Read This First: Recommended Cybersecurity Best Practices

Schneider Electric Is Focused on Cybersecurity

Schneider Electric has incorporated cybersecurity best practices and solutions in our products. Our security by design approach makes our products more resilient against cyberattacks. We implemented 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.

Implement strong authentication controls (DO THIS NOW!)

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

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 steps.

- 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.
- Restrict external network connectivity to your systems and devices.
- Continually monitor for events that could warn of attempted unauthorized access.
- Limit access to internal networks where devices reside.
- Isolate control and safety system networks and remote devices from the business network.

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, anti-virus 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 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 encouraged for any Internet-connected device. You can also subscribe to our newsletter to receive security notifications.

Implement secure access controls
Laptops that have connected to any other network should never be allowed to connect to the safety or control network without proper sanitation. Also, all methods of data exchange, such as CDs or USB drives, should be scanned before use in any node connected to the network. You may also want to split your networks and devices into groups isolated from one another and restrict access. Reducing the pathways into and within your networks and implementing security protocols on the pathways that exist makes it more difficult for a threat to enter your system and gain access to other areas.

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.

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 critical systems and data frequently, it is important to test your recovery procedures. Ensure you have multiple backups over time, so you can restore from a version that predates any infection.

Set up measures for detecting compromises
Minimize the risk of compromise by monitoring and auditing system events 24/7. Use intrusion detection systems (IDSs), intrusion prevention systems (IPSs), anti-virus 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.

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 for cybersecurity recommendations and best practices directly related to your Schneider Electric products.

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.

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.

The Cybersecurity Framework
National Institute of Standards and Technology (NIST)
https://www.nist.gov/cyberframework/framework

Cybersecurity Best Practices
Center for Internet Security
https://www.cisecurity.org/cybersecurity-best-practices/

IEC 62443 Security for Industrial Automation and Control Systems
International Society of Automation (ISA)
https://isasecure.org/en-US/

Cybersecurity at Schneider Electric:
Addressing IT/OT convergence in a versatile Cyber ecosystem
Part Number 998-20244304

https://www.se.com/us/en/download/document/IT_OT/

Cybersecurity by Design:
Building a Company Culture to Strengthen a Digital Business
Part Number 998-2095-12-06-18AR0

https://www.se.com/us/en/download/document/998-2095-12-06-18AR0_EN/

Document # 7EN52-0390-02

Life Is On Schneider Electric