Network security auditing

CANADIAN CENTRE FOR CYBER SECURITY

December 2022 | ITSAP.00.086

Network security auditing is the process of independently examining information relating to your organization's IT controls, security systems, and risk mitigation policies and procedures. The goal of auditing is to identify threats, areas of weaknesses, and compromises as well as to ensure an organization is meeting regulatory requirements (e.g. System and Organization Controls (SOC), North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP), and Payment Card Industry Data Security Standard (PCI DSS)). Auditing should be conducted by IT professionals who have security and network management backgrounds and are not responsible for managing the network or systems under audit.

What are the benefits of network security auditing?

A security audit is an important activity that enables your organization to understand how effective your security controls are against cyber security threats. Some of the major benefits of regular network security auditing include:

- Improving weak organizational policies and practices.
- Verifying device use compliance against organizational policies.
- Facilitating the assessment of policies and processes against required regulatory and compliance standards.
- Facilitating the evaluation of the overall health of your network infrastructure.
- Discovering network inefficiencies and hardware or firmware issues.
- Discovering potential security weaknesses, vulnerabilities, and configuration errors within a network.
- Detecting rogue or unauthorized devices on the network.
- Assisting with identifying the source and extent of a compromise during the investigations of security incidents.
- Facilitating effective risk-based decision making.

Cloud service providers (CSP) and network auditing

If your organization subscribes to a cloud service, be informed and understand how your CSP is protecting you and your valuable assets. Some examples of questions to ask are:

- How often is auditing done and by whom?
- What kind of auditing is performed?
- What is the log data retention and destruction policy?
- Are the CSPs audited and by whom?
- Are audit reports available to client subscribers?
- Can client subscribers audit the service?
- What log data is available to client subscribers?

Network Security Auditing Best Practices

The information gathered from a security audit enables you to gain visibility into any potential issues within your network infrastructure. By implementing the following best practices, you can rectify these issues before without causing downtime or impacting your business operations.

- ☐ Conduct regular inventory of all the devices running on the network. Track details like hostnames, IP addresses, serial numbers, configuration settings, and code versions.
- ☐ Leverage the use of tools to perform network inventory, assess device configurations, and analyze network performance.
- ☐ Identify which devices are supported by the vendor (software and hardware), or are obsolete and need to be replaced or upgraded.
- ☐ Perform vulnerability scans of your networks to detect known security issues and identify areas of weaknesses.
- ☐ Verify that all network components have up to date security patches. For more information, see Top 10 IT security action items: No.2 patch operating systems and applications (ITSM.10.096).
- ☐ Set up a robust logging system for collecting data from all necessary sources within your network. Ideally, log data is exported to a centralized log server and is protected (in transit and at rest). For more information, see Network security logging and monitoring (ITSAP.00.085).
- ☐ Assess connections to other networks, especially untrusted ones (e.g. Internet), to ensure they are approved, and appropriate boundary protections are in place.
- ☐ Evaluate internal policies and processes, including physical access, configuration management, network upgrade, incident handling, and disaster recovery procedures.
- ☐ Evaluate password management and encryption practices.
- ☐ Evaluate user and group accounts for appropriate access levels and permissions. For more information, see Top 10 IT security actions: No.3 managing and controlling administrative privileges (ITSM.10.094).
- ☐ Assess data backup and recovery strategies. Ensure that the selected strategy is tested. For more information, see Tips for backing up your information (ITSAP.40.002).
- ☐ Audit your Bring Your Own Device (BYOD) policy to ensure that personal devices do not expose the network to threat actors. For more information, see End user device security for Bring-Your-Own-Device (BYOD) deployment models (ITSM.70.003).
- ☐ Audit your network's bandwidth consumption to understand usage and to better manage the flow of traffic.
- ☐ Conduct regular network security audits and share the findings and recommendations with relevant stakeholders in the organization.
- ☐ Synchronize all network devices to a central time server to ensure that recorded audit logs use the same time source. Set up a minimum of three time servers to facilitate maintenance and troubleshooting issues.

Communications Security Establishment | Centre de la sécurité des télécommunications

Canada