Cybersecurity Best Practices

Document B0852AB_A

Executive summary

This whitepaper describes 12 basic cybersecurity recommendations that can help users of Schneider Electric Industrial Automation Control Systems reduce exploitable weaknesses and defend against avoidable data breaches and cyberattacks. The information presented here is derived from various sources, including the U.S. Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), the FBI, and the Information Technology ISAC.

Contents

Get Everyone Involved

1. Involve Executives in Cybersecurity
2. Implement an Employee Cybersecurity Awareness Program

Be Proactive, Be Prepared

3. Maintain an Accurate Inventory of Control System Devices to Minimize Equipment Exposure to External Networks
4. Use Secure Remote Access Methods
5. Implement Network Segmentation and Apply Firewalls
6. Establish Role-Based Access Control and Implement System Logging
7. Require Strong Passwords and Add Password Security
8. Develop and Enforce Policies on Mobile Devices

Be Vigilant

9. Maintain Awareness of Vulnerabilities and Implement Patches and Updates
10. Implement Measures for Detecting Compromises
11. Develop a Cybersecurity Incident Response Plan
12. Maintain Current Backups for Faster Data Recovery

Get Everyone Involved

Best practices to ensure everyone – executives and employees – are aware of cybersecurity issues

1. Involve Executives in Cybersecurity

A third of security survey respondents say C-level executives are never updated on security incidents.

Researchers have found that organizational leaders often lack sufficient awareness of cybersecurity threats and needs. This is surprising, given the continued proliferation of cyber threats and the far-reaching effects of cyberattacks. Cyphort and the Ponemon Institute published a study in March 2016 titled The State of Malware Detection and Prevention that identified serious challenges organizations face in preventing and detecting cyber attacks and prioritizing and investigating malware alerts. Only 36 percent of respondents say IT and others who are responsible for cybersecurity have the necessary information to make the C-suite aware of advanced threats. The report also notes that 34% of respondents say C-level executives are never updated on security incidents.

While organizations are increasingly elevating cybersecurity to the executive level by adding the role of Chief Information Security Officer (CISO), many organizations remain unprepared for cyber threats. IBM's paper, Securing the C-Suite, surveyed 700 executives worldwide to assess how well non-technical executives understand cyber threats. The results identified four signs that an organization is not prepared for cybersecurity threats: 1) misidentification of the actual threats, 2) lack of a chief information security officer (CISO), 3) not including all C-suite members in cybersecurity planning, and 4) a reluctance to share information about cybersecurity threats with external organizations.

Cybersecurity Questions for CEOs (US-CERT)

ICS Cybersecurity for the C-Level (ICS-CERT)

2. Implement an Employee Cybersecurity Awareness Program

Provide initial and periodic cybersecurity training to your employees to help keep your organization secure. Stress safe internet browsing and explain attacks methods directed at employees.

Cybersecurity is extremely important for critical infrastructure sectors that operate Industrial Control Systems, because these systems are increasingly being targeted. When employees aren't involved in cybersecurity, vulnerabilities and threats can go unnoticed more easily. Your employees can unintentionally become conduits through which attacks are executed. To prevent these situations, provide initial and periodic cybersecurity training to your employees to help maintain the security of the organization as a whole.

Certain cybersecurity topics should be emphasized for general awareness. One key topic is social engineering, which involves emails ("phishing"), phone calls, or other types of personal interactions. These methods continue to be popular ways for cyber criminals to prey upon unsuspecting employees. Malicious actors attempt to entice employees into providing sensitive personal or corporate information, such as account passwords or details about information technology infrastructure. Sometimes these actors attempt to make employees pay for alleged services, download infected attachments, or visit malicious websites. Employees need to be aware that they must view unsolicited emails, phone calls, and other correspondence from unknown senders with particular caution.

Among the key points in Booz Allen Hamilton's Industrial Cybersecurity Threat Briefing for 2016, one-third of ICS operators around the world were breached in 2015 and spear phishing was the primary method of attack. In spear phishing incidents, the vulnerabilities were the users who were compromised through social engineering. The primary threats included ransomware targeting ICS operators, the sale of access to SCADA systems as a service, freely available attack resources, attacks against the supply chain, and improper access control. The briefing included detailed descriptions of incidents per sector, and also mitigation practices.

Employee training should also stress the importance of smart Internet browsing practices. Visiting suspicious websites may expose users to infection by malware embedded on the site (a "drive-by download" attack). Even legitimate websites, as well as the files on them, may be compromised. Cyberattackers may employ a variation of this type of tactic, a "watering-hole" attack, to target the employees of a company they know will visit the website. Therefore, exercising caution is critical everywhere a user navigates and with any materials that are downloaded.

Avoiding Social Engineering and Phishing Attacks (US-CERT)

Recognizing and Avoiding Email Scams (US-CERT)

Be Proactive, Be Prepared

Best practices to implement today to help prevent cyberattacks

3. Maintain an Accurate Inventory of Control System Devices to Minimize Equipment Exposure to External Networks

Eliminate superfluous channels between devices on the Industrial Control System and any external networks.

Organizations are encouraged to conduct thorough assessments of their Industrial Control Systems, including the corporate enterprise segments. After completing an inventory of your systems, machines, and software, you can eliminate any elements that are not serving a purpose. Reducing your footprint will reduce your attack surface, making it harder for malicious actors to find a vulnerability to exploit.

It is important to manage the risks in connecting any machine on an Industrial Control System (ICS) to a machine on a business network or to the Internet. Even though your ICS may not directly face the Internet, pathways may exist. If any ICS systems are connected to a different part of the network, like the corporate side, you have a communications channel to external (non-trusted) resources (the Internet). While you may not even realize a connection exists, a persistent cyber threat actor can find these pathways and use them to access and exploit systems to try to create a physical consequence. To reduce network vulnerabilities, eliminate superfluous channels between devices on the control system and equipment on other networks. Follow cybersecurity best practices to protect communication throughout your organization.

ICS-ALERT-11-343-01A Control System Internet Accessibility

CIS Contols - Inventory of Authorized and Unauthorized Software

4. Use Secure Remote Access Methods

Implement a secure method for remote users to access your network, such as a VPN.

Implement a secure method for remote users to access your network, such as a Virtual Private Network (VPN). A VPN is an encrypted data channel for securely sending and receiving data via public IT infrastructure (such as the Internet). Through a VPN, users can remotely access internal resources like files, printers, databases, or websites as if directly connected to the network. However, your VPN is only as secure as the devices connected to it. A laptop computer infected with malware can introduce those vulnerabilities into the network, leading to additional infections and negating the security of the VPN. You can further harden remote access by reducing the number of Internet Protocol (IP) addresses that access the VPN. You can set up network devices and firewalls to allow only specific IP addresses and/or ranges and from within the U.S.

Virtual Private Networking – An Overview (Microsoft)

5. Implement Network Segmentation and Apply Firewalls

Restrict access to network areas by isolating them entirely or by implementing firewalls.

Network segmentation entails classifying and categorizing IT assets, data, and personnel into specific groups, and then restricting access to these groups. By placing resources into different areas of a network, a compromise of one device or sector will not compromise your entire system. Otherwise, cyber threat actors would be able to exploit any vulnerability within your organization's system – the "weakest link in the chain" – to gain entry and move laterally throughout a network and access sensitive equipment and data. The "Internet of Things" now links more devices to systems and the web, including many devices previously not Internet-connected, such as video cameras and HVAC systems. Adding more connected devices makes it even more important to segment your networks.

Restrict access to network areas by isolating them entirely from one another, which is optimal in the case of Industrial Control Systems, or by implementing firewalls. A firewall is a software program or hardware device that filters the inbound and outbound traffic between different parts of a network, or between a network and the Internet. For connections that face the Internet, a firewall can be set up to filter incoming and outgoing information. Reduce the number of pathways into and within your networks and implement security protocols on the pathways that do exist so it is more difficult for a threat to enter your system and gain access to other areas.

Creating network boundaries and segments empowers your organization to enforce both detective and protective controls within your infrastructure. The capability to monitor, restrict, and govern communication flows provides a practical way to baseline network traffic (especially traffic crossing a network boundary) and to identify abnormal and potentially malicious behavior. Boundaries and segments provide opportunities to detect movement from device to device within a specific zone or movement across zones. You can also spot network footprinting and enumeration as hackers try to determine the best entry points to your network.

Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies (ICS-CERT)

Guidelines for Application Whitelisting in Industrial Control Systems (ICS-CERT)

6. Establish Role-Based Access Control and Implement System Logging

Limit employee permissions through role-based access control and add logging to monitor system activity.

Role-based access control grants or denies access to network resources based on job functions. This type of control limits the ability of individual users – or attackers – to reach files or parts of the system they should not access. For example, SCADA system operators likely do not need access to most administrative files or to the billing department. Define permissions based on the level of access each job function needs to perform its duties. Work with human resources to implement standard operating procedures to remove network access from former employees and contractors. Implementing strict role-based access control allows better auditing and reduces risk by minimizing the privileges associated with each group.

Implementing a logging capability allows you to monitor system activity. This enables you to find the sources of issues in the system, which may have been the activities of an employee or an outsider. Monitoring network traffic also helps your organization determine if a user is making unauthorized actions or if an outsider is in the system, providing opportunities to intervene before problems are manifested.

Targeted Cyber Intrusion Detection and Mitigation Strategies (ICS-CERT)

7. Require Strong Passwords and Add Password Security

Require longer, stronger passwords and consider multi-factor authentication.

Require the use of strong passwords to keep your systems and information secure. Force users to have different passwords for different accounts. Hackers can use readily available software tools to try millions of character combinations to attempt an unauthorized login – this is called a "brute force attack." Passwords should have at least eight characters, but longer passwords are stronger, because of the greater number of characters to guess. Require users to include uppercase and lowercase letters, numerals, and special characters.

Change default passwords when new software is installed, particularly for administrator accounts and control system devices, and regularly after that. Add password security features, such as an account lock-out that activates when too many incorrect passwords have been entered. Consider adding multi-factor authentication so users must verify their identities whenever they sign-in. Users receive a code on a device they previously registered and then cannot sign in until they enter the code.

Choosing and Protecting Passwords (US-CERT)

8. Develop and Enforce Policies on Mobile Devices

Ensure that mobile devices in your workplace cannot be easily exposed to malicious actions.

The proliferation of laptops, tablets, smartphones, and other mobile devices in the workplace presents significant security challenges. Mobile devices are potentially exposed to external, compromised applications and networks and malicious actors. Also, contributing to this challenge is the policy of allowing employees to use their personal electronic devices for work – "Bring Your Own Device (BYOD)".

It is important to develop policies for use of mobile devices in your office and on your networks. These measures should be strictly enforced for all employees and contractors. Devices should be password protected to ensure only authorized users can log in. This prevents unauthorized users from accessing restricted networks and files using an authorized user's device. Employees should avoid or be cautious about using devices that do not belong to them, because they may not be properly protected or comply with established policy. These devices may even be infected, and using them could put your organization's information and networks at risk.

Cybersecurity for Electronic Devices (US-CERT)

Be Vigilant

Best practices to help keep things running safely and smoothly

9. Maintain Awareness of Vulnerabilities and Implement Patches and Updates

Implement a monitoring system to be sure you always apply the latest patches and updates.

Most vendors work diligently to develop patches for identified vulnerabilities. Even after patches and updates are released, many systems remain vulnerable because organizations are either unaware of or choose not to implement these fixes. Effective patching can also stop a large number of attacks, considering that the top ten cyber vulnerabilities accounted for 85% of successfully exploited traffic.

In its 2016 Data Breach Investigations Report, Verizon found that in most industries, 75% of incidents and breaches are covered by only three patterns. For utilities, these patterns were cyber espionage, crimeware, and denial of service. Verizon suggested that understanding the building blocks of an attack (e.g., a kill chain) can help organizations construct defenses and detect a breach.

To protect your organization from these opportunistic attacks, implement a system of monitoring for and applying system patches and updates. Schneider Electric regularly posts information on vulnerabilities and patches that it receives from its partners at the U.S. Department of Homeland Security's ICS-CERT and United States Computer Emergency Readiness Team (US-CERT), other ISACs, and cybersecurity firms, among others. These updates are designed to fix known vulnerabilities and are strongly encouraged for any Internet-connected device.

Recommended Practice for Patch Management of Control Systems (ICS-CERT)

10. Implement Measures for Detecting Compromises

Monitor logs from firewalls, intrusion detection and prevention sensors, and servers for compromises.

Despite the many preventive measures organizations implement, many still experience compromises. Indeed, many cybersecurity experts have noted that experiencing a compromise is not really a question of "if," but more of a question of "when." When a compromise occurs, the organizations that fare the best will be those that quickly detect the issue and have a plan in place to respond.

Implementing measures such as intrusion detection systems (IDSs) and intrusion prevention systems (IPSs), anti-virus software, and logs (each described in the links following #4) can help detect compromises in their earliest stages. Most IDSs and IPSs use signatures to detect port scans, malware, and other abnormal network communications. New viruses are discovered daily and anti-virus programs are usually set to look automatically for the latest threat signatures. Still, you should not rely solely on anti-virus software for detecting infections. You should monitor logs from firewalls, intrusion detection and prevention sensors, and servers for signs of infections.

Maintenance, Monitoring, and Analysis of Audit Logs

11. Develop a Cybersecurity Incident Response Plan

Your Incident Response Plan should result from collaboration among all stakeholders potentially affected by a cybersecurity incident.

Incident response plans are a critical and underutilized component of emergency preparedness and resilience. An effective cybersecurity incident response plan will limit damage, increase the confidence of partners and customers, and reduce recovery time and costs. Your plan should include measures for reacting to destructive malware in an ICS environment. In this situation, you should be prepared to isolate your ICS environments by disconnecting from non-ICS networks. You should be capable of going to “manual operations” if necessary. As an example, if network conditions impact visibility from the SCADA system, malware could render control devices inoperable by automated means.

Rather than being developed by a single entity, the plan should be a product of collaboration among all departments that would be stakeholders in a cybersecurity incident. This will ensure a cooperative and unified response that leverages all of your organization’s resources to the greatest extent possible. For enhanced responsive capability in the event of a cybersecurity incident, your organization should consider forming a Computer Security Incident Response Team (CSIRT).

This task is not complete once the plan has been developed. It is critical that plans be routinely reviewed and updated to ensure they remain relevant and usable when they are needed. To truly understand the cybersecurity incident response plan, your organization must practice through regular exercises. This will ensure that all stakeholders understand the procedures to be implemented in the event of a significant cyber disruption or breach, enabling an effective and efficient response.

Preparing for Cyber Incident Analysis (ICS-CERT)

12. Maintain Current Backups for Faster Data Recovery

The simplest way to handle a machine encrypted by malware is by restoring from a backup.

Backups are the single most effective way to recover from a malware attack. Ensure that each system is backed up at least weekly, and more often for systems storing sensitive information. To enable you to rapidly restore a system from backup, be sure include all critical software and data on each machine in the backup procedure. All items you back up do not have to be included in the same backup file or use the same backup software. Ensure you have multiple backups over time, so that in the event of malware infection, you can restore from a version that predates the original infection.

Confirm that your backup policies are compliant with any regulatory or official requirements.

CIS Controls: Data Recovery Capability

Resources

Booz Allen Hamilton Industrial Cybersecurity Threat Briefing for 2016
https://www.slideshare.net/BoozAllen/booz-allen-industrial-cybersecurity-threat-briefing

Center for Internet Security (CIS) Top 20 Critical Security Controls
https://www.cisecurity.org/cybersecurity-best-practices/

FBI Cyber Crime
https://www.fbi.gov/investigate/cyber

Guide to Industrial Control Systems (ICS) Security
https://www.nist.gov/publications/guide-industrial-control-systems-ics-security

Industrial Control Systems Cyber Emergency Response Team
https://ics-cert.us-cert.gov/

The State of Malware Detection and Prevention
http://go.cyphort.com/Ponemon-Report-Page.html

Virtual Private Networking: An Overview
https://msdn.microsoft.com/en-us/library/bb742566.aspx

WaterISAC Water Security Network
https://www.waterisac.org

Contact Us

For more information, refer to the Schneider Electric Cybersecurity Support Portal:
http://www.schneider-electric.com/b2b/en/support/cybersecurity/overview.jsp

© 2017 Schneider Electric. All rights reserved.
Schneider Electric and Life Is On Schneider Electric are trademarks owned by Schneider Electric SE or its affiliated companies. All other trademarks are the property of their respective owners.