AuditScripts

Auditing Authentication

AuditScripts 5 Crucial Questions (v2.2)

SECURITY enclave

Auditing Authentication

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 authentication systems, auditors should consider at a minimum asking the following questions:

1. Are clear-text authentication methods ever utilized in the organization?
2. Does the organization have a well-defined password standard for using passwords with lower sensitivity systems?
3. Is authentication performed at multiple layers (operating system, network, encryption, etc.)?
4. Does the organization utilize two-factor authentication for access to sensitive resources and systems?
5. Does the organization log all authentication events for both successful and unsuccessful attempts to authenticate?

Standards References

CIS Critical Controls (v6.1):
1, 3, 5, 11, 12, 13, 14, 16

NERC CIP (v5):
Not Applicable

NIST 800 Series:
NIST SP 800-63
NIST SP 800-73
NIST SP 800-76
NIST SP 800-118
NIS TSP 800-120

NIST 800-53 (rev4):
AC-7—14

COBIT 5:
APO13, DSS05

ISO 27000:2013:
11.1—3

NIST Cybersecurity Framework:
PR.AC-1

IIA GTAGs:
Not Applicable

PCI DSS (v3.1):
2, 3, 4, 6

HIPAA / HITECH:
HIPAA 164.308(a)(1)
HIPAA 164.312(a)(4)
HIPAA 164.312(c)(1)
HIPAA 164.312(d)

Other Standards:
All current FIPS Publications (especially FIPS 140-2)