Bizar conflict LUMC-Chipsoft toont wurggreep door zorg-ICT-leverancier

Op de website van het online magazine Zorgvisie stond op 25 september 2018 een opmerkelijk artikel: "LUMC beklaagt zich bij Inspectie over Chipsoft" . Daarin vertelt de bestuursvoorzitter, Willy Spaan, van het Leids Universitair Medisch Centrum(LUMC) over de klacht die door het bestuur ingediend is bij de Inspectie Gezondheidszorg en Jeugd(IGJ). Die gaat over een in de ogen van het LUMC onveilige update van het ziekenhuisinformatiesysteem(ZIS) van Chipsoft. Volgens het LUMC maakt Chipsoft gebruik van een dominante marktpositie om een update af te dwingen. Die leidt in de ogen van de veiligheidsexperts en specialisten van het LUMC tot onveilige zorg. Het bestuur vindt dit onacceptabel. Het LUMC stelt dat het ministerie van VWS en de IGJ hun verantwoordelijkheid moeten nemen. De discussie met de IGJ loopt nog steeds en heeft blijkbaar nog geen definitieve stellingname van de IGJ opgeleverd. Het is een probleem dat eigenlijk alle ziekenhuizen met Chipsoft als ZIS raakt. Uit het artikel blijkt dat andere ziekenhuizen schoorvoetend overstag zijn gegaan, maar dat het LUMC de poot stijf hield. Wel ging het LUMC onder tijdsdruk akkoord met een aangepaste update. Dit roept toch wel veel vragen op over de veiligheid van zorg-ICT-systemen, in het bijzonder die in ziekenhuizen en de druk die een leverancier blijkbaar kan uitoefenen.

Probleem

Blijkens het Zorgvisie-artikel dateert het conflict vanaf 2017. Chipsoft heeft laten weten thans in 2018 haar oude software van 2017 niet meer te ondersteunen. Ze kwam met de nu betwiste software- update. Het ZIS Chipsoft verzorgt niet alleen het vastleggen en in het ziekenhuis transporteren van data maar ook de koppeling van medische onderzoeksystemen in het ziekenhuis aan het ZIS. Daarbij doel ik op laboratoriumcomputers, computers die gekoppeld zijn aan beeldvormende appratuur, zoals MRI-, CT-scan etc. Die hebben vaak ook hun eigen besturingssysteem en dienen ook de laatste updates daarvan te hebben, die dan ook dienen samen te werken met het ziekenhuis-brede ZIS. Mogelijk zit in die koppeling de grootste bottleneck.

Geen bewerkersovereenkomst

Waarschijnlijkheid speelt daarnaast ook een rol dat CHIPSOFT als leverancier weigert bewerkersovereenkomsten te tekenen. Dat is in januari 2018 al door Mark van Houdenhoven CEO van de Maartenskliniek in Nijmegen aangekaart in het magazine Medisch Contact. Ook die deed een oproep aan het ministerie van VWS om in te grijpen. Chipsoft weigert namelijk een bewerkersovereenkomst te tekenen. Voor bedrijven die programma's leveren waarin data worden verwerkt geldt een namelijk een bewerkersovereenkomst waarin is vastgelegd hoe de bewerker met de persoonsgegevens moet omgaan. Dataverwerkers zijn bijvoorbeeld websitebouwers, ontwikkelaars van laboratoriumsystemen, leveranciers van personeelsadministratiesystemen, maar ook leveranciers van elektronische patiënten dossiers zoals Chipsoft. Dit is dan wel geen softwareupdate-probleem, maar is geen goede zaak in de relatie klant-leverancier.

Wurggreep

Het probleem maakt duidelijk dat in een markt waar eigenlijk maar twee grote ZIS-sen actief zijn, Chipsoft en EPIC, er

naast een “vendor lockin”(onmogelijkheid om makkelijk van andere leverancier te wisselen) ook zonder plan om van ZIS te veranderen een enorme afhankelijkheid van de leverancier bestaat. Uit eigen ervaring als lid van de raad van advies van een gebruikersvereniging van een huisartsinformatiesysteem(HIS) weet ik dat een leverancier soms een heel ander ontwikkelingspad voor ogen heeft dan de gebruikers(vereniging).

Onveilige ZIS-sen

Zoals in de eerste alinea al gezegd zijn andere ziekenhuizen dan het LUMC met tegenzin akkoord gegaan met een update die veiligheidsexperts en specialisten binnen het LUMC vinden leiden tot onveilige zorg. De LUMC-bestuursvoorzitter Willy Spaan, zegt ook dat de andere ziekenhuizen het met het LUMC eens waren. Blijkbaar is de schaalgrootte van het LUMC de enige machtsfactor geweest die het mogelijk heeft gemaakt een tussen-release van de software af te dwingen. Op zich is dat al triest. Heel triest is het om te constateren dat er nu blijkbaar tientallen ziekenhuizen met onveilige CHIPSOFT-software werken, omdat zij hetzij per ziekenhuis, hetzij collectief juridisch gezien geen brede borst hebben kunnen of willen maken richting CHIPSOFT. **Het kan en mag nooit zo zijn dat de onmogelijkheid van klanten om een vuist te maken richting hun leverancier leidt tot onveilige zorg.**

ACM?

Het bestuur van het LUMC heeft zich nu gewend tot de IGJ en daarmee ook tot het ministerie van VWS waaronder de IGJ ressorteert. Het is daarnaast de vraag of de beschreven problematiek ook niet het gevolg is van een te machtige marktpositie van de twee ZIS-sen, Chipsoft en EPIC. Daarmee komen we dan automatisch uit bij een eventuele mede-beoordeling van deze kwestie door de Autoriteit Consument en Markt(ACM). Het is te hopen dat de IGJ uit praktische overwegingen de ACM ingelicht heeft over het onderzoek dat het

LUMC-bestuur de IGJ vroeg te doen.

Bizar

Het hierboven beschreven probleem is eigenlijk een tamelijk bizarre situatie. Ik mag aannemen dat CHIPSOFT geen onveilige software wil leveren en dat het LUMC op zich geen enkel belang erbij heeft om iets nodeloos op de spits te drijven. Het is dan ook tamelijk bizar dat betrokkenen niet tot een onderling vergelijk konden komen en de situatie geëscaleerd is tot wat er nu speelt.

Triest is het om te constateren dat blijkbaar alleen een grote omvang van een organisatie die ook één van de grootste spelers binnen de universitaire medische wereld is, een bepalende machtsfactor is om in ieder geval een tussen-release van software te bewerkstelligen.

Helemaal triest is dat kleinere ziekenhuizen door akkoord te gaan met de 2018 release van de Chipsoft-software nu opgescheept zitten met software die binnen het LUMC als onveilig wordt beschouwd.

W.J. Jongejan, 27 september 2018

Aanvulling 4 oktober 2018: Op Twitter doet Marc van der Gracht @MarcGr8 de volgende suggestie over de aard van het probleem: Het artikel lijkt te suggereren dat zorgaanbieders met wel geüpdatete EPD een veiligheidsrisico zouden lopen. Ik denk dat dit risico enkel is voor de oude EZIS-dossiers die niet meer op veiligheid gemonitord worden, net als destijds met systemen die nog op Windows XP draaiden.