Groei in gebruik wearables vergroot risico van stelen data

15 februari 2022

Kaspersky schat dat bijna de helft van de Nederlanders inmiddels zelf lichaamsfuncties meet via een wearable om zo zijn of haar gezondheid in de gaten te houden. Vooral sporthorloges en stappentellers – al dan niet als app op de smartphone – groeien al een aantal jaren in populariteit. Die wearables zijn echter vrij eenvoudig te hacken.

Wearables erg kwetsbaar

Zo ontdekte Kaspersky recent ruim 30 kwetsbaarheden in het meest gebruikte protocol voor gegevensoverdracht van wearable devices die worden gebruikt voor patiëntmonitoring op afstand. Van de 33 kwetsbaarheden waren er 18 kritiek in 2021. Het aantal kwetsbaarheden groeit, want dit zijn er 10 meer dan in het jaar ervoor. Veel van deze kwetsbaarheden blijven ongepatcht, terwijl sommige ervan het cybercriminelen mogelijk maken om gegevens te onderscheppen die vanaf wearables worden verzonden.

Ook de versnelde digitalisering van processen in de zorgsector, onder meer wegens noodgedwongen zorg of afstand en overbelasting van zorgpersoneel, brengt risico's met zich mee. Met wearable devices zoals smart watches, smart bands en slimme pleisters kunnen instellingen in cure en care continu of met tussenpozen de gezondheidsindicatoren van een patiënt/cliënt volgen, zoals hartactiviteit en bloeddruk.

Encryptie zelden gebruikt

Het MQTT-protocol is volgens Kaspersky het meest gebruikte protocol voor het uitwisselen van gegevens van wearable devices en sensoren – omdat het gemakkelijk en efficiënt is. Daarom wordt het gebruikt in bijna elk smart device, niet alleen in wearables. Bij MQTT is authenticatie echter optioneel en wordt er zelden encryptie gebruikt.

Dit maakt MQTT zeer gevoelig voor 'man in the middle'-aanvallen. Hierbij plaatsen cybercriminelen zich tussen twee communicerende partijen, zoals een patiënt en behandelaar. Gegevens die online worden uitgewisseld, kunnen dan gestolen worden. In het geval van wearables kan die informatie zeer gevoelige medische gegevens, persoonlijke informatie of zelfs de bewegingen van een persoon omvatten.

Sinds 2014 zijn er 90 kwetsbaarheden in MQTT ontdekt, waaronder kritieke, waarvan er veel tot op de dag van vandaag nog niet gepatcht zijn. Door al deze kwetsbaarheden lopen patiënten het risico dat hun gegevens worden gestolen. Bovendien kunnen wearables zowel gezondheidsgegevens als locatie en bewegingen bijhouden. Dit opent niet alleen de mogelijkheid van het stelen van gegevens, maar ook van potentieel stalken.

Sterke groei e-healthmarkt

De pandemie heeft geleid tot een sterke groei van de e-healthmarkt. Dat betreft volgens Tim de Groot, Territory Manager, Benelux & Nordics bij Kaspersky niet alleen beeldbellen, maar een hele reeks complexe, snel ontwikkelende technologieën en producten. Daaronder gespecialiseerde toepassingen, draagbare apparaten, implanteerbare sensoren en cloudgebaseerde databases.

"Veel ziekenhuizen maken echter nog steeds gebruik van niet-geteste diensten van derden om patiëntgegevens op te slaan, en er zijn nog steeds kwetsbaarheden in wearable devices en sensoren voor de gezondheidszorg." Voordat zorgaanbieders zulke apparaten toepassen, moeten zij zoveel mogelijk te weten komen over het beveiligingsniveau ervan om de gegevens van hun organisatie en patiënten veilig te houden."

Download hier het volledige rapport van Kaspersky over security-risico's op e-health gebied.