Wat als de CT- of MRI-scanner gekaapt is door malware?

In mei 2017 hebben we kunnen zien hoe het Wannacry-virus huishield bij de National Health Service(NHS) in het Verenigd Koninkrijk. Deze malware slaagde erin grote aantallen ICT-systemen van zorgaanbieders plat te leggen dan wel ernstig te verstoren. De National Audit Office bracht er verslag over uit op 24 oktober 2017. Onder de aangedane systemen waren ook MRI-scanners, die evenals CT-scanners, een uiterst belangrijke rol spelen bij onderzoek met beeldvormend technieken in ziekenhuizen. Deze apparaten hebben vaak een op Windows gebaseerd eigen besturingssysteem en zijn gekoppeld aan het ziekenhuisnetwerk.

Een onderzoeksgroep aan de Ben-Gurion University of the Negev, in Beer-Sheva(Israël) publiceerde in maart 2018 een artikel over dit onderwerp, genaamd: "Know your enemy: Characteristics of Cyber-Attacks on Medical Imaging Devices." In het artikel beschrijven de onderzoekers een uitgebreide risico analyse over de kwetsbaarheid van MRI- en CT-scanners, als Medical Imaging Devices(MID). Ze beschrijven een aantal kwetsbaarheden en potentiele doelen, waardoor met deze appraten niet meer gewerkt kan worden. Dat zou een ramp zijn, omdat MID's zeer intensief in de zorg gebruikt worden voor diagnose, behandeling en preventie van ziekten. In mijn bijdrage zal ik de inhoud van het artikel in het kort bespreken.

Grootste risico

Van de MID’s lopen de CT-scanners het grootste risico van slag te worden gebracht door malware. Dat heeft te maken met de centrale rol die deze apparaten spelen bij beeldvormend onderzoek in de acute zorg. Daarom focusten de onderzoekers zich na een beschrijving van de rol van de MID’s in de hedendaagse zorg en een beschrijving van de Wannacry-cyberaanval op de problemen die met CT-scanners kunnen ontstaan bij dat soort aanvallen.

Vier categorieën aanvallen

De onderzoekers beschrijven een viertal ernstige verstoringen van CT-systemen die zij zelf hebben kunnen uitproberen. Het gaat bij de aanvalsgevolgen om gevaar voor de patiënt die in het apparaat ligt, maar ook voor andere patiënten. Daarnaast kan ook de technische staat van een CT-scanner ernstig aangetast worden.

1. Een CT-scanner opereert op basis van een configuratie-bestand dat in de besturingscomputer opgeslagen is . Het zorgt voor een correcte werking van de scanner. Door het aanpassen van dat bestand kan de hele werking van de scanner gemodificeerd worden, bijv. de hoeveelheid straling die de röntgenapparatuur in de scanner afgeeft.
2. De MID’s hebben een flink aantal elektromotoren aan boord die instructies krijgen vanuit de computer met het specifieke besturingssysteem. Het ongeautoriseerd overnemen van de controle over deze motoren kan ongewenste bewegingen van het apparaat ten gevolge hebben. De patiënt in de scanner kan daar grote schade van ondervinden, maar ook de scanner zelf.
3. Uit de ruwe data die een CT-scanner tijdens een onderzoek produceert worden door een bij de scanner horend ICT-systeem de beelden gevormd en aan de betreffende patiënt gekoppeld. Na het maken van de beelden worden die volgens een specifiek protocol(DICOM=

Digital Imaging and Communications in Medicine) verder getransporteerd en opgeslagen. Een aanval op de in dit punt genoemde systemen kan er toe leiden dat het onderzoek bij een patiënt verstoord wordt en een tweede onderzoek met daardoor extra stralingsbelasting nodig is. Bij een meer diepgaan verstoring kan het scanresultaat veranderd zijn, waardoor het ook zeer moeilijk te zeggen is wat er fout is. Tenslotte kan met een nog gehaaidere aanval het scanresultaat aan een andere persoon gekoppeld worden.
4. Ook kan zogenaamde ransomware bestanden versleutelen, waarna een geldsom(evt in cryptocurrency) geëist kan worden om die weer ontsleuteld te krijgen.

Preventie

De onderzoekers stellen dat met cyberaanvallen op MID's steeds meer rekening moet worden gehouden en dat leveranciers van deze apparatuur en andere zorg-hard-/software voor een enorme uitdaging staan. Gebruikers dienen zich bewust te zijn van de risico's en het mechanisme achter de potentiële aanvallen moet begrijpen om ze te voorkomen. De Wannacry-cyberaanval kon zo uitgebreid toeslaan omdat veel software binnen de ziekenhuizen, ook de besturingssystemen van CT- en MRI-scanners onvoldoende geüpdatet waren. Sommige systemen draaiden nog onder Windows XP! Het probleem met de scanners is dat de ontwikkelingstijd van nieuwe scanners vaak lang duurt en dat een eenmaal in het begin gekozen besturingssysteem vaak niet zomaar overgezet kan worden naar een nieuw als het eerste door bijvoorbeeld Microsoft uitgefaseerd wordt. Het installeren van krachtige antivirus-software kan wel iets betekenen, maar is beslist niet afdoend in het geval van verouderde besturingssystemen. Toch blijft het van eminent belang om bestaande systemen continu van nieuwe patches te voorzien.

Oplossingsrichting

De auteurs stellen als extra oplossingsrichting een meer functionele voor. Zij stellen naast de eerder genoemde maatregelen voor om het dataverkeer van de besturende en data-verwerkende systemen met de scanner zelf continu te monitoren en met artificiële intelligentie(lerende systemen) te beoordelen. Daardoor kunnen afwijkingen van bestaande processen gedetecteerd worden en ingegrepen worden voor er iets misgaat.

Uitval van één MID-systeem door malware of andere vorm van hacken kan een heel ziekenhuissysteem platleggen. Maar omgekeerd geldt ook dat een gecompromitteerd ziekenhuis-informatiesysteem beeldvormende apparatuur volkomen plat kan leggen.

W.J. Jongejan