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.