AuditScripts

Auditing Wireless Security

AuditScripts 5 Crucial Questions (v2.2)

SECURITY enclave

Auditing Wireless 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 wireless systems, auditors should consider at a minimum asking the following questions:

1. Are only appropriate users authorized to utilize wireless networking systems from the organization's systems?
2. Is AES-CCMP used to encrypt all wireless data in transit on 802.11 wireless networks?
3. Is EAP/TLS used for authentication to each of the organization's sensitive 802.11 wireless networks?
4. Is the use of Bluetooth or ad hoc networks explicitly denied on each of the organization's systems?
5. Has the organization deployed a Wireless IDS (WIDS) solution to monitor for the use of inappropriate wireless systems?

Standards References

CIS Critical Controls (v6.1):
1, 2, 3, 11, 12, 15

NERC CIP (v5):
Not Applicable

NIST 800 Series:
NIST SP 800-48
NIST SP 800-97
NIST SP 800-98
NIST SP 800-120
NIST SP 800-121
NIST SP 800-127
NIST SP 800-153

NIST 800-53 (rev4):
AC-18

COBIT 5:
APO13, DSS05

NIST Cybersecurity Framework:
ID.AM-1

IIA GTAGs:
Not Applicable

PCI DSS (v3.1):
4, 6

HIPAA / HITECH:
HIPAA 164.312(e)(1)

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