Industrial Control System (ICS) Cybersecurity Best Practices

Author: Michael Amiri, Senior Analyst

Critical infrastructure is increasingly in the crosshairs of threat actors, especially as geopolitical tensions continue to exacerbate worldwide. A cyberattack on critical infrastructure could potentially disrupt a country's ability to function. Envisioning the devastating effects of a full-fledged cyberattack on critical infrastructure is not hard to imagine, as distressing as it may be.

Railroads would shut down.

Homes wouldn't receive any heat.

Supermarket shelves wouldn't be stocked.

Preventing these doomsday scenarios requires a well-guarded Industrial Control System (ICS)—the heart of critical industrial operations. This guide provides a comprehensive gameplan for companies to protect their ICSs as they contend with increasingly complex tactics from cyber threat actors. More specifically, this guide assesses best practices for securing your ICS from both the endpoint and network standpoint.

How to Secure ICS Endpoints

In this section, I'll explain some ICS hardening solutions that effectively protect ICS endpoints from cyber threats.

Endpoint Detection and Visibility

Given the long life spans of an industrial control system, bolstering the security of legacy ICS equipment is paramount. But, as ICS security research **shows us**, bolt-on security is more vulnerable to an attack than built-in ICS.

To secure legacy ICS network endpoints, industrial companies can use the following methods and strategies:

- **Segment the legacy ICS** by using firewalls, Virtual Local Area Networks (VLANs), and air gapping techniques. This will limit access to the system.
- **Shrink the attack surface** by disabling unnecessary devices and network connection protocols.

- **Improve authentication** by implementing access control, strong passwords, or Multi-Factor Authentication (MFA) for questionable, unverified, or untrusted devices and platforms.
- **Conduct regular security assessments** for legacy ICSs to help identify weak points. That will enable you to apply appropriate security measures, including patching where possible.

Identity, Authentication, and Access Management Technologies

As industrial companies digitally transform their operations, digital Identity Access Management (IAM) technologies are gaining popularity for safeguarding industrial control systems.

Trusted Platform Modules (TPMs) are also a mainstay for ICS security. The usefulness of TPMs in industrial control system security is in their ability to store cryptographic keys securely. TPMs authenticate devices and verify that the firmware and software within the ICS environment can be trusted.

Proper Device Onboarding

Using the pre-configured credentials of ICS components presents a security vulnerability. If, for example, your organization receives a shipment of **PLCs**, be sure to change their credentials and configure them before putting them to use. Having stronger passwords is a critical enabler in protecting industrial control systems.

Proper device onboarding is also essential for integrations and functionality within the ICS. When devices are not adequately onboarded, there's a greater risk of display communication hindrances with other devices in the ICS environment.

Patch Management and Hot Patching

With cyber threats **on the rise**, updating and patching the devices and networks associated with your industrial control system is one of the best ways to circumvent attacks from malicious actors. You must:

- Identify where vulnerabilities lie in your ICS network.
- Conduct a detailed inventory of all ICS devices.
- Consider hot patching to avoid operational downtime when updating the ICS.

Next, we share how companies can secure their ICS at the network level.

Securing the ICS at the Network Level

The following best practices will help ensure that your industrial control system network is secure in the age of Industry 4.0.

Promote Network Visibility

Through various interviews with industrial stakeholders, ABI Research has learned that network visibility is the highest ICS security priority. Companies can promote network visibility by mapping the network with port scanners and network mapping software to identify network topology, system configurations, and communication patterns.

Monitor Network Data Flows

Monitoring data flows within the network is imperative to identify when malware has infiltrated the industrial control system. For example, the Stuxnet worm and the Havex Trojan malware both use data packets to attack ICSs.

Set up Firewalls and Unidirectional Flows

Firewalls, such as Cisco's Firepower Next-Generation Firewall and Adaptive Security Appliance (ASA), are an effective ICS security solution. Firewalls are an established market with many vendors offering ICS protection solutions. Moreover, unidirectional gateways provide better ICS security, but are substantially more expensive.

Leverage Machine Learning (ML)

Recent research into ML strategies for industrial control system security **has shown** promising results for intrusion detection in the ICS environment. This is particularly important in detecting cyberattacks in mobile cloud computing. ML-based intrusion detection schemes are reportedly a superior cybersecurity technique to current "rule-based" security schemes.

Set Honey Pot Traps

In the context of ICS security, a honeypot refers to a fake network that lures would-be attackers of the actual network. It's important that the attacker genuinely believe the *real* ICS has been infiltrated. For example, the "honeypot" could pretend to be a Programmable Logic Controller (PLC) and enable the attacker to acquire control of it. This security best practice keeps the ICS safe by diverting the attacker's attention from critical aspects of the system. Honeypots can either be low-interaction or high-interaction, with the latter **requiring much more resources**.

Next Steps

As recent headlines **allude to**, industrial control systems are highly vulnerable to cyberattacks. As threat actors become smarter and more sophisticated, industrial companies and their cybersecurity service partners must leverage innovative solutions and proven ICS security best practices.

To help you on the journey, subscribe to ABI Research's **Industrial Cybersecurity Research Service**. Access to our global team of analysts means your organization will get its hands on Analyst Insights, various market forecasts, and long-form research reports that discuss the latest industrial security challenges, solutions, market outlooks, vendor profiles, and more.

Related Content

- 9 Accomplished ICS Cybersecurity Companies That Can Protect Your Industrial Operations from Attacks [Blog]
- ICS Protection from Cyberthreats: What Will It Take? [Research Highlight]
- What Is Intellectual Property Theft, and How Can Manufacturers Prevent It? [Blog]