IoT : quels sont les maillons faibles en entreprise ?

L'Internet des objets (IoT) constitue un nouvel eldorado pour certains industriels. Il peut aussi constituer un risque non négligeable, soit comme point d'entrée dans les réseaux des entreprises ou en tant que cible principale de malwares spécialisés.

C'est ce que met en exergue une étude* de Forescout Technologies. Le fournisseur de solutions déclare avoir analysé les données de 8 millions de dispositifs connectés aux réseaux de grandes entreprises dans le monde. 5 secteurs sont concernés : les services financiers, le secteur public, les soins de santé, la production industrielle et le commerce de détail.

Les 10 dispositifs connectés qui exposent le plus les réseaux des entreprises (du fait de ports ouverts par défaut et de problèmes de connectivité) sont les suivants :

1. Solutions de contrôle d'accès physique
2. Systèmes connectés de chauffage, ventilation et climatisation (CVC)
3. Caméras réseau de surveillance
4. Contrôleurs logiques programmables
5. Systèmes de radiothérapie
6. Contrôleurs hors bande
7. Postes de travail en radiologie
8. Systèmes de communication et d'archivage d'images
9. Points d'accès sans fil
10. Cartes de gestion de réseau

Plus largement, les bâtiments intelligents, les appareils médicaux connectés, les équipements réseau et les téléphones IP forment le groupe de dispositifs IoT les plus exposés.

Configuration et OS à risque

Autre enseignement du rapport : plus de 35% des postes de travail gérés sous Windows dans le secteur des soins de santé, et plus de 30% dans le secteur de la production industrielle, s'appuient sur des versions du système d'exploitation dont Microsoft n'assure plus le support.

De surcroît, dans les services financiers, près de 30% des postes gérés sous Windows n'ont pas été mis à jour avec le correctif de Microsoft permettant de colmater la faille BlueKeep.

Le spécialiste américain du contrôle d'accès réseau souligne également que, dans le secteur public (gouvernements), près de 10% des appareils étudiés ont le port Telnet 23 ouvert par défaut, et 12% ont les ports FTP 20 ou 21 ouverts par défaut.

Un manquement qui peut être lourd de conséquences. « La récente découverte des vulnérabilités Ripple20 nous rappelle que de nombreux équipements peuvent être à risque pour les organisations. Soit le device sera hacké lui-même, avec des conséquences directes sur le service

qu’il assure, soit les hackers s’en serviront comme porte d’entrée pour accéder au réseau de l’entreprise », a déclaré Julien Tarnowski, directeur France et Luxembourg de Forescout. Pour le fournisseur, elles ont donc intérêt à s’équiper des solutions qui leur permettent d’automatiser l’identification, la gestion et la sécurité de ces dispositifs connectés.

(crédit photo © Shutterstock)