LE MAGAZINE DE L'INNOVATION
POUR LA RECHERCHE ET L'INDUSTRIE

PAROLE AUX PARTENAIRES
LCIE
Bureau Veritas

LE DÉFI MAJEUR DE LA CYBERSÉCURITÉ DE L'IoM (INTERNET DES OBJETS MÉDICAUX)

Philippe SISSOKO
Directeur des Opérations
Electrical & Electronic Business Line, EMEA Region
LCIE Bureau Veritas and Bureau Veritas Consumer Products Services

L'évaluation de la cybersécurité des dispositifs médicaux (DM) connectés par les essais de pénétration sur les interfaces physiques (Bluetooth, WiFi, Ethernet…) est un défi majeur à prendre en compte.

Le développement des produits connectés et la mobilité ouvrent des enjeux industriels énormes. L'industrie des équipements connectés concerne désormais tous les secteurs avec des possibilités de développement également des systèmes embarqués construits à partir des technologies existantes (Cellulaire, LoRa, Wifi, Zigbee, RFID, Bluetooth, …). La plupart des études pointent un nouveau risque majeur : les cyber attaques qui pourraient menacer la sécurité de ces objets mais également frapper toute la «supply chain» des différents secteurs (automobile, médical, aéronautique, énergie…).

La plupart des entreprises ne regardent désormais plus la cybersécurité sous l'angle d'obstacle au changement ni comme un coût supplémentaire. Elles comprennent que les solutions peuvent aussi être porteuses de croissance et de sources importantes de différenciation.
Il devient primordial de comprendre et d'évaluer les enjeux et risques liés à l'intégration de ces technologies en matière de cybersécurité.

L'Internet des Objets Médicaux (IoM) est la collection d'appareils médicaux et les applications de soins de santé connectés à des systèmes informatiques. Les dispositifs médicaux communicants (sans fils ou filaires) permettent la transmission efficace des données critiques pour assurer des soins personnalisés, les rendant alors plus accessibles à une intrusion externe malveillante.

Les exemples de IoM incluent :
- la surveillance à distance des patients avec des conditions chroniques ou à long terme
- le suivi des ordonnances de médication des patients et l'emplacement des patients admis dans les hôpitaux
- les dispositifs portables des patients, qui peuvent envoyer l'information aux soignants
- les pompes à perfusion qui se connectent aux tableaux de bord analytiques et aux lits d'hôpitaux équipés de capteurs qui mesurent les signes vitaux des patients.

Une augmentation des flux de données numériques entre les partenaires industriels impose des mesures de sécurisation des systèmes d'information, de production, d'exploitation et d'approvisionnement. Leur maitrise constitue une composante importante qui rend indispensable le développement de solutions de tests, de certifications capables de réduire ces risques et surtout de mieux connaitre les vulnérabilités des produits.

L'un des principaux problèmes et blocages dans le déploiement massif de dispositifs IoM est l'absence pour le moment d'un véritable cadre réglementaire (et normatif structuré) qui peut garantir leur utilisation sûre et sécurisée. Plusieurs initiatives ont été lancées, se concentrant de manière plus importante au niveau de la réglementation, des guides/recommandations émanant de groupes d'experts. Le temps est venu pour une meilleure convergence vers une harmonisation plus globale et une compréhension adaptée aux besoins des industriels quant aux solutions à mettre en œuvre.

Une intensification de la législation en matière de cybersécurité en Europe ces dernières années avec la conformité réglementaire qui s'impose de plus en plus comme un enjeu de taille pour les entreprises

En ce qui concerne la réglementation Européenne des dispositifs médicaux (DM), le nouveau Règlement Européen entré en vigueur en Mai 2017 définit les exigences en termes de sécurité pour les logiciels dispositifs médicaux. Néanmoins, l'intégralité de la problématique cybersécurité n'est pas couverte par cette réglementation, ou de façon insuffisante.

Les dispositifs médicaux sont donc tout autant concernés, et probablement même davantage, que les autres systèmes d'information par la cybersécurité. Certaines industries ont déjà un atout pour la sécurité de leurs systèmes d'information par leur culture de la sûreté de fonctionnement et disposent souvent en interne de compétences pour leurs systèmes d'information et de certifications déjà obtenues sur la base des réglementations nationales sur les Critères Communs ou de type CSPN délivrées en France par l'ANSSI.

Une intensification de la législation en matière de cybersécurité en Europe ces dernières années avec la conformité réglementaire qui s'impose de plus en plus comme un enjeu de taille pour les entreprises

Il faut désormais que ces deux cultures se rencontrent et que les forces s'unissent pour protéger convenablement les systèmes industriels. Ce service propose une offre complémentaire pour les produits non couverts par les processus de certification type « CSPN » et Critères Communs.

La FDA (Food and Drug Administration) a également publié un guide exigeant la prise en compte de la cybersécurité dans la phase de conception, tout en incluant également une démarche assez pro-active dans la phase post-commercialisation.
Plus récemment, L'Internet of Medical Things Resilience Partnership Act a chargé la FDA et d'autres organismes gouvernementaux d'élaborer des recommandations et des lignes directrices visant à renforcer la cybersécurité ainsi que la résilience des dispositifs médicaux en identifiant les principales vulnérabilités du système.

Pour ces nouvelles applications, les caractéristiques de cybersécurité ne devraient pas être considérées comme des mesures facultatives par les fabricants. Elles doivent faire partie du système global, intégrées dès le début dans la spécification de l'architecture système. Le but de la cybersécurité est de protéger les fonctions de sécurité (la protection des fonctions contre la manipulation involontaire ou illégale), les données (informations personnelles et confidentielles).

QUELS SONT LES VECTEURS D'ATTAQUES DISPONIBLES ?

Les DM sont principalement soumis à trois types de cyberattaques : les accès non autorisés, les logiciels malveillants et les attaques par déni de service (DoS : denial of service ; DDoS : distributed denial of service). Un accès non autorisé correspond à l'interception du flux de données sans fil entre le DM et un capteur ou ordinateur par un individu malveillant.
Plusieurs vecteurs d'attaques (figure 1) peuvent être identifiés et (chacun à son niveau de risque) peuvent offrir l'accès à différentes fonctions plus ou moins critiques.
Les vecteurs 1 et 2 d'attaques, sont inter-reliés et plus faciles d'accès. Le premier est le réseau des équipements IoM connectés à l'internet (service télésanté) et le deuxième est le logiciel de gestion d'un ou de plusieurs dispositifs (application, site internet spécifique, etc). Un attaquant pourrait rechercher sur internet les passerelles accessibles et avoir accès aux informations confidentielles du patient.

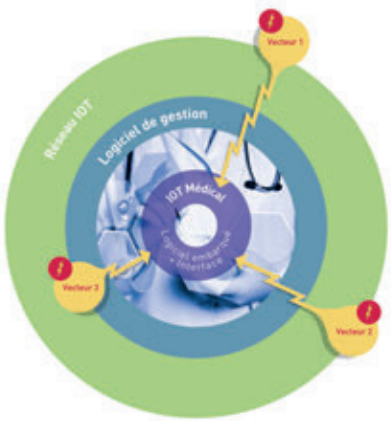

Fig. 1 - Représentation vecteurs d'attaques

Mais il peut aussi prendre le contrôle afin de modifier les dosages ou des configurations d'équipements employés par le patient, tels que des respirateurs ou des pompes à insuline, ce qui pourrait remettre en cause la vie des patients utilisant ces équipements.
Le vecteur 3 d'attaque est le plus difficile d'accès, car l'attaquant doit être connecté physiquement aux dispositifs via leurs interfaces de connexions (filaire ou sans fil). Cependant le nombre de produits connectés sans fil ne cessant de croitre dans les lieux publics comme résidentiels, cette propension à ce que tout se connecte ne va que s'étendre de plus en plus, rendant ces interfaces de types hertziennes de plus en plus accessibles à chacun.

Parmi ces interfaces les plus sensibles demeurent, évidemment, les interfaces sans fil de courte et longue portée (Bluetooth, Wifi, Lora, 2G/3G/4G…). Mais les interfaces filaires ne doivent pas être négligées (Ethernet, USB, Bus de données terrain…).
Ces attaques peuvent avoir un impact plus grave, car elles vont viser l'équipement qui est le plus près de l'utilisateur ou du patient avec comme résultat le plus probable, la mise en danger de la vie de l'utilisateur de l'IoM.

DIFFÉRENTES SOLUTIONS PROPOSÉES EXISTENT DONT LA NÉCESSITÉ ABSOLUE DE BIEN CARACTÉRISER LES INTERFACES PHYSIQUES D'UN ÉQUIPEMENT CONNECTÉ AFIN D'ÉVALUER SES VULNÉRABILITÉS

Ayant identifié le troisième vecteur comme étant l'un des plus critiques, compte tenu de l'émergence des objets connectés, LCIE Bureau Veritas a développé une solution de test veillant à proposer un niveau raisonnable de cybersécurité pour les IoM (figure 2). Cette offre d'évaluation de la cybersécurité permet de détecter d'éventuelles vulnérabilités à partir d'un profil de sécurité spécifique à l'interface.

Dans ce cadre, LCIE Bureau Veritas s'est équipé d'un banc d'essai qui réalise des suites de tests de validation basées sur des techniques de « Misuse » et d'« Abuse » concentrées sur les interfaces physiques du périphérique.
La procédure d'essai suppose que tout attaquant peut accéder aux connexions physiques du périphérique, sans nécessairement accéder au périphérique lui-même.

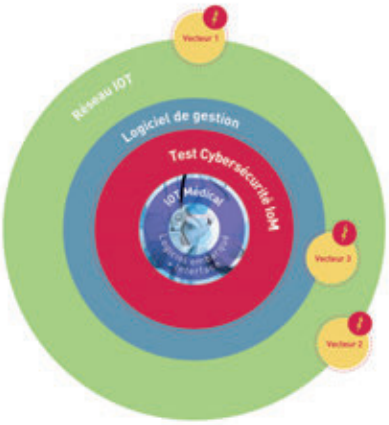

Fig. 2 - Positionnement du test Cybersécurité IoM entre les vecteurs d'attaques

Le banc d'essai évalue la sécurité des interfaces du périphérique, en particulier les liens physiques et la robustesse du protocole de communication associé. Enfin, l'outil analyse les interfaces filaires et sans fils tels que : Modbus protocol, Bluetooth, ZigBee, USB, Ethernet, NFC et prochainement les interfaces WIFI.

En conclusion, bien que la cybersécurité nécessite une approche globale et structurée à tous les niveaux, cette évaluation par les interfaces physiques peut constituer une manière intéressante de maitriser les vulnérabilités - même si celles-ci peuvent être d'origines multiples - tout au long du cycle de vie du produit.

Face à de tels enjeux, les fabricants d'équipements se doivent d'élargir leurs actions au-delà du simple cadre réglementaire actuel qui ne couvre que les systèmes soumis aux exigences couvertes par les certifications étatiques de type Critères communs, CSPN, NIST...

Il est donc nécessaire d'intégrer cet aspect de cybersécurité dans les fonctionnalités des DM car les mesures prises pour l'instant concernent davantage la protection des données personnelles stockées, et moins le piratage direct des DM via leurs interfaces physiques.