Rockwell Automation Security Governance Overview

Introduction

Rockwell Automation's cybersecurity program is based on a holistic strategy to ensure Rockwell Automation and its Connected Enterprise Ecosystem – the company's infrastructure, products, and customers - is safe, secure, and resilient. The program aligns to industry leading security standards / frameworks, which enables the enterprise to identify, protect, detect, respond, and recover from potential cybersecurity threats. The program also governs development and delivery of products, solutions, and services using secure, certified product and service lifecycles. This letter provides an overview of the governance program's controls used to protect Rockwell Automation's enterprise IT and OT environments, products, services, and solutions, and describes services that Rockwell Automation can offer to support any customer's potential security concerns.

Security Governance Framework

Rockwell Automation recognizes the importance of security in industrial control systems environments. While no company is 100% immune to an attack, Rockwell Automation continues to make significant investments in its people, processes, and technologies to mitigate the risks which potentially threaten Rockwell Automation and its customers. The cornerstone of Rockwell Automation's security governance program is the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). The NIST CSF is a risk-based approach aimed at managing cybersecurity risks. Based on the principles of Identify, Protect, Detect, Respond, and Recover, it focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's overall risk management strategy. Rockwell Automation has applied the framework to the following areas of its business:

- Enterprise Functional Operations
- Manufacturing Operations
- Product and Services Development

The framework is dynamic in nature allowing Rockwell Automation to internally and externally assess its level of maturity related to cybersecurity controls on a regularly reoccurring basis in order to continuously adapt to changing technologies, threats, and capabilities.

Security Organizational Structure and Personnel

Rockwell Automation manages cybersecurity risk as part of our overall Enterprise Risk Management program. Our strategy was developed and is being executed by security leaders from across the company, including our Chief Information Officer, Chief Information Security Officer, Chief Product Security Officer, VP General Manager Customer Support and Maintenance, and VP General Manager Systems and Solutions Business, with support from our business leaders and liaisons within each business unit and function, and with oversight by the board of directors. These organizations work together in alignment to the NIST CSF in order to ensure Rockwell Automation operates with a security focus on its enterprise operations as well as its development of products, applications, and services. Rockwell Automation has also established an Executive Security Council (ESC) composed of members of Rockwell Automation's senior level management who provide additional oversight to the security strategy program.

Identify, Protect, Detect, Respond, and Recover Capabilities

Protection from cyber attacks is multi-faceted, involving a mix of people, processes, and technology. Rockwell Automation's operational response to an attack encompasses four dimensions, all linked to the NIST CSF:

1. **Coordinated Security Controls and Process:** Rockwell Automation operates a cyber defense capability to identify emerging threats, detect intrusions, initiate containment, and perform remediation activities. Threat intelligence from governmental, vendor, supplier, and relevant trade associations supplement these efforts, especially in the areas of threat identification and mitigation.
2. **Enterprise-Wide Defense in Depth:** Perimeter controls consist of next generation application layer firewalls with integrated controls. Firewalls are actively and centrally managed with full vendor support. Regional datacenters are protected with network-based controls and are vendor managed with threat profiles maintained via human and machine intelligence. Endpoints are fully encrypted running both signature-based antivirus and next generation threat detection software agents.
3. **A Focus on Protecting Our Mission-Critical Assets:** Rockwell Automation utilizes a four-level information classification procedure in order to identify and protect mission-critical assets. Formal policies, standards, configurations and processes are in place for the development and hardening of systems, including penetration testing, in order to minimize any potential attack surface. In addition, capabilities related to the discovery of system, network, and endpoint vulnerabilities are closely coordinated with solution and application vendors.
4. **The "Human Element":** Rockwell Automation's employees are a key element in the secure operation of its business. Screening is performed on all new employees and contractors prior to employment. Formal information security training is required to be completed upon hire and on an annual basis after hire. Security training is regularly refreshed with new content in order to keep up with the latest security threats and allow for the renewal of employee acceptance to security policy. Additional training modules are also required based on employee job function as necessary. Phishing assessments are conducted regularly in order to promote efficient phish reporting and prevent potential attacks from occurring. Employee access to sensitive systems or information is reviewed bi-annually with a default action of revocation unless appropriate business justification exists. Overall, it is expected that every employee and contractor act as a "Human Firewall" while performing his or her workday responsibilities.

Incident Response

Rockwell Automation maintains a 24x7 Security Operations Center (SOC) that utilizes industry leading security information and event management (SIEM) software to monitor and detect any incidents relating to its infrastructure, applications, and information. All security related incidents are handled through an incident response procedure operated and maintained by the Cybersecurity Incident Response Team (CSIRT). Incidents are initially reviewed and assigned an appropriate severity level in order to determine appropriate response procedures. Any significant cybersecurity incident or potential significant incident invokes the Cyber Crisis Management Team. This is a cross-functional team composed of members from CISO, Cyber Defense, Product Security, IT, Customer Support and Maintenance, Legal, information security business liaisons, and communications specialists. This specialized team is convened to immediately prioritize the handling of the incident or to fully investigate a potential incident or attack vector. From a customer perspective, this team actively works with Rockwell Automation's customer facing employees or teams as necessary. Rockwell Automation harmonizes its internal response with the experiences and needs of its customers depending on the nature, extent, and impact of a given incident from identification through resolution.

Software Development and Download Integrity

Rockwell Automation maintains an ISA/IEC 62443-4-1 third party-certified software development lifecycle process. ISA/IEC 62443-4-1 is a specialized industrial automation-based security certification that requires a formal lifecycle that is institutionalized across development teams and includes security requirements definition, secure design, secure implementation, verification, validation, defect management, patch management, vulnerability management, and product end-of-life management. Rockwell Automation also employs several layers of security to protect its software that is available for customer download from its managed web sites. Digital signatures are used in non-legacy product firmware and software (Microsoft Authenticode) which can be used to verify software authenticity. Rockwell Automation has also published guides for Microsoft Applocker and Symantec CSP, which assist customers in properly verifying software authenticity. Keys used for the creation of digital signatures are stored in highly restricted, access-controlled, and encrypted hardware security module (HSM) devices. Digitally signed and authentic software installation files are hosted and made available for download by Akamai, a highly respected secured content delivery network provider. Lastly, all software downloads from managed sites occur over an encrypted HTTPS / TLS file transfer connection providing confidentiality and integrity of the software content in transit.

Secure Remote Service Connections

Rockwell Automation's Secure Remote Access Platform for applicable services consists of multiple security layers. Authentication is where it starts. All users have a preconfigured role that only allows access to predefined sites and assets. Authentication methods consist of centralized access control, dual authentication between the server and the site, role-based visibility and access by user/site/device, complete end-user control, surveillance, and audit logs.

Security of the connection is equally important, so all remote connections are compliant with Converged Plantwide Ethernet (CPwE) practices. In addition, Rockwell Automation does not require bi-directional communication through a given customer's firewall. Only a single outbound port with acknowledgment is required. The data is protected with SSL data encryption and multiple security certificates between Rockwell Automation's servers and onsite agents. Finally, Rockwell Automation's remote connections are brokered through a hosted Service Center. This means that a direct connection is never made between a remote worker's computer and the remote site.

How Rockwell Automation Can Partner with Its Customers on Cyber Security

Rockwell Automation offers various services to assist in addressing its customer's security concerns. A few of those offerings include the following:

- **Qualified Patch Management Services:** Provide Rockwell Automation tested and approved anti-virus definitions and Microsoft Windows patch lists to a customer's on-site WSUS responsible for managing patches of the implemented ICS software systems (FactoryTalk Software). This will allow for a timely and disciplined approach to keeping up to date with the latest anti-virus signature files and addressing operating system related vulnerabilities. (Additional management options available)
- **Security Assessment:** Evaluate and understand risk posture of an ICS environment to identify areas of improvement against established ICS Cyber Security Standards such as ISA/IEC 62443, NIST 800-82 and NIST CSF.
- **Anomaly and Threat Detection Services:** Provide visibility into control systems, protocols and networks, real-time monitoring and analytics to detect anomalies and threats that may impact the security and operational integrity of an ICS environment.
- **Incident Response:** Partner with security firms to help customers respond to incidents in the event of a breach.
- **TechConnect:** Receive knowledgebase email alerts on Rockwell Automation product security with access to the latest software and firmware updates.
- **Application White Listing:** Validate and only allow explicitly permitted applications to execute.
- **Security Control Implementations:** Provide turnkey implementation of security controls that help address gaps/risks that have been identified in specific areas such as zone-based segmentation, device hardening, threat/anomaly detection and network access control.
- **Network Assessments:** Perform on-site visit to collect data, identify issues, and analyze the gap with industry best practices in order to ensure all infrastructure is meeting the availability requirements of an ICS environment.
- **Network Design and Implementation:** Provide a turnkey network infrastructure which is scalable, resilient and future ready, based on industry best practices such as Converged Plantwide Ethernet (CPwE).
- **iDMZ Design and Implementation:** Secure the data flow between enterprise systems and plant systems, plus optionally setup secure remote access for OEMs and vendors.
- **FactoryTalk Security:** Consult on how to best utilize the security features available through Rockwell Automation products.
- **Remote Monitoring and Administration:** Converged IT/OT monitoring and administration support of infrastructure, end nodes and industrial applications throughout their lifecycle.