Network Security Audit Checklist

A comprehensive network security audit is usually done by a Managed IT Service Provider, but to uncover any potential network weaknesses, there are general overview items which can be checked periodically for a general overview by an SMB IT team.

☑ Define Scope

Because network security refers to data as well as hardware and software that connect with the internet, it's necessary to identify what the audit will cover, who will be doing the audit, and how it will be done.

☑ Policy Review

Review company policies and update when needed. Common policies include Acceptable Use Policy, Internet Access Policy, Email and Communications Policy, Network Security Policy, Remote Access Policy, BYOD Policy, Encryption Policy, and Privacy Policy.

☑ Password Security

Weak passwords are an easy entry point for attacks. Review and evaluate the password policy and authentication methods. Make sure that all employees understand the importance of using and storing passwords in a secure manager.

☑ Bandwidth & Traffic

Understand how the network distributes bandwidth and check the overall bandwidth usage to tell if users or equipment are consuming more bandwidth than usual. Monitor all traffic coming through the firewall and make sure to cross-check logs.

☑ Patch Updates

Check that firewall and anti-virus software are secure and updated with the most recent security patches.

☑ Device & Software Inventory

Taking inventory of all software and devices, including remote and mobile, will help identify suspicious activity and needed updates.

☑ Data & File Security

Review how you collect, store, process and distribute data. Sensitive data should be stored separately and accessed only by authorized users.

☑ Remote Access

Allowing remote access to the network is a critical access point for a system breach. Remote traffic should be funneled through a VPN. Two-factor authentication should be required and permissions should only be granted to those who are approved.

☑ Email Restrictions

Inbound and outbound email should be scanned while message encryption, spam filter and antivirus software should be standard to prevent malware, phishing, and spam.

☑ Data Backup

Review data backup process and schedules so data loss is minimized if a security breach occurs. You should also regularly test the data recovery process to make sure that the stored encrypted data can be successfully recovered.

Visual Edge IT