Are You Managing Your Security Risks?

As organizations look to leverage modern technologies with goals of improving their operational efficiency, industrial networks must be designed to provide the ability to provide seamless flow of information from control devices to enterprise systems. The emergence of these increasingly connected systems places a greater demand on design focusing on robust, fast, available and secure solutions. Rockwell Automation takes a holistic, systems-oriented approach to industrial security by providing expertise, products and professional services that help companies proactively assess and address potential security risks throughout their system. Using a "defense-in-depth" security approach, Rockwell Automation can help address internal and external security threats. This approach is based on implementation of multiple layers of security using both technical and non-technical solutions that allow you to mitigate both malicious and unintentional security threats. Rockwell Automation can help you secure your control system while continuing to provide the ability to leverage the use of a standard network and modern technologies.

1. **Remote Access**

   Do you need to communicate with a control system over a non-production network (e.g. public or business networks)?

   The Stratix 5900™ Services Router enables users the ability to protect their information using encryption technology permitting access to authorized users while still leveraging the existing untrusted network.

2. **Unauthorized Access**

   Have you ever lost production because someone made a change they weren't permitted to make (e.g. downloading a program to the wrong controller)?

   With FactoryTalk® Security, you can control the extent to which users can interact with your controllers.

3. **Intellectual Property Protection**

   Are you worried that your machines could be duplicated by your competitors?

   Logix Source Protection, a feature in Studio 5000™, enables you to assign a password to any Routine or Add-On instruction allowing for protection of the valuable intellectual property contained within the applications.

4. **Outside Hacker**

   Have you experienced performance issues or suspicious network traffic and suspect malicious activity, such as malware or a virus?

   With the Stratix 5900, enforce network segmentation and policy with the use of Access Control Lists and firewall features – ensuring only authorized users and appropriate traffic reach your control system assets.

5. **Unauthorized Changes**

   As a machine builder, have you ever been suspicious that your customers have made changes they weren't supposed to make? As an end user, have there ever been changes made to your system that went undetected for a long period of time?

   Using Controller Change Detection in Studio 5000, you can quickly detect changes to determine if any unauthorized modifications were made to your code.

Ten Actionable Steps

Enhance your industrial reliability and security with these ten actionable steps.

1. Control who has access to various areas of your network using features such as Access Control Lists and port blocking features.

2. Ensure robust and reliable operations by limiting and managing network traffic through the use of Firewalls and Intrusion Detection/Prevention Systems.

3. Protect PC assets by using anti-virus and application whitelisting. Reference material: *Achieving Secure, Remote Access to Plant-Floor Applications and Data*, Publication # ENET-WP009.

4. Establish a system patching policy to keep software up to date. Reference material: *Computer System Security Updates*, Publication # SECUR-WP002.

5. Develop security policies to manage the "human factor", for example: managing and protecting passwords, managing removable media and use of personal devices.

6. Implement a level of physical control by putting the key-switch on your Logix Controller in Run Mode.

7. Control who is allowed to do what from where in the application with FactoryTalk® Security.

8. Monitor what is going on in your system with Controller Change Detection and FactoryTalk® AssetCentre.

9. Protect your intellectual property with Logix Source Protection.

10. Limit access to automation equipment by implementing physical controls such as locking cabinets and doors.