La connectivité Internet augmente le risque de failles de sécurité, mais cette connectivité est une exigence obligatoire pour de nombreux projets d'automatisation, ce qui rend les procédures de cyberprotection absolument vitales.

Connectivité au nuage, accès à distance, mise à jour des recettes, sauvegarde des données et contrôle à distance pour la maintenance : la nécessité d'une connectivité externe crée de nouveaux défis dans le domaine de la sécurité de l'information, car elle augmente l'exposition potentielle et le risque. La responsabilité de la prévention des failles de sécurité incombe au personnel d'exploitation et de contrôle, qui programme et connecte les contrôleurs à un réseau externe.

Unitronics offre une variété de solutions et d'outils qui peuvent être utilisés pour atténuer les risques et prévenir les failles de sécurité. **Ce document détaille les principaux outils et recommandations destinés à élever le niveau de cyberprotection des projets d'automatisation et des machines basées sur les contrôleurs Unitronics de la série UniStream®.**

1. Niveau d'équipement

Bases

a. **Restez informé via** http://www.unitronicsplc.com - Unitronics développe et améliore ses produits tout au long de leur cycle de vie. Le site web de l'entreprise contient les versions les plus récentes des logiciels et des systèmes d'exploitation, qui peuvent inclure des avancées en matière de cyberprotection.

b. Documents Release Notes : mis à jour à chaque version, ces documents peuvent contenir des informations de sécurité relatives à une version spécifique. **Unitronics recommande de mettre à jour les contrôleurs et les outils de développement à la version 1.32 et plus.**

c. **Permissions d'accès et mots de passe**

- Contrôler strictement les autorisations d'accès au contrôleur et à l'équipement associé.
- Modifier les mots de passe par défaut de l'automate et les stocker conformément aux pratiques reconnues. La modification du mot de passe par défaut et la définition d'un nouveau mot de passe d'accès au contrôleur empêcheront **un utilisateur occasionnel** de se connecter au contrôleur via UniLogic.

d. Les produits UniStream prennent en charge plusieurs niveaux de sécurité et de protection. Le développeur et l'utilisateur doivent mettre en œuvre les fonctionnalités suivantes en fonction des exigences du système :

- Définir les mots de passe pour VNC via la gestion du serveur VNC.
- Définir les autorisations pour UniApps via la gestion des mots de passe.
- Définir les utilisateurs et les autorisations pour les écrans des utilisateurs via le Contrôle d'accès des utilisateurs.
- Définir les utilisateurs et les autorisations pour les écrans du serveur Web. Pour les systèmes où le téléchargement de l'application utilisateur se fait à l'aide d'un lecteur Flash ou d'une carte SD, il faut veiller à définir les différents mots de passe aux endroits prévus à cet effet.

2. Niveau du réseau

Communication sécurisée

a. **Le contrôleur en tant que client Internet :** Si le contrôleur doit communiquer avec des composants ou des serveurs sur Internet, assurez-vous que le contrôleur agit en tant que client, en initiant la communication.

b. **Connexion des équipements d'automatisation à l'internet :**

- Assurez-vous que tous les équipements se trouvent derrière un pare-feu et qu'aucune règle de pare-feu n'expose le réseau LAN à une entrée depuis le réseau WAN. (qu'il s'agisse d'un routeur cellulaire ou d'un réseau câblé).
- Vérifiez qu'il n'y a pas de paramètres de transfert de port exposant l'équipement d'automatisation directement au réseau public. Pour mettre en œuvre rapidement et facilement une protection au niveau du réseau, il est recommandé d'utiliser les produits UCR, la série de routeurs industriels d'Unitronics qui comprend des fonctionnalités intégrées de pare-feu et de VPN. Pour une connexion rapide, reportez-vous à la section **Configuration du VPN sur les produits UCR en quatre étapes.**

3. Solution complète

Connexion sécurisée - basée sur UniCloud

La plateforme IIoT **UniCloud** d'Unitronics permet une connexion sécurisée **sans avoir besoin d'adresses IP** fixes ou publiques - aucune connaissance préalable en cyber ou informatique n'est nécessaire pour la mise en œuvre.

La plateforme contient plusieurs couches de cryptage et de protection avancés qui, ensemble, fournissent une solution complète et sécurisée permettant de restreindre l'accès par niveau d'autorisation et de suivre les connexions réelles.

International Headquarters: P.O.B. 300, Ben Gurion Airport 7019900, Israel. Tel: +972 3 977 88 88, global.sales@unitronics.com