Meditsiini-IT nõrgad kohad lubavad häkkida eluliselt olulistesse seadmetesse

10 aastat tagasi - 08.04.2016 Autor: AM

Vanu Windows 95-ga masinaid võib meditsiinis veel palju kohata, sest nende ülesanne pole end Internetirünnakute eest kaitsta ja tihti on keeruline erialane tarkvara kunagi loodud just nende vanade operatsioonisüsteemide jaoks. Kõik töötab ja milleks vahetada? Kui aga kuskilt paotub netiligipääs, võib asi olla halb.

Kasperski Lab´i Globaalse Ohtude Uuringute ja Analüüsi Keskus (GReAT) viis läbi uuringu ühes erakliinikus, püüdes leida selle turvalisuse poolest nõrku kohti ja pakkuda vastumeetmeid. Meditsiiniseadmetes tuvastati turvaaugud, mis avasid küberkurjategijatele ligipääsu patsientide andmetele ning nende füüsilise seisundi infole.

Keerulised meditsiiniseadmed kujutavad endast täielikke installitud operatsioonisüsteemi ja rakendustega arvuteid. Arstid loodavad oma töös üsna suures osas ka arvutitele ning kogu info hoitakse digiformaadis. Paljud tervisekaitse tehnoloogiad on ka ühendatud Internetiga. Ehk siis pole midagi imelikku selles, kui haigla meditsiiniseadmed ja võrk juba ongi ka häkkerite sihtmärgiks.

Kõige värskemad näited sellistest juhtumitest on rünnakud USA ja Kanada haiglatele lunaraha nõudvate arvutiprogrammide abil.

Kliinikud hoiavad oma patsientide isikuandmeid ja samal ajal saavad kasutada väga kalleid, keerulisi ja raskesti asendatavaid seadmeid, mis teeb nendest potentsiaalselt atraktiivse eesmärgi väljapressimiseks ja andmete varastamiseks**.**

Meditsiiniorganisatsioonile tehtud edukas küberrünnak võib kaasa tuua selliseid tagajärgi:

- patsientide isikuandmete kuritahtlik kasutamine: teabe edasimüük kolmandatele pooltele või nõue, et kliinik tasuks lunaraha, et saada tagasi konfidentsiaalne teave patsientide kohta;
- analüüsitulemuste või patsientide diagnooside tahtlik võltsimine;
- meditsiiniseadmete kahjustamine võib tekitada nii füüsilist kahju patsientidele kui ka hiigelsuurt rahalist kahjumit kliinikule;
- negatiivne mõju kliiniku mainele.

Interneti ees on paljud seadmed kaitsetud

Kaspersky Lab’i ekspert hindas kõigepealt, kui palju meditsiiniseadmeid üle maailma on ühendatud Internetiga.

Esimene Internetiga ühendatud seadmete otsing käis läbi Shodani otsingusüsteemi ja näitas sadu seadmeid: välja ilmusid magnetresonantstomograafid, kardioloogia- ja radioaktiivsed meditsiiniaparaadid ning samuti muud kliiniku olulised seadmed. Kokkuvõte on murettekitav – mõned nendest masinatest töötavad siiani vanadel operatsiooniseadmetel - näiteks Windows XP parandamata turvaaukudega, aga mõned keerulised aparaadid kasutavad endiselt vaikimisi pandud salasõnu, mida on kerge kasutusjuhenditest leida.

Kasutades neid turvaauke, saavad kurjategijad kergelt ligipääsu kasutajaliidesele ja võivad mõjutada seda, kuidas seade töötab.

Kliiniku lokaalvõrgu sisse saab ka vaadata

Ülalkirjeldatud võimalus läbi vanade operatsioonisüsteemide ja vaikimisi paroolidega on üks viisidest, kuidas küberkurjategijad võivad saada ligipääsu kliiniku kriitilisele taristule. Aga kõige ilmsem ja loogilisem on rünnata lokaalvõrku. Uuringu käigus avastati turvaauk kliiniku WiFi-ühenduses. Tänu nõrgale sideprotokollile saadi ligipääs lokaalvõrgule.

Uurides kliiniku lokaalvõrku, avastas Kaspersky Lab’i ekspert mõned meditsiiniseadmed, mis tuvastati ka varem Shodani otsingusüsteemi kaudu. Aga seekord ei läinud vaja mingeid salasõnu, sest lokaalvõrk oli seadme jaoks nö kaitstud nii rakenduste kui meditsiiniseadmete kasutajate jaoks.

Meditsiiniseadmete rakenduses avastati ka korralikult suur turva-auk. Kasutajaliideses oli kasutatud käsutöötlusprogrammi, mis võimaldab küberkurjategijatele ligipääsu patsientide isikuandmetele, sealhulgas nende haigusloole ja meditsiinianalüüside andmetele ning samuti kodustele aadressidele ja muudeleisikuandmetele. Turvaaugu kaudu sai rikkuda seadme tööd.

„Kliinikud pole enam arstid ja meditsiiniseadmed, vaid ka infotehnoloogia ja -teenused. Kliiniku siseturvalisuse teenistuste töö tagab patsiendi andmete turvalisuse ja kliiniku seadmete töötamise. Kui kõne all on uued tehnoloogiad, tuleb käsitleda turvalisuse küsimusi teadusuurimus- ja katsekonstrueerimistööde esimeses staadiumis. Turvalisuse küsimusi võiksid aidata lahendada ka ettevõtted, mis tegelevad infoturbega infotehnoloogiaseadmete kasutamisel,“ ütles Sergei Ložkin, Kaspersky Lab’i juures töötava GReAT Keskuse antiviiruste vanemekspert.

Kaspersky Lab soovitab: mida teha kliinikute küberkaitseks?

• kasutage kindlaid salasõnu kõikide väliste ühenduspunktide kaitsmiseks;

• uuendage turvalisuse tagamise poliitikat IT-valdkonnas, parandused ja uuendused tuleb teha õigel ajal;

• kaitske meditsiiniseadmete rakendusi lokaalvõrgus tugevate salasõnade abil;

• kaitske taristut pahavara ja häkkerirünnakute eest turvalahenduste abil;

• tehke regulaarselt kriitilisest info varukoopiaid ja hoidke neid võrgust väljaspool

- Uudised
- Turvalisus