Fax in zorg kwetsbaar voor hackers

21 augustus 2018

De fax wordt nog altijd veelvuldig gebruikt in de zorgsector, in de informatie-uitwisseling tussen bijvoorbeeld (huis)artsen en apotheken. Uit het onderzoek van Check Point blijkt volgens Z-Cert echter dat er kwetsbaarheden zitten in de fax-functionaliteit van HP Inkjet printers. Het is onbekend in hoeverre dit ook geldt voor andere printers.

Fax verbonden met interne netwerk

De fax is verbonden met het telefoonnetwerk en het interne netwerk. Hackers kunnen via de telefoonlijn toegang krijgen tot het interne netwerk. Ze krijgen zo toegang tot de gegevens op dit netwerk.

De medische sector is interessant voor hackers vanwege de grote hoeveelheid persoons- en medische gegevens die opgeslagen liggen in bijvoorbeeld EPD's. Verder kunnen malware-aanvallen leiden tot besmetting met ransomware. Uit onderzoek van de NOS in 2017 bleek dat ziekenhuizen in Nederland hiervan regelmatig het slachtoffer zijn.

Z-CERT beveelt zorginstellingen die gebruikmaken van HP Inkjetprinters aan om de update te installeren die door HP beschikbaar is gesteld. Daarnaast is het verstandig het faxgebruik tot een minimum te beperken en modernere oplossingen te kiezen voor het uitwisselen van medische gegevens.

Fax-apparatuur nog dagelijks gebruikt

De onderzoekers die de kwetsbaarheden in de OfficeJet Printers ontdekten stelden dat ook andere printers/faxen en mogelijk ook fax-to-email toepassingen kwetsbaar kunnen zijn. Hier is echter nog geen aanvullende informatie voor gegeven, maar Z-CERT stelt aan de hand van eigen onderzoek dat dergelijke faxapparatuur dagelijks gebruikt wordt binnen de zorgsector.

Volgens de organisatie kan op basis van de huidige geldende normen op het gebied van informatiebeveiliging en privacy worden gesteld dat de fax niet langer geschikt is voor het uitwisselen van medische gegevens. Het is verstandig om op meer moderne digitale communicatie zoals mail of digitale uitwisseling via platforms zoals het LSP over te gaan.

Over Z-Cert

Z(org)-CERT is een Computer Emergency Response Team van specialisten dat nauw samenwerkt met het Nationaal Cyber Security Center (NCSC). Z-CERT heeft een tweeledige functie: de experts bieden hulp bij security-incidenten, waaronder ransomware en hackpogingen, en deze helpen preventief door dagelijkse monitoring van internet op mogelijke risico's en dreigingen. Daarnaast geven zij een waarschuwing of advies op het moment dat zich een dreiging voordoet die impact kan hebben op de organisatie.

De oprichting van Z-Cert werd in 2016 aangekondigd. Begin 2018 ging het security-team officieel van start. Afgelopen voorjaar begon Z-Cert met een pilot om te onderzoeken hoe het zorginstellingen van dienst kan zijn. De pilot gaat dit jaar van start in samenwerking met met de langdurige zorg (ActiZ), gehandicaptenzorg (VGN) en zelfstandige klinieken (ZKN).

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!