AuditScripts

Auditing Server Security

AuditScripts 5 Crucial Questions (v2.2)

SECURITY enclave

Auditing Server Security

AuditScripts 5 Crucial Questions (v2.2)

Purpose:

Organizations audit their information security stance to protect the confidentiality, integrity, and availability of their information systems. Auditing and assessment allow an organization to validate their compliance with the standards they have set for themselves and to measure the levels of risk they are currently accepting.

AuditScripts has created the "5 Crucial Questions" series of audit checklists to provide auditors with a list of the five most important questions to ask when auditing a specific scope. Heavily influenced by the 20 Critical Security Controls project, these questions should serve as the starting point for any assessment.

5 Crucial Questions to Ask:

When performing an audit of an organization's servers, auditors should consider at a minimum asking the following questions:

1. Does an up-to-date inventory exist of all servers currently managed by the organization?
2. Is at least one data owner and custodian assigned to every server in the organization?
3. Are all servers in the organization physically secured to ensure that unauthorized individuals do not have access to them?
4. What percentage of servers in the organization are up-to-date with the latest software patches installed?
5. Do any high or medium security vulnerabilities exist on the server after scanning it with a vulnerability scanner?

Standards References

CIS Critical Controls (v6.1):
1, 2, 3, 5, 9, 13, 14, 16, 18

NERC CIP (v5):
CIP-007-5

NIST 800 Series:
NIST SP-43
NIST SP-44
NIST SP 800-53
NIST SP 800-64
NIST SP 800-123
NIST SP 800-125
NIST SP 800-147
NIST SP 800-167

NIST 800-53 (rev4):

COBIT 5:
APO13, DSS05

ISO 27000:2013:
7.1, 7.2, 9.1, 9.2, 10.1, 10.3—7, 10.10, 11.1—6, 12.4, 12.6, 14.1

NIST Cybersecurity Framework:
ID.AM-1, PR.DS-4, PR.DS-5
PR.DS-6

IIA GTAGs:
Not Applicable

PCI DSS (v3.1):
2, 3, 5, 6, 10, 11

HIPAA / HITECH:
164.308(a)(4), 164.308(a)(7)
164.310(b)
164.310(c)
164.310(d)(1)
164.312(a)(1)