# Comment connecter vos machines obsolètes de façon cybersécurisée

12 octobre 2021, 02:00

Annanda Rath
Christophe Michiels
Tatiana Galibus

*Sirris a récemment lancé son service de cybersécurité pour l'industrie manufacturière. Alors que nous commençons à nous adresser aux entreprises par le biais de notre séance d'accueil gratuite ou coaching individuel, nous recevons de plus en plus de questions relatives à la connectivite. Si la matière peut sembler complexe pour les fabricants, quelques conseils bien structurés permettent de s'en sortir facilement.*

Il n'existe aucune solution universelle qui puisse garantir la cybersécurité d'un équipement hérité et, comme nous le savons, la force d'une chaîne est égale à celle de son maillon le plus faible. Voilà pourquoi il est essentiel de construire plusieurs *couches* pour consolider les systèmes anciens et ainsi *réduire le risque* de problèmes liés à la cybersécurité.

## Stratégies et interventions possibles

- Première grande stratégie à mettre en place : **empêcher vos équipements de sombrer dans l'*obsolescence***, ou au moins retarder ce processus. Vous pouvez, pour ce faire, consigner toutes les modifications et mises à jour effectuées au niveau de la machine. Si celle-ci contient un système d'exploitation sur PC, veillez à bien appliquer tous les correctifs (de sécurité). Ce conseil vaut également pour les équipements DCS ou PLC. Cette partie du contrat de maintenance peut être conclue entre vous et votre fournisseur/intégrateur. Si, avec le temps, une pièce ne peut plus être corrigée par voie logicielle, envisagez une mise à niveau avec du matériel neuf. Cette décision implique une surveillance constante et des investissements continus. Compte tenu du coût des dommages potentiels liés aux cyberattaques modernes, le jeu en vaut la peine.

- Seconde stratégie : **conserver une vue d'ensemble de tous vos actifs connectés**, y compris les systèmes DCS ou PLC à l'intérieur des machines. On part ici du principe qu'on ne peut pas protéger ce que l'on ne connait pas. Il est donc essentiel de tenir un inventaire. Le mettre régulièrement à jour représente un vrai défi, mais c'est une tâche importante ! Comme les vulnérabilités connues évoluent au fil du temps, vous devez absolument exécuter des analyses fréquentes de vos appareils pour les détecter. Visualisez cet aperçu pour voir quelle action de renforcement aura un impact sur quelle partie de votre production ou quelle machine. La planification et la conception de votre infrastructure s'en trouveront facilitées.

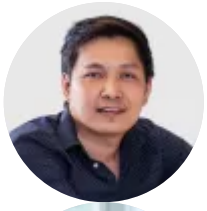
- Il faut au minimum **séparer votre équipement informatique de bureau de votre équipement OT de production**. Pour ce faire, il vous suffit de placer un pare-feu industriel distinct entre les deux. Mieux encore : vous pouvez aller plus loin en cloisonnant les différents départements, lignes ou machines. Inutile de dire que les pare-feu en eux-mêmes doivent être gérés et mis à jour par l'application de correctifs fournis par le fabricant. En fonction de la taille de votre infrastructure, il est également recommandé d'utiliser des appareils de marques différentes.

- La **surveillance du trafic réseau** entrant ou sortant d'une machine permet de garder un œil sur un système de manière non intrusive. Cette pratique, qu'on appelle patch virtuel, consiste d'abord à installer un appareil entre la machine et le reste du réseau. Lorsqu'il détecte l'exploitation d'une vulnérabilité connue, il bloque le trafic réseau et informe l'administrateur de cet événement.

- Il arrive parfois qu'on utilise encore de **vieux logiciels** afin de générer des fichiers pour un certain type de machine (CNC, par ex.). Ceux-ci ne tournent bien souvent que sous Windows 98 ou XP. Dans de tels cas, il est conseillé d'exécuter le SE et le logiciel anciens dans une machine virtuelle sur un PC moderne. Cette solution ne résoudra pas tous les problèmes potentiels, mais réduira grandement la surface d'attaque.

Les astuces que nous vous donnons dans ce billet de blog ne représentent qu'un petit aperçu des différentes manières de consolider votre infrastructure OT héritée. Notre masterclass « La cybersécurité pour les entreprises manufacturières » approfondira le sujet avec des exemples pratiques et une feuille de route étape par étape pour sécuriser vos machines connectées. Inscrivez-vous dès maintenant et rejoignez-nous le 8 novembre 2021 !

## Auteurs

Annanda Rath



Christophe Michiels



Tatiana Galibus