwd bij het opsporings- en vervolgingsbeleid van de politie en justitie in Nederland voor zover hierbij een journalist betrokken is. Zo is in 2012 de Aanwijzing toepassing dwangmiddelen tegen journalisten van het College van procureurs-generaal aangepast mede naar aanleiding van het Sanoma-arrest van het EHRM van 14 september 2010.
Eveneens naar aanleiding van het Sanoma-arrest is een aanvulling van het wetsvoorstel Bronbescherming in voorbereiding genomen, waarin voorafgaande rechterlijke toetsing van dwangmiddelen tegen verschoningsgerechtigden is opgenomen. Zoals in de brief van 7 december 2012 van de Minister van Binnenlandse Zaken en Koninkrijksrelaties, mede namens mij, is aangekondigd, is inmiddels een aanvullend advies gevraagd aan de Raad van State (Kamerstukken II, vergaderjaar 2012–2013, 30977, nr.[2]. De voorbereiding van het wetsvoorstel is aangehouden omdat wij de uitspraak van het EHRM in de zaak van De Telegraaf tegen de Staat wilden afwachten teneinde met de resultaten daarvan tijdig rekening te kunnen houden. In dezelfde brief treft u de conclusies die wij aan het arrest hebben verbonden.

Vraag 4
Weet u dat in een korte tijd meerdere kwetsbaarheden bij zorggerelateerde instellingen aan het licht zijn gebracht? Is het beleid om iedereen die een misstand aan het licht brengt te vervolgen? Zijn er ook omstandigheden denkbaar waarbij u samenwerkt met deze personen met als hoger doel kwetsbaarheden in de beveiliging van computersystemen te voorkomen en bestrijden?

Antwoord 4
Ja, dat is bekend. Het is goed wanneer kwetsbaarheden bij zorggerelateerde instellingen aan het licht worden gebracht. Dat neemt niet weg dat, indien het aantonen van kwetsbaarheden gepaard gaat met een strafbaar feit, dit strafrechtelijk kan worden onderzocht door het openbaar ministerie. Dit vloeit voort uit het zeer zwaarwegend maatschappelijk belang dat gemoeid is met de bescherming van gevoelige persoonsgegevens zoals medische informatie. Bij een hack uit «ethische» motieven kan sprake zijn van het ontbreken van de materiële wederrechtelijkheid, dat wil zeggen dat de verdachte het feit bewijsbaar heeft begaan maar dat hij hiervoor niet strafbaar is. Er moet dan wel zijn gebleken dat er voor de hacker geen andere (minder ingrijpende) methoden voorhanden waren om de kwetsbaarheden aan te tonen en dat hij hierbij de nodige zorgvuldigheid heeft betracht; belangen van derden mogen niet onnodig zijn geschonden. In deze zaak waren er redenen om te twijfelen aan de zorgvuldigheid en de ethische motieven van de verdachte.
Bij het Team High Tech Crime van de Nederlandse Politie werken personen die over dezelfde vaardigheden beschikken als hackers. Zij spelen een belangrijke rol in de opsporing van ernstigere vormen van cybercrime.

Vraag 5, 6, 7, 8
Bent u bekend met het richtsnoer van het College bescherming persoonsgegevens met betrekking tot de NEN-7510 norm (de door het Nederlands Normalisatie-instituut ontwikkelde norm voor Informatiebeveiliging voor de zorgsector in Nederland)? Deelt u de visie van experts dat de NEN-norm de minimale basis voor beveiliging in de zorg vormt? Zo nee, waarom niet?

---

[2] http://www.geenstijl.nl/mt/archieven/2013/03/groene_hart_hack.html

Kunt u een actuele lijst samenstellen van zorgverleners en zorginstellingen waar is getoetst op de NEN-norm, waar deze toetsing niet heeft plaatsgevonden en wat de resultaten van de toetsing is geweest? Zo nee, waarom niet?
Bent u van mening dat het mogelijk is te beginnen met een Landelijk elektronisch patiëntendossier (EPD) of een Landelijk Schakelpunt op het moment dat een aangesloten zorgverlener of zorginstelling niet aan de NEN-norm voldoet? Kunt u uw antwoord toelichten?
Welke capaciteit wordt door de overheid ingezet voor het afdwingen van deze NEN-norm en het verlenen ondersteuning daarbij?

Antwoord vraag 5, 6, 7, 8
Ik ben bekend met de Richtsnoeren Beveiliging van het College bescherming persoonsgegevens (CBP). Zorgaanbieders zijn verantwoordelijk voor de juistheid, actualiteit en beveiliging van de zorginhoudelijke gegevens. In artikel 13 van de Wet bescherming persoonsgegevens (Wbp) staat deze verplichting tot beveiliging in algemene zin opgenomen. Specifiek voor informatiebeveiliging in de zorg zijn normen beschikbaar van het Nederlands Normalisatie-instituut, te weten NEN-normen 7510 tot en met 7513. Op 21 december 2012 is het wetsvoorstel inzake cliëntenrechten bij elektronische verwerking van gegevens aangeboden aan uw Kamer (Kamerstukken II, vergaderjaar 2012–2013, 33509, nr.[3]. Naar de genoemde NEN-normen zal in de algemene maatregel van bestuur op grond van artikel 26 Wbp dwingend worden verwezen.
De Inspectie voor de gezondheidszorg (IGZ) houdt zorgbreed risicogericht toezicht. Er worden geen lijsten bijgehouden van zorgverleners en zorginstellingen waar is getoetst op de NEN-norm. Uiteraard wordt wel een overzicht bijgehouden van zorgaanbieders waar de IGZ inspecties heeft uitgevoerd. In haar toezicht op de informatiebeveiliging door zorginstellingen betrekt de IGZ ook de NEN-normen. In 2003 en in 2007 heeft de IGZ telkens bij 20 Nederlandse ziekenhuizen een onderzoek uitgevoerd naar de mate van informatiebeveiliging. Het onderzoek in 2007 heeft de IGZ overigens samen met het CBP uitgevoerd. De onderzoeksresultaten waren voor de IGZ aanleiding om vervolgens aan *alle* ziekenhuizen te vragen zich in 2010 extern te laten auditen op de mate van informatiebeveiliging. Alle ziekenhuizen hebben hieraan gehoor gegeven en hebben toen uiteindelijk een voldoende score laten zien.
Voorwaarde voor aansluiting op de zorginfrastructuur (voorheen het Landelijk Schakelpunt) is dat het zorginformatiesysteem van de zorgaanbieder, en het gebruik daarvan, voldoet aan de eisen van een goed beheerd zorgsysteem (GBZ). Deze GBZ-eisen zijn onder andere gebaseerd op relevante onderdelen van de NEN-norm 7510. Op sommige onderdelen zijn specifiekere eisen gesteld. Het is aan de zorgaanbieder om aan deze eisen te voldoen.
Het is overigens aan de verantwoordelijke van het informatiesysteem om te borgen dat de informatie-uitwisseling tussen zorgaanbieders voldoet aan geldende wet- en regelgeving. Hier wordt ook strikt op toegezien; enerzijds ziet het CBP toe op de naleving van de Wbp en aanverwante wetten, anderzijds ziet de IGZ erop toe dat er verantwoorde zorg wordt geleverd en dat de beveiliging van medische dossiers op orde is. Het toezicht op de informatiebeveiliging is momenteel voldoende belegd bij de IGZ en het CBP en de huidige wettelijke bepalingen en bestaande veldnormen bieden voldoende aanknopingspunten voor toezicht op de beveiliging van medische dossiers.

Vraag 9
Welk prioritering geeft de overheid aan het naleven van beveiligingsnormen binnen het zorgdomein in relatie tot het aanpakken van hackers die actief lekken kenbaar maken?

Antwoord 9
Dit onderwerp krijgt momenteel nadrukkelijk de aandacht van de overheid en van het veld. Zoals ik reeds heb aangegeven in de «Leidraad om te komen tot een praktijk van responsible disclosure» (Kamerstukken II, vergaderjaar 2012–2013, 26 643, nr. 264) kan responsible disclosure een belangrijk middel

[3] http://www.geenstijl.nl/mt/archieven/2013/03/groene_hart_hack.html

zijn om bij te dragen aan ICT-beveiliging. Door een kwetsbaarheid op een meer besloten wijze en in samenwerking met de getroffen organisatie kenbaar te maken (de verantwoorde of «responsible» disclosure) kunnen de gevolgen voor deze organisatie beperkt worden terwijl ook het publieke belang wordt gediend. Dit heeft nadrukkelijk de voorkeur boven het direct volledig publiekelijk bekend maken van een kwetsbaarheid (full disclosure). De door het Nationaal Cyber Security Centrum (NCSC) opgestelde leidraad dient dan ook om het toepassen van responsible disclosure bij alle partijen te stimuleren. Deze zal in de Zorg *Information Sharing and Analysis Center* (ISAC) onder de aandacht worden gebracht van het zorgveld.
Overigens wordt er gewerkt aan een meldplicht voor datalekken die inhoudt dat datalekken onder meer moeten worden gemeld bij het CBP. Dit is verwerkt in het wetsvoorstel «Gebruik camerabeelden en meldplicht datalekken» van de Staatssecretaris van Veiligheid en Justitie en de Minister van Binnenlandse Zaken en Koninkrijksrelaties.

Vraag 10
Hoeveel opsporingscapaciteit is ingezet bij het opsporen van hackers die kwetsbaarheden bij het Groene Hart Ziekenhuis hebben aangetoond?

Antwoord 10
Het onderzoek naar de hack op het Groene Hartziekenhuis is nog niet afgerond. Om die reden kan ik geen uitspraken doen over de hoeveelheid opsporingscapaciteit die is ingezet bij het opsporen van de hackers.