Pourquoi la sécurité des objets connectés médicaux doit être très rapidement prise au sérieux ?

Les incidents de sécurité liés à l'Internet des Objets (IoT) dans le domaine médical vont connaître une forte augmentation en 2019. Ce signal d'alarme vient d'être tiré par l'association américaine HIMMS, oeuvrant à l'amélioration des soins de santé, par l'utilisation de la technologie. La raison est simple : le nombre d'objets connectés explose littéralement dans le domaine médical, et les cybercriminels y voient donc des opportunités de gagner beaucoup d'argent

Des applications et objets connectés de plus en plus présents dans le secteur de la santé

Les technologies IoT ont été très largement adoptées et des millions d'appareils connectés vont apparaître dans des secteurs clés tels que la santé et les soins médicaux. D'après une étude récemment menée par le CNEH, l'IoT a représenté plus de 60% des projets d'innovation du secteur de la santé en 2018. Avec ces nouveaux objets connectés, les hôpitaux et les cabinets médicaux désirent améliorer l'expérience du patient et réduire les tâches manuelles. Un hôpital de Los Angeles a, par exemple, aménagé des chambres avec des enceintes connectées, afin d'apporter aux patients un sentiment de plus grande indépendance. En France, le Centre Hospitalier Eure-Seine a installé un robot aux urgences pédiatriques pour accueillir les enfants, diminuer leur stress et les mettre en confiance. Ces deux exemples démontrent le potentiel des appareils médicaux et dispositifs portables IoT pour aider les patients durant leur convalescence.

Les organismes de santé, cible privilégiée des hackers

Des attaques à grande échelle telles que les rançongiciels WannaCry et NotPetya, ont déjà affecté des organisations de santé utilisant des logiciels obsolètes, et ce n'est qu'une question de temps avant qu'une autre attaque désastreuse soit révélée. WannaCry, par exemple, a coûté environ 100 millions de livres au service national de la santé du Royaume-Uni (le NHS) après avoir entrainé la fermeture des hôpitaux et l'annulation de 19 000 rendez-vous patients.

À mesure que le nombre d'organisations de santé déployant des solutions IoT augmente, les incidents de sécurité dus aux innombrables vulnérabilités des appareils connectés augmentent également. HIMMS explique dans son étude que près de 76% des établissements de santé ont subi une cyberattaque au cours de l'année écoulée, notamment des attaques très sophistiquées, APT (Menaces persistantes avancées) et des attaques issues de l'interne. L'email est véritablement le principal outil utilisé par les attaquants pour réaliser leurs piratages, puisque 30% des attaques ciblant des organismes de santé, ont été initiées par un email de phishing ou spear phishing. Parmi les principales menaces, se trouvent aussi évidemment, les fuites de données (11,8%), les rançongiciels (11,3%) et les logiciels malveillants volant des informations d'identification (11%).

Des efforts visibles mais la cybersécurité ne progresse pas assez vite, face à l'ampleur de l'enjeu

Les menaces visant des dispositifs médicaux tels que des pacemakers, contrairement à d'autres objets connectés, peuvent avoir un impact dramatique. C'est pour cela que la sécurité des patients reste la priorité numéro un dans le secteur de la santé. Au-delà des pertes financières ou du vol de données, c'est la santé du patient qui est en jeu.

Bien que leurs efforts soient visibles et positifs, le sujet de la sécurité n'avance encore pas assez vite. Les organismes de soins de santé doivent continuer à travailler sur la sécurité de leurs dispositifs IoT, en mettant en place notamment de vrais programmes de gestion des menaces, en réalisant régulièrement des tests d'intrusion afin de corriger les vulnérabilités des infrastructures. Le but étant d'encadrer les IoT de manière sécurisée. L'étude HIMMS explique que même s'ils souhaitent intégrer une technologie médicale intelligente, seuls 6% - ou moins - du budget informatique total des organismes de santé, est consacré à la protection des informations et des actifs IoT. C'est trop peu. Les organismes de santé sont considérés comme étant des structures « à risques » en termes de cybersécurité et dans le cadre de l'IoT, la détection doit être faite avec attention et les failles de sécurité ainsi que les vulnérabilités doivent être surveillées.

Si la cybersécurité n'avance pas au rythme souhaité, c'est aussi parce que le secteur se heurte à des obstacles à la prévention des incidents : toujours selon HIMMS, les raisons sont le manque de personnel qualifié en cybersécurité (52,4%), le manque de ressources financières (46,6%), un grand nombre de vulnérabilités applicatives (28,6%), trop de endpoints - serveurs, postes de travails, PC, etc. (27,5%) et les nombreuses nouvelles menaces émergentes (27%).

Les problèmes de sécurité liés aux appareils connectés doivent constituer une préoccupation majeure pour les administrateurs de services de santé, car tout dysfonctionnement pourrait mettre les patients en danger. Non seulement pour les patients utilisant des stimulateurs cardiaques intelligents ou des pompes à insuline, mais également pour ceux dont les dossiers médicaux pourraient être vendus sur Internet (Darkweb) et manipulés à des fins d'usurpation d'identité et de fraude. Nous nous attendons à ce que les attaques liées aux soins de santé deviennent de plus en plus sophistiquées, car les hackers feront tout ce qui est en leur pouvoir pour mettre la main sur des informations personnelles et compromettre le matériel médical. Comme nous l'entendons globalement dans tous les secteurs, il faut organiser la riposte, mais cela est encore plus urgent dans le domaine de la santé !