Gestion de la cybersécurité pour les appareils médicaux et l'IoT

La plateforme Asimily Insight, cliniquement validée, combine l'inventaire de tous les appareils IoMT et IoT avec une gestion efficace des vulnérabilités, y compris la priorisation et la remédiation des risques spécifiques à l'appareil.

Aucun hôpital ne peut se passer d'appareils médicaux en réseau, par commencer par le moniteur patient jusqu'au système d'IRM. Il en va de même pour les environnements industriels, les infrastructures critiques et le secteur des transports. Tous misent de plus en plus sur les appareils IoT pour la surveillance et le contrôle. Il est évident que dans ces secteurs, la cybersécurité se doit d'être particulièrement renforcée, non seulement pour les systèmes informatiques, mais aussi pour les appareils médicaux (IoMT, internet of medical things) et les appareils IoT en général.

La gestion de la vulnérabilité informatique ne suffit pas

L'utilisation de dispositifs IoMT et IoT comporte des risques qui ne sont pas faciles à déterminer et à éliminer. Par exemple, les appareils ne peuvent souvent pas être patchés ou les fabricants ne fournissent que rarement des mises à jour. Les risques spécifiques aux appareils qui en découlent peuvent être soit critiques, soit plutôt insignifiants. La question se pose donc de savoir quels risques doivent être éliminés et avec quel degré d'urgence. Pour compliquer encore les choses, l'IoMT et l'IoT fonctionnent en grande partie avec des protocoles spécifiques, souvent propriétaires, des fabricants respectifs, qui ne sont pas connus des services informatiques.

Les solutions courantes de gestion des vulnérabilités pour les environnements informatiques n'apportent donc qu'une aide limitée. Elles ne maîtrisent pas les protocoles et les risques dans les domaines médical et industriel et n'offrent donc pas de possibilité rapide pour identifier et classer les points faibles dans ces environnements, et encore moins pour les éliminer ou les contourner rapidement avec un minimum de travail pour le personnel.

Asimily maîtrise l'IoMT et l'IoT

Le fabricant américain Asimily comble cette lacune en proposant une plateforme complète de gestion de la cybersécurité pour les appareils IoT et médicaux. La plateforme Asimily Insight collecte toutes les informations disponibles sur les appareils en temps réel et présente les conclusions sur un tableau de bord clair. Une gigantesque base de données contenant des informations sur les appareils, des indications MDS2 et des SBOM des fabricants ainsi que des informations provenant de la communauté des utilisateurs sert de base à l'identification des points faibles.

En outre, Asimily tient compte du type et de la configuration de chaque appareil. Par exemple, les appareils qui traitent des informations de santé protégées ou qui contrôlent directement des installations industrielles représentent un risque massivement plus important que beaucoup d'autres. L'évaluation CVSS, généralement utilisée par les solutions de gesti-

on des vulnérabilités, ne reconnaît pas de telles différences. Avec sa base de données qui couvre notamment plus de 1000 appareils médicaux, Asimily a incontestablement une longueur d'avance.
Comme Asimily traite en priorité les problèmes de sécurité qui ont une forte probabilité de se produire ou qui ont un impact de grande ampleur, le temps consacré à chercher à les résoudre est nettement réduit – tout ce qui n'est pas important peut être laissé de côté.
Dans la pratique, Asimily permet de réduire jusqu'à 90 % la charge de travail manuel des analystes en gestion des vulnérabilités.
La solution d'Asimily permet en outre de corriger de nombreuses vulnérabilités quasiment en appuyant sur un seul bouton – le bouton «Fix». La plateforme travaille pour cela avec les systèmes NAC et autres systèmes de sécurité et peut ainsi par exemple fermer les ports à risque, apporter des patches là où c'est possible ou procéder à une (micro-)segmentation de l'appareil en question.

Asimily: les points forts

- Plateforme complète de gestion de la cybersécurité IoT/IoMT
- Permet de dresser un inventaire, de réduire les risques, de réagir aux incidents et de garantir la disponibilité des appareils
- Identifie et priorise les risques de chaque appareil en fonction de sources de données spécifiques et de la configuration de l'appareil
- Offre une correction automatisée des vulnérabilités via le bouton «Fix»
- Fonctionne avec des scanners de vulnérabilité comme Tenable et des systèmes NAC comme Cisco ISE ou Aruba Clearpass, ainsi qu'avec les pare-feu de Palo Alto, Fortinet ou Checkpoint
- Utilisable comme solution sur site ou en cloud
- Sans agent, c'est-à-dire qu'aucune installation de logiciel n'est nécessaire sur les appareils

BOLL
IT Security Distribution

BOLL Engineering SA
Jurastrasse 58
5430 Wettingen

Tél. 056 437 60 60
info@boll.ch
www.boll.ch

→ **boll.ch/asimily**