Auditing Windows Servers

Checklist for Auditing Windows Servers

Company

Date

No	Checklist
1	Obtain the system information and service pack version, and compare with policy requirements.
2	Determine if the server is running the company-provisioned firewall.
3	Determine if the server is running a company-provisioned antivirus program.
4	Ensure that all approved patches are installed per your server management policy.
5	Determine if the server is running a company-provisioned patch-management solution.
6	Review and verify startup information.
7	Determine what services are enabled on the system and validate their necessity with the system administrator. For necessary services, review and evaluate procedures for assessing vulnerabilities associated with those services and keeping them patched.
8	Ensure that only approved applications are installed on the system per your server management policy.
9	Ensure that only approved scheduled tasks are running.
10	Review and evaluate procedures for creating user accounts and ensuring that accounts are created only when there's a legitimate business need. Also review and evaluate processes for ensuring that accounts are removed or disabled in a timely fashion in the event of termination or job change.
11	Ensure that all users are created at the domain level and clearly annotated in the active directory. Each user should trace to a specific employee or team.
12	Review and evaluate the use of groups, and determine the restrictiveness of their use.
13	Review and evaluate the strength of system passwords.
14	Evaluate the use of password controls on the server, such as password aging, length, complexity, history, and lockout policies.
15	Review and evaluate the use of user rights and security options assigned to the elements in the security policy settings.
16	Review and evaluate the use and need for remote access, including RAS connections, FTP, Telnet, SSH, VPN, and other methods.
17	Ensure that a legal warning banner is displayed when connecting to the system.
18	Look for and evaluate the use of shares on the host.
19	Ensure that the server has auditing enabled per your policies or organization's practices.
20	Review and evaluate system administrator procedures for monitoring the state of security on the system.
21	If you are auditing a larger environment (as opposed to one or two isolated systems), determine whether there is a standard build for new systems and whether that baseline has adequate security settings. Consider auditing a system freshly created from the baseline.