Hoogleraar informatiebeveiliging acht opzet LSP achterhaald en onveilig

Op 5 april j.l. heeft de vaste Eerste Kamercommissie voor VWS een twee uur durend gesprek gevoerd met deskundigen over cliëntenrechten bij elektronische verwerking van gegevens. Het ging over de kansen en risico's van de invoering van het wetsvoorstel 33509. Dit wetsvoorstel poogt de elektronische medische datacommunicatie een wettelijk fundament te geven. Het lijkt te gaan om alle vormen van die datacommunicatie, maar is volledig toegesneden op het gebruik van het Landelijk SchakelPunt(LSP). De inbreng van professor Eric Verheul, hoogleraar bij de Digital Security Group van de Radboud Universiteit van Nijmegen, was uitermate helder. Hij stelde in zijn betoog, dat de opzet van het LSP thans volledig achterhaald is. De huidige opzet beschouwt hij als kwetsbaar. De kern van het systeem acht hij onwenselijk en technisch niet noodzakelijk. Hij is niet zomaar iemand die dit zegt, maar een wiskundige met veel kennis van zaken betreffende cryptografie en veiligheidsmanagement op ICT-gebied.

Verslag

Deze week werd op de website van de Eerste Kamer het verslag van het deskundigengesprek gepubliceerd. Op pagina 18 en 19

staat de bijdrage van professor Verheul. Bij het LSP maakt binnen de centrale computer gebruik van een verwijsindex waarin bijgehouden waar van een bepaalde burger(specifiek burgerservicenummer) medische gegevens zijn vastgelegd en opvraagbaar zijn. Hij zegt daarover:

“Dat is eigenlijk heel grote tabel in een centraal systeem. Je kunt het zien als een grote matrix, waarbij op de rijen de bsn-nummers van de gebruikers staan. De wet voorziet erin dat er toestemming wordt gegeven voor het gebruik van het bsn. In de kolommen staan de zorgaanbieders. Je kunt je voorstellen dat waar beide elkaar kruisen, staat: deze man of vrouw is patiënt bij deze zorgaanbieder. Zo’n verwijsindex wordt eigenlijk impliciet genoemd in het wetsvoorstel. Dat is een heel gevoelige tabel, die onwenselijk en technisch gezien niet noodzakelijk is. Dat is het belangrijkste punt dat ik wil maken. In eerdere besprekingen van landelijke schakelpunten is al naar voren gekomen waarom het onwenselijk is. Als zo’n tabel in verkeerde handen valt, is plots duidelijk wie waar patiënt is. Het kan ook om een hiv-kliniek of een ggz-instelling gaan. Daarom wil je een centraal systeem met zo’n verwijsindex vermijden. Het is een heel grote tabel die heel lastig te beveiligen is. Het is technisch gezien niet noodzakelijk en dat biedt een perspectief dat in het verleden niet echt is besproken of bekeken.”

Anders

Hij geeft ook aan dat het anders kan:

“In 2014 hebben we allerlei cryptografische technieken ontwikkeld om de privacy binnen zo’n eID-stelsel te beschermen. De technieken die in 2014 zijn ontwikkeld, zou je relatief gemakkelijk kunnen toepassen in verwijsindexen die volledig gepseudonimiseerd zijn. De functionaliteit van de systemen van VZVZ en de gespecificeerde toestemming kun je daarin regelen, maar je houdt wel een systeem over dat veel cleaner is, omdat er geen persoonsgegevens maar pseudoniemen

in worden verwerkt.”

Zijn opmerkingen laten niets aan duidelijkheid te wensen over.

Niet van deze tijd

Al enige tijd terug werd duidelijk dat informatie die via het LSP getransporteerd wordt, korte tijd zich onversleuteld in de centrale computer bevindt. Bij alle gelegenheden waarbij kritiek op die manier van werken wordt geuit, bestrijdt VZVZ altijd dat dit een veiligheidsissue is. Professor Verheul stelt hierover:

“Die gegevens worden versleuteld verstuurd naar het LSP, zeg maar de hub, de centrale spil. Ze worden daar ontsleuteld en vervolgens opnieuw versleuteld naar de opvragende zorgaanbieder verstuurd. Dat is een manier van werken die tien jaar geleden, toen dit soort systemen werd ontwikkeld, misschien nog wel logisch was, maar op dit moment is het niet meer gebruikelijk dat gegevens eventjes in the clear, onversleuteld, in zo’n centraal systeem staan. Met het eID kun je met een bankmiddel, bijvoorbeeld een bankpas van de ING, inloggen bij de Belastingdienst. Uiteindelijk krijgt dan de Belastingdienst het bsn van de gebruiker, maar dat bsn staat op geen enkel moment eventjes in plain text op de systemen van de ING. Die oude manier van werken, waarbij die versleuteling even ongedaan wordt gemaakt op een centrale plek, is niet meer van deze tijd”

Gehakt

Het moge duidelijk zijn dat professor Verheul met deze uitspraken gehakt maakt van de huidige opzet van het LSP. Zowel de opzet van de centrale verwijsindex als de ontsleuteling van data, die de centrale computer passeren, acht hij niet meer van deze tijd. Het zijn waarschuwende woorden uit onverdachte hoek. Het wordt tijd dat de politiek die ter harte neemt, maar ook dat de zorgkoepels die nu nog in VZVZ meebeslissen over het LSP hun verantwoordelijkheid nemen.

W.J. Jongejan