High Tech Crime Unit van KLPD droeg bij aan Verizon-rapport over medische datalekken

Sinds 2008 brengt het Amerikaanse bedrijf Verizon jaarlijks een rapport uit over datalekken, waarbij zo wijd mogelijk over de wereld gekeken wordt. Dit jaar werd voor het eerst apart gerapporteerd over data-inbreuken(o.a. data-diefstal) bij gezondheids(zorg)gegevens. Ronduit schrikwekkend is het beeld dat in die publicatie geschetst wordt. Namelijk, dat van 2009 tot nu bij elkaar opgeteld alle incidenten op dat gebied alleen al in de Verenigde Staten(VS) een aantal mensen betreft, dat zo groot is als de helft van de bevolking van de VS (pagina 29). Data-inbreuken bij medische gegevens trekken een sterke wissel op de openheid die de patiënt normaliter betracht bij het consulteren van een arts. De Nationale High Tech Crime Unit(NHTCU) van het Korps Landelijke Politiediensten(KLPD) draagt sinds 2011 bij aan de jaarlijkse rapporten van Verison.

Verison

Eén van de grootste telecom-bedrijven in de VS is Verison met ongeveer 177.300 man personeel in 2014. Vanaf 2008 is het bedrijf jaarlijks een rapport gaan uitgeven over data-inbreuken: het DataBreach Investigations Report(DBIR). In 2009 rapporteert het bedrijf andermaal op basis van eigen informatievergaring. In 2010 gaat de US Secret Service deelnemen. Deze dienst heeft een tweetal taken. Naast de

beveiliging van staatshoofd, diens vervanger en oud-presidenten heeft deze dienst de opdracht te waken over financiële misdaden als valsemunterij, bewaking van de "schatkist"en het onderzoeken van grootschalige fraude. In 2011 gaat als tweede externe deelnemer, als eerste buitenlandse organisatie, de Nationale High Tech Crime Unit(NHTCU) van het Korps Landelijk PolitieDiensten(KLPD) deelnemen. In de daaropvolgende jaren 2012, 2013, 2014 en 2015 neemt het aantal deelnemende internationale bedrijven, waaronder accountantskantoren als Deloitte en buitenlandse overheidsdiensten gestaag toe. Dit jaar verscheen een apart rapport over data-inbreuken gezondheids(zorg)gegevens: het Protected Helath Information Data breach Report(PHIDBR).

Definitie

Waar het rapport op hamert, is dat medische gegevens niet alleen in de zorgsector zijn opgeslagen, maar dat ogenschijnlijk niet-medische bedrijven toch gezondheidsgegevens op grote schaal opslaan en bewerken, die als vertrouwelijk te beschouwen zijn. Het gaat dan niet alleen om medische dossiers, maar ook om biometrische data(lengte, bloeddruk, vingerafdruk, stemregistraties etc etc.). Het kunnen ook biometrische gegevens zijn, die iemand op een app zet op zijn smartphone. Het zijn vaak gegevens die tot een persoon herleidbaar zijn. Ook gegevens die de financiële afwikkeling van medisch zorg betreffen vallen er onder, waaronder verzekeringsgegevens. Met kennis van die gegevens kan ook weer fraude gestart worden.

Veroorzakers datalekken

In het rapport is te lezen(pag.7) dat de helft van de Protected Health Information(PHI) data-inbreuken wordt veroorzaakt door externe actoren. Schrikbarend is dat het bij 7 procent gaat om inbreuken door "partners" en maar liefst 43 procent door eigen personeel. Het gaat daarbij niet alleen om kwaadwillende acties. Soms gaat het daarbij om het verliezen/

of gestolen worden van een laptop met PHI-informatie, maar een deel van de datalekken door eigen personeel zijn beslist kwaadwillend van opzet.

Consequenties

De datalekken met medische informatie kunnen verregaande consequenties hebben ten aanzien van de wijze hoe een patiënt aankijkt tegen de wijze waarop zijn zorgverleners omgaan met de vertrouwelijkheid van die data. Er zijn studies die laten zien dat patiënten minder geneigd zijn vertrouwelijke informatie te delen met hun behandelaar als men weet dat de vertrouwelijkheid verbroken kan worden door data-inbreuken en data-diefstal. Dat heeft grote nadelen voor de patiënt in de eerste plaats. Ook is het voor te stellen, dat in het geval van een besmettelijke ziekte of andere ziekte, die grote gevolgen voor de bevolking in zijn geheel heeft, een tijdige diagnose zeer wenselijk is.

Waar zijn de datalekken?

Het rapport gaat ook in op de locaties waar de datalekkage plaats vond(pag.15, figuur 8.). Voor alle soorten van PHI-dataverlies, van het verloren gaan van een laptop tot malware-installatie en hacken blijkt de bulk van de incidenten zich voor te doen bij ambulante gezondheidszorgvoorzieningen (poliklinieken, dokters- en tandartspraktijken). Deze constatering is zeker van belang voor Nederland waar de automatisering in de eerstelijns zorg 100 procent is. Ook in ziekenhuizen doen zich veel incidenten voor, maar minder dan erbuiten. In verpleeghuizen en sociale voorzieningen voor patiënten is het dataverlies zeer beperkt, maar niet afwezig.

Aanbevelingen

Gelukkig worden ook suggesties gedaan om medisch dataverlies zo veel als mogelijk te beperken. Idealiter dient elk verlies voorkomen en elke aanvaller afgeslagen te worden. Het treffen van meerdere, essentiële, niet per se samenhangende,

maatregelen wordt aanbevolen, omdat elke extra maatregel de veiligheid meer dan lineair doet toenemen. Diefstal of verlies van een laptop kan niet altijd voorkomen worden, maar als de data die daar op staan versleuteld zijn, maakt dat de beschikbaarheid van de data voor kwaadwillende lieden veel kleiner. Ook aanscherping van de toegangsregels voor medische datasystemen wordt aanbevolen. Bewustwording over de kans op dataverlies binnen de organisaties en bedrijven blijft van het grootste belang.

NHTCU

De Nationale High Tech Crime Unit(NHTCU) valt onder de Dienst Landelijke Recherche van het Korps Landelijk PolitieDiensten(KLPD). In 2012 verscheen een zeer uitgebreid verslag van waar men zich zo al mee bezig hield, wat het wettelijk kader is waar binnen men opereert en wat men als wenselijk ziet. De medewerking met Verison, als private onderneming, dateert van 2011. In het genoemde verslag uit 2012 van de NHTCU wordt dat ook gemotiveerd. Over 2013 verscheen in samenwerking met KPN en TNO ook een lijvig verslag over cybercrime. De dienst heeft iets meer dan 100 personeelsleden.

Tenslotte

Zoals eerder gemeld ging in 2010 de US Secret Service deelnemen aan de het DBIR-onderzoeken en rapportages van de firma Verizon. Het geeft een vreemd gevoel te lezen dat enerzijds die dienst zich blijkbaar met Verizon druk maakt om datalekkage, o.a. ten aanzien van medische data, terwijl anderzijds andere geheime diensten van de VS zich bezig houden met MEDINT(medical intelligence) om zoveel mogelijk informatie over tegenstanders, maar ook medestanders te verkrijgen. Recent wijdde ik hier een artikel aan.

W.J. Jongejan