

Groot aantal dossiers niet aangemeld op LSP met corona-opt-in



Vanwege de coronacrisis heeft de minister van VWS recent bewerkstelligd, dat met instemming van de Autoriteit Persoonsgegevens (AP), in huisarts-informatie-systemen (HISsen), samenvattingen van zorgdata van meer Nederlanders in te zien zijn op huisartsenposten. Dat kan met gebruikmaking van het Landelijk SchakelPunt (LSP). De noodprocedure waarbij opt-in-toestemming van hen die nog geen besluit hierover genomen hebben in de HISsen automatisch op "ja" wordt gezet, blijkt nogal wat haken en ogen te hebben. Hetgeen voor kenners ook wel te verwachten was. Nu blijkt dat een substantieel deel van de geforceerde opt-in-toestemmingen de LSP-computer niet bereikt. Bij gebruikers van minimaal één huisartsinformatiesysteem (HIS), MicroHIS, blijkt 20 tot 25 % van de dossiers niet aangemeld te worden. Dat blijkt te berusten op het niet geregistreerd zijn van de toegangspas voor het LSP, de UZI-pas, binnen dat huisartsinformatiesysteem. Bij andere HIS-sen kan uiteraard hetzelfde spelen.

UZI-pas

Om de toegang te regelen voor het LSP is jaren terug de UZI-pas in het leven geroepen. UZI staat voor Unieke Zorgverlener Identificatie. Die passen verstrekt het UZI-register. De chipkaart dient ter identificatie en authenticatie van de gebruiker. Die UZI-pas heeft een zorgverlener nodig om met behulp van een kaartlezer die aan zijn/haar systeem bevestigd is toegang tot het LSP te krijgen. In een aantal gevallen dient de UZI-pas ook om in te loggen in het HIS. De levering

en het gebruik van de UZI-passen is niet zonder problemen. (A, B, C, D, E)

MicroHIS

Huisartsen die gebruik maken van het systeem MicroHIS kregen eerst op 15 april 2020 van de leverancier DXC Technology bericht van een emergency-update. Aardig detail bij deze leverancier is dat die ook het LSP zelve ontwikkelde en daar het onderhoud van doet. Daarmee zette de software in het HIS automatisch de opt-in-toestemming op "ja" voor alle patiënten die nog niets hadden laten noteren. Op 21 april 2020 kregen de gebruikers een brief met de kop "**Groot aantal dossiers niet aangemeld op LSP**". Het bleek na meerdere dagen dat de systemen 20 tot 25 % van de dossiers niet aangemeld hadden bij het LSP. Na onderzoek bleek dat bij de meeste huisartsen geen UZI-pas in het systeem geregistreerd was. Om patiënten aan te kunnen melden bij het LSP moet voldaan zijn aan twee voorwaarden. In de eerste plaats moet bij de patiënt een definitief BSN zijn vastgelegd, na verificatie met identiteitsbewijs. In de tweede plaats moet een geldige UZI-pas van de huisarts in het HIS geregistreerd zijn.

Registreren binnen HIS

Binnen een huisartspraktijk dient men binnen het HIS per medewerker de geldigheid van de UZI-pas te verifiëren. Daarnaast moet men de pas ook binnen het HIS geregistreerd staan. Is dat niet gebeurd dan worden van die arts geen dossiers aangemeld op het LSP. Binnen groepspraktijken kunnen huisartsen patiënten op eigen naam hebben staan. Daardoor kan het bij niet registreren van een UZI-pas het voorkomen dat niet alle mensen van die praktijk met een corona-opt-in aangemeld worden in het LSP. Mogelijk speelt die problematiek bij MicroHIS ook omdat het systeem twee inlogmogelijkheden kent. Eén zonder UZI-pas met inlogcode en wachtwoord en één met pas.

Te ingewikkeld

Met de UZI-pas speelt eigenlijk dat aanvraag, levering en gebruik veel te ingewikkeld is. Het gebruik is aan nogal wat voorwaarden gebonden zoals u hierboven hebt kunnen lezen. In de hectiek van de dagelijkse praktijkvoering kan het voorkomen dat niet aan alle randvoorwaarden voor het gebruik voldaan wordt. In de huidige corona-tijd is elke administratieve handeling extra er één te veel.

Nooit 100%

De corona-opt-in-maatregel zal sowieso een beperkt resultaat hebben. In de eerste plaats heeft rond de 20% van de huisartspraktijken geen aansluiting op het LSP. Daarnaast kunnen huisartspraktijken eigenstandig besluiten de corona-opt-in-update van hun HIS eventueel niet uit te voeren. Plus nu de sores van het niet geregistreerd zijn van UZI-passen binnen een HIS met de vraag of huisartsen dit probleem verhelpen door het alsnog uitvoeren van de registratie.

Kritiek

De corona-opt-in-maatregel heeft bij kritische organisaties, zoals het Platform Burgerrechten, Privacy First en Bits of Freedom zeer veel wind gevangen. Zeer bedenkelijk is de rol van de Autoriteit Persoonsgegevens daarbij. Die gooide plotseling haar basisvoorwaarde voor het LSP, de opt-in-toestemming, overboord en introduceerde op vreemde wijze een opt-out bij bezoek aan de huisartsenposten. De drive van VWS om voluit los te gaan op digitale oplossingen bij de coronacrisis levert verbazingwekkende taferelen op. We mochten dat het afgelopen weekend ook zien bij het debacle van de corona-apps.

W.J. Jongejan, 23 april 2020

Afbeelding van maz-Alph via Pixabay

Met het updaten van een HIS gaat er nogal eens wat mis



Huisarts Informatie Systemen(HIS-sen) zijn geen statische programma's. Aan deze elektronische medische dossiers vindt continu onderhoud plaats. De leverancier zorgt regelmatig voor updates van het HIS. Daarbij loopt niet altijd alles vlekkeloos. Een bekend verschijnsel bij meerdere HIS-sen is dat na een update de "performance" soms opeens achteruit gaat. Daarmee wordt de snelheid bedoeld, waarmee de schermopbouw plaats vindt na aanklikken van een keuze. Ook vliegt de gebruiker dan soms ongewild uit het programma, waardoor opnieuw opstarten nodig is. Eén en ander is betekent een enorme verstoring van de workflow in de praktijken. De problemen lost men na kortere of langere tijd op. Het leidt echter tot veel irritatie op de werkvloer. Ondanks uitgebreid testen van een update door leverancier en huisarts-testers blijkt het toch mis te kunnen gaan. De hoofdreden is dat een HIS een soort kerstboom geworden is met wat eigen ballen, maar ook heel veel andersoortige ballen.

Kerstboom

In de jaren 90 van de vorige eeuw, toen huisartsautomatisering op gang kwam, was er sprake van losse systemen bij praktijken zonder externe koppelingen. Je had dan een betrekkelijk kale kerstboom waar maar enkele ballen in hingen. Behoudens het updaten van het HIS moest hooguit regelmatig een nieuw medicijnbestand ingeladen worden, de zogenaamd G-Standaard. Later zijn er aan de HIS-sen veel hulpprogramma's gehangen plus allerlei externe verbindingen. Bij de hulpprogramma's

denk ik dan aan NHGDOC. Dat is een beslis-ondersteunend programma. Bij de externe connecties moet je denken aan verbindingen met apotheken om recepten en medicatiegegevens uit te wisselen. Verder bijv. Zorgdomein, een digitaal platform waarop zorgverleners zorg vragen, zorg aanbieden en op een snelle, veilige manier patiëntinformatie kunnen uitwisselen. Dat gaat dan bijv. om verwijsbrieven die elektronisch naar de specialist gaan of het kunnen zien van wachttijden voor poliklinieken.

Dieper gaande koppelingen

De laatste tien jaar zijn er nog dieper gaande koppelingen tot stand gebracht in het kader van het uitwisselen van zorgdata via het Landelijk SchakelPunt(LSP). I.v.m. het beveiligen van de toegang kwam daar op elke werkplek een kaartlezer bij voor de UZI-pas . Daarvoor is dan ook weer apart connectieprogramma nodig. Voor het declaratieverkeer dat vanuit het HIS plaatsvindt is ook weer een met een certificaat beveiligde verbinding nodig van het HIS met VECOZO, het declaratie-portaal van de zorgverzekeraars. Los daarvan zijn er de verschillende configuraties waarmee huisartsen met hun HIS werken: op een eigen server, op een met anderen lokaal gedeelde server of met een ASP-provider die het HIS op een serverpark draait en waarbij de huisarts met een beveiligde verbinding werkt. Het zijn steeds meer ballen die aan dezelfde boom hangen. Bronnen voor problemen te over dus.

Recente voorbeelden

Elk HIS kent dit soort problemen. Het vinden van de oorzaak kan soms van korte duur zijn, maar ook veel langer duren. Enkele voorbeelden van de afgelopen 12 maanden:

- Medio 2019 blijkt na een update Promedico ASP plotseling zeer traag te werken. Op Twitter is dat te zien. Tot in oktober 2019 blijkt het probleem voort te duren getuige een Tweet.

- MicroHIS kende in januari 2020 voor een aantal gebruikers een plotse vertraging van de performance vlak na een update. Systemen met de server in eigen beheer hadden het probleem niet. Onder ASP-werkende systemen weer wel. Inmiddels lijkt na anderhalve weken het lek boven water: de koppeling met een extern systeem. Nu wacht men op een update waarin het euvel verholpen wordt.
- Medicom kende op 29 januari 2020 het probleem dat een aantal huisartsen niet meer konden inloggen in hun systeem, dus er niet meer mee konden werken. Men had een “achtergrondproces” gewijzigd. Ondanks testen bleek er toch een flinke verstoring te zijn die gelukkig maar enkele uren duurde.

Problem-shooting en -solving

Door de veelheid van ballen die in de kerstboom zijn komen te hangen en de verschillen in configuratie is het soms zeer lastig om het lek boven water te krijgen. Vaak is het een oplettende programmeur die het licht ziet, soms zijn het gebruikers die opeens de “clue” zien. Gevallen van serendipiteit dus. Zo kan ik me uit eind jaren '90 me een zeer weerbarstig probleem herinneren met MicroHIS. Ik weet niet meer hoe het probleem eruit zag, maar de ene praktijk had er wel last van en de andere niet. Uiteindelijk was er een opmerkelijke huisarts die ontdekte dat het probleem op een werkstation met Windows 95 zich wel voordeed en niet op één met Windows 98. Het letten op verschillen in performance tussen praktijken met verschillende hard- en softwareconfiguratie blijft nog steeds belangrijk bij de probleemoplossing.

Wordt vervolgd

Het moge uit het voorgaande duidelijk zijn dat ondanks grote inspanningen van leveranciers, pakketcommissies, testers en

gebruikers, problemen met het updaten van elektronische medische dossiers, zoals de HIS-sen onvermijdelijk blijven. Het blijft uiteindelijk mensenwerk.

W.J. Jongejan, 4 februari 2020

Afbeelding van Gerd Altmann via Pixabay

Deel UZI-certificaten voor toegang zorgsystemen voldeden niet aan basiseisen browserpartijen



Versneld laat het UZI-register ongeveer 3000 UZI-certificaten van zorgaanbieders vervangen door nieuwe. Daartoe hebben die eind augustus 2019 een email en een brief ontvangen om uiterlijk voor 17 september 2019 een aanvraag voor een nieuw certificaat te doen. Het komt omdat meerdere grote webbrowserpartijen, zoals Google, Apple en Mozilla aangaven dat die servercertificaten niet voldoen aan basiseisen die ze stellen. Het gaat om de UZI-register Server CA G21-certificaten. De reden is dat de standaarden voor certificaten verplichten dat die over een 64-bit serienummer moeten beschikken. Twee certificaatautoriteiten betreft het: het CIBG van het ministerie van VWS waar het UZI-register onder valt en KPN. Die hebben certificaten uitgegeven die effectief over een 63-bit serienummer beschikten. Dit kwam door een onjuiste standaardinstelling van de gebruikte uitgiftesoftware EJBCA. De deadline voor het vervangen zijn van de certificaten is 1

oktober 2019. Beroepsverenigingen als de Landelijke HuisartsenVereniging roepen hun leden op snel te handelen

Veiligheid

Van overheidswege benadrukken het UZI-register en de minister voor medische zorg Bruno Bruins dat er geen sprake is van een beveiligingsrisico. Ook Logius, de dienst van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties, zegt dit. Logius beheert de generieke ICT-voorzieningen voor de overheid. Maar waarom vervangt het UZI-register dan een paar duizend UZI-certificaten die medio maart 2020 vanzelf al zouden verlopen? De resterende looptijd zou nog maar 6 maanden zijn. **Juist omdat er een, weliswaar klein, veiligheidsrisico bestaat.** Webbrowser-fabrikanten oefenen niet voor niets nu druk uit op certificaatuitgevers om te zorgen dat die veilige waar leveren.

Reden

Hoewel deze certificaten niet voor gebruik in internetverkeer zijn uitgegeven, is het wel mogelijk ze voor internetverkeer te gebruiken. De certificaten moeten volgens de genoemde browserpartijen voldoen aan de eisen die deze stellen.

Inloggen

Om in het elektronische medische berichtenverkeer er zeker van te zijn dat men met de juiste partij communiceert(authenticatie) en het berichtenverkeer versleuteld is (encryptie) maakt men gebruik van (software)certificaten(UZI-Certificaten) die op de server geïnstalleerd worden plus elektronische passen(UZI-passen) met paslezers om die servers te gebruiken. De gewraakte certificaten vallen onder de PKI-stelsel(Public Key Infrastructure) van de overheid. Nadat was vastgesteld dat de servercertificaten niet meer aan de eisen voldeden, heeft het

UZI-register met toestemming van Logius besloten om de in omloop zijnde servercertificaten via natuurlijk verloop uit te faseren. Dat ging echter niet snel genoeg naar de mening van de webbrowser-partijen. Die hebben nu druk op de ketel gezet.

Ook KPN

Uit berichtgeving van de browsermaker Mozilla blijkt dat medio maart 2019 duidelijk was dat het probleem behalve bij CIBG, dus bij het UZI-register, ook bij KPN voorkwam. Er staat: **“3/15/2019 09:39 CIBG indicates that the same issue that plagued KPN also affects them”**. Ook is uit het document duidelijk dat de browsermakers het probleem zien als een schending van de basiseisen die aan certificaten gesteld worden, de Basic Requirements.

Trage actie

Zeer interessant is een bericht van 4 september 2019 van een Mozilla-medewerker. Daarin spreekt deze zijn verwondering uit over het trage tempo waarin alles gebeurt. Hardop vraagt hij zich af waarom het van half maart 2019(melding van CIBG aan Logius) tot half augustus duurde voordat Logius zichtbaar adequaat actie ondernam. Ook vraagt hij zich af waarom Logius als overkoepelende organisatie van gevoelige overheids-ICT-zaken niet zelf het probleem wat het CIBG rapporteerde ontdekt had. Te meer omdat dat wat het CIBG meldde ook te benaderen was vanuit publiek toegankelijke bronnen.

Overheid en ICT

Eens te meer blijkt weer eens dat overheid en ICT geen gelukkig huwelijk is. Slagvaardig handelen ontbreekt vaak. Als er binnen de overheid een organisatie wordt opgetuigd om slagvaardig te handelen, zoals het BIT(Bureau ICT-toetsing) dan ervaren de ministers en de ambtelijke top dat als bijzonder lastig.

Werkveld

In de dagelijkse praktijk is zo'n plotse certificaatwijziging weer extra overlast. Administratieve handelingen moeten onder tijdsdruk plaats vinden. Zorgaanbieders moet of zelf of een systeembeheerder vragen snel het nieuwe certificaat te installeren. Niet installeren zal de continuïteit van het elektronische medische berichtenverkeer in gevaar brengen.

W.J. Jongejan, 9 september 2019

Afbeelding van Gerd Altmann via Pixabay, bewerking door W.J.J.

UZI-pas en rijbewijs: een slechte combinatie



Afgelopen week bereikten mij een drietal verhalen van huisartsen, die een nieuwe UZI-pas aanvroegen en daar geen vrolijke herinneringen aan overhielden. Voor het inloggen in elektronische zorgcommunicatiesystemen, maar ook in een aantal gevallen het inloggen in het eigen huisarts-informatie-systeem(HIS) is een UZI-pas nodig. UZI staat voor Unieke Zorgverlener Identificatie. Het UZI-register, als onderdeel van de dienst CIBG(Centraal Informatiepunt Beroepen Gezondheidszorg) valt onder het ministerie van VWS. Aangezien de UZI-passen een geldigheidsduur van drie jaar hebben, moet er nogal eens een pas vervangen worden. Soms noopt de komst van een nieuw personeelslid tot een nieuwe pas. Zowel het aanvragen als het in ontvangst nemen van een UZI-pas kan tot gekke situaties leiden. Ik neem u de komende minuten mee in de ervaringen van

drie huisartsen.

Huisarts 1

Deze had een pas die het einde van de geldigheidsduur naderde. Hij vroeg een nieuwe aan. UZI-passen kunnen met een speciale koeriersdienst in de praktijk bezorgd worden. De aanvraag verliep vrij soepel. Hij kreeg een week voor de bezorging een email, dat hij een geldig legitimatiebewijs moest kunnen laten zien. Een geldig legitimatiebewijs zou zijn een rijbewijs of een paspoort. Dit stond in de mail. De huisarts was met een rijbewijs in de praktijk, toen de bezorger kwam. Een uur voor de koerier kwam kreeg hij nog een mail over de UZI pas. Of hij er wel om wilde denken, dat als hij meer dan één voornaam had, het rijbewijs ineens GEEN geldig legitimatiebewijs is. De koerier kwam. Hij toonde hem de oude UZI-pas en het rijbewijs. Hij kreeg de UZI-pas niet, want hij heeft twee voornamen... Dan geldt het rijbewijs ineens niet als legitimatiebewijs. Hij moest weer een nieuwe afspraak maken voor het opnieuw sturen van een koerier.

Vervolg

De koerier kwam nadien voor de tweede keer langs. Hij zou komen tussen 8:00-13:00 uur. De huisarts was een visite (10 minuten) aan het rijden en uitgerekend toen kwam de koerier. Hij wilde geen minuten wachten, dus: weer geen UZI pas. Daarop weer een afspraak gemaakt voor de volgende dag en toen lukte het.

Overheen lezen

Wat stond er nu in de mail waar de huisarts achteraf van besepte dat hij er overheen gelezen had:

Bij het afleveren van de UZI-pas moet de koerier uw identiteit controleren aan de hand van een geldig wettelijk

identiteitsdocument (rijbewijs is ook geldig mits u slechts 1 voornaam heeft en deze volledig staat vermeld of heeft u meerdere voornamen dan kan een rijbewijs enkel als u ook een geldig geboorteakte kunt overhandigen). (Vet WJJ) Meer informatie hierover kunt u lezen op www.uziregister.nl. Hieronder leest u in het kort hoe de procedure in zijn werk gaat:

- U toont de koerier een geldig wettelijk identiteitsdocument (paspoort, rijbewijs, identiteitskaart, diplomatiek paspoort, dienstpaspoot of verblijfsdocument).*
- Uw identiteitsdocument wordt op echtheid gecontroleerd;*
- U zet uw handtekening op een handtekeningkaart, de koerier controleert deze aan de hand van de handtekening op uw identiteitsdocument; etc etc.*

Vreemd

Bij twee voornamen is een rijbewijs opeens geen geldig identiteitsbewijs, maar weer wel als men een geldige geboorteakte kan overleggen. Dat zal geen huisarts zo maar bij de hand hebben. Het ware wenselijker als het rijbewijs als identiteitsbewijs voor het in ontvangst nemen van een UZI-pas gewoon geschrapt wordt en zo geen verwarring meer kan veroorzaken.

Huisarts 2

Deze heeft een hidha sinds kort in de praktijk, een huisarts in dienst van een huisarts. Zij is medewerkster in zijn praktijk. Vanwege haar diensten als huisarts op de huisartsenpost heeft hij voor haar a raison van 250 euro een medewerker-UZI-pas aangevraagd. Fout helaas. Dat had een zorgverlenerspas moeten zijn. Een medewerkerspas is alleen bestemd voor personeel dat niet BIG-geregistreerd is. Opnieuw dus pas, maar wel de goede, aangevraagd. Weg 250 euro.

Huisarts 3

Deze verlengde zijn zorgverlenerspas en ook zijn pas werd bezorgd op de praktijk. De eerste keer was hij weggeroepen en ging de koerier zijns weegs. De tweede keer nam de koerier geen genoegen met de kopie van het paspoort uit de personeelsmap, waardoor een derde keer nodig was.

Weerbarstige materie

Uiteraard koppelt men aan de bezorging van UZI-passen de nodige controles vast. Deze geven in de praktijk toch de nodige praktische problemen. Vooral het gebruik van het rijbewijs als identiteitsbewijs kan beter volledig buiten beeld gebracht worden. En ja, heb je eenmaal je UZI-pas dan is maar helemaal de vraag hoe strikt er intern mee gewerkt wordt in praktijken. Logt een medewerker telkens uit en een nieuwe weer in als ze na elkaar op hetzelfde werkstation moeten werken of even naar het toilet gaan?

Dat is dan weer een heel ander verhaal.

W.J. Jongejan, 15 april 2019

**Nog steeds niet beschikbare
UZI-pas(niet op naam) maakt
illegaal handelen tot
noodzaak**



Voor een aantal medewerkers bij zorgverleners, als apotheken, huisartsen en ziekenhuizen, bestaan "UZI-passen-niet-op-naam". Deze zijn bedoeld voor personeelsleden die het informatiesysteem van de zorgverlener voor hun werk moeten gebruiken, maar niet geautoriseerd zijn om via het Landelijk SchakelPunt handelingen te verrichten. Eind mei 2017 liet de instantie die de passen uitgeeft, het UZI-register, onder verantwoordelijkheid vallend van het CIBG, plotseling weten dat zulk soort passen tot 1 maart 2018 niet te verlengen of nieuw te verkrijgen zouden zijn. We leven nu in juni 2018 en deze UZI-passen- niet op naam- zijn nog steeds niet te krijgen. Koepelorganisaties van zorgverleners, als de Koninklijke Nederlandse Maatschappij ter bevordering van de Pharmacie(KNMP), de Landelijke HuisartsenVereniging(LHV) en INEEN waarschuwden de afgelopen week dat deze passen nog steeds niet beschikbaar zijn. De oorspronkelijke negen maanden die het UZI-register zelf voorspelde in 2017 zijn nu ruim elf geworden. Het gevolg van het niet leveren van nieuwe passen is dat zorgverleners hun personeel in toenemende mate met workarounds toch hun werk moeten laten doen. Dat gebeurt dan op andermans UZI-passen. Dat is in wezen illegaal, maar wel noodzakelijk om op de werkvloer alles goed te laten verlopen. Ik schreef erover op 23 mei 2017.

Reden

De reden van het plotsklaps niet meer kunnen aanmaken van nieuwe UZI-passen(niet op naam) was gelegen in gewijzigde eisen waaraan het UZI-register moet voldoen als Trusted Service Provider. Daar viel bijvoorbeeld het opnemen van Kamer van Koophandel(KvK)-nummers in UZI-passen. En daar was de chip

op de kaart niet op berekend. Zowel het UZI-register zelf als de passen moesten aangepast worden. In 2017 heeft men het probleem te laat zien aankomen, waardoor slechts in de laatste week van mei nog passen die verliepen opnieuw aangevraagd en uitgeleverd konden worden. Onder de oppervlakte wordt continu gesleuteld aan de UZI-passen. Ik vond een document waarin het CIBG-een dienst onder verantwoordelijkheid van het ministerie van VWS- één en ander opsomt. Op pagina 10 ziet u het schema van de mutaties rond de helft van het jaar 2017. In hoofdstuk 1.1.2. ook wat opmerkingen over de genoemde pas.

Onvindbaar

Als u nu zoekt op de website www.uziregister.nl dan is er niets over de UZI-passen-niet- op-naam te vinden. Alle links die ik in het hierboven genoemde artikel van mij van 23 mei 2017 plaatste met betrekking tot pagina's op de website van het UZI-register zijn dood. Het lijkt erop alsof ze van de aardbodem verdwenen zijn om lastige vragen te voorkomen zolang de gewraakte kaart net beschikbaar is.

Illegaal

De niet op naam staande passen zijn normaliter in gebruik bij administratieve medewerkers van zorgaanbieders. Het gaat om leerling (apothek)assistentes, administratieve krachten, bezorgers en stagiaires. Het niet hebben van de passen leidt tot verstoring van werkprocessen. Om deze toch normaal hun werk te kunnen laten doen laten hun werkgevers hen nu werken op werkstations waarop andere pashouders ingelogd zijn. Het doel waarvoor de passen-niet-op-naam ooit gemaakt zijn, wordt daarmee volledig voorbij geschoten. Logging van wie wanneer op welk werkstation deed is nu deels onmogelijk.

Uitlokking

Wat hier gebeurt, is het uitlokken van illegaal handelen. Het inloggen op andermans passen is iets waarvoor het ministerie van VWS continu gewaarschuwd heeft, mede naar aanleiding van

de resultaten van een onderzoek uit 2011. Daaruit bleek dat vaak met andermans pas werd ingelogd of dat medewerkers bij het tijdelijk verlaten van de werkplek niet uitlogden.

Het geeft ook weer eens aan hoe weerbarstig ICT-problemen in de zorg zijn. ICT-projecten bij de overheid, waarbij deadlines niet gehaald worden zijn zeer talrijk. De overheid wil dan nogal eens net doen of de neus bloedt en het probleem doodzwijgen, bagatelliseren of in het ergste geval ontkennen.

W.J. Jongejan, 15 juni 2018

Een blik achter de schermen van het LSP met VZVZ-leaks



Elk jaar houdt de Vereniging van Zorgaanbieders Voor Zorgcommunicatie(VZVZ), die verantwoordelijk is voor het Landelijk SchakelPUNT(LSP) een leveranciersdag. Zo ook op 7 oktober 2016. Tijdens die dag wisselden prominente werknemers van VZVZ van gedachten met leveranciers over technische en organisatorische zaken rond het LSP. Het programma van die dag is openbaar, maar de inhoud van dat overleg is normaliter niet

openbaar. Ook niet voor de op het LSP aangesloten zorgaanbieders, die een ledendag hebben daags voor de leveranciersdag. Ook de notulen van de leveranciersdag zijn nooit openbaar geweest. Dankzij een VZVZ-medewerker die de notulen van deze dag op een hoekje van zijn privé-website zette, is nu een inkijk in de ontwikkelingen en de problemen rond het LSP mogelijk. Deze notulen zijn normaliter alleen met behulp van een gebruikersnaam en wachtwoord toegankelijk op de VZVZ-website. Ik zal puntsgewijs de zaken langslopen die in de notulen aan de orde komen. Laat ik ze maar de VZVZ-leaks noemen

Versiebeheer met bouwstenen

In de discussiesessie met bovenstaande titel gaat het om de opbouw van berichten en de manier waarop met het versiebeheer van de onderdelen ervan omgegaan moet worden. De opbouw van via het LSP verstuurd berichten gaat volgens zogenaamde zorginformatiebouwstenen waarover Nictiz het beheer voert. Die hebben in de loop der tijd telkens een andere versie. Het blijkt dat ondanks vijf jaar privaat LSP-gebruik en daarvoor drie jaar publieke ontwikkeling dat nog steeds discussie bestaat over het versiebeheer van alle bij het LSP gebruikte software. Bij het versiebeheer is telkenmale van belang dat de software backwards compatible is, omdat niet iedereen tegelijk dezelfde versie in gebruik heeft.

Aanmelden Bronsysteem

In deze discussiesessie gaat het om de vraag op welke wijze gegevens worden aangeboden aan de centrale verwijzindex. Dat is dat deel van het LSP dat bijhoudt waar wat van wie in een broncomputer staat. Dat aanmelden kan op bouwsteen-, op zorgtoepassing- en op dossierniveau. Men blijkt gekozen te hebben voor het bouwsteenniveau, maar dat heeft ook weer consequenties voor het functioneren van het systeem en heeft ook forse juridische en politieke aspecten. Dat is op te

maken uit de uitgebreide discussie daarover. Eén en ander heeft te maken met de verwijfsindex die zo kaal mogelijk moet zijn en zelf geen medische data mag bevatten of iets wat daarop lijkt. Met de keuze voor bouwstenen als basiselement bij het versturen van data zou het wel zo zijn dat er medische content in de verwijfsindex komt. De verwijfsindex hoeft alleen maar te weten wie iets weet over een patiënt, maar dan is er met een recent geïntroduceerde signaalfunctie een probleem. Die moet ervoor zorgen dat gebruikers een signaal krijgen als er nieuwe data zijn aangemeld en is bedoeld om nu onnodig vaak voorkomende raadplegingen te beperken. Men lijkt er nog niet helemaal uit te zijn. Bij VZVZ zijn ze als de dood om onderwerp te worden van een politieke discussie.

Gebruik UZI-pas

Uit de notulen van deze sessie blijkt dat het LSP-gebruik in ziekenhuizen helemaal niet van een leien dakje loopt. Het blijkt dat de er een grote inzet nodig is van leveranciers om problemen op te proberen te lossen. Men loopt o.a. aan tegen problemen met Citrix-software die gebruikt wordt bij het netwerkverkeer in de zorginstelling en tegen de aanwezigheid van veel werkstation die zogenaamde "thin clients" zijn. Het is een naam voor kleine, relatief zwakke computers die de hoofdmoot van de benodigde computercapaciteit van een centrale computer betrekken en één gebruiker tegelijk bedienen. De kleine computer fungeert daarbij als client ('klant') van de centrale computer. Blijkbaar vereist onder andere de software voor het gebruik van een UZI-kaart-lezer per werkstation te veel systeembronnen daarvan om goed te kunnen werken. Ook de Terminal Server-software die op de werkstations draait geeft problemen. Men zoekt trouwens de grens op van wat mag, want VZVZ-medewerker Marcel Settels beschrijft namelijk een gerealiseerde situatie waarmee op één werkstation verschillende sessies van meerdere medewerkers draaien. Daarbij loggen die medewerkers achter elkaar in

met verschillende passen. De vraag daarbij is uiteraard of na inloggen op deze wijze medewerkers niet in elkaars sessie kunnen gaan werken. Ik denk van wel.

Commerciële pas?

In dezelfde sessie komt het NUZI-project ter sprake. Nergens op het internet is uitleg over deze afkorting te vinden, maar ik denk dat NUZI staat voor Nieuwe UZI-pas. Al de acties van NUZI zijn gericht op de ontlasting van de leveranciers bij het werken met verschillende authenticatiemiddelen. Uit de discussie over de UZI-pas blijkt overduidelijk dat ook de leveranciers door hebben dat het gebruik van de UZI-pas door zorgverleners als hinderlijk wordt ervaren gezien de tijd die het kost om in te loggen. Alternatieven passeren de revue. Marcel Settels zegt dat de UZI-pas over drie jaar een herijkingsmoment krijgt en het UZI-register mogelijk een andere rol. Er zou dan mogelijk geen UZI-pas pas meer van overheidswege meer komen, maar een commerciële pas met specifieke voorzieningen. Interessant is het te lezen dat in oktober 2016 50.000 UZI-passen voor LSP-verkeer uitgegeven zijn en nog eens 50.000 die gebruikt worden voor het inloggen bij instanties als VECOZO en SBV-Z.

Prefetchen

Het niet realtime, maar voor-ophalen van medische data via het LSP neemt nog een zeer grote plaats in. Dat blijkt ook uit een hele discussiesessie over dit onderwerp. Men kan eigenlijk in een aantal gevallen niet anders. Zoals ik al eerder publiceerde gaf Marcel Settels van VZVZ op de leveranciersdag aan dat je in een als realtime bedoeld systeem eigenlijk niet aan dat prefetchen zou moeten doen. De conclusie bij deze discussiesessie is toch dat prefetching nodig is en blijft. Zeer openhartig is trouwens de opmerking dat de opvrager bij het prefetchen veel foutmeldingen terug krijgt die hij zelf moet oplossen.

Verstoringsen

Het berichtenverkeer via het LSP loopt vaak niet vlekkeloos. Dat blijkt uit de speciale discussiesessie over dit onderwerp. Het blijkt deels te gaan om te voorkomen verstoringen maar ook om lokale verstoringen die door de aangesloten zorgverlener gepercipieerd worden als "het LSP werkt niet". Foutmeldingen zijn er met exotische afkortingen zoals RTEDEST (de apotheek of huisartsenpraktijk is niet bereikbaar of QABRTITI (er is een fout opgetreden tijdens de opvraging (time-out)). Het bronsysteem (de huisartsenpraktijk of apotheek) reageert niet binnen 60 seconden). Blijkbaar moet een opvragende zorgverlener tot een minuut wachten tot er antwoord komt!!

Iets met DUO???

In de brainstormsessie met de titel "Wat kan beter?" blijken allereerst een aantal zeer basale onderwerpen de revue te passeren, zoals:

- Wanneer moet er iets echt af zijn?
- Wanneer begint iets, wanneer eindigt iets?
- Releasekalender?
- Werkplan?

Het is in mijn ogen vreemd dat na drie jaar publiek en vijf jaar privaat werken met het LSP dit soort vragen nog steeds bestaan. Men komt tenslotte tot de conclusie dat VZVZ zich meer moet profileren naar de leden toe en haar rol duidelijker moet maken voor eindgebruikers en zorgkoepels. Wat betreft toekomstige samenwerking blijkt men niet alleen te denken aan het Nederlands Centrum voor Jeugd en Gezin, maar ook aan de stichting DUO die studiefinanciering regelt voor studenten, scholieren en leraren. Hiermee gaat men zich toch echt buiten de zorg begeven en is sprake van een enorme function-creep van een zorgcommunicatiesysteem.

Conclusie

Het lezen van deze notulen bevestigt mijn gevoel dat ondanks een half miljard euro aan uitgaven aan het LSP het nog steeds niet is wat het lijkt te zijn. Het is één en al werk in uitvoering, zelfs bij reeds gerealiseerde functionaliteit. Basale zaken, als wat leveranciers en VZVZ van elkaar verwachten en weten bij het uitvoeren van werkzaamheden zijn nog steeds onderwerp van discussie tussen deze partijen.

W.J. Jongejan

Voor de geïnteresseerde lezer hier alle notulen op een rijtje: A, B, C, D, E, F, G, H, I, J, K, l, M, N, O, P, Q.

En toen waren er 9 maanden geen nieuwe UZI-passen(niet-op-naam)



Vanaf 1 juni 2017 tot begin maart 2018 zullen er geen nieuwe UZI-passen-niet-op-naam verstrekt kunnen worden door de uitgifteorganisatie, het UZI-register. Passen die in die tussentijd verlopen kunnen alleen de komende week(tot 1 juni 2017) nog aangevraagd worden. Doet een zorgorganisatie, waar medewerkers dat type inlogpas gebruiken dit niet, dan kunnen die medewerkers niet meer inloggen in de zorgsystemen waar ze mee werken. Het is niet een tekort aan UZI-passen, noch een

tekort aan mankracht, maar een probleem dat door regelgeving ontstaan is. Het komt door gewijzigde eisen waaraan het UZI-register moet voldoen als Trusted Service Provider, waaronder het opnemen van Kamer van Koophandel(KvK)-nummers in UZI-passen. Zowel het UZI-register als de passen moeten aangepast worden. Je zou verwachten dat zowel de regelgevers als de uitgevers van de UZI-passen dit probleem op grote afstand hadden zien aankomen. Het korte tijdsbestek van een week waarin nog passen die de komende negen maanden verlopen aangevraagd kunnen worden doet vermoeden dat men daar heeft zitten slapen. Bij dit alles moet men bedenken dat het UZI-register onder de uitvoeringsorganisatie CIBG valt. Deze organisatie is een onderdeel van het ministerie van VWS. Die is dus uiteindelijk verantwoordelijk voor deze rare situatie.

Soorten passen

Het Unieke Zorgverlener Identificatienummer(UZI) is een in 2006 geïntroduceerd nummer dat in Nederland gebruikt wordt om een bij het zorgproces betrokken persoon te identificeren. De introductie is onlosmakelijk verbonden met het opzetten van het publieke Elektronische landelijke patiënten Dossier(L-EPD), het latere, private, Landelijk SchakelPunt(LSP)-gebruik. Het nummer is gekoppeld aan het gebruik van de UZI-pas, een chipkaart die tot doel heeft om bij elektronische uitwissing van patiëntgegevens de veiligheid van die gegevens te garanderen. De kaart wordt zowel gebruikt ter identificatie(wie logt er in) als authenticatie(is degene die inlogt wie hij beweert te zijn) van een bij het zorgproces betrokken persoon.

Er bestaan drie soorten passen:

- **de zorgverlenerspas.** Dit is een pas voor zorgverleners waarvan het beroep is geregeld in artikel 3(bijv. arts , apotheker, psychotherapeute etc.) of artikel 34(apothekersassistente, diëtist etc.) van de Wet BIG.

- **de medewerkerspas op naam.** Dit is een persoonlijke pas voor een medewerker van een zorgverlener of organisatie. Het gaat om medewerkers die voor hun werk toegang nodig hebben tot zorginformatie van personen.
- **de medewerkerspas niet op naam.** Ook dit is een pas voor medewerkers. Deze UZI-pas bevat een beperkte hoeveelheid informatie en heeft minder mogelijkheden. Op deze pas staat niet de naam, maar wel de functie van de medewerker. Deze functienaam mag niet een wettelijke beschermde titel zijn of hier op lijken. Wel kunnen bijv. functienamen er op staan als: medewerker patiëntenadministratie, (dokters)assistente of medewerker apotheek.

Uitnodiging tot workaroud

Wat kunnen we de komende negen maanden verwachten. In de eerste plaats zal er een enorme berg aanvragen in de komende week gedaan worden bij de uitgifte-organisatie: het UZI-register. Die berg zal bij de uitgifte als een prop gaan fungeren. Die zal ervoor zorgen dat de wachttijd voor alle UZI-passen zal gaan uitlopen. Daarbij moet men ook beseffen dat recent de geldigheidsduur van alle UZI-passen van drie naar twee jaar ingekort is. Dit zorgt ook voor extra werk. In de tweede plaats zal het gaan voorkomen dat medewerkers van zorgverleners of zorgorganisaties die niet op tijd een nieuwe pasaanvraag deden niet meer met hun bestaande pas kunnen inloggen en een workaroud gaan bedenken. Men wil gewoon doorwerken volgens de dagelijkse routine en niet gehinderd worden door het ontbreken van een UZI-pas. Dat betekent dat mensen gaan werken op de geldige pas van een ander of medewerkers na het verlaten van een werkplek de pas tijdelijk in de kaartlezer laten zitten zodat een ander op dat werkstation zijn of haar ding kan doen. Reeds in 2011 werd vastgesteld dat zoiets bij apothekers gebeurde. Toen werden er al Kamervragen over gesteld.

Man-made disaster

Wat we hier voor onze ogen zien gebeuren is een typisch voorbeeld van man-made disaster. Vanuit de gedachte dat alles in de (zorg)ICT wel te regelen zou zijn, zijn in elkaar grijpende systemen bedacht met dito-regelgeving. Het benul dat het één en ander te gecompliceerd ging worden is bij niemand opgekomen. Het is weer eens een naar gevolg van wat ik techno-optimisme noem. Het is naar dat dit UZI-pas gedoe zich voordoet, omdat werkers in de zorg gehinderd worden in de uitvoering van hun normale taken. Bovendien is het een uitnodiging voor het niet-reguliere gebruik van de UZI-passen.

W.J. Jongejan

Nonsens-antwoord minister VWS op Kamervragen UZI-pas- probleem



Minister Schippers is er gisteren in geslaagd een onzinnig antwoord te geven met wegwuiven van de eigen verantwoordelijkheid van het ministerie van VWS bij de beantwoording van Kamervragen. Deze waren op 27 september gesteld door de D66-kamerleden Verhoeven en Dijkstra. Deze gingen over het advies van het UZI-register, vallend onder de

dienst CIBG van het ministerie, aan zorgaanbieders om de webbrowser op hun systemen tijdelijk niet te updaten. Dat heeft te maken met het gebruik van verouderde Java- en ActiveX browser- plug-ins door de UZI-pas software. Deze pas die de overheid uitgeeft is niet alleen in gebruik voor de autorisatie en authenticatie als een zorgaanbieder gebruik wil maken van het Landelijk SchakelPunt(LSP)om zorgdata uit te wisselen. Veel apotheek- en huisartsinformatie-systemen, maar ook de software van huisartsenposten maken gebruik van de UZI-pas om werkers in te laten loggen in het systeem. Browserupdates die de ondersteuning van Java uitschakelen kunnen er dan ook voor zorgen dat de software van zorgaanbieders niet meer werkt en het niet updaten van browser-software maakt deze kwetsbaar voor indringers omdat verse beveiligingsupdates niet plaatsvinden.

Ontwijkend

In het antwoord van minister Schippers, gedateerd 25 oktober 2016 , zegt zij dat ze op de hoogte is dat het stoppen van de ondersteuning al sinds januari 2016 bekend is. Het probleem speelt tussen de leveranciers van softwarepakketten en de afnemers van deze pakketten (zorgaanbieders). Omdat er signalen waren dat de softwareleveranciers dit probleem niet overal onderkend en opgelost zouden hebben, is besloten actie te ondernemen volgens haar. De UZI-pas van de overheid heeft voor het functioneren software nodig die door externe partijen gemaakt wordt om te functioneren in samenwerking met software van zorgverleners. Specificaties voor die software zijn door de overheid verstrekt. Door te stellen dat het probleem speelt tussen leveranciers van software en zorgaanbieders ontkent de minister volkomen ten onrechte alle eigen verantwoordelijkheid van het ministerie. Die is er wel degelijk omdat door het maken en verplicht stellen van de UZI-pas voor identificatie en authenticatie bij zorgsystemen de overheid wel degelijk een partij is bij dit probleem. De overheid heeft zich tussen softwareleverancier en

zorgaanbieder genesteld met de UZI-pas. Bovendien is het zo dat de het systeem niet voldoet aan de web-richtlijnen van de overheid. Daarin staat dat een browser-plug-in de functionaliteit mag uit breiden, maar dat alle informatie ook zonder plug-in toegankelijk moet zijn. (zie commentaar in het artikel in deze link)

Mist

Iets verder in haar antwoord op de Kamervragen geeft de minister een antwoord dat ik ter overdenking hier integraal afdruk.

Zorgverleners hebben een eigen verantwoordelijk ten aanzien van beveiliging van de eigen ICT-omgeving. Het is belangrijk dat zorgverleners zelf de afweging maken tussen beveiliging en mogelijke beperking in functionaliteit. Om deze afweging te kunnen maken heeft het CIBG besloten via de betreffende de mail de zorgverleners te informeren. Ik ben mij bewust van het belang van beveiligingsupdates en zal in beginsel altijd adviseren beschikbare beveiligingsupdates van browsers en bijhorende plug-ins te installeren. In de mail van 21 september jl. adviseert het CIBG om automatische updates niet meer te laten plaatsvinden. Dit betekent dat deze updates alleen kunnen plaatsvinden in een gecontroleerd proces waarbij ook getest wordt of het pakket waar de zorgaanbieder mee werkt, ook na de update blijft werken. Op basis van een eigen risico inventarisatie dient de aangeschreven zorgverlener te beoordelen op welke wijze hij het advies van het CIBG implementeert. Bij de initiële e-mail is het NCSC niet betrokken geweest. Op dit moment is het NCSC betrokken bij het dossier.

Hierin zegt ze in eerste instantie dat het altijd goed is om de browsers te updaten en plug-ins te installeren. Daarna komt ze met het mistige verhaal dat de up[dates in een "gecontroleerd proces" getest moeten worden om te zien of alles nog werkt na de update. Vervolgens komt ze met de

opmerking dat de zorgverlener een eigen risico-inventarisatie moet maken om te beoordelen of het advies van het CIBG om de browser maar even niet te updaten opgevolgd wordt.

Verantwoordelijkheid

Enerzijds geeft de minister aan dat de eigen dienst CIBG een verantwoordelijkheid heeft in deze kwestie, maar anderzijds schuift ze volkomen ten onrechte de verantwoordelijkheid af naar eindgebruiker, de zorgaanbieder. Kwalijk is ook dat het CIBG een advies gaf aan alle UZI-pashouders dat consequenties heeft voor de zorgverlener-systemen zonder het Nationaal Cyber Security Center (NCSC) daarin te kennen. Dat is een zeer duidelijke omissie.

De kern van het probleem is dat het ministerie met de UZI-pas zich tot op detailniveau heeft genesteld in het al dan niet goed functioneren van de software van zorgaanbieders. Als de UZI-pas dan opeens niet kan werken heeft dat zeer grote consequenties.

W.J. Jongejan

**Kamervragen over onveilige
webbrowsers i.v.m. UZI-pas.
VZVZ dekt zich in**



Op 21 september meldde ik op deze website dat alle UZI-pas-houders een email van het UZI-register gekregen hadden. Het UZI-register valt onder de dienst CIBG van het ministerie van VWS. In die email stond het dringende verzoek om met ingang van 1 oktober geen update van de webbrowsers te doen. Dat is dus overmorgen. Het heeft te maken met het uitfaseren per 1 oktober van de browser-hulpprogramma's Java en Active X door de leveranciers van webbrowsers. Doet men de browser-updates wel, dan zal de UZI-pas niet meer werken was de boodschap. Deze pas is niet alleen in gebruik voor de autorisatie en authenticatie als een zorgaanbieder gebruik wil maken van het Landelijk SchakelPunt(LSP)om zorgdata uit te wisselen. Veel apothek- en huisartsinformatie-systemen maken gebruik van de UZI-pas om werkers in te laten loggen in het systeem. Dat maakt dit probleem zeer pregnant. Inmiddels zijn door de Tweede Kamerleden Verhoeven en Dijkstra vragen gesteld over deze materie.

Webbrowsers

De Kamerleden focussen niet zozeer op het niet meer kunnen werken van zorgaanbieders door het uitvallen van het inlogsysteem met de UZI-pas, maar meer op het feit dat een webbrowser, waaraan geen updates uitgevoerd worden, snel kwetsbaar wordt voor indringers. Er komen namelijk geen beveiligingsupdates voor de webbrowser meer binnen. Een indringende vraag van hen is dan ook of de inhoud van de brief door het ministerie van VWS gecoördineerd is met het Nationaal Cyber Security Centrum (NCSC)? Indien dat niet het geval is vragen de Kamerleden of de minister bereid is alsnog advies in

te winnen bij het NCSC. Op zich is dit een zeer relevante vraag, maar daarnaast zou er ook aan de minister gevraagd moeten worden hoe ze denkt om te gaan met de verantwoordelijkheid voor de goede werking van zorginformatiesystemen van zorgaanbieders(huisartsen en apotheken). Onder verantwoordelijkheid van het ministerie is een inlog-systematiek opgetuigd met de UZI-pas, die alleen maar kan werken als een keten van software(en hardware) naar behoren werkt. Daarbij blijken nu hulpprogramma's voor webbrowsers de zwakke schakels in de keten te zijn.

VZVZ

Het kan geen toeval zijn dat de Vereniging van Zorgaanbieders Voor Zorgcommunicatie(VZVZ) op het zorgverleners- en het ICT-leveranciersdeel van haar website net 24 uur voordat het UZI-register haar dringende email deed uitgaan een onschuldig lijkend artikel publiceerde, genaamd: “Werken in de LSP-keten”. Daar zal wel enige overleg kort ervoor met het ministerie(UZI-register) als initiatiefnemer aan vooraf zijn gegaan. Wel heel toevallig gaat het artikel over storingen in de LSP-keten, waarbij een paar mogelijkheden werden genoemd met als laatste het geval dat de UZI-pas niet goed werkt. De zorgverlener kan dan klikken op een link naar een document genaamd “Storingen in het LSP-Incidentmanagement”. De inhoud van dit zeer recent gemaakte stuk komt het erop neer dat de op het LSP-aangesloten zorgaanbieder vooral de helpdesk van de eigen ICT-leverancier moet bellen. Fijntjes wordt gewezen op het Convenant gebruik landelijke infrastructuur 2016-2020 waar de rollen van alle deelnemers in beschreven staan. Mocht het totaal onduidelijk zijn waar een storing in de LSP-werking vandaan komt dan ziet VZVZ nog wel een faciliterende taak voor haar eigen helpdesk.

Pers

Inmiddels hebben diverse media op het internet dit probleem met de UZI-pas opgepikt. Meerdere websites uit de ICT- en

beveiligingsbranche brengen het bericht over de email van het UZI-register aan de pashouders. Op de website www.huisartvandaag.nl stond in een reactie op het eerdere artikel over dit onderwerp van mijn hand (dat ook daar verscheen), dat een huisarts op 25 september al meldde dat een update van Windows 10 bleef hangen op de software van Safe Sign(UZI-pas software). De waarschuwing verscheen bij hem dat installeren van de update de software van de UZI-pas onbruikbaar maakte. Het is net geen oktober. Over een paar dagen gaan we zien hoe groot het probleem wordt.

Wordt uiteraard vervolgd. Morgen is het 1 oktober.

W.J. Jongejan

UZI-pas-problemen door stoppen Java en ActiveX-ondersteuning webbrowsers



Vandaag (21-09) stuurt het UZI-register aan de klanten van het UZI-register een bericht per email over het mogelijk niet goed meer werken van de UZI-pas vanaf oktober 2016. Dat komt volgens het afdelingshoofd UZI-register, Esther Dekkers, omdat

leveranciers van webbrowsers, zoals de Internet Explorer of Google Chrome, vanaf oktober een tweetal externe onderdelen, namelijk Java en ActiveX, uit de browsers laten verdwijnen. De UZI-pas-lezer maakt gebruik van bepaalde webbrowser-onderdelen voor identificatie, authenticatie en het plaatsen van digitale handtekeningen op medisch gerelateerde documenten. Het is daardoor weer eens duidelijk hoe kwetsbaar het UZI-pas-systeem is voor mutaties in externe software. De UZI-pas maakt gebruik van een hele keten van softwaretoepassingen, waarbij een kink in de kabel bij één onderdeel het hele kaartgebruik kan stilleggen. Dat heeft uitermate grote consequenties, omdat de moderne huisarts-/zorgsystemen vaak gebruik maken de UZI-pas voor het inloggen. Een niet werkende UZI-pas betekent dan niet kunnen inloggen in het eigen zorgsysteem. Ook de medische datacommunicatie via het Landelijk SchakelPunt(LSP) is afhankelijk van het gebruik van de pas. Zonder inlog met de UZI-pas is er geen dataverkeer via het LSP mogelijk.

Java en ActiveX

De UZI-pas-lezer maakt in veel gevallen gebruik van bepaalde webbrowser-onderdelen. Java en Active X zijn er twee van. Beide onderdelen worden niet door de webbrowser-leverancier(Microsoft, Google etc) zelf gemaakt, maar zijn softwareprogramma's die als applicaties in de browser geïnstalleerd kunnen worden. Het doel daarbij is om bepaalde andere software in de browser te kunnen inladen en te laten draaien. Omdat de browser-leveranciers deze onderdelen vanaf oktober 2016 niet meer ondersteunen loopt de werking van de UZI-pas en daardoor de praktijkvoering nu gevaar.

Zeer kort, negen dagen, voor het begin van de maand oktober wordt nu gewaarschuwd om niets te veranderen aan de huidige browser-configuratie en te wachten tot een oplossing beschikbaar is. Het houdt bijvoorbeeld in dat als u in uw scherm een melding krijgt dat u de Java- of ActiveX- software moet updaten, u geen update daarvan meer installeert. Overleg

met uw eigen softwareleverancier voor de praktijksoftware lijkt me uitermate zinvol. Al was het maar om in gezamenlijkheid te zien of er niet ingesteld is dat de updates voor de nu gewraakte software automatisch plaatsvindt.

Kwetsbaarheid

Al eerder was duidelijk hoe kwetsbaar de softwareketen is rond de UZI-pas. Zo was een update van Windows 10 Enterprise in december 2015 verantwoordelijk voor het uitvallen van de werking van de UZI-pas. Pas na een nieuwe update van deze versie van Windows 10 was het probleem opgelost. De cascade van aan elkaar gekoppelde software en de afhankelijkheid van leveranciers ervan maakt het geheel zeer kwetsbaar. Andermaal blijkt dit nu weer. Het is een kwestie van wachten voor weer een voorbeeld hiervan voorbij komt. Het nare is dat de praktijkvoering van veel zorgaanbieders inmiddels afhankelijk is van de goede werking van de UZI-pas. Men zou er goed aan doen de afhankelijkheid van externe software voor het pasgebruik te minimaliseren en liefst tot nul terug te brengen.

W.J. Jongejan