Schneider Electric

Cyber Security Services by Schneider Electric

Cyber Security Best Practices

Table of Contents

Cyber Security Best Practices **2**

Always apply and maintain the latest Schneider Electric-authorized Operating System (OS) and application patches 2

Always use current anti-virus definitions 2

Update authorized application software 2

Enable Network Anti-Virus / Intrusion Prevention System 2

Do not use a USB stick unless it has been scanned and confirmed that it is free of problems with the latest DAT file 3

Harden servers and workstations. 3

Change default admin passwords 3

Control User Rights 3

Wherever Group Policies are in use 3

Always implement backup and restoration. 4

Take inventory of network assets 4

Use physical network isolation when possible 4

Use logical network segmentation (secure zones) when possible with strict firewall rules 4

Enable firewall logging 5

Use a Network Management System (NMS) 5

Don’t click links or files that aren’t verified 5

In the event of a Cyber Incident 5

Download and run latest McAfee Stinger tool 6

7 Cornerstones of Cyber Security **6**

Identification of Critical Assets 6

Electronic Access Controls 6

User Access Controls 6

Patch Management 6

Anti-Virus and Device Control 6

Disaster Recovery 6

Event Logging 7

Cyber Security Best Practices

Cyber security best practices are intended to provide guidelines on global network security that will not only reduce external threat vectors, but also internal. Items are presented in order of priority.

☑ Always apply and maintain the latest Schneider Electric-authorized Operating System (OS) and application patches.

- Download updates directly from the patch source or via secure file server.
- Assess which patches are required for each individual asset and apply as necessary, ensuring deployment does not impact operations.
- Ensure all required patches have been successfully applied.
- WITHOUT applying the current Schneider Electric-authorized patches, individuals will be increasing the attackable surfaces of individual DCS workstations and servers.

☑ Always use current anti-virus definitions.

- Ensure that the latest anti-virus definition files have been downloaded and installed from the Schneider Electric Support Website.
- Verify through the McAfee client that the update was successfully installed.
- Test new DAT in a test bed environment, prior to release into production environment.
- Without keeping anti-virus current, the servers and workstations will not have the current malware signatures, leaving the equipment vulnerable to attacks.

☑ Update authorized application software.

- Ensure application software such as Adobe, if authorized, is updated. File types such as .pdf are one of the top distributors of malware if not routinely updated.
- Without updating third-party software on the inventoried system, additional vulnerabilities will remain in place.

☑ Enable Network Anti-Virus / Intrusion Prevention System.

- Ensure that the most current anti-virus definition files and Intrusion Prevention System policies are enabled on all capable network appliances protecting the second Ethernet networks.
- Without using a device that incorporates an Intrusion Detection System (IDS), you will not have a baseline of normal network activities versus an attack. An anti-virus module will provide an alert and a secondary screen for network malware.

☑ Do not use a USB stick unless it has been scanned and confirmed that it is free of problems with the latest DAT file.

- Designate and use specific USB equipment where required.
- If using USB equipment to bridge air-gaps, always use a specific designated station in conformance with DCS security policies.
- Without restriction on USB devices, their portable nature can be used to compromise your global security perimeter.

☑ Harden servers and workstations. Hardening Non-DCS assets is a requirement and typically will not have negative effects on the DCS. Hardening DCS assets will vary from hardening Non-DCS assets.

- Ensure all software and hardware patches and updates are current.
- Run anti-virus scans.
- Disable all unused ports and services.
- Harden the bios.
- Use static IP addresses, disable DHCP on the interfaces, and disable unused interfaces.
- Disable NetBIOS, unless specifically mandated by the IT department; disable NetBIOS over TCIP/IP (via WINS tab).
- Without hardening servers, there is greater risk for attacks. Hardening reduces the attackable profile of the system.

☑ Change default admin passwords.

- Use strong passwords consisting of more than 6-8 characters using special characters when applicable.
- Without policies to ensure that admin passwords are changed, individuals can use admin passwords to escalate their privilege levels. Global automated attacks by malware using admin passwords are prevalent.

☑ Control User Rights.

- Verify that only authorized accounts are members of the local system administrators group.
- Do not use accounts across domains.
- When applications cannot use special characters, a service account should be created with authentication compatible with the application.

☑ Wherever Group Policies are in use:

- Change local system administrator passwords.
- Implement password aging, history, and complexity requirements.
- Ensure that Restricted Group Policy is enabled and used.
- Without policies that specify user privilege criteria, individuals can receive privileges beyond those required for the task at hand. If too many users have elevated privileges beyond their needs, malware can use this as a global threat vector.

☑ Always implement backup and restoration.

- Use a network backup repository.
- Back up the network repository to a geographically disperse secondary storage site for disaster recovery or to removable media that can be stored offsite.
- If using removable media, then a rotation policy should be implemented to ensure that multiple copies of the backup exist offsite.
- Periodically conduct recovery exercises using test bed equipment.
- Determine relative storage capacity available and automate a backup schedule for individual workstations and servers.
- Without implementing a backup policy, customers will have no recourse to restore to a condition prior to an attack date if required.

☑ Take inventory of network assets.

- Keep inventory current of all network assets and status.
- Update inventory as network changes are made to both hardware and software.
- Run network scans to collect asset information (log files, etc.) where authorized. Non-DCS assets may typically be scanned without issues, but DCS asset scanning should incorporate a limited tuned methodology.
- Run regular network audits to ensure all systems are up to date.
- Without a network inventory, you do not have a baseline of what normal network assets are and what goes toward the network scan, complicating what are known devices and what are known patches. Knowledge of what specific network firmware is running and what network security equipment is present can be critical in determining whether or not vulnerabilities exist.

☑ Use physical network isolation when possible.

- Without using physical network isolation, cross-contamination of the DCS platform is possible from the corporate system.

☑ Use logical network segmentation (secure zones) when possible with strict firewall rules.

- Isolate and control flow of information between Business Network(s) from PCN through use of firewalls.
- Require strict firewall rules with specific (/32) source, destination, port, and protocol.
- Use Demilitarized Zones (DMZs).
- Without using a secure zone, there will be no buffer before the network traffic traverses into the DCS network.

☑ Enable firewall logging.

- Ensure that all firewall policies protecting the Process Control Network (PCN) and supporting infrastructure have logging enabled.
- Monitor firewall logs as appropriate, paying special attention to locate potentially malicious or abnormal traffic.
- Without firewall logging, you will not have visibility into dropped traffic or attacked traffic.

☑ Use a Network Management System (NMS).

- Implement a NMS to provide system audit and logging.
- Monitor system logs for failed login attempts.
- Generate and review reports for abnormal events.
- Without a NMS, there will not be a consolidated location for viewing all logs. The NMS reports provide consolidated insight into all systems, which is invaluable for day-to-day operations and in the event of a cyber attack.

☑ Don't click links or files that aren't verified.

- DCS assets should not have internet access; some Non-DCS assets may have outside DCS access to business network website interfaces. Even business networks could be compromised, so verify all access leaving the DCS network to untrusted networks.
- Ideally, the DCS network should be isolated from internet-connected networks.
- Without policies restricting web access, users can potentially comprise the security perimeter by clicking on malicious links and installing unauthorized software.

☑ In the event of a Cyber Incident:

- Create an Incident Response Plan before an Incident so that you are prepared in the event of an Incident. Steps that are typically part of Incident Response Plans are:
    - Do not start updating anti-virus.
    - Do not start running anti-virus patches.
    - Do get a triage team together.
    - Do get copies of all the logs.
    - Do make a VM image of the affected system.
- Without an incident response team and procedures, the opportunities to collect the forensic evidence required to determine the attack vector and point of origin can be lost or compromised, depriving the client the opportunity to work with the anti-virus vendor and other agencies.

☑ Download and run latest McAfee Stinger tool.

- Without collecting the necessary forensic evidence to work with the anti-virus vendor, the client may not detect the variant that was not completely remediated by the Stinger tool.

7 Cornerstones of Cyber Security

1. Identification of Critical Assets

Critical assets are the items that are essential to business continuity. If these items are destroyed, damaged, or tampered with, it would negatively impact the safety and reliability of the network, facility, or equipment. This often leads to loss of revenue and consumer confidence.

2. Electronic Access Controls

Electronic access controls can include equipment like firewalls to help detect and block intruders trying to gain unauthorized access to critical company assets. Other forms of electronic access control can include application whitelisting or physical security measures such as key card access.

3. User Access Controls

User access controls can help prevent network interruption by ensuring users are only able to access certain areas of the network. Using a “least privilege” methodology prevents users from accessing confidential company data as well as inadvertently or maliciously tampering with network settings.

4. Patch Management

A patch is a piece of software designed to fix security vulnerabilities and other bugs and improve the usability or performance of systems and software. Patching closes security holes in applications that computer hackers and viruses can exploit. A patch management server acts as a centralized console to audit; review applications, ports, and .dat files; and pull and apply system patches. The patching solution is fully configurable and can be scheduled.

5. Anti-Virus and Device Control

Anti-virus software and device control policies help prevent malware and malicious cyber events from taking the network offline. Device control policies can extend to USB drive usage and other removable devices to minimize insider risks such as data loss and malware introduction. ePO provides a centralized and unifying management console for controlling and managing advanced malware features. ePO makes risk and compliance management simpler, enabling clients to connect security solutions to their BMS and EMS infrastructure increasing visibility, efficiencies, and strengthening protection. ePO has flexible automation capabilities streamlining workflows, dramatically reducing the cost and complexity of security and compliance administration for BMS and EMS cyber asset owners. The ePO platform also leverages Active Directory domain services for organization structure and policy groups.

Device control protects your data from falling into the wrong hands via removable storage devices and media, such as USB drives, MP3 players, CDs, DVDs, COM, LPT, and more. It enables you to specify and categorize which devices may or may not be used and enforce what data can and cannot be transferred to these devices—in the office, at home, or on the move. Device Control provides content- and context-aware, device-blocking capabilities. Device control ‘Denies by Default and Allows by Exclusion,’ providing greater strength of security. Controls can specify which devices can and can’t be used, define what data can and can’t be copied onto allowed devices, and restrict users from copying data from specific locations and applications.

6. Disaster Recovery

Backups refer to the various strategies and procedures involved in protecting a database against data loss and reconstructing the database after any kind of data loss. A backup is a copy of data from a database that can be used to reconstruct that data. Backups can be divided into physical backups and logical backups. The Backup File Storage service provides centralized backup and restoration capabilities by using the SCS Server as a centralized file repository for backups. Centrally manage backup and recovery tasks for multiple desktops across the network. Schedule backups to run automatically, including event-triggered backups, without disrupting network usage.

7. Event Logging

Logging is integral in ensuring an ICS is secure and stays secure. It can show when, where, and how a security intrusion was attempted and if it was successful. Logging is also a company's necessary audit trail that is required for some industry and government regulations. SMNP element managers provide centralized logging for SNMP, SYSLOG, and Microsoft Windows events. It also updates logging software to minimize unneeded events and alert notifications. Event log aggregates and centralizes all logs (SYSLOG, Trap log) onto the logging server.

To learn more about Schneider Electric Cyber Security Services, contact your sales representative or visit:
http://software.invensys.com/services/security-and-compliance-services/cyber-security-services/