The Top 10 Security Findings and Remedies in OT Networks

Master the cybersecurity challenges of your digital transformation with Siemens

SIEMENS
Ingenuity for life

Insufficient network separation and access control

Insufficient network segregation and network access controls allows attackers to access critical infrastructure from unauthorized networks and services

- Insecure access from Internet/Intranet
- Networks with different protection needs are not segmented
- Improperly configured routers and firewalls
- Insecure remote connections, e.g., insecure communication channels, insecure wireless communication
- Improper network access control

- Limit access to authorized systems only, use jump hosts to access and manage devices in a separate security zone and use network segmentation to improve control of traffic flows across the network
- Design the network to incorporate the necessary levels of protection
- Configure and manage firewalls securely, e.g., by using white-listing, instead of black-listing
- Use secure service, e.g., using encryption, integrity checks and authentication
- Tunnel insecure protocols via secure tunnels e.g. encrypted VPN tunnel
- Use secure remote access services and secure cloud connections, e.g., using secure encryption, authentication, and authorization mechanisms

Asset management issues

An inventory is not comprehensively made of all systems, software, services, and communication relations

- Missing asset ownership
- Missing, wrong, or outdated asset data
- Network architecture is unknown, and therefore cannot be controlled
- Unknown communication relations / communication matrix, in turn weak or incomplete firewall rule sets

- Establish an asset management system and according processes
- Integrate asset management process into standard operation processes, e.g. change management to improve quality
- Keep an up-to-date communication matrix that shows valid communication between assets, e.g., to set firewall rules
- Classify assets according to criticality

Missing Anti-Malware concept

No protection concept for detecting malicious software on sensitive hardware, e.g., service laptops, USB Sticks

- Missing or outdated end point protection
- Users unaware of digital risks

- Establish an end-point protection concept, e.g., central antivirus update server, white-listing secure software components, and use technical solutions to enforce policies
- Increase user awareness with security trainings
- Implement a virus scanner station for removable storage and restrict physical access to USB ports

Missing maintenance windows for security tasks

24/7 production does not allow downtime, which is needed to manage security

- Not possible to install security updates
- Penetration tests are not possible because critical production systems could be made unavailable

- Use planned maintenance windows to perform security tasks
- Perform threat and risk analysis to determine costs and benefits of security maintenance windows
- Implement centralized operation and management solutions to speed up maintenance tasks, e.g.,for distributing software patches

Missing/Weak authentication

Weak or nonexistent authentication mechanisms allows unauthorized access

- No or weak authentication, e.g. legitimate users can be impersonated by malicious actors
- Users share credentials
- Unknown or maintenance accounts with hard-coded credentials of vendors increase the attack surface ("backdoors")

- Strong authentication, such as two-factor authentication (if feasible)
- Use personal accounts/passwords with unified/ centralized account management
- Restrict access to services via network segmentation
- Implement secure kiosk solutions (e.g., using dedicated keypads), instead of providing full access to manufacturing PCs. This allows machine clients to be locked down when user authentication fails rather than the manufacturing PC
- Adopt the principle of least privilege, where any user, program or process has the minimum privileges required to perform its function, and do not run applications and services as a "superuser" which has unlimited privileges
- Require secure coding guidelines in contracts for suppliers, and test coding in acceptance tests

Insecure operation / missing security framework

Detecting and resolving problems in the overall production environment is hampered without the proper OT operation processes and procedures

- Missing / insufficient general secure operation processes for the production environment
- Unclear responsibilities for assets, especially on the interfaces between the office IT and production IT
- Regular security assessments not performed

- Define and implement adequate operation processes in all areas of the environment
- Define clear responsibilities for all assets
- Document procedures (e.g., for hardening) and track activities
- Raise security awareness among employees and suppliers, establish contact persons for security on shop floors
- Perform regular security assessments (procedural, technical)

Weak physical security

Unauthorized physical access to critical systems is possible (e.g., access to control equipment or physically unprotected switches, along with missing network protection

- Weak physical access protection
  - open doors, open campus
  - square spanner lock mechanism used instead of keys
- Physical access controls without access control monitoring

- Design physical access controls according to protection needs, e.g., smart cards, the 4-eye principle, high-security locks, security guards, CCTV

Missing security monitoring

Ineffective or nonexistent security monitoring of production networks and services

- Missing or insufficient logging of security related events
- Missing evaluation process for security log data

- Adopt and use a Security Information and Event Management (SIEM), Intrusion Detection System (IDS)
- Establish a process to detect, evaluate, and respond to security incidents

Weak application level security

Web applications, rich clients, network services have vulnerabilities

- Well know web application vulnerabilities
- Client-side security
- Remote code Execution (RCE) and memory corruption

Insecure software & components

Software components or 3rd party software solutions, such as Windows, Adobe Flash, custom protocol stacks, etc., are outdated, not patched, misconfigured, or no longer supported by suppliers

- Missing awareness
- Missing patch management concept
- Security updates no longer available from vendor (end of life)
- Insecure configuration
- Missing inventory of components

- Install a centrally managed update process, including all kinds of software components ranging from operating systems (Windows) to e.g. algorithmic libraries
- Implement additional mitigations to ensure adequate security level, e.g., networks should be effectively separated if software updates are not possible (defense-in-depth)
- Configure systems according to vendor security guidelines, e.g., use the principle of least privilege (Note: often, OT vendor guidelines do not address security)
- Keep an inventory of all used software and hardware components (see also: Asset Management)

Find out more and request a cyber security health check
siemens.co.uk/industrial-security