Kwaadwillend knoeien met medische digitale beelden realiteit

Het blijkt zeer wel mogelijk digitaal beeldmateriaal van bijv. een CT- of MRI-scanner met malware te manipuleren. Afwijkingen toevoegen, maar ook aangetoonde afwijkingen verwijderen bleek mogelijk. Op 3 april 2019 publiceerden wetenschappers van het Cyber Security Research Center behorend bij de Ben-Gurion University of the Negev in Beer-Sheeva(Israël) daarover. The Washington Post zette er op diezelfde dag een uitgebreid artikel op haar website. In Nederland zag ik er tot heden slechts één bericht op 4 april op de website Security.nl over. Wetenschappers lieten zien dat het mogelijk was beelden die onderschept waren tussen de computer van de beeldvormende apparatuur en de PACS-server. PACS staat voor Picture Archiving and Communication System. Het is een beeld-verwerkend systeem dat het mogelijk maakt om via computers de digitale beelden (met verslag) gemaakt op de afdeling radiologie van een ziekenhuis te verwerken, te archiveren en te verspreiden bij de aanvragende medisch specialisten.

Modus operandi

De onderzoekers produceerden software waarbij ze afwijkingen - zij namen daarvoor longkanker- op de CT-scan naar believen konden toevoegen, dan wel echt bestaande verwijderen. Ze

voerden een penetratieaanval uit in een ziekenhuis, dat op de hoogte was dat er een soort aanval kon komen. Ze maakten er een video over. Het was een zogenaamde een man-in-the-middle-aanval. Ze deden dat door een Raspberry Pi 3 Mode B computertje te gebruiken in combinatie met een USB-to-ethernet-adapter. Die kostten bij elkaar ongeveer 40 dollar. Een onderzoeker plaatste in 30 seconden de apparaatjes na insluiping in de avonduren bij de scanner in het netwerk. De signalen bestemd voor de PACS-server onderschepte men zo. Na modificatie van de data werden die met een vertraging van slechts enkele milliseconden doorgegeven aan de PACS-server.

Resultaten

Het bleek zeer goed mogelijk de radiologen die de beelden moesten beoordelen om de tuin te leiden. In bijna alle gevallen van toegevoegde tumoren(99%) en nauwelijks minder bij verwijderde(94%) hadden de radiologen het aan het verkeerde eind. Ook speciale artificial-intelligence-software die men gebruikt bij het helpen beoordelen van MRI- en CT-beelden ziet niet dat er gemanipuleerd is.

Authenticiteit / Integriteit

Het probleem is dat de authenticiteit van de beelden in het geding is. In de praktijktest met de interceptie bleek het ziekenhuis het encryptie-protocol(TLS v1.2), in gebruik bij het verzenden van data van scanner naar PACS-server, niet goed geïmplementeerd te hebben. Daardoor verzond het systeem “plain text”, d.w.z. onversleutelde informatie. Ook maakte men geen gebruik van een digitale ondertekening van het databericht waardoor het veranderd zijn van de informatie niet gedetecteerd kon worden. Zowel deugdelijke end-to-end-encryptie m als het aanbrengen van een digitale handtekening in de data kan veel ellende voorkomen.

Nachtmerrie

Het is natuurlijk de nachtmerrie van elke patiënt en arts, of dat nu de behandelaar is of de radioloog, dat beelden die gemaakt zijn met digitale beeldvormende apparatuur niet te vertrouwen zijn. De auteurs van het artikel zeggen zelf dat een aanvaller dit kan doen om een politieke leider of kandidaat te verwijderen, onderzoek te saboteren of vervalsen, een moord of terrorisme uit te voeren of gegevens voor losgeld te gijzelen. Dat is nogal boud gesteld, maar wel mogelijk. Het belangrijkste is echter het niet uit kunnen gaan van de integriteit en de authenticiteit van de beelden.

Zwakke plekken

Het is dan ook van groot belang dergelijke problemen te voorkomen door alert te zijn op mogelijke zwakke plekken in de keten. En die zijn er. Een information security officer van de Mayo Clinic in Minnesota stelde dat PACS-netwerken over het algemeen geen encryptie kennen. Ziekenhuizen gaan er volgens hem vaak onterecht van uit dat wat op hun interne netwerken gebeurt niet toegankelijk is voor de buitenwereld. Niets in minder waar.

Toename aanvallen

De laatste jaren is er in toenemende mate interesse van kwaadwilligen die d.m.v. hacken proberen medische informatie te verkrijgen of te beïnvloeden. Ik schreef op 25 april 2018 een artikel over de Orangeworm-hackersgroep die met het W32/Kwampir-virus de medische sector aanviel. Ook toen was duidelijk dat onvoldoende geupdate en beveiligde software en besturingssystemen dit soort aanvallen mede mogelijk maken.

Eerdere publicaties

Twee van de auteurs van het recente stuk, namelijk Tom Mahler en Yuval Elovici schreven in maart 2018 a ook een artikel met

de titel “Know your enemy, Characteristics of Cyber-Attacks on Medical Imaging Devices”. Ik schreef daar op 18 april 2018 en artikel, getiteld: ”Wat als de CT- of MI-scanner gekaapt is door malware” over.

Bij het gebruik van geavanceerde zorgICT-toepassingen dient men ook geavanceerd te blijven denken en state-of-the-art-beveiliging te gebruiken.

W.J. Jongejan, 10 april 2019