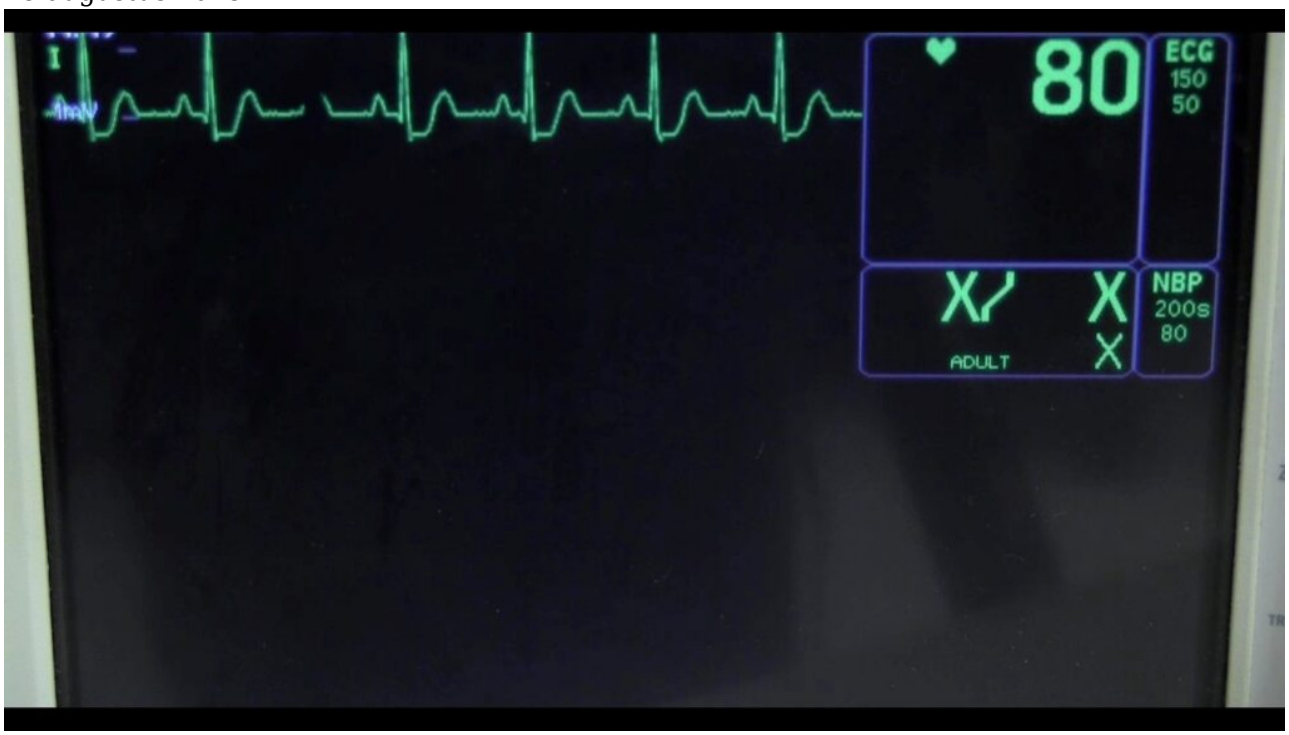
Hacken bewakingsstations kan tot foute besluiten arts leiden

15 augustus 2018



Tijdens het onderzoek hebben de onderzoekers de patiëntenmonitor, die altijd de ware gegevens liet zien, niet gewijzigd. Wel is volgens hen bewezen dat de impact van een aanval beduidend kan zijn. Een dergelijke aanval kan ertoe leiden dat patiënten de verkeerde medicijnen krijgen, extra worden getest en langer in het ziekenhuis liggen – wat allemaal onnodige kosten met zich mee kan brengen en zelfs levens in gevaar kan brengen.

Om de nagebootste gegevens geloofwaardig te maken, moet een aanvaller zich op hetzelfde netwerk bevinden als de apparaten en kennis hebben van het netwerkprotocol. Elke wijziging aan de patiëntgegevens zou voor medische professionals geloofwaardig moeten zijn om er enige impact op te hebben, aldus de onderzoekers van de Amerikaanse security-aanbieder.

Maatregelen tegen hacken

Zowel leveranciers van de medische systemen als medische faciliteiten kunnen maatregelen nemen om de dreiging van dit soort aanvallen drastisch te verminderen. Zo kunnen leveranciers netwerkverkeer tussen de apparaten coderen en authenticatie toevoegen. Deze twee stappen zouden de drempel voor dit soort aanvallen drastisch verhogen.

Leveranciers bevelen doorgaans ook aan dat medische apparatuur wordt gebruikt op een volledig geïsoleerd netwerk met zeer strikte netwerktoegangscontroles. Als zorgaanbieders zoals ziekenhuizen deze aanbevelingen volgen, hebben aanvallers fysieke toegang tot het netwerk nodig, wat de aanvalsmogelijkheden aanzienlijk helpt verminderen.

Medici vertrouwen op technologie

Met de explosie van groei in technologie en de invloed ervan op het leven van mensen, worden we er in toenemende mate afhankelijk van, benadrukken de onderzoekers. De zorg is geen uitzondering: medische professionals vertrouwen op technologie om hen te voorzien van accurate informatie en baseren levensveranderende beslissingen over deze gegevens. De dreiging van hacks en hun impact groeit echter ook, terwijl zorginstellingen volgens onderzoek van het Rathenau Instituut onvoldoende beveiligd zijn.

Om een geschikt doelwit te selecteren voor het onderzoek, is met een arts overlegd. Uit dit gesprek bleek hoe belangrijk de nauwkeurigheid van de vitale functies van een patiënt is voor medische professionals. “Gegevens over vitale functies zijn integraal onderdeel van klinische besluitvorming”, stelt Dr. Shaun Nordeck. Patiëntenmonitoren en aanverwante systemen zijn essentiële componenten die medische professionals voorzien van informatie die ze nodig hebben om beslissingen te nemen.

Meerdere patiënten observeren

De meeste patiëntbewakingssystemen omvatten ten minste twee basiscomponenten: een bedmonitor en een centraal meldpunt. Deze apparaten zijn bekabeld of draadloos verbonden via TCP / IP. Het centrale meldpunt verzamelt vitale functies van meerdere monitoren, zodat een enkele medische professional meerdere patiënten kan observeren.

Met de hulp van eBay kochten de onderzoekers zowel een patiëntmonitor als een compatibel centraal meldpunt tegen een redelijke prijs. De patiëntmonitor bewaakte hartslag, zuurstofniveau en bloeddruk. Het heeft zowel bedrade als draadloze netwerken en bleek patiëntinformatie op te slaan. Het centrale controlestation draaide Windows XP Embedded, met twee Ethernet-poorten. Beide apparaten werden geproduceerd rond 2004; verschillende lokale ziekenhuizen hebben bevestigd dat deze modellen nog steeds in gebruik zijn.

Geloofwaardige veranderingen niet gecontroleerd

Hoewel de monitor in de kamer van de patiënt niet direct wordt beïnvloed, is realtime modificatie van groot belang omdat medische professionals de centrale bewakingsstations gebruiken om cruciale beslissingen te nemen over een groot aantal patiënten, in plaats van elke kamer afzonderlijk te bezoeken. Zolang de veranderingen geloofwaardig zijn, zullen ze niet altijd worden geverifieerd, zo blijkt.

Dr. Nordeck vertelt over de impact van de tijdens het onderzoek uitgevoerde aanval: “Fictieve hartritmes kunnen leiden tot langere ziekenhuisopname, extra testen en bijwerkingen van medicijnen die foutief zijn voorgeschreven om het hartritme te beheersen, of stolsels te voorkomen. Ook kan een ziekenhuis uiteindelijk last krijgen van onnodig gebruik van producten en diensten.”

Beveiligingsproblemen

Een van de doelen van het McAfee Advanced Threat Research-team is het identificeren en belichten van een breed scala aan bedreigingen in het complexe en voortdurend veranderende landschap van vandaag. Sommige al door hacks getroffen medische apparaten, zoals pacemakers en insulinepompen, zijn al onderzocht op beveiligingsproblemen. De resultaten

van het huidige onderzoek zijn gedeeld met de leverancier wiens producten zijn getest.

Openingsmanifestatie van de e-healthweek 2019
Meer weten over hoe de zorg haar toekomst implementeert? Wilt u deze mede inrichten, er invloed op uitoefenen en/of de relevante innovaties ervaren? Bezoek dan op 21 januari 2019 de jaarlijkse ICT&health Openingsmanifestatie van de e-healthweek. Entreekaarten zijn na registratie gratis maar nu al beperkt beschikbaar! Dus wacht niet en meld u snel aan!