Gestion des actifs OT – essentielle pour la vue d'ensemble et la gestion des risques

La gestion globale de tous les appareils OT et Medical IoT apporte des avantages en matière de sécurité et d'économie et renforce la gestion des risques ainsi que le respect de la conformité.

Les environnements industriels de toutes sortes – des infrastructures critiques aux installations de production et à l'automatisation des bâtiments – ainsi que le secteur de la santé ne peuvent aujourd'hui plus se passer de la numérisation. Dans tous ces secteurs, d'innombrables appareils et dispositifs en réseau sont utilisés, fonctionnant avec différents protocoles, se trouvant à différents endroits et pouvant, comme tout appareil numérique, présenter des points faibles. Qu'il s'agisse d'OT (operational technology) ou de Medical IoT, les environnements industriels, tout comme les technologies de l'information, offrent une multitude de possibilités, mais comportent aussi des risques de sécurité qui doivent être identifiés et minimisés.

Un inventaire toujours à jour est fondamental

Afin d'identifier et évaluer correctement les risques de sécurité, puis les réduire ou les éliminer au cas par cas, par exemple par des mises à jour de micrologiciels, des correctifs virtuels ou le remplacement de l'appareil concerné, il est indispensable de disposer d'un inventaire actualisé en permanence de l'ensemble du parc d'appareils ou d'installations. Sans une gestion des actifs complète ou sans une connaissance détaillée de l'équipement disponible, de son importance et des risques de sécurité associés, il est impossible de dresser un inventaire efficace. Sans cette transparence, la gestion globale des risques devient une mission impossible.

Ruedi Kubli, *Business Development Manager IoT/OT, BOLL*

Gestion des actifs OT – qu'est-ce que cela signifie?

Une gestion efficace de tous les appareils OT ou Medical IoT en termes de sécurité implique un inventaire, une surveillance et une gestion de tous les appareils tout au long de leur cycle de vie. Ce qui permet de disposer d'une documentation toujours actuelle sur l'environnement et l'état des différents appareils. Et de clarifier des questions essentielles, par exemple «Quel risque de sécurité se cache dans un appareil?». Selon son importance, le risque peut être plus ou moins élevé et une mise à jour n'est pas forcément nécessaire. Si c'est le cas, il faut se poser les questions suivantes: les failles de sécurité peuvent-elles être corrigées par un nouveau firmware ou des correctifs, ou l'appareil ne peut-il pas être patché? Dans

ce dernier cas, le patching virtuel peut être utile: il s'agit de placer en amont de l'appareil à risque un système actualisable qui bloque les attaques de manière fiable. La gestion des actifs est particulièrement importante, car les cycles de vie des appareils OT sont généralement très longs. Par exemple, les installations industrielles sont souvent conçues pour une utilisation de plusieurs dizaines d'années, et même à l'hôpital, un tomodensitomètre est rarement remplacé tous les deux ans. L'inventaire des appareils permet par ailleurs de savoir si un appareil est encore suffisamment utilisé ou s'il peut être mis hors service, et sert donc, outre les considérations de sécurité, à contrôler les coûts et à assurer une exploitation économique. Selon le secteur et l'entreprise, des recommandations ou des prescriptions réglementaires telles que NIS2 ou la norme minimale suisse pour les TIC s'appliquent également. Pour leur conformité, l'inventaire complet et la surveillance de tous les appareils IT, OT et IoT sont pratiquement indispensables, ce qui profite à son tour à la gestion des risques.

Intégration dans d'autres systèmes

Les solutions de gestion des actifs OT, telles que celles proposées par Claroty ou Asimily, ainsi que les fonctions de gestion des actifs des fournisseurs de sécurité comme Fortinet ou Palo Alto Networks, peuvent également être intégrées dans des systèmes et processus existants tels que la gestion des changements ou la ticketing. Un exemple: le système de gestion des actifs détecte un problème et génère un ticket correspondant pour le système de ticketing. Parallèlement, une notification est envoyée au pare-feu qui ajuste une règle ou en crée une nouvelle et l'active. En conséquence, sur la base des informations fournies par la gestion des actifs, le risque de l'appareil concerné peut être réévalué.

BOLL
IT Security Distribution

BOLL Engineering SA
Jurastrasse 58
5430 Wettingen

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

La gestion globale de tous les appareils OT et Medical IoT renforce la gestion des risques ainsi que le respect de la conformité.

→ **boll.ch**