Internetkonnektivität erhöht das Risiko von Sicherheitsverletzungen, aber diese Konnektivität ist eine zwingende Voraussetzung für viele Automatisierungsprojekte und macht Cyber-Schutzverfahren absolut notwendig.
Cloud-Konnektivität, Fernzugriff, Rezeptaktualisierung, Datensicherung und Fernsteuerung für die Wartung: Die Notwendigkeit externer Konnektivität schafft neue Herausforderungen im Bereich der Informationssicherheit, da sie die potenzielle Gefährdung und das Risiko erhöht. Die Verantwortung für die Vermeidung von Sicherheitsverletzungen liegt beim Betriebs- und Kontrollpersonal, das die Steuerungen programmiert und mit einem externen Netzwerk verbindet. Unitronics bietet eine Reihe von Lösungen und Tools an, die zur Risikominderung und zur Vermeidung von Sicherheitsverletzungen eingesetzt werden können.

Dieses Dokument enthält die wichtigsten Tools und Empfehlungen zur Erhöhung des Cyberschutzes von Automatisierungsprojekten und Maschinen, die auf Steuerungen der Unitronics UniStream®-Serie basieren.

1. Ausrüstung

Grundlagen

a. **Bleiben Sie auf dem neuesten Stand über** http://www.unitronicsplc.com - Unitronics entwickelt und verbessert seine Produkte während ihres gesamten Lebenszyklus. Auf der Website des Unternehmens finden Sie die aktuellsten Versionen von Software und Betriebssystemen, die auch Fortschritte beim Cyber-Schutz enthalten können.

b. Dokumente mit Versionshinweisen: Diese Dokumente werden bei jeder Versionsfreigabe aktualisiert und können Sicherheitsinformationen enthalten, die für eine bestimmte Version relevant sind. **Unitronics empfiehlt, Steuerungen und Entwicklungstools auf Version 1.32 und höher zu aktualisieren.**

c. **Zugangsberechtigungen und Passwörter**

- Kontrollieren Sie die Zugriffsrechte auf das Steuergerät und die zugehörigen Geräte strengstens.
- Ändern Sie die Standardpasswörter der SPS und bewahren Sie sie entsprechend der anerkannten Praxis auf. Das Ändern des Standardpassworts und das Festlegen eines neuen Zugangspassworts für die Steuerung verhindert, dass sich ein gelegentlicher Benutzer über UniLogic mit der Steuerung verbindet.

d. UniStream-Produkte unterstützen mehrere Sicherheits- und Schutzebenen. Der Entwickler und Benutzer muss die folgenden Funktionen entsprechend den Systemanforderungen implementieren:

- Setzen Sie Passwörter für VNC über die VNC-Server-Verwaltung.
- Berechtigungen für UniApps über die Passwortverwaltung festlegen.
- Legen Sie Benutzer und Berechtigungen für Benutzerbildschirme über die Benutzerzugriffskontrolle fest.
- Legen Sie Benutzer und Berechtigungen für Web-Server-Bildschirme fest.

  Bei Systemen, bei denen das Herunterladen der Benutzeranwendung über ein Flash-Laufwerk oder eine SD-Karte erfolgt, muss darauf geachtet werden, dass die verschiedenen Passwörter an den vorgesehenen Stellen gesetzt werden.

2. Netzwerke

Sichere Kommunikation

a. **Steuerung als Internet-Client:** Wenn die Steuerung mit Komponenten oder Servern im Internet kommunizieren muss, stellen Sie sicher, dass die Steuerung als Client fungiert und die Kommunikation initiiert.

b. **Anschluss von Automatisierungsgeräten an das Internet:**

- Vergewissern Sie sich, dass sich alle Geräte hinter einer Firewall befinden und dass keine Firewall-Regeln vorhanden sind, die das LAN-Netz dem Zugriff aus dem WAN-Netz aussetzen.
  (unabhängig davon, ob es sich um einen Mobilfunk-Router oder ein kabelgebundenes Netzwerk handelt).
- Vergewissern Sie sich, dass es keine Portweiterleitungseinstellungen gibt, die Automatisierungsgeräte direkt mit dem öffentlichen Netz verbinden. Um einen Schutz auf Netzwerkebene schnell und einfach zu implementieren, empfiehlt sich die Verwendung von UCR-Produkten, der industriellen Router-Serie von Unitronics, die über eine integrierte Firewall- und VPN-Funktionalität verfügt. Für eine schnelle Verbindung siehe **Einrichten von VPN auf UCR-Produkten in vier Schritten.**

3. Vollständige Lösung

Sichere Verbindung - UniCloud-basiert

Die **UniCloud**-IIoT-Plattform von Unitronics ermöglicht eine sichere Verbindung, **ohne dass feste oder öffentliche Internet-IP-Adressen erforderlich** sind - für die Implementierung sind keine Cyber- oder IT-Vorkenntnisse erforderlich. Die Plattform enthält mehrere Ebenen fortschrittlicher Verschlüsselung und Schutz, die zusammen eine vollständige, sichere Lösung bieten, die es ermöglicht, den Zugriff durch Berechtigungsstufen zu beschränken und tatsächliche Verbindungen zu verfolgen.

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