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 Steuerungspersonal, das die Steuerungen programmiert und mit einem externen Netzwerk verbindet.

Unitronics bietet eine Vielzahl von Lösungen und Tools, die zur Risikominderung und zur Vermeidung von Sicherheitsverletzungen eingesetzt werden können. In diesem Dokument werden die wichtigsten Tools und Empfehlungen zur Erhöhung des Cyber-Schutzes von Automatisierungsprojekten und Maschinen, die auf Steuerungen der Serien Samba™ und Vision™ von Unitronics basieren, beschrieben.

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. **Zugriffsberechtigungen und Passwörter** - Kontrollieren Sie streng die Netzwerkzugriffsberechtigungen für das Steuergerät und die zugehörigen Geräte.

c. Verwalten und definieren Sie die **Fernzugriffsberechtigungen** entsprechend den Anforderungen des Systems und der Benutzer, um unnötige Risiken zu minimieren. Das PCOM-Protokoll (ein integriertes Kommunikationsprotokoll für Entwicklung und Verwaltung) ermöglicht beispielsweise Schutz auf verschiedenen Ebenen:

- Gesperrter Zugriff: Stellen Sie sicher, dass die Kontrolleure die Verbindung zu diesem Protokoll erst dann zulassen, wenn es nur noch zur Ansicht benötigt wird.
- Bediener: Einsehen und Aktualisieren von Daten.
- Techniker: Fehlersuche, Ändern von Steuerungseinstellungen und Aktualisieren von Versionen.

2. Sicherheit der 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 der Client ist, der 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 Port-Weiterleitungseinstellungen gibt, die Automatisierungsgeräte direkt mit dem öffentlichen Netz verbinden.

Um einen Schutz auf Netzwerkebene schnell und einfach zu implementieren, empfiehlt sich der Einsatz von UCR-Produkten, der industriellen Router-Serie von Unitronics, die über eine integrierte Firewall- und VPN-Funktionalität verfügt. Für eine schnelle Verbindung, siehe: **Definition von VPN in UCR-Produkten in 4 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