INTERVIEW GUIDO VAN 'T NOORDENDE

Hoe veilig is de AORTA rond het kloppend EPD?

Op 18 februari 2010 schreef Guido van 't Noordende een brief aan de Eerste kamer der Staten Generaal met als onderwerp Beveiliging landelijk Elektronisch Patiënten Dossier (EPD). Op dat moment zat de regering in een roerige periode en moest een beslissing worden genomen over de voortgang van de uitrol van het EPD. De brief is geschreven na het afronden van het eerste wetenschappelijke onderzoek naar de architectuur en beveiliging van het EPD. De resultaten spraken boekdelen, volgens dit onderzoek ontbraken basale veiligheidskleppen. Er is bijvoorbeeld geen sprake van een *end-to-end* authenticatie en de wijze waarop artsen bevoegdheden kunnen delegeren aan medewerkers is onveilig.

TOBIAS HOUWERT EN FREDERIK MIJNHARDT

Van 't Noordende is onderzoeker security en privacy in gedistribueerde systemen en als onderzoeker verbonden aan de System and Network Engeneering (SNE) groep die onder leiding staat van Prof. Dr. Ir. Cees de Laat. In de SNE-groep leidde hij het security subprogramma van het Nederlandse project Virtual Laboratory for e-Science (VL-e). Hij heeft diverse publicaties op zijn naam staan op basis van zijn onderzoek. Van 't Noordende is op dit moment bezig zijn promotieonderzoek af te ronden en hij doceert daarnaast aan de Vrije Universiteit Amsterdam informatiebeveiliging en privacy.

Bijna een jaar na de brief spreken we af met Guido van 't Noordende op het Science Park in Amsterdam waar hij zijn werkplek heeft aan de Universiteit van Amsterdam. Wij hebben Guido gevraagd om met ons te spreken over zijn onderzoeksveld en het onderzoek naar de architectuur van het EPD vanuit een beveiligings- en privacy oogpunt.

Wat is de aanleiding van je onderzoek geweest?

'Ik hoorde in 2007 eens een lezing over het EPD. Er werd in die tijd heel vaak gezegd dat het EPD geen centrale database was, en dat het daarom veiliger was dan een centraal systeem. Hierdoor raakte ik geïnteresseerd in de vraag hoe het systeem werkte en hoe veilig dit werkelijk was.'

Van 't Noordende krijgt de ruimte van de Universiteit om in 2008 een onderzoek te starten naar de infrastructuur van het landelijk EPD, ook wel aangeduid met de AORTA[1]. Het vooronderzoek werd onder zijn leiding uitgevoerd door een student [SIJM08], die heeft gekeken naar de werking van de AORTA. Uit het vooronderzoek en zijn eigen onderzoek [NOOR10] komen opmerkelijke bevindingen naar boven die Van 't Noordende aanzetten om de Eerste Kamer in februari 2010 te informeren over de uitkomsten. Bij de huidige architectuur van de AORTA zijn basale beveiligingsmechanismen niet geïmplementeerd, waardoor het systeem onnodig onveilig is en waardoor mogelijk misbruik kan worden gemaakt van de gegevens die opvraagbaar zijn via het Landelijk Schakel Punt (LSP). Het ministerie stelde bovendien in verschillende communicatie dat het systeem aan de hoogste beveiligingseisen voldoet.

> 'Een GBZ-kwalificatie of een penetratietest geeft geen garantie dat er niet in ingebroken kan worden'

Een andere aanleiding om een brief naar de Eerste kamer der Staten Generaal te schrijven, was de brief van de toenmalig minister van Volksgezondheid, Welzijn en Sport, Ab Klink in 2008. In deze brief geeft Ab Klink aan dat het EPD er komt en dat burgers bezwaar kunnen maken via het generieke 'opt-out systeem'.[2] In de brief spreekt de minister uit dat het landelijk EPD als belangrijkste doel heeft het aantal medicatiefouten terug te dringen.

'Ik ben het niet eens met het opt-out systeem. Ik vind dat een dergelijke alles of niets-keuze niet past bij een systeem dat niet 100 procent veilig is. En aangezien je geen 100 procent veilig systeem kunt ▶

bouwen, is een alles of niets-keuze voor dit soort gevoelige informatie niet geschikt'.

Korte omschrijving werking Landelijk EPD
Het berichtenverkeer van het landelijk EPD loopt via het Landelijk Schakel Punt (LSP). Als een behandelaar in de toekomst gegevens over een patiënt wil opvragen omdat hij weet dat de patiënt elders is behandeld, zal hij een aanvraag doen via zijn Goed Beheerd Zorgsysteem (GBZ 1) bij het LSP. In het LSP vindt toegangscontrole plaats op basis van de autorisatie van de behandelaar. In het LSP is een tabel aanwezig (Verwijsindex (VWI)) waarin op basis van het Burger Service Nummer (BSN) gegevens bekend zijn van burgers. Op basis van de tabel kan het LSP het verzoek doorsturen naar alle zorgaanstellingen waarvoor bij het LSP bekend is dat de zorginstelling beschikt over patiënt gegevens (GBZ 2,3, en 4). Een ontvanger van het verzoek (GBZ 2) verwerkt het verzoekbericht van het LSP en stuurt de medische gegevens van de patiënt naar het LSP. Het LSP verzamelt alle berichten en stuurt op haar beurt de gegevens terug naar de aanvrager (GBZ 1), waar de behandelaar de juiste medische gegevens krijgt gepresenteerd.

Op dit moment zijn alleen huisarts- en medicatiegegevens beschikbaar via het LSP.

Wat was de belangrijkste bevinding?
'Het meest opvallende punt en ook het meest eenvoudige om aan te pakken, is het ontbreken van end-to-end authenticatie. Dit is een hele rare fout, omdat het zo'n basale beveiligingstechniek is'.
Van 't Noordende merkt op dat berichten (de aanvraag voor inzage medische gegevens), die via het LSP lopen, ongeauthenticeerd worden doorgezet naar de aangesloten systemen (waar gegevens van patiënten zijn opgeslagen). De aangesloten systemen (GBZ'en) kunnen de authenticiteit van deze verzoeken niet controleren.
'Al beveilig je het LSP nog zo goed, als het daar mis gaat en iemand bijvoorbeeld een Trojan Horse weet te installeren in het LSP, heb je echt een probleem. In de huidige architectuur is het mogelijk dat een kwaadwillende ergens in het LSP software installeert om gericht patiënt gegevens op te vragen.'

De oplossing van het probleem is redelijk eenvoudig en kan bewerkstelligd worden door de handtekening over het bericht die het LSP ontvangt, door te sturen naar de GBZ-systemen, waar deze eenvoudig met behulp van het PKI-certificaat van de zorgverlener kan worden gecontroleerd.

'Toen ik hier achterkwam, heb ik mezelf afgevraagd: moet ik zoiets nu aan de buitenwereld gaan vertellen? En is daar niet eerder onderzoek naar gedaan? In eerste instantie was ik niet van plan de publiciteit te zoeken, maar ik vond het uiteindelijk toch te belangrijk. Het gaat immers over de privacy van alle burgers.'

Een belangrijk argument dat de overheid gebruikt om aan te geven dat het LSP veilig is, betreft de logging. Van 't Noordende legt uit dat van alle verzoeken die behandelaars doen bij het GBZ en op het LSP een log wordt bijgehouden. Deze loggegevens zijn in de toekomst voor de burger online in te zien via een nog in te richten klantportaal. Van 't Noordende is het niet eens met het standpunt van de overheid dat logging een afdoende beveiliging tegen misbruik is. 'Het is natuurlijk belangrijk, maar niet genoeg'. Hij benadrukt het feit dat het voor een burger bijzonder lastig is om logging te lezen, en dat als de burger de berichten al kan lezen, het bijzonder lastig is om te beoordelen welke zorgverleners tijdens een behandeling toegang moeten hebben tot zijn of haar dossier. Het analyseren van de logging is omslachtig en als je een dergelijk grootschalig systeem opzet, moet je eigenlijk preventieve controles inbouwen in plaats van detectieve controles zoals deze logging.

Kun je nog iets vertellen over de mandatering?
'De tweede bevinding van het onderzoek is het mandateren van medewerkers door een behandelaar, de arts. Hierbij krijgt een medewerker van de arts dezelfde rechten als de arts om gegevens in het landelijk EPD te registreren en op te vragen. Via een mandateringstabel is de zorginstelling verplicht bij te houden welke medewerkers zijn gemandateerd en welke niet. In de praktijk werkt dit niet. De mandateringstabel zal vaak zo worden ingevuld, dat elke medewerker zo breed mogelijk inzetbaar is. Als je de mandateringstabel zo breed definieeert zal het niet werken. Uit mijn onderzoek is ook gebleken dat de mandateringstabel niet nodig is om een informatieverzoek in te dienen via het

LSP. Het enige wat nodig is, is een aansluiting op het LSP vanuit een gecertificeerd GBZ. Je hebt een zogenaamd server certificaat nodig waarmee de verbinding kan wordt opgezet, vervolgens kun je daar een bericht invoeren dat ondertekend is met een willekeurige UZI-pas[3]. In het bericht staat een veld waarin de naam van een willekeurige arts van een ziekenhuis kan worden opgenomen. Om een hack te zetten, moet je gewoon een manier zien te vinden om het bericht te injecteren. Dan heb je niks te maken met een mandateringstabel.'

Als we met Van 't Noordende praten over een oplossing vertelt hij dat het essentieel is dat juist de architectuur afdwingt wat de procedure is. 'Als je technisch afdwingt dat de procedure moet zijn dat de arts met zijn UZI-pas een digitale handtekening zet die bevestigt dat één van zijn medewerkers bevoegd is, dan wel gemandateerd is om in het EPD te komen voor een bepaalde tijd, dan voorkom je daarmee dat in de avonduren misbruik wordt gemaakt van de pas. Zelfs niet als de pincode van de pas is gestolen, omdat de mandatering simpelweg niet geldig is.'

Wat zou in jouw ogen een verbetering zijn van het huidige systeem?

'Ik zou graag een verandering willen zien in de wijze waarop mensen toestemming kunnen geven om mee te doen aan het systeem. Transparantie is daarbij essentieel voor alle partijen. De overheid heeft daarin een taak en zou meer moeten doen om burgers bewust te maken van de risico's. Maak dit duidelijk aan de patiënt en geef ze daarmee een reële keuze in het proces, zodat ze zelf kunnen bepalen welke gegevens worden aangemeld bij het LSP of niet. Een simpel voorbeeld: als ik bij de huisarts zit en hij noteert in het kader van de behandelrelatie gegevens die mogelijk uitgewisseld worden met het LSP, dan kan ik als patiënt de vraag krijgen of de samenvatting van die gegevens wel of niet worden aangemeld bij het LSP. Dat hoeft niet een ingewikkeld proces te zijn, men moet gewoon mee kunnen kijken op het scherm van de arts. Want, zodra de informatie eenmaal in het EPD is opgeslagen en aangemeld, kan het niet zomaar worden verwijderd of ongedaan worden gemaakt.'

Is er opvolging gegeven aan de bevindingen uit het onderzoek?

Door het ministerie van VWS is aangegeven dat de resultaten van het onderzoek worden meegenomen tijdens de evaluatie en voortgangsrapportages en dat nader onderzoek zou worden gedaan. Nu, maanden later, is niet duidelijk wat er met de resultaten is gedaan. Dat is opmerkelijk, omdat juist transparantie met betrekking tot de privacy en beveiliging van het EPD de zorg bij de burger kan wegnemen en daarmee het EPD een succes kan worden.

'Ik ben geen tegenstander van het EPD, maar wel tegenstander van een onveilig EPD. Er moeten voldoende waarborgen voor de privacy zijn. Je moet dié communicatietechnieken gebruiken die de privacy het beste beschermen. Voor sommige informatie is dat beveiligde e-mail, voor andere informatie misschien een dossier zoals het EPD. Maar dan moet het wel afdoende beveiligd zijn. Ook is het te betreuren dat niet tijdig een onderzoek naar de veiligheid heeft plaatsgevonden. Je moet de gebruikers niet laten wennen aan een onveilig systeem, maar juist aan een veilig systeem waar autorisatie goed is geregeld.'

> 'Je moet de gebruikers niet laten wennen aan een onveilig systeem, maar aan een veilig systeem waar autorisatie juist goed geregeld is'

Welke rol zie je voor de IT-auditor weggelegd?

De IT-auditor kan in de toekomst een belangrijke rol vervullen in het onderzoek naar de risico's ten aanzien van privacy en beveiliging van patiëntinformatie. Op basis van deze onderzoeken kan de IT-auditor de overheid adviseren zodat de privacy van het systeem en de beveiliging gewaarborgd blijven.

'Het is mij niet duidelijk of en wat voor onderzoeken auditors hebben uitgevoerd en of daar assurance bij is afgegeven. De overheid schermt met het feit dat er naar de GBZ'en is gekeken en dat applicaties die worden aangesloten op het LSP eerst gecertificeerd moeten worden. Dat is natuurlijk niet voldoende. Een GBZ-kwalificatie of een penetratie-test geeft geen garantie dat er niet in ingebroken kan worden. De beveiliging is een geheel. Er moet worden gezorgd dat een inbraak ergens in het land geen consequenties heeft voor het hele systeem. Ook moet de overheid meer transparantie tonen en de onderzoeken die gedaan worden openbaar maken, zodat bijvoorbeeld de Tweede Kamer duidelijk kan zien hoe het staat met de beveiliging van onze medische gegevens.'

Tot slot merkt Van 't Noordende op dat hij de indruk heeft dat de overheid een houding aanneemt waarbij zij de huidige architectuur als een gegeven neemt en dat vervolgens wordt gekeken hoe de risico's gemanaged moeten worden. Beter zou zijn dat er wordt gekeken naar mogelijkheden die de architectuur biedt. ■

Noten

1. De AORTA is de naam van de ICTbasisinfrastructuur, gedefinieerd door Nictiz, die elektronisch berichtenverkeer tussen zorgpartijen mogelijk maakt.
2. Opt-out systeem: alle burgers in Nederland hebben een brief ontvangen waarbij elke burger bezwaar kan maken tegen het uitwisselen van zijn/haar gegevens via het landelijk elektronisch patiëntendossier (EPD).
3. UZI staat voor: Unieke Zorgverlener Identificatie. Het is de pas waarmee een zorgverlener zich kan identificeren bij het Landelijk Schakel Punt.

Literatuur

[SIJM08] Sijm, N., Onderzoeksrapport LSP, *Privacy en security in het Landelijk Schakelpunt,* 30 juni 2008.

[NOOR10] Van 't Noordende, G., *Security in the Dutch Electronic Patient Record System 2nd ACM workshop on security and privacy in medical and home-based systems (SPIMACS)*, pp. 21-31, Chicago IL, October 2010.

http://staff.science.uva.nl/~noordend/