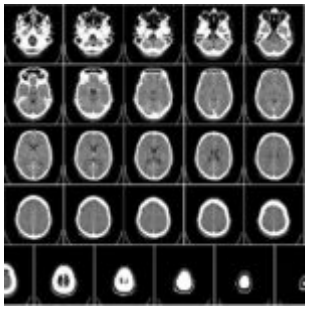
Wereldwijd nog steeds ruim 45 miljoen radiologiebeelden vrij toegankelijk



Op 19 september 2020 schreef ik op deze website dat zeer grote aantallen radiologiebeelden, waaronder MRI- en CT-scans, open en bloot op het internet te vinden waren. Het Duitse cybersecurity-bedrijf Greenbone Networks liet dat toen weten. Het ging om beeldmateriaal plus bijbehorende metadata(identificerende patiëntgegevens, naam aanvragende arts, instelling etc). Ook in Nederland en het Caraïbische deel ervan speelde dat. Het ging om beelden die volgens de DICOM-standaard digitaal opgeslagen zijn op NAS-servers(Network Attached Servers) zonder afdoende beveiliging. Een vervolgonderzoek twee maanden later liet zien dat er enige verbetering was. De openstaande Nederlandse servers verdwenen van de lijst. **Nu is het een Franse cybersecurity-firma, CybelAngel, die aandacht voor hetzelfde, nog steeds wereldwijd bestaande probleem vraagt.** CybelAngel publiceerde op 15 december 2020 een persbericht waarin men duidelijk maakt dat op basis van een zes maanden durend onderzoek veel onbeschermde radiologie-beelden op het internet vindbaar waren.

Omvang

Het bedrijf liet weten dat men 4,3 miljard IP-adressen scande en daarbij 45 miljoen unieke medische beelden vond op 2140 onbeschermde servers.. Het betreft servers in 67 landen, inclusief de Verenigde Staten, het Verenigd Koninkrijk, Frankrijk en Duitsland. Nederland staat niet in de persverklaring. Helaas is het volledige rapport niet te

downloaden, omdat het aanvraagformulier consequent elk mailadres als onjuist aanduidt. CybelAngel verkreeg de gegevens evenals Greenbone Networks in 2029 zonder gebruik hacking-tools. Gewoon door te zoeken naar servers met DICOM-data. DICOM is de de-facto standaard die men in de gezondheidszorg gebruikt om radiologisch beeldmateriaal te versturen en te ontvangen.

Metadata

Het bedrijf acht het ook uitermate zorgelijk dat de bij de beelden horende metadata soms een omvang hadden van 200 computerregels. Daarin gegevens die aangeven om wie het gaat met naam, adres, geboortedatum, lengte, gewicht , diagnose etc. Deze konden verkregen worden zonder login-naam en wachtwoord. Soms was het portaal waar de data op stonden toegankelijk zonder in de desbetreffende velden een gebruikersnaam of wachtwoord in te vullen

Besmetting met malware

Tijdens de zoektocht naar openstaande, onbeschermde servers, bleek ook dat ze vaak niet de eersten waren die buiten de gebruikers waarvoor de servers bedoeld waren, naar die data keken. Men ontdekte dat de een aantal van de DICOM-servers besmet waren met malware. Ze bevatten “malicious-scripts”. Ze stellen dan ook vast dat de infectie van onbeschermde servers vaak voorkomt. Vaak blijkt dat op basis van geautomatiseerde scripts te zijn, speciaal om Bitcoins of ander cybergeld te “minen”.

Adviezen

Het bedrijf geeft een aantal adviezen, waarbij de laatste uiteraard is om hen in te schakelen voor risicobeoordeling,

- **Determine if pandemic response exceeds your security policies:**Ad hoc NAS devices, file-sharing apps and

contractors may take data beyond your ability to enforce access controls

- **Ensure proper network segmentation of connected medical imaging equipment:**Minimize any exposure critical diagnostic equipment and supporting systems have to wider business or public networks
- **Conduct real-world audit of third-party partners:**Assess which parties may be unmanaged or not in compliance with required policies and protocols.
- **CybelAngel provides a complimentary, comprehensive 30-day data exposure assessment**healthcare and other organizations use to measure their risk and uncover priority issues.

Wakeup-call

Je zou zeggen dat na een waarschuwing als die van Greenbone Networks in 2019 dat er na een jaar wereldwijd veel veranderd zou zijn bij de opslag van radiologie-beelden. Niets is minder waar. Hardnekkig traag zijn systeembeheerders met het updaten van besturingssystemen van opslag-servers, waardoor deze systemen zeer kwetsbaar zijn. Cybersecurity blijkt vaak een ondergeschoven kind te zijn. Tot het grandioos verkeerd gaat, dan huilt iedereen tranen met tuiten. Dit onderzoek van CybelAngel moet een wake-up call zijn. Ook in Nederland.

W.J. Jongejan, 21 december 2020

Afbeelding van WikiImages via Pixabay