Trois conseils pour la cybersécurité

La cybersécurité est une préoccupation croissante pour les fabricants, de nouvelles souches de rançongiciels et d'autres virus système étant créés chaque semaine.

Toute entreprise peut être la cible d'une cyberattaque. La meilleure façon de les éviter est d'anticiper et de se préparer à l'inattendu.

1

Dispositifs connectés

Les avantages des appareils mobiles se retrouvent dans la surveillance des conditions, ainsi que dans la maintenance et l'analyse prédictives. Pour les fabricants utilisant des dispositifs connectés, des mises à jour de sécurité régulières et des audits logiciels réguliers doivent être une priorité s'ils souhaitent identifier et résoudre les défaillances de leurs systèmes.

2

Anciens systèmes

En général, les systèmes informatiques industriels ne sont pas mis à jour ni remplacés aussi souvent que les technologies grand public, ce qui peut exposer les fabricants à des méthodes d'attaques déjà anciennes, telles que Heartbleed ou Shellshock.

Les anciens systèmes peuvent être dotés de leur logiciel OpenSSL d'origine. Les vulnérabilités d'un tel logiciel peuvent exposer le système à des pirates, qui peuvent intercepter ou voler des données.

De nombreux éditeurs de logiciels ont distribué gratuitement des mises à jour critiques pour lutter contre les vulnérabilités. Tout ce que les fabricants doivent faire est de mettre à jour leurs logiciels.

3

Systèmes de production automatisée

Les réseaux et les systèmes d'entreprise ne sont pas les seuls exposés au risque. Les systèmes de contrôle industriel peuvent également être pris pour cibles par les rançongiciels. Si une attaque verrouille les ordinateurs de fabrication, cela peut entraîner une interruption coûteuse. Les fabricants doivent protéger les systèmes de production automatisée via une protection cellulaire, constituant une forme efficace de défense contre les attaques de l'homme du milieu.

À l'ère d'Industrie 4.0, les dispositifs connectés et les systèmes automatisés peuvent faire l'objet de menaces supplémentaires. La meilleure façon d'empêcher une attaque est d'anticiper et de se préparer à l'inattendu.