Gestion des vulnérabilités dans le réseau clinique

La technologie médicale et l'informatique se développent de plus en plus conjointement. Selon les exigences légales actuelles, les dispositifs médicaux en réseau doivent être protégés contre les cyberrisques de la même manière que les systèmes informatiques. Cependant, les dispositifs médicaux ne sont pas en soi conçus pour la cybersécurité – la solution réside dans des plateformes de logiciels telles que Medigate et InsightVM.

Les dispositifs médicaux en réseau, du perfuseur aux moniteurs des patients en passant par les scanners IRM, sont devenus incontournables dans le quotidien clinique. Comme pour tous les appareils connectés à un réseau, il convient également d'assurer la plus grande sécurité possible pour ces dispositifs IoMT (Internet of Medical Things) et de prendre rapidement des mesures correctives en cas de failles de sécurité. Dans le monde informatique classique, c'est là que les solutions de gestion des vulnérabilités (Vulnerability Management ou VM) entrent en jeu. Ces plates-formes de logiciels analysent activement tous les appareils du réseau à la recherche de vulnérabilités et évaluent leur risque. Par des recommandations aux administrateurs ou par des processus de remédiation automatisés, elles contribuent à renforcer la sécurité – ceci en combinaison avec d'autres solutions telles que les systèmes de gestion des correctifs (Patch Management) et les pare-feu (firewalls).

Les scannages de vulnérabilité mettent les appareils à rude épreuve

Le scannage actif de vulnérabilité est un processus invasif qui impose une charge inhabituelle au matériel des dispositifs analysés, par exemple, des tentatives de connexion multiples ou une communication simultanée sur plusieurs ports non utilisés en fonctionnement normal. D'autres méthodes nécessitent l'installation d'un agent sur les appareils. Cependant, cela n'est généralement pas possible avec les dispositifs IoMT: le fabricant ne le permet pas, ou l'appareil devrait être alors recertifié après l'installation de l'agent – un processus coûteux et long.

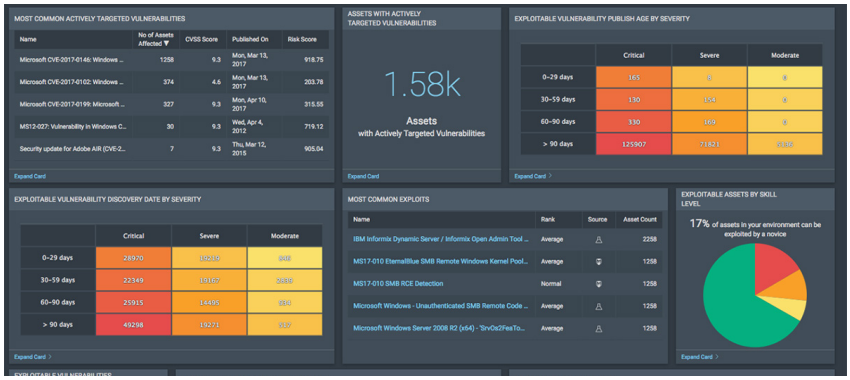
Jusqu'à présent, les organisations de santé étaient très sceptiques quant à la gestion de la vulnérabilité des équipements médicaux. Certains hôpitaux ne vérifient même pas la vulnérabilité de leurs équipements médicaux. La raison: si un scannage actif provoque un dysfonctionnement ou même la défaillance d'un appareil en cours d'utilisation, la sécurité du patient est immédiatement et gravement compromise. Il est évident que cela ne doit pas se produire dans la pratique clinique quotidienne. En outre, les solutions de VM ne sont généralement pas conçues pour l'IoMT, ne peuvent pas identifier proprement les dispositifs correspondants et ne sont même pas conscientes des vulnérabilités des systèmes de dispositifs médicaux.

La gestion des vulnérabilités devient indispensable

Les hôpitaux ne peuvent néanmoins plus se passer de la cybersécurité dans leurs équipements médicaux. Rien que pour des raisons juridiques. Par exemple, depuis le 26 mai 2021, la loi suisse révisée sur les dispositifs médicaux stipule que les établissements de santé doivent protéger tous les dispositifs médicaux pouvant être connectés à un réseau contre les cyberrisques en prenant des mesures appropriées dans le cadre d'un système de gestion du risque (ODim Art. 74). Des réglementations comparables s'appliquent en Allemagne, et des lois correspondantes sont en préparation en Autriche.

Pour des raisons techniques, il est également nécessaire d'aborder la question de la sécurité des dispositifs IoMT. Pour ce faire, il est toutefois nécessaire de connaître l'état actuel de tous les dis-

positifs médicaux en réseau. En effet, ce n'est que lorsque l'on dispose d'une visibilité complète que des mesures peuvent être prises pour protéger les dispositifs médicaux en réseau. Cette visibilité fait souvent défaut aujourd'hui. Bien que les dispositifs IoMT soient généralement gérés par un logiciel central, les données relatives aux dispositifs sont généralement saisies manuellement et certaines informations, telles que les vulnérabilités, ne sont pas reconnues ou enregistrées, ce qui nuit à la mise à jour.



Ce qu'il faut, c'est une solution qui fournit dans un premier temps un inventaire complet de tous les appareils en réseau, avec des détails tels que le type d'appareil, le modèle, la version du micrologiciel et de l'application, le numéro de série, l'emplacement, le segment de réseau, l'utilisation et le service responsable. Deuxièmement, la solution doit être capable d'analyser les dispositifs IoMT sans scannage actif. Troisièmement, les fonctions classiques de gestion des vulnérabilités ne doivent pas manquer. Et quatrièmement, la solution doit analyser la communication des appareils et déclencher des alarmes en cas de soupçons et d'anomalies.

Inventaire, analyse et évaluation des risques pour les dispositifs IoMT

Avec Medigate, le fabricant du même nom propose une plateforme spécialisée dans l'IoMT, qui commence par créer automatiquement un inventaire complet de tous les appareils en réseau. On utilise une procédure passive qui n'affecte pas les appareils: un senseur sous forme d'appliance examine le trafic réseau à l'aide de switch-ports, filtre les informations pertinentes pour l'IoMT à partir du flux de données en utilisant l'inspection approfondie des paquets et les transmet pour analyse. Seules les métadonnées du dispositif et aucune donnée sur le patient sont transmises. Après que Medigate a analysé les données du dispositif, celles-ci sont enrichies d'informations détaillées grâce à sa propre base de données. Medigate conserve plus de 2 millions de dispositifs dans sa base de données, comprend plus de 100 protocoles de technologie médicale propriétaires et peut donc fournir des informations précises sur le parc de dispositifs existants.

Medigate présente les dispositifs inventoriés et les vulnérabilités connues qui leur sont associées sur une interface web claire qui permet de comprendre chaque détail. En analysant le trafic réseau, la plateforme est également capable de détecter en temps réel des anomalies telles que des connexions et des ouvertures de session non souhaitées ou des communications avec Internet, d'émettre des alertes et, en coopération avec d'autres solutions de sécurité telles que les pare-feu, d'empêcher les communications dangereuses. La solution prend donc également en charge la définition et le respect des règles de sécurité.

Un duo gagnant: Medigate et InsightVM

Medigate fonctionne de manière bidirectionnelle avec d'autres plateformes via des intégrations. La combinaison avec la plateforme VM InsightVM de Rapid7 est particulièrement réussie. Pour s'assurer que seuls les dispositifs informatiques sont activement analysés par Rapid7 pendant l'analyse de vulnérabilité, Medigate transmet les détails du dispositif IoMT à InsightVM et informe ainsi InsightVM des dispositifs médicaux qui doivent être exclus des tâches de scannages actifs. En outre, Medigate informe InsightVM des vulnérabilités IoMT (Clinical CVEs) qui sont connues grâce aux recherches de Medigate et des fabricants de dispositifs.
Inversement, Medigate obtient de Rapid7 des informations sur les vulnérabilités de tous les appareils détectés (y compris les appareils non IoMT).
Medigate peut ainsi calculer un score de risque pour chaque appareil en réseau détecté, qui tient également compte des vulnérabilités générales concernant le système d'exploitation, la connectivité réseau, diverses propriétés techniques et d'autres paramètres, et le présenter directement dans sa propre interface. Un autre avantage de l'intégration est que toutes les vulnérabilités sont visibles dans un tableau de bord (soit via Medigate, soit via InsightVM) et peuvent donc être enregistrées, surveillées et traitées de manière centralisée.

En bref, l'intégration bidirectionnelle de la visibilité détaillée des dispositifs de Medigate avec les fonctions d'analyse des vulnérabilités d'InsightVM crée une capacité sans précédent pour traiter les vulnérabilités de tous les appareils en réseau (IoMT, IoT et IT), évaluer et gérer les risques dans l'ensemble de l'hôpital, et prendre les mesures appropriées en fonction de la priorité des problèmes de sécurité.

BOLL
IT Security Distribution

BOLL Engineering SA
En Budron H15,
1052 Le Mont-sur-Lausanne

Tél. 021 533 01 60
vente@boll.ch
www.boll.ch

→ **www.boll.ch/de/medigate**