Smartphones in de zorg veilig ontsluiten op het netwerk

31 augustus 2017

Het aantal mobiele apparaten zal in de toekomst fors toenemen [1]. Vroeger had iedereen een vast bureautoestel, maar het beleid in zorginstellingen is nu vaak ‘mobiel tenzij’. Naast smartphones zijn dat ook tablets en draadloze handsets.
Een andere ontwikkeling is Internet of Things (IoT): alles is met alles verbonden. Vrijwel alle apparaten die tegenwoordig worden ontwikkeld, hebben een netwerkstekker. Denk bijvoorbeeld aan de koelkast, het koffiezetapparaat of camera’s. De verwachting is dat er in 2020 zo’n negen miljard IoT apparaten op het netwerk aangesloten zullen zijn. Dit brengt nieuwe risico’s met zich mee.

> Zodra IoT apparatuur is gecompromitteerd, kunnen deze aanvallen van binnenuit komen

Snepvangers: “Als je in het ziekenhuis komt, dan wordt het gastenwifi door iedereen gebruikt. Een verpleegster met haar privé smartphone, een bezoeker met zijn laptop of een patiënt met zijn tablet. Iedere gebruiker op het netwerk kan worden van binnenuit kunnen komen. Het is dus belangrijk om de beveiliging te verplaatsen richting de gebruikers. Die zitten immers al op het netwerk, met of zonder toegang tot kritische systemen en dossiers. Een firewall naar internet is niet afdoende.”

Combinatie IoT en toename mobiele apparaten

Door de combinatie van IoT en de toename van het aantal mobiele apparaten op het netwerk

wordt het risico groter dat organisaties van binnenuit worden aangevallen. Snepvangers geeft aan: “Bij de ontwikkeling van deze nieuwe apparaten staat security niet voorop. Veel apparaten worden gemaakt in een opensource community: iedereen kan er aan meewerken. Dit komt de usability sterk ten goede, maar er is nauwelijks aandacht voor security.” Nieuwe apps en devices ontsluiten gevoelige patiëntgegevens, maar bieden tegelijk hackers en virussen toegang tot diezelfde bronnen. Met alle gevolgen van dien.’