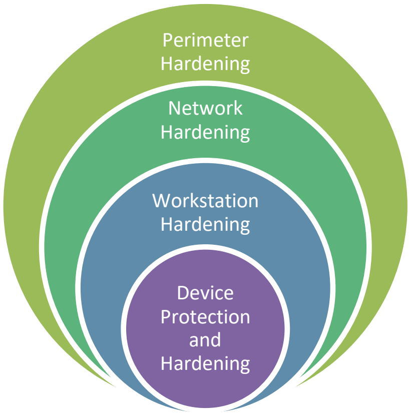
Read This First: Recommended Cybersecurity Best Practices

Schneider Electric Is Focused on Cybersecurity

Schneider Electric incorporates cybersecurity best practices and solutions in our products, systems, and services. Our security by design approach makes our products more resilient against cyberattacks. We implement mechanisms to mitigate threats, reduce exploitable weaknesses, and defend against avoidable data breaches and cyberattacks.

Recommended Cybersecurity Best Practices



To help keep your Schneider Electric products secure and protected, we recommend that you implement these cybersecurity best practices. Following these recommendations may help significantly reduce your company's cybersecurity risk.

Perimeter Hardening

Set up firewalls

Always place Schneider Electric systems and devices behind firewalls and other security protection appliances that limit access to only authorized remote connections. Building a highly protected network that helps prevent outside access is the most critical line of defense against cyberattacks. We recommend that you follow these guidelines.

- Limit access to the networks on which Schneider Electric devices are placed.
- Ensure that Schneider Electric systems and devices are not accessible from the internet, unless placed behind firewalls and other security protection appliances.
- Restrict external network connectivity to your systems and devices.
- Continually monitor for events that might indicate attempted unauthorized access.
- Limit access to internal networks where devices reside.
- Isolate control and safety system networks and remote devices from the business network.

Network Hardening

Implement secure access controls

Reduce the pathways into and within your networks and implement security protocols on the existing pathways to make it more difficult for a threat to enter your system and gain access to other areas. Be sure that all laptops and other systems that have been connected to any other network are properly sanitized, with fully updated software programs and antivirus protection. Consider splitting your networks and devices into groups isolated from one another and restricting access.

Use secure remote access methods

Implement secure methods for remote users to access your network. Require all remote users to connect and authenticate through a single, managed interface before conducting software upgrades, maintenance, and other system support activities.

Set up measures for detecting compromises

Minimize the chances of compromise by monitoring and auditing system events 24/7. Use intrusion detection systems (IDSs), intrusion prevention systems (IPSs), antivirus software, and usage logs to help you detect compromises in their earliest stages. Despite implementing these preventive measures, you may still experience compromises. Have a plan in place to quickly detect the issue and respond.

Workstation Hardening

Implement strong authentication and authorization controls

Change default passwords when new software is installed and regularly after that. This is particularly important for administrator accounts and control system devices. Use role-based access with multi-factor authentication to help prevent security breaches and provide a log of access activity. Consider adding password security features, such as an account lockout that activates when too many incorrect passwords are entered.

Set up blacklisting to deny access to known suspicious or malicious entities

Blacklisting can help prevent known viruses, spyware, Trojans, worms, and other kinds of malware from accessing your system. Antivirus tools, spam filters, intrusion detection systems, and other security software commonly incorporate blacklisting to help control access. One of the biggest advantages of blacklisting is its simplicity. Any entity not on the blacklist is granted access, but anything that's known or expected to be a threat is blocked. Most organizations use lists created by third parties, such as security service providers. In addition, you should create your own blacklist of users, IP addresses, applications, email addresses, domains, and anything else you want to keep off your system.

Add whitelisting to help keep your systems safe from unwanted software

Add whitelisting software to your defenses to help ensure only software you know and trust is allowed to run on your workstation. Whitelisting software works with your blacklisting software to allow only known software to run. Adding whitelisting software helps you be more confident that installed files and loaded executables have maintained their integrity and are authentic. This additional protection results in a higher degree of trust for the workstation by helping to prevent sophisticated attacks.

Encourage secure workstation habits

Everyone in your company can contribute to cybersecurity efforts by keeping their workstations as safe as possible. Scan any devices used to exchange data, such as external hard drives or USB drives, before using them in any node connected to the network. Remove unnecessary programs and services from workstations and store sensitive data on a server. Regularly back up data from hard drives. Finally, be sure everyone gets into the habit of locking their screen when they aren't in use.

Device Protection and Hardening

Install physical controls to help prevent unauthorized access

While this isn’t just a cybersecurity issue, it’s important to put physical controls in place so that no unauthorized person can access your equipment. Keep all controllers in locked cabinets and limit access to any connected devices.

Check the documentation for product-specific information

Schneider Electric provides detailed information with every product. Review the product guides on the Schneider Electric website or that accompany your products to find cybersecurity recommendations and best practices directly related to your Schneider Electric products.

More Best Practices to Help Minimize Your Risk

Manage 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 stop a large number of attacks, so implement a monitoring system to be sure you always apply the latest patches and updates for operating systems, antivirus tools, and any other software.

Be aware of vulnerabilities

Schneider Electric regularly posts security notifications with information on vulnerabilities and patches that it receives from entities such as the U.S. Department of Homeland Security’s ICS-CERT, Computer Emergency Readiness Teams (CERTs) from various countries, cybersecurity ISACs (Information Sharing and Analysis Centers) around the world, and cybersecurity firms. These updates are designed to fix known vulnerabilities and are encouraged for any Internet-connectable device. You can also subscribe to our newsletter to receive security notifications.

Maintain current backups and test your recovery procedures

Backups are the most effective way to recover from a malware attack. In addition to backing up systems and data frequently, it is important to test your recovery procedures. Confirm that you have multiple backups over time, so you can restore from a version that predates any infection.

Train your people

Provide cybersecurity training to your employees to help keep your organization secure. Explain phishing emails, infected attachments, malicious websites, and other methods that attack them directly. Require any contractors or managed services vendors to complete the equivalent cybersecurity training.

For More Information and Assistance

For details and assistance on protecting your installation, contact your local Schneider Electric Industrial Cybersecurity Services organization or see Cybersecurity Services on the Schneider Electric website.

For additional information on cybersecurity best practices, review these resources.

Quick Start Guide: An Overview of the ISA/IEC 62443 Series of Standards
ISA Global Cybersecurity Alliance (ISAGCA)

Cybersecurity Best Practices
Center for Internet Security

IEC 62443 Security for Industrial Automation and Control Systems
International Society of Automation (ISA)

e-Guide: Building a Cybersecurity Strategy for the Digital Economy
© 2019 Schneider Electric

Cybersecurity by Design: Building a Company Culture to Strengthen a Digital Business
© 2019 Schneider Electric

Document download:
https://www.se.com/ww/en/download/document/CS-Best-Practices-2019-340/
https://www.se.com/us/en/download/document/7EN52-0390/

Document # 20765160 - June 2020

THIS DOCUMENT IS INTENDED TO HELP PROVIDE GENERAL SECURITY RECOMMENDATIONS AND IS PROVIDED ON AN “AS-IS” BASIS WITHOUT WARRANTY OF ANY KIND. SCHNEIDER ELECTRIC DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL SCHNEIDER ELECTRIC BE LIABLE FOR ANY DAMAGES WHATSOEVER INCLUDING DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF SCHNEIDER ELECTRIC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE USE OF THIS DOCUMENT, INFORMATION CONTAINED HEREIN, OR MATERIALS LINKED TO IT ARE AT YOUR OWN RISK. SCHNEIDER ELECTRIC RESERVES THE RIGHT TO UPDATE OR CHANGE THIS DOCUMENT AT ANY TIME AND IN ITS SOLE DISCRETION.