323000 radiologiebeelden van 25000 Nederlanders op 4 systemen open en bloot

Diverse media meldden op 17 september 2019 dat radiologie-beelden makkelijk toegankelijk zijn voor derden via het internet. Het betreft een in Duitsland gestart onderzoek dat de Tagesschau van de Bayerischer Rundfunk en de Amerikaanse organisatie ProPublica naar publiceerden. Daarbij gaat het wereldwijd om 400 miljoen medische radiologische beelden van vele miljoenen mensen in minimaal 52 landen. In Nederland gaat het om 323000 radiologiebeelden van 25000 Nederlanders op 4 systemen. Voorwaar geen geringe aantallen. Het gaat om Röntgenfoto's, MRI- en CT scans en mammografieën . Het verbazingwekkende is dat het niet echt gaat om het hacken van systemen. Het gaat gewoon om het kunnen inkijken omdat de deur tot die data wagenwijd openstaat. Berichtgeving in Nederland(op de website van ICT&Health en Security.nl) tot nu toe vermelden niet om welke aantallen het in ons land gaat. Wat diepgaandere bestudering van de onderliggende publicatie levert die gegevens wel op.

Onderzoek

Het onderliggende onderzoek van de publicaties berust op werk van de Duitse cybersecurity-firma Greenbone Networks . Die ontdekte dat het probleem speelt in minstens 52 landen op elk continent. Dirk Schrader van Greenbone Networks deelde zijn ontdekking met de Bayerischer Rundfunk die het vervolgens met ProPublica deelde. Dat met de vraag om verder te onderzoeken wat de mate van blootstelling in de V.S. was. Schrader had 5 servers in Duitsland gevonden en 187 in de V.S. Uiteindelijk

gaat het om 5 miljoen patiënten in de V.S. en miljoenen op wereldschaal. **In Nederland blijkt het ook om een aanzienlijk aantal te gaan. 323000 beelden van 25000 patiënten op 4 servers.** Zie hiervoor de afbeelding op pagina7 van de link met het rapport van Greenbone. De 4 servers zijn die waarvan men het aantoonde. Er kunnen meer openstaan.

Hoe kan dat nu?

Resultaten van beeldvormende onderzoeken iin de zorg slaat men op in zogenaamde PACS-servers. PACS staat voor Picture Archiving and Communication System. Het protocol dat daarvoor gebruikt heet DICOM(Digital Imaging and Communications in Medicine). Het is een standaard uit 1985 die aangeeft hoe apparaten die medische afbeeldingen maken met elkaar communiceren en data delen. Het DICOM-protocol bepaalt hoe de data vanuit de onderzoeksapparaten op een opslag-server komen. Maar ook hoe een viewer de beelden weer zichtbaar kan maken. Veelal staan op de servers verouderde besturingssystemen. Wanneer de servers direct toegankelijk vanaf het internet zijn zonder Virtual Private network-verbinding(VPN) of firewall, of wanneer er geen veilig wachtwoord ingesteld is, kan men zonder veel moeite opgeslagen gegevens benaderen. Het was mogelijk de beelden te bekijken met een van het internet te downloaden viewer die de onversleutelde beelden kon tonen.

Analyse

De analyse van Greenbone Networks leverde dat honderden PACS-servers verbonden zijn met het internet zonder enige vorm van bescherming of firewall. Daarnaast vond men vanwege het gebruik van verouderde besturingssystemen en andere software 10.000 kwetsbaarheden, waarvan 2000 ernstig.

Niet alleen beelden

Het onderzoek laat ook zien dat het niet alleen om de beelden gaat, maar ook om:

- Voor- en achternaam van patiënt
- Geboortedatum
- Onderzoeksdatum
- Omvang van het onderzoek
- Type van beeldvormend onderzoek
- Arts verantwoordelijk voor de uitslag
- De zorginstelling
- Aantal van de beelden per onderzoek

Consequenties

Deze inzagemogelijkheid voor onbevoegden maar dat niet alleen de privacy geschonden is van de betrokken patíënten. Het opent de mogelijkheid om met de gegevens die naast de beelden naar buiten kunnen komen (verzekerings)fraude, chantage of andere malafide praktijken uit te voeren. Los daarvan is als de toegang tot de opslagservers zo makkelijk is ook manipulatie van opgeslagen beelden mogelijk. Dat onderzochten Greenbone/ Bayerischer Rundfunk en ProPublica niet. Greenbone stipt die mogelijkheid wel expliciet aan. Dat manipulatie mogelijk is en wat het betekent beschreef ik eerder op 19 april 2019.

Gevaren bij koppelingen

In Nederland heeft men het Twiin(eerst TWIN)-project opgezet om medisch beeldmateriaal vooral sneller, simpeler en betrouwbaar te delen. Als er tussen de opslagplaatsen van medisch beeldmateriaal nu zoals aangetoond met het Greenbone-onderzoek een paar fors rotte appelen zitten is het maar helemaal de vraag of de toegang en de veiligheid wel afdoende beschermd zijn. Ik vermoed dat met de nu beschikbaar gekomen binnen meerdere instituten/zorginstellingen flink wat huiswerk moet gaan verrichten. Het is onbestaanbaar dat

medische informatie zo makkelijk toegankelijk is voor niet betrokkenen.

W.J. Jongejan, 19 september 2019

Afbeelding van Pexels via Pixabay