Top 8 Security Findings and Remedies in Cloud Environments

Master the cybersecurity challenges of your digital transformation with Siemens

SIEMENS
Ingenuity for life

Physical location

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
- Regular security assessments not performed
- Cloud provider has no security certifications or certifications that do not fit to your own business risks

- 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)
- Take care that your cloud provider has relevant certifications in place – like ISO 27001 – that include your business risks, and does not only include your physical security risks
- Take care that your cloud provider allows you to audit processes and technical security by yourself, that you do not need to rely only on third party assessment results

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- Missing, wrong, or outdated asset data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

Applications
Container, Microservices

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

- 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

Insufficient 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

Identity and Access Management

Cloud
Technological Stack

Operating System

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

Runtime Environment

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
- Keep an inventory of all used software and hardware components (see also: Asset Management)

Infrastructure
Compute / Storage / Network

Network Configuration

Insufficient 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 accounts with hard-coded credentials of vendors increase the attack surface ("backdoors")
- Insufficient key management; keys for cloud APIs and administration of cloud components stored in insecure places (e.g. desktops, scripts)

- 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
- 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

Insufficient Anti-Malware protection

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

Customer Data

Hypervisor

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