Aanvalsvlak LSP voor indringers weer groter door PGD-LSP-koppeling

In het eerste kwartaal van 2016 zal in Friesland onder auspiciën van Gerrit-Net een proef starten waarbij de patiënt zelf toegang krijgt tot het Landelijk SchakelPunt(LSP) om medicatiegegevens in te zien. Dat gebeurt via een koppeling van het Persoonlijke Gezondheids-Dossier(PGD) van een patiënt met het LSP. Hoewel het LSP een regionale indeling heeft is de infrastructuur toch landelijk van opzet. De infrastructuur wordt daardoor kwetsbaarder met de toename van het aantal aangeslotenen. Het aanvalsvlak neemt verder toe. Naast de zeer vele zorgaanbieders die de Vereniging voor Zorgaanbieders Voor Zorgcommunicatie(VZVZ) toegang wil geven tot het LSP komen daar nu de patiënten zelf bij, die ook op een geheel andere wijze toegang krijgen tot het LSP dan de zorgaanbieders.

Plannen

Al langer zijn er plannen op PGD's aan het LSP te koppelen. Ik schreef er eerder over. In dat artikel gaf ik aan hoe de overheid op de achtergrond al langere tijd aanstuurt op de ontwikkeling van aan het LSP koppelbare PGD's. Ik beschreef de problemen die kunnen ontstaan als burgers/patiënten door instanties/overheden onder druk worden gezet om gegevens uit hun PGD te openbaren. In Friesland werd door Gerrit-Net begin 2015 de opzet van een pilot PGD-LSP gemaakt. Daarvan werd op 9

april 2015 tijdens een podium-bijeenkomst verslag gedaan. In die pilot werken samen: enkele zorgaanbieders in Zuidwest-Friesland, Zorgkluis B.V., de VZVZ, de Nederlandse Patiënten en Consumenten Federatie, Microsoft, Nictiz en enkele overheidsinstanties. Daarin wordt duidelijk op welke wijze de patiënt toegang krijgt tot het LSP om de medicatiegegevens op te halen bij de bron. Op de derde sheet van de presentatie staat in een schema vermeld hoe de communicatie gaat verlopen. De patiënt maakt gebruik van een intelligente Persoonlijk medicatiedossier(iPMD)-app, die voor de opslag van de data communiceert mate het PGD van Microsoft(MS-HealthVault). Met de app(op de smartphone) maakt de patiënt contact met het VZVZ via een portaal van VZVZ in het zogeheten GBP-koppelvlak. Onder een GBP verstaat VZVZ een Goed Beheerd zorgPortaal. VZVZ zegt hierover dat het een portaal is dat voldoet aan eisen voor aansluiting op het LSP en toegang geeft aan een burger tot zijn/haar landelijke elektronische patiëntendossier. De authenticatie, de vraag of de patiënt degene is die hij/zij beweert te zijn geschiedt door middel van het gebruik van de DigiD plus Remote Document Authentication(RDA).

RDA

Remote Document Authentication maakt gebruik van de contactloze chip in paspoorten, rijbewijzen en identiteitskaart die door een NFC(Near Field Communication)-chip in een moderne versies van smartphones uitgelezen kunnen worden. Eind 2014 was 50% van de smartphones hiermee uitgerust, o.a. voor contactloos betalen. De volgorde is dat de patiënt met DigiD plus SMS-authenticatie inlogt op het LSP-portaal en zich nader authenticeert middels de RDA-procedure. Het identiteitsbewijs met de chip wordt dus voor de smartphone gehouden. Daarna kan de patiënt zijn medicatiedossier opvragen bij het LSP. De beveiliging van online-diensten wordt ingedeeld in zogenaamde STORK-niveau's(1 t/m 4). Door het gebruik van RDA wordt het beveiligingsniveau verhoogd naar het ISO 29115/Stork betrouwbaarheidsniveau 3, terwijl alleen

DigiD-gebruik(inlognaam en wachtwoord) STORK 2 is en DigiD plus sms-bericht STORK 2+ is.

Veel ervaring met de RDA-procedure is er in Nederland nog niet veel. De RijksDienst voor het Wegverkeer(RDW) doet er nog een pilotproject mee, waar de firma Logius aan meewerkt. De overheid worstelt ook al lang met de problemen met de toegang tot online-diensten.

Verkregen data

De patiënt zet de verkregen informatie in het eigen PGD(MS-HealthVault in dit geval) en kan die informatie zelf aanvullen met bijv. ervaringen en zonder recept gekochte medicatie toevoegen. Indien de patiënt naar aanleiding van de verkregen informatie de zorgverlener aanvullende informatie of correcties wil doorgeven zal dat via beveiligde zorgmail via de iPMD-app richting zorgverlener gaan.

Aanvalsvlak

Hoewel gezegd wordt dat de werking van het LSP regionaal is blijft het een landelijk systeem met een centrale computer bij de firma CSC te Utrecht. Het aantal personen en systemen dat toegang heeft bepaalt de grootte van het aanvalsvlak bij pogingen tot kwaadwillende toegang. Dat is en blijft het probleem met een centraal werkend systeem. Nu reeds hebben enkele tienduizenden huisartsen, apothekers en medisch specialisten middels een UZI-pas en kaartlezer toegang tot het LSP. Voor de nabije toekomst voorziet VZVZ een nog groter aantal gezien de recente uitbreiding van de koepeladviesraad met vertegenwoordigers van koepelorganisaties van jeugdgezondheidszorg (ActiZ-JGZ), artsenlaboratoria en diagnostische centra (SAN), instellingen voor geestelijke gezondheidszorg en verslavingszorg (GGZ Nederland) en artsen voor verstandelijk gehandicapten (NVAVG). Ook werd een pilot in de regio Drechtsteden-Gorinchem gestart met vertegenwoordigers van de care-sector. De gevaren van het

incorrecte gebruik van UZI-passen werd al eens in 2011 beschreven. Nu komen er via het GBP-portaal, op de hierboven beschreven wijze, ook burgers bij die weer op een andere wijze toegang krijgen tot het LSP. De kwetsbaarheid van het systeem neemt hiermee dan ook toe.

Waar met een UZI-pas altijd nog een “grondstation” in de vorm van een kaartlezer nodig is, zal het “grondstation” van de RDA-procedure een mobiele telefoon(of tablet) zijn. Beide inlogmogelijkheden hebben hun zwakken kanten door diefstal van de middelen/codes en incorrect gebruik. Daarnaast zal met de toegang tot het GBP van het LSP de veiligheid van de iPMD-app een cruciale rol spelen, bijv. ten aanzien van de vraag of deze app te hacken is. Nu zijn het vermoedelijk nog enkele honderden patiënten in Friesland die via het LSP hun medicatiegegevens kunnen opvragen. Indien men dit verder wil gaan uitrollen dan neemt het aanvalsvlak logaritmisch toe.

Inherent veiliger

Een communicatiesysteem zonder centrale computer, van de ene zorgverlener naar de andere, zonder een computer-in-the middle, kent dergelijke problemen niet en is derhalve veel veiliger. Het heeft een uitermate nauw aanvalsvlak en is schaalbaar. Een voorbeeld hiervan is de Whitebox.

In het concept van Gerrit-Net is naast het Amerikaanse bedrijf CSC(van het LSP) nog een groot Amerikaans bedrijf ingeschakeld, nl Microsoft, die de MS-Healtvault-data in de cloud opslaat. Beide bedrijven vallen onder de Patriot Act. Hierover is in het kader van het LSP al het nodige gezegd.

W. J. Jongejan