Privacy met het EPD
Onderzoeksvaardigheid
Minor Smart devices in de zorg

van

Paul Sohier (0806122)

CMI-Opleiding *Technische Informatica* – Hogeschool Rotterdam

1 november 2011

Eerste docent *A. Chamani Foumenidana*
Tweede docent

Inhoudsopgave

Inleiding

In 2008 werd besloten tot de invoering van een landelijk elektronische patienten dossier (EPD) voor het opvragen van informatie van medewerkers van zorginstellingen en zorgverleners. In het EPD zou alle informatie die artsen en zorgverleners hebben opgeslagen worden, waarbij iedere medewerker welke werkt met de patient toegang heeft tot zijn of haar gegevens. Iedere Nederlander kreeg in eind 2008 een brief toegestuurd met de vraag of ze bezwaar tegen het EPD hebben. In december 2008 hadden ongeveer 330.000 mensen bezwaar gemaakt tegen het opnemen in het EPD[1]. Een groot bezwaar was dat de privacy in het geding was wanneer er centraal gegevens opgeslagen werden en hulpverleners gemakkelijk bij de gegevens kunnen.

De toegang tot het EPD wordt centraal geregeld met een UZI[1]-pas. In het UZI-register staat opgeslagen welke zorgverleners er zijn, met hun naam en functie beschrijving, en waartoe ze toegang hebben. Voor een veilige communicatie wordt er gebruik gemaakt van certificaten die uitgegeven worden door de overheid, of door een door de overheid aangesteld bedrijf.

De gegevens die in het EPD opgeslagen staan worden niet bij de overheid zelf bewaard, maar bij een commercieële partij welke de Europese aanbesteding gewonnen heeft. De certicaten die nodig zijn voor het EPD worden uitgegeven door de overheid onder de Staat der Nederlanden root Certification Authority (CA). Dit root CA is eigendom van de Nederlandse Staat en werd vertrouwd door alle besturingssystemen en internet browsers. De Nederlandse Staat heeft het uitgeven van Certificaten onder dit root CA uitbesteed aan diverse bedrijven, zoals bijvoorbeeld Getronics in het geval van het EPD[2].

Een groot deel van het EPD is uitbesteed aan commercieële bedrijven waarvan de vraag is of deze daadwerkelijk als doel hebben de privacy van de personen te waarborgen of zelf primair winst te halen uit het project. In dit onderzoek wordt gekeken of het uitbesteden van het EPD de privacy waarborgd, of dat de overheid het beheer van het EPD beter zelf in handen kan houden.

[1] Unieke zorgverlener identificatie

Certificaten moeten veiliger

Om ervoor te zorgen dat de gegevens die opgevraagd worden in het EPD beveiligd over het internet verstuurd wordt maakt het EPD gebruik van certificaten. Hiermee wordt het verkeer dat over het internet gaat versleuteld en kan een ongewenst persoon niet de gegevens lezen welke verstuurd zijn. Voor ieder certificaat is er een publiek en een private deel, waarmee de server en de ontvanger de data kan encrypten en decrypten.

Om deze manier van communiceren goed te laten werken is vertrouwen een belangrijk onderdeel. Certificaten worden door de certificate authority uitgedeeld op basis van vertrouwen bij het aanvragen van een certificaat. De aanvrager moet erop kunnen vertrouwen dat de CA alleen certificaten uitgeeft aan personen die daadwerkelijk te vertrouwen zijn en die ook daadwerkelijk recht hebben op een certificaat.

Om ervoor te zorgen dat de uitgave van certificaten onder het root certificaat Nederlandse Staat goed verlopen zijn hiervoor richtlijnen gemaakt door Logius[9]. Logius is een organisatie welke onderdeel is van het Ministerie van Binnenlandse zaken en welke publieke dienstverleners diensten levert die ervoor moeten zorgen dat de ICT-infrastructuur betrouwbaar is. Verwacht zou worden dat door het naleven van deze richtlijnen het vertrouwen in de leveranciers van de certificaten gewaarborgd zijn, aangezien slechts een beperkt aantal bedrijven daadwerkelijk voldoen aan deze richtlijnen.

In augustus 2011 bleek echter dat dit niet het geval is[6]. Bij het bedrijf Diginotar had in juli 2010 een hack plaatsgevonden en hadden de hackers toegang gekregen tot de systemen waarop certificaten gegeneerd konden worden. Het bedrijf zelf had op dat moment niet naar buiten gebracht wat er had plaatsgevonden, pas toen het in Iran bleek dat er certificaten voor onder andere gmail.com waren uitgegeven door Diginotar werd het bekend. De eerste reacties van Diginotar en het ministerie waren dat het certificaat van de Staat der Nederlanden en daarbij de CA van Diginotar welke onder de Staat der Nederlanden viel niet in handen waren gevallen door de hackers. Ook beweerde Diginotar dat alle certificaten welke waren aangemaakt door de hacker al in juli waren ingetrokken, op één na voor google.com[3]. Maar op hetzelfde moment konden ze niet garanderen dat er niet nog meer certificaten aangemaakt waren, Diginotar zelf had geen idee wat de hacker had gedaan en had ook geen lijst met certificaten welke er aangemaakt waren. Hierdoor kon niemand zeggen of er daadwerkelijk geen valse certificaten meer aanwezig waren. Op 2 september, 4 dagen na het ontdekken van het eerste certificaat laat Google weten dat ze 247 certificaten valse certificaten gevonden hebben[5]. Diginotar kon ook op dit moment niet bevestigen dat dit waar was, en of dat er nog meer valse certificaten waren uitgegeven, maar Diginotar hield wel vol dat het CA van de Staat der Nederlanden nog steeds veilig was en gewoon gebruikt kon blijven. Het ministerie besloot dit advies van Diginotar over te nemen en kwam dus ook met het bericht dat Diginotar nog steeds te vertrouwen is en de sites beveiligd met een Diginotar certificaat van de Staat der Nederlanden ook gewoon veilig zijn.

Onder andere Mozilla, Google en Microsoft besloten om de certificaten die door Diginotar uitgegeven waren te markeren als gevaarlijk, wat betekend dat de normale gebruikers foutmeldingen krijgen dat de site niet langer veilig is. Mozilla wou in eerste instantie alle CA's van Diginotar intrekken, maar onder druk van de Nederlandse regering besloot Mozilla dit niet te doen. Ze vertrouwden, op dat moment, dus nog expliciet de Staat der Nederlanden. Wanneer Mozilla (En andere bedrijven die browsers maken) dit niet hadden gedaan zou bijvoorbeeld DigiD niet langer werken zonder foutmelding, aangezien DigiD gebruik maakten van een certificaat uitgegeven door Diginotar.

Een belangrijk onderdeel van het certificaat stelsel is vertrouwen. Diginotar laat met de hack al zien dat ze hun beveiliging niet op orde hebben en dat hun communicatie en kennis over wat er gebeurd was bij de hack zeer minimaal en op sommige delen gewoonweg incorrect is. Browsers hadden al het vertrouwen opgezegd na enkel de hack, maar uitendelijk blijkt dat er veel meer mis is bij Diginotar.

Na een onderzoek door Onderzoeksbedrijf FoxIt blijkt op 3 september 2011 dat ook het certificaat van de Staat der Nederlanden misbruikt is[4]. Op dit moment besluit het ministerie dat ze geen vertrouwen meer hebben in Diginotar[8]. Uit het onderzoek van Diginotar blijkt dat er een mis is met de beveiliging van Diginotar en dat ze niet voldeden aan de eisen welke Logius opgesteld had. Uit het onderzoek blijkt bijvoorbeeld dat de hackers voor lange tijd toegang gehad hebben tot de systemen van Diginotar. Dit kwam mede doordat er compleet geen anti-virus software was geinstalleerd op de gebruikte computers binnen het netwerk, inclusief de server voor het generen van de certificaten. Ook werd er gebruik gemaakt van wachtwoorden welke gemakkelijk geraden konden worden. Het is gebruikelijk om de certificaat servers buiten het netwerk te houden zouden deze niet via het internet bereikbaar zijn waardoor het hacken van een (deel) van het netwerk niet schadelijk is en een hacker geen toegang krijgt tot de servers en sleutels waarmee certificaten gegenereerd worden.

Het is duidelijk dat Diginotar het vertrouwen zwaar beschadigd heeft. Om deze reden heeft de Opta ook besloten dat Diginotar niet langer certificaten uit mag geven en heeft het moederbedrijf van Diginotar het failisement van Diginotar aangevraagd.

Website veiligheid

Tegenwoordig heeft ieder bedrijf en iedere gemeente een eigen website. Wanneer je begint met het ontwikkelen van webapplicaties is één van de belangrijke onderdelen de veiligheid van de websites. Helaas is uit proeven van Webwereld.nl, Geenstijl en Nu.nl gebleken dat gemeente sites niet in alle gevallen veilig zijn[11]. In dit geval spreken we niet over problemen zoals eerder beschreven met certificaten, maar met veiligheidsproblemen op de website zelf. Hierbij kon een onbevoegd persoon toegang krijgen tot data waartoe hij geen toegang hoorde te hebben, zoals bijvoorbeeld backups van de websites en privegegevens van ambtenaren. Ook kon in sommige gevallen toegang tot gegevens van burgers verkregen worden doordat je als onbevoegd persoon toegang kon krijgen tot DigiD van burgers.

Gemeenten reageerden hierbij in sommige gevallen op door de onderzoeksjournalist brieven van een advocaat te sturen met het verzoek het niet te publiceren, maar te rectificeren dat de gemeente niet fout zat. Ze wilden hierbij niet toegeven dat de gemeente fout zat.

ICT projecten

Ook ICT projecten lopen niet altijd even goed bij de overheid. Een voorbeeld hiervan zijn de ICT systemen bij de politie[10]. Dit systeem zorgde voor de politie voor zo'n slecht werk klimaat dat het niet meer te doen was om met de systemen te werken. Het systeem was specifiek voor de Nederlandse politie ontworpen, maar hierbij was geen rekening gehouden met de gebruikers die met het systeem moesten gaan werken en was er ook niet gekeken naar budget. Hierdoor kwam er aan het eind van het project een product uit dat totaal niet te gebruiken was voor de politie en dat ook nog eens ver over het budget gegaan was.

Om het probleem bij de politie op te lossen is er weer besloten om een geheel nieuw systeem voor de politie te ontwikkelen. De vraag is hierbij natuurlijk of dit nieuwe systeem niet hetzelfde soort problemen gaat krijgen als het huidige systeem, wat om eenzelfde reden is ontwikkeld.

Conclusies en aanbevelingen

Zowel bij de overheid zelf als in het bedrijfsleven gaat er het nodige mis bij ICT projecten en ICT dienstverleners in het algemeen. Bij het gebruik van commerciele bedrijven, zoals bijvoorbeeld Diginotar, is er geen controle op de werking en beveiliging van het bedrijf en heeft Logius geen overzicht of de bedrijven daadwerkelijk nog voldoen aan het programma van eisen. Zodra een bedrijf eenmaal toegang tot de Public Key Infrastructure (PKI) van de Overheid (PKIOverheid) heeft lijkt het erop dat de overheid en daarmee met name Logius niet langer controleert of een bedrijf daadwerkelijk voldoet aan de gestelde eisen door Logius zelf. Doordat Logius de richtlijnen niet controleert heeft Logius en dus de overheid geen idee of de bedrijven voldoen en of de infrastructuur die de overheid gebruikt voor de diensten die ze aanbieden aan de burger daadwerkelijk veilig zijn. Bij het Diginotarschandaal had de overheid in eerste instantie niet door dat het probleem daadwerkelijk zo groot was dat alle overheids sites, waaronder bijvoorbeeld DigiD en de Rijksdienst van het Wegverkeer, niet langer veilig konden communiceren met burgers. De veiligheid was niet gegarandeerd, aangezien niemand kon zeggen of het certificaat dat gebruikt was daadwerkelijk een geldig en goed gecontroleerd certificaat was.

Zowel het intern beheren van het EPD binnen de overheid als het uitbesteden aan commercieële bedrijven leveren problemen op voor de privacy en veiligheid van de data. Bij de overheid zelf worden projecten er op een verkeerde manier aangestuurd, waardoor projecten over budget gaan en de Tweede Kamer hierna in veel gevallen beslist dat er bezuinigd moet worden op de projecten. Deze bezuiniging levert weer problemen op doordat het project dan gewoonweg niet volledig afgemaakt wordt en de gebruiker (zoals bijvoorbeeld de politie) met een ICT infrastructuur komen te zitten welke niet voldoet aan de eisen die ze gesteld hebben. In het geval van het systeem bij de politie had dit uiteindelijk tot gevolg dat de politietop besloot dat de complete infrastructuur opnieuw vervangen moest worden naar een systeem dat wel correct werkt en dat niet tot gevolg had dat agenten meer tijd kwijt waren aan administratie dan aan hun dagelijkse taken.

De enige conclusie die je kunt trekken is dat geen van beide opties voor het beheer, het intern beheren bij de overheid en het uitbesteden naar een commerciële partij, eigenlijk een optie is. Als we kijken naar de geschiedenis van ICT projecten gaat er zo ontzettend veel mis dat de veiligheid van het product dat gebruikt gaat worden niet gegarandeerd kan worden en dat de privacy van burgers in in het geding is. Doordat communicatie tussen de verschillende locaties (In het geval van het EPD tussen zorgverleners en de centrale opslag) beveiligd wordt met certificaten hoort het, wanneer de richtlijnen van Logius gevolgd worden, in principe beveiligd te worden. Het voorbeeld van Diginotar laat hierbij zien dat dit niet het geval is en niemand heeft een idee of het bij de andere uitgevers van certificaten van de overheid wel correct zijn uitgegeven en of ze voldoen aan de richtlijnen die gesteld zijn door Logius.

Voordat de overheid gaat beginnen aan nieuwe grote projecten moet ze eerst de huidige ICT infrastructuur op orde krijgen. Hieronder valt niet alleen de veiligheid van de diverse infrastructuur die ze beheert of uitbesteedt maar ook het controleren van de richtlijnen welke gesteld zijn

om ervoor te zorgen dat bedrijven welke werk uitvoeren voor de overheid zich houden aan deze richtlijnen. Om ervoor te zorgen dat dit alles correct wordt gedaan is het verstandig om een derde partij te vragen dit te controleren en hierin te adviseren. Uiteraard dient deze derde partij geen connecties te hebben met zowel de overheid zelf als de partij welke het werk uitvoert voor de overheid. Zodra de huidige problemen met de ICT projecten binnen de overheid zijn opgelost kan er opnieuw naar gekeken worden hoe het beste nieuwe projecten uitgevoerd kunnen worden en of deze uitbesteed kunnen worden aan een andere partij. Door de controlerende functie bij een andere partij onder te brengen wordt er voor gezorgd dat geen van beide partijen invloed kunnen hebben op de controle, wat de kwaliteit van de te leveren dienst of infrastructuur verbeterd. De overheid zelf zal uiteraard ook eigen controles moeten uitvoeren om ervoor te zorgen dat de kwaliteit en veiligheid op een niveau blijven welke voldoen aan de eisen.

Naast de controles moet de eerste opdracht van het creeëren van de dienst of de infrastructuur ook op een manier worden opgesteld dat er rekening gehouden wordt met de veiligheid en de uitendelijke werking van het af te leveren product. Wanneer de eerste stap in dit proces al verkeerd is, wat bijvoorbeeld gebeurd is bij de nieuwe aanbesteding van DigiD waarbij het niet langer een eis was om SMS ondersteuning te hebben voor de controle bij het inloggen, zal het uiteindelijk product ook van een kwaliteit zijn die niet voldoet aan hetgeen het eigenlijk hoort te voldoen. Minister Opstelten is het hier echter niet[7] mee eens, en is van mening dat het in de eigen organisatie hoort. Hij stelt hierbij wel dat dit financieel gezien niet rendabel is. Ik ben hierbij van mening dat bij veiligheid, ook op het internet, financiën niet het probleem moeten zijn, en dit dus niet als argument gebruikt moet worden. De minister gebruikt financiën echter als argument om het juist uit te besteden.

Ook moet er naast de controle ook een draaiboek klaar liggen voor het geval zich toch nog een probleem voordoet bij één van de betrokken partijen waardoor de partij vervangen kan worden door een andere. Zo kan bijvoorbeeld een leverancier van certificaten vervangen worden door een andere leverancie. Op deze manier kan je bij problemen voorkomen dat het probleem groter wordt dan nodig is door snel te reageren op problemen. Hierbij is communicatie naar alle betrokkenen, dus in veel gevallen ook de burgers, zeer belangrijk.

Voor het EPD is de overheid als we kijken naar de richtlijnen die gesteld zijn op zich goed bezig. Hierbij is niet gecontroleerd of deze richtlijnen ook daadwerkelijk gevolgd worden en of deze afdoende zijn. Er is door de overheid echter wel over nagedacht. Het helpt hierbij ook dat er algemeen bekend is wie de leveranciers zijn van bepaalde hardware en diensten, wat zorgt voor openheid en controleerbaarheid voor derden.

Bronnen

[1] ”bezwaarprocedure epd”. http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2008/12/19/bezwaarprocedure-epd.html.

[2] ”certification practice statement (cps)”. http://www.uziregister.nl/doc/pdf/CPS%20UZI-register%20(UZ52.01)_28435.pdf.

[3] ”diginotar: mogelijk nog valse certificaten in omloop”. http://webwereld.nl/nieuws/107764/diginotar--mogelijk-nog-valse-certificaten-in-omloop.html.

[4] ”diginotar public report version 1”. http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2011/09/05/diginotar-public-report-version-1.html.

[5] ”google onthult 247 valse diginotar certificaten”. http://webwereld.nl/nieuws/107790/google-onthult-247-valse-diginotar-certificaten.html.

[6] ¨iran kan gmail aftappen door nederlands certificaat”. http://webwereld.nl/nieuws/107747/iran-kan-gmail-aftappen-door-nederlands-certificaat--update-2--.html.

[7] ”minister vindt afhankelijkheid van securitybedrijven onwenselijk”. http://tweakers.net/nieuws/77552/minister-vindt-afhankelijkheid-van-securitybedrijven-onwenselijk.html.

[8] ”nederlandse overheid doet diginotar in de ban”. http://webwereld.nl/nieuws/107809/nederlandse-overheid-doet-diginotar-in-de-ban.html.

[9] ”programma van eisen”. http://www.logius.nl/producten/toegang/pkioverheid/aansluiten/programma-van-eisen/.

[10] ”rekenkamer: ’ict-systemen politie niet echt gebruiksvriendelijk’”. http://tweakers.net/nieuws/74867/rekenkamer-ict-systemen-politie-niet-echt-gebruiksvriendelijk.html.

[11] ”vijftig gemeentesites blijken nauwelijks beveiligd”. http://tweakers.net/nieuws/77290/vijftig-gemeentesites-blijken-nauwelijks-beveiligd.html.