

Overlooked Issues in Wireless Security

Corporate security policies must be in place to address the unique risks of wireless technologies. These standards and policies should evaluate and document the risks that a company is willing to accept and the controls that will be implemented to mitigate them. Formal standards and policies also implement a baseline to which all access points can be configured, and against which they can be tested. Unfortunately, many companies have not developed the necessary wireless security policies. The following is a list of commonly overlooked issues in organizational security policies.

Define responsibilities

Wireless policies rarely define the parties who are responsible for configuring wireless devices and monitoring for unauthorized behavior.

Collaborate with the data classification policy

Most security policies do not align with the data classification and protection policies. This coordination is essential to determine the security controls necessary to protect the integrity, availability, and confidentiality of information.

Periodically communicate wireless risks and vulnerabilities to end-users

Security begins and ends with people. Unfortunately, many organizations do not inform their people regarding the security risks created by wireless technologies, such as the ways in which an unauthorized access point could impact the security of an entire organization.

Register approved wireless access points and clients

Often, no formal inventory is maintained to document all wireless devices within an organization. Without complete inventory tracking, it is almost impossible to distinguish between authorized and rogue (unauthorized) access points during wireless security assessments.

Regularly apply patches and security enhancements

Companies rarely patch devices that are not available to the Internet, especially networking devices on internal networks. Unfortunately, new vulnerabilities are discovered frequently, leaving the corporate network open to exploitation if the perimeter security is breached.

Define minimum wireless architecture, encryption, authentication, and monitoring standards

Wireless deployment and configuration policies are often not formalized, resulting in inconsistent and insecure networking configurations. Many wireless implementations do not use even the most basic, built-in security features. Approximately two-third of all wireless networks are not configured with adequate security.

Maintain knowledge of wireless network technology and vulnerabilities

Wireless technologies change rapidly, making it difficult for many organizations to stay up to date with vulnerabilities and ways to mitigate risks.

Regularly perform location reviews to identify wireless presence

Reviews to ensure accuracy of access point inventory, security of configurations, or identification of unauthorized devices are not performed sufficiently frequently.

Protect physical security

Often physical security controls are overlooked around wireless implementations. Companies do not take advantage of physical security personnel to identify unauthorized wireless devices in a building, or war drivers in the parking lot. Additionally, wireless access points are not protected against physical access and can often be reset to an unsecured configuration.

This information was contributed by Protiviti KnowledgeLeader.

KnowledgeLeader is a subscription-based website for internal audit, technology audit and risk management professionals. The website provides continuously updated tools, checklists, best practices and other resources to help organizations manage risk and improve their internal audit function.

For more information, see <http://www.knowledgeleader.com/>. **Free 30-Day trials are available.**

For questions please telephone: 1 866 923 8513. For requests from outside the U.S. or Canada, call +1 925 598 7771.

Material from the KnowledgeLeader® Internal Audit and Risk Management Community

<http://www.knowledgeleader.com>

© 2003 Protiviti. All right reserved.

Material from the KnowledgeLeader® Internal Audit and Risk Management Community

<http://www.knowledgeleader.com>

© 2003 Protiviti. All right reserved.