Bijlage: Samenvatting van constateringen en aanbevelingen

Uit het artikel blijkt dat de protocollen en architectuur zoals die zijn beschreven in de AORTA documentatie geen afdoende bescherming bieden tegen reëele bedreigingen en van buitenaf én van binnenuit. Ten gevolge van een aantal belangrijke ontwerpbeslissingen in de architectuur van het EPD, zijn de beveiligings- en privacyrisico's ten gevolge van een eventuele succesvolle aanval op het inwendige van het EPD (LSP, GBZ systemen) groter dan nodig. Dit is gevolg van onder meer de centrale rol van het LSP, de manier waarop mandatering is geimplementeerd, en van de grote hoeveelheid (historische) informatie die wordt bijgehouden in het LSP.

Vertrouwen in het LSP

De op het LSP aangesloten GBZ systemen hebben op dit moment geen mogelijkheid om onafhankelijk van het LSP te controleren (verifiëren) of een inkomend verzoek om patiëntgegevens op de vragen daadwerkelijk afkomstig is van een zorgverlener. Als gevolg hiervan kan kwaadaardige software vanuit het LSP op grote schaal patiëntgegevens opvragen uit de op het LSP aangesloten informatiesystemen, zónder dat de GBZ-systemen tijdig kunnen opmerken dat het hier om niet-legitieme opvragingen gaat. Alhoewel het risico dat een dergelijke situatie zich voordoet wellicht klein is, is de potentiële impact van deze aanvalsmogelijkheid (onnodig) groot. Dit probleem kan opgelost worden door een herziening van de manier waarop berichten in het EPD worden afgehandeld, zodat de noodzakelijke end-to-end authenticatie kan plaats-vinden; de noodzakelijke voorzieningen zijn reeds aanwezig. Het huidige protocol mag dan niet langer ondersteund worden.

Vertrouwen in GBZ systemen

Er wordt in het EPD ontwerp in hoge mate uitgegaan van een goed beheer, en dientengevolge een hoge graad van veiligheid, van de op het LSP aangesloten GBZ systemen. Echter, in specifieke gevallen zullen noch het Programma van Eisen van het Nictiz, noch de toepasselijke NEN normen, een compromittering van GBZ-systemen altijd kunnen voorkomen. Een GBZ bestaat uit vele verschillende software systemen en componenten, afkomstig van vele leveranciers, zoals werkstations, applicatieservers en communicatieservers. Het berichtenverkeer richting het LSP vindt bijvoorbeeld in een aantal gevallen plaats over een communicatieserver. Kwaadwillende software op zo'n server kan de berichten die naar het LSP worden verstuurd onderweg manipuleren met als doel meer informatie op te vragen dan de zorgverlener oorspronkelijk bedoelde. Dit specifieke probleem kan worden opgelost door het zoveel mogelijk beperken van de opdrachten die naar het LSP worden verstuurd, waarbij de (zoek)opdrachten van zorgverleners dan volledig en controleerbaar vastgelegd moeten worden in de beveiligingsinformatie die wordt meegestuurd met een bericht.

Het mandateringsmodel

Een groter probleem betreft het mandateringsmodel, welke sterk afhankelijk is van de interne beveiliging van decentrale GBZ systemen. Het mandateringsmodel leunt op controle achteraf door middel van verplichte, decentraal bijgehouden mandateringstabellen. De geldigheid van mandateringen kan echter niet worden gecontroleerd in het LSP ten tijde van het verwerken van een verzoek. Daardoor kan kwaadwillende software in een GBZ systeem –in combinatie met een UZI pas van een willekeurige medewerker of gecombineerd met kwaadaardige software op de PC van een medewerker– gegevens opvragen namens willekeurige zorgverleners. Het risico is met name groot, doordat (technisch, vanuit het LSP bezien) met elke UZI pas (op naam) patiëntendossiers kunnen worden opgevraagd uit naam van elke zorgverlener in een GBZ – ongeacht de functie of (medische) beroepstitel van die zorgverlener.

Medewerkers krijgen op dit moment de volledige rechten van de mandaterende zorgverlener, waaronder zelfs de mogelijkheid om voor de eerste keer patiëntgegevens op te vragen of in het LSP te registreren. Behandelrelaties worden op dit moment alleen decentraal in de GBZ systemen vastgelegd. Daarom ziet het LSP een eerste opvraag of registratie van gegevens van een nieuwe patiënt door een zorgverlener impliciet als een 'claim' van een nieuwe behandelrelatie. Dergelijke operaties kunnen door de zorgverlener zelf wordt uitgevoerd, maar ook door een gemandateerde medewerker. Wij zouden verwachten dat operaties die een nieuwe behandelrelatie impliceren, maar ook de registratie van (nieuwe) gegevens in het LSP, zouden zijn voorbehouden aan zorgverleners – zeker in het licht van de gebrekkige controleerbaarheid van mandateringen.

Aangezien het moeilijk kan zijn om aan te tonen dat een zorgverlener daadwerkelijk betrokken was bij een bepaalde (misbruikte) mandatering, kunnen bovengenoemde aspecten ook consequenties hebben voor aansprakelijkheid. Immers, het aantonen van de betrokkenheid van een zorgverlener bij de acties of de mandatering van medewerkers kan in de praktijk moeilijk zijn. Dit wordt versterkt doordat het gebruik van UZI passen en mandatering van medewerkers technisch (vanuit het LSP gezien) op geen enkele manier beperkt is: UZI passen (op naam) kunnen gebruikt worden om namens een willekeurige zorgverlener binnen hetzelfde GBZ te acteren – ook wanneer deze zorgverlener geen directe relatie met de medewerker heeft.

De enige barrière die op dit moment tegen misbruik van het mandateringsmechanisme wordt opgelegd, is de beveiliging die GBZ systemen intern en ten aanzien van (het gebruik van) de UZI passen bieden. Technische maatregelen zijn nodig om ook bij een eventueel falen van de beveiliging van GBZ systemen een effectieve beveiliging tegen misbruik te kunnen bieden. Het is tenminste noodzakelijk dat mandatering technisch verifieerbaar is op het nivo van het LSP, zodat kan worden aangetoond dat een medewerker daadwerkelijk gemandateerd is door de opgegeven zorgverlener vóórdat het mandaat gebruikt kan worden. Daarnaast zijn nog aanvullende maatregelen nodig, die in het artikel worden besproken.

Aangezien zorgverleners ook in persoon toegang tot het EPD kunnen krijgen, lijkt de noodzaak tot mandateren in de huidige situatie niet op te wegen tegen de risico's. Het is daarom aan te raden om mandateringen in het geheel niet toe te staan totdat er een sluitende oplossing voor de bovengenoemde problemen is gevonden.

Authenticatie en identificatie van patienten

Er bestaan reeds eerder gerapporteerde tekortkomingen in het geplande authenticatie (identificatie) mechanisme voor patienten door middel van DigiD met SMS authenticatie[1]. In het geval dat een aanvaller toegang krijgt tot de authenticatie infrastructuur die onder DigiD ligt, is het mogelijk om willekeurige patientendossiers op te vragen. De potentiële impact hiervan is groot en vergelijkbaar met de impact van een aanval op de centrale LSP infrastructuur. Dit probleem is oplosbaar door de invoering van een sterk authenticatiemiddel voor patiënten, zodat volledige 'end-to-end' authenticatie van patiënten ten opzichte van het EPD (LSP) mogelijk wordt, zonder de tussenstap van DigiD.

1 B. Jacobs, S. Nouwt, A. de Bruijn, O. Vermeulen, R. van der Knaap, C. de Bie: "Beveiligingseisen ten aanzien van identificatie en authenticatie voor toegang zorgconsument tot het Electronisch Patientendossier (EPD)", rapport in opdracht van VWS uitgevoerd door PriceWaterhouseCoopers, Universiteit Nijmegen, en Universiteit van Tilburg, December 2008.

Historische gegevens en inherente risico's van opslag van gegevens in het LSP

Het LSP slaat veel (historische) informatie op. Een deel van deze informatie is nodig: het bijhouden van een verwijsindex is in de huidige opzet bijvoorbeeld onvermijdelijk – hoewel het de vraag is of het verstandig is om de inhoud van de verwijzingen tot in detail in de wet vast te leggen, zoals nu het geval is. Echter, er worden in het LSP ook historische (verkeers)gegevens bijgehouden ten behoeve van beheersfuncties. Verkeers- en reconstructiegegevens moeten worden gezien als persoonsgegevens; uit deze gegevens kunnen patiëntgegevens worden afgeleid, en indirect ook behandelrelaties[2] – afhankelijk van hoe lang historische gegevens worden opgeslagen mogelijk tot ver in het verleden.

In tegenstelling tot verwijzingen kunnen historische gegevens niet in opdracht van patiënten uit het LSP worden verwijderd. Omdat ten behoeve van de toezichthouder de situatie voor een willekeurige datum in het verleden kunnen worden gereconstrueerd[3], is het voor een patient niet mogelijk om alle informatie aangaande een eenmaal aangemeld dossier volledig uit het EPD te verwijderen - terwijl een patient mogelijk vanwege de privacygevoeligheid deze informatie juist uit het EPD wilde verwijderen. Deze gegevens zijn kwetsbaar bij een aanval op het LSP of op de beheersfuncties van het EPD. Merk op dat de onmogelijkheid tot volledige verwijdering van persoonlijke gegevens uit het EPD niet in lijn is met het in WBP en WGBO vastgelegde recht tot vernietiging van (persoons)gegevens. De opslag van historische informatie in het EPD heeft hiermee dus opmerkelijke consequenties.

Het invoeren van een sterk patiënten authenticatie (identificatie) middel kan een oplossing bieden, doordat met deze techniek patiëntgegevens kunnen worden versleuteld zodat ze alleen voor de patiënt -of met medewerking van de patiënt- volledig leesbaar of reconstrueerbaar zijn. Daarmee zijn de gegevens niet langer leesbaar zijn voor een aanvaller van het LSP of voor toezichthouders, echter een reconstructie achteraf ten behoeve van bijvoorbeeld een gericht onderzoek naar een beveiligingsincident is nog steeds mogelijk.

Informed consent

Het voorkomen van registreren van van gegevens in de EPD infrastructuur lijkt uiteindelijk de enige manier om 100% zeker te zijn dat gevoelige informatie nooit via het EPD kan uitlekken. Er bestaat echter voor patiënten juist op het punt van het registreren van gegevens in het EPD geen concrete manier om in te grijpen, op een volledig of per-zorgaanbieder bezwaar na. In mijn artikel beargumenteer ik dat ingrijpen achteraf middels het virtuele klantenloket onvoldoende waarborgt dat de toegang tot en eventuele verwijdering van patiëntgegevens tijdig en volledig kan plaatsvinden.

Patiënten hebben het recht om volledig bezwaar te maken, of per zorginstelling bezwaar aan te tekenenen tegen het gebruik van het EPD. Echter, de haalbaarheid van een (volledig) bezwaar is op lange termijn ongewis – zeker wanneer het EPD de aangewezen manier wordt om veilig en efficient gegevens in de zorg uit te wisselen.

2 AORTA beschrijft dat de toegangslog opslaat welke patiëntgegevens door welke zorgaanbieder zijn opgevraagd (Nictiz, Bedrijfsarchitectuur AORTA v6.5.0.0, 30 November 2009, p. 68, par. 9.3). Echter, Nictiz geeft aan dat toegang op het nivo van de zorgverlener (detailgegevens van de UZI pas en eventuele mandaterende partij) wordt gelogd (persoonlijke communicatie). Dit is te begrijpen vanuit de nodige inzage in de toegangsgegevens door patiënten. Echter, aangezien normaliter alleen zorgverleners met een behandelrelatie toegang tot patiëntgegevens kunnen krijgen, impliceert dit dat uit de toegangsgegevens behandelrelaties zijn af te leiden.

3 Nictiz, Informatiesysteemarchitectuur AORTA, v6.0.1.0, 16 April 2009, p.55, par. 4.9

Het voorstel voor de kaderwet EPD, Artikel 13f lid 3, geeft aan dat de patiënt toestemming moet geven voordat een zorgaanbieder gegevens mag opvragen uit het EPD; een dergelijke bepaling bestaat echter niet ten aanzien van de registratie (aanmelding) van gegevens (Artikel 13f lid 2). In dit geval wordt een "geen bezwaar" methode gehanteerd, waarbij de zorgaanbieder mag veronderstellen dat de informatie geregistreerd mag worden indien de patiënt geen bezwaar heeft gemaakt (bij de zorgaanbieder of algeheel). Dit is concreet al van toepassing bij bijvoorbeeld het (retrospectief) registreren van gegevens uit ziekenhuisapotheken, voor patienten die geen bezwaar hebben gemaakt tegen het gebruik van het EPD. In het huidige consentmodel mogen zorgverleners (en informatiesystemen) het ontbreken van bezwaar als toestemming voor het gebruik van het EPD interpreteren ten aanzien van het aanmelden van gegevens[4]. Hierdoor kan het voor patiënten ondoorzichtig worden of, en zo ja welke en wanneer, gegevens in het EPD worden geregistreerd. Inzage in het virtuele klantenloket geeft daarbij pas na enige tijd informatie – wanneer de patiënt inlogt – en bovendien kan verwijdering van gegevens niet instantaan[5], noch volledig plaatsvinden.

Een oplossing kan worden gevonden in het aanbieden van een mogelijkheid voor patiënten om (bijvoorbeeld middels het authorisatieprofiel) aan te geven dat zij gekend willen worden –of toestemming moeten worden gevraagd– voordat gegevens in het EPD worden geregistreerd. Dit hoeft alleen wanneer de patiënten daar zélf aanleiding toe ziet. Door deze keuzemogelijkheid kunnen patienten die dat willen vooraf invloed uitoefenen op welke persoonlijke gegevens verwerkt (geregistreerd) worden in het LSP. Bij constatering van de wens van de patiënt om vooraf aan registratie geinformeerd te worden, kan namelijk van (al dan niet automatische) registratie van gegevens op basis van veronderstelde toestemming geen sprake meer zijn. Er kan op dit moment bijvoorbeeld een pop-up scherm worden getoond, waarmee de zorgverlener expliciete toestemming moet vastleggen, of de registratie kan (afhankelijk van de informatiecategorie) tijdelijk worden doorgevoerd in het LSP waarna de patiënt deze elektronisch moet bevestigen om de registratie definitief te maken. Dit laatste kan helpen om de zorgverlener te ontlasten.

Uiteraard moeten patiënten, ten behoeve van de werkbaarheid, er ook voor kunnen kiezen om de beslissing om gegevens in het EPD te registreren aan de zorgverlener over te laten, zoals dat feitelijk ook in de huidige situatie gebeurt. Daarnaast zijn ook uitzonderingen denkbaar zoals in WGBO verwoord, waarbij het medisch of algemeen belang kan prevaleren boven de wens van de patient om gegevens buiten het EPD te houden. Mogelijk ten overvloede vermeld ik dat het hier voorgestelde consentmodel in lijn lijkt te zijn met WGBO en het zelfbeschikkingsrecht zoals dat is uitgewerkt in de Wet Bescherming Persoonsgegevens.

4 Memorie van Toelichting bij de Wijziging van de Wet gebruik burgerservicenummer in de zorg in verband met de elektronische informatieuitwisseling in de zorg, Tweede Kamer, vergaderjaar 2007-2008, 31 466, nr.3, paragraaf 1.6.

5 Het verwijderen van gegevens vindt niet direct in het LSP plaats, maar vindt plaats vanuit de verantwoordelijke zorgaanbieder. Er kan dus enige tijd overheen gaan voordat een verwijdering van gegevens daadwerkelijk is uitgevoerd.