Industrial Security Best Practices

Industrial control systems are comprised of connected and interrelated products configured to safely, securely, and reliably work together to accomplish a task.
Rockwell Automation recommends security as a key consideration in the design and operation of all industrial control systems. Good security practices help reduce system and control product susceptibility to accidental or unauthorized activities that affect safety, operational integrity and data confidentiality.

Layered Security

Industrial control system security relies on layers of security using multiple controls, methods and techniques that work together to help protect a system's assets, operations, and those who depend on its safe, reliable operation.
Technical controls, including physical and electronic mechanisms that compensate for risk, should be accompanied and balanced by non-technical controls such as company policies, procedures and guidelines.

Defense-in-Depth

For enhanced protection, a Defense-in-depth security strategy is applied to a system design to complement layered security technical and non-technical protective measures. This security posture uses diverse measures that operate as a deterrent and can slow and thwart unauthorized activities against a control system. Such an approach enhances the likelihood that threats are detected and prevented before reaching their goal.
The combination of a layered security model and the Defense-in-depth strategy are best practices which enhance the security posture of a control system and help protect against threats that can originate from inside or outside a control system environment.

Product and System Security

Industrial control products are essential components of a control system. Product security is critical to the control system and vice versa. To help protect key assets, Rockwell Automation recommends users (where possible) employ specific product-level security and protection features. Furthermore, products should be used in systems that apply security best practices, including layered security and a Defense-in-depth strategy.

Security Recommendations

Customers are encouraged to assess and mitigate risks to control systems, while remaining vigilant against potential security threats that may put people, property, and information at risk.

Reference Architectures for Manufacturing

Rockwell Automation Plantwide Reference Architectures Network Design Guides detail comprehensive methods that introduce layered security solutions to a control system architecture. More information about implementing validated architectures is available at http://www.ab.com/networks/architectures.html.

Network & Security Services

Rockwell Automation Network & Security Services consulting services are also available to assist with assessing and improving the state of security of industrial control systems that use Rockwell Automation and other vendor controls products. More information is available at http://www.rockwellautomation.com/services/security.

General Recommendations

- Restrict physical and electronic access to automation products, networks and systems to individuals authorized to be in contact with control system equipment.
- Evaluate firewall configurations to ensure non-essential traffic is blocked.
- Configure firewalls or access control lists (ACL) in the network infrastructure components (such as network firewall appliances and managed switches) to block access to the 17185/UDP port.
- Block all traffic to the EtherNet/IP or other CIP protocol based devices from outside the Manufacturing Zone by blocking access to TCP and UDP Port# 2222 and Port# 44818 using appropriate technology such as a firewall, UTM devices, or other security appliance.
- Follow a regimented, timely patch management process for all products.
- Use end-point protection software (e.g. antivirus, anti-malware) on control system PCs and keep all signatures up to date.
- Periodically and frequently change product passwords and discard previously used passwords.
- Establish rigorous policies and procedures so only authorized individuals have administrative rights on computers and other devices.
- Obtain all software, firmware and other related product-specific electronic content directly from trusted sources (product vendor preferred).

www.rockwellautomation.com

Power, Control and Information Solutions Headquarters

Americas: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
Europe/Middle East/Africa: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
Asia Pacific: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publication SECUR-AT001A-EN-E — May 2012