La FDA veut protéger les stimulateurs cardiaques du piratage

La FDA, agence du Département américain de la Santé en charge des denrées alimentaires et des médicaments, a publié un guide sur la cybersécurité des dispositifs médicaux. Dans la version de ce document datée du 28 décembre dernier, la FDA (Food and Drug Administration) réaffirme l'importance d'une maintenance et de mises à jour régulières pour réduire le risque de cyberattaques et de vol de données. En impliquant davantage les fabricants.

L'agence américaine met également l'accent sur l'analyse du risque et les mécanismes destinés à atténuer ce risque (paramétrer les contrôles de sécurité du dispositif). Pour renforcer son propos, la FDA décrit un scénario possible, mais pas enviable, auquel ferait face un fabricant. Dans cet exemple, le fabricant est alerté d'une vulnérabilité présente dans ses stimulateurs cardiaques et ses défibrillateurs implantables. Or, une telle vulnérabilité si elle est exploitée peut impacter négativement la santé des patients, voire menacer leur vie. Un tiers non autorisé ayant la possibilité d'accéder aux dispostifs du fabricant et en modifier l'action, théoriquement…

Des pompes à insuline vulnérables

Pour définir une stratégie visant à limiter le risque, informer ses clients et revendeurs de l'existence d'une faille, corriger la vulnérabilité et, enfin, distribuer le correctif à l'attention des utilisateurs de ses produits, le fabricant aurait eu besoin de deux mois, selon le scénario proposé par la FDA. Ce temps de réponse est long, surtout lorsque des vies sont en jeu. Malheureusement, le secteur de la santé n'est pas le mieux préparé en matière de cybersécurité. Des évènements récents en témoignent.

L'automne dernier, une faille a bel et bien été détectée dans des pompes à insuline d'une filiale du groupe Jonhson & Johnson. L'entreprise nord-américaine jugeait alors le risque d'un piratage « *extrêmement faible* ». Mais elle a tout de même recommandé aux patients diabétiques de désactiver le lecteur distant de leur machine, pour éviter qu'un tiers n'obtienne un accès non autorisé à la pompe… La mutiplication des objets connectés (IoT) impose d'affûter les politiques de cybersécurité.

Par ailleurs, selon Département américain de la Santé et des Services sociaux, depuis 2009, plus de 1700 violations de données majeures, touchant chacune 500 personnes ou plus, ont été signalées. Selon *Techcrunch*, le nombre de violations non signalées est probablement plus élevé.

Lire aussi :

Des pompes à insuline de Johnson & Johnson trop facilement vulnérables
Sécurité : Conficker revient infecter l'IoT médical
Ransomware, haro sur le monde hospitalier

crédit photo © Epstock-Shutterstock