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 apotheek- 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