

Wireless Security Test

Wireless networks, if implemented insecurely, can allow attackers access to internal corporate resources from external locations beyond the physical perimeter of the company premises. Rogue wireless infrastructure within a physical location can likewise provide an access point for internal attack.

IRM's Wireless Security Test evaluates the security of all the key components making up that wireless solution using proven methodologies to assess the security of the wireless architecture. The result is a comprehensive assessment of risks and exposures present within the wireless deployment.

IRM will identify the key components providing security within the wireless deployment and will highlight possible architectural flaws that would allow an attacker to gain access to sensitive information such as customer data.

A complete Wireless Security Test includes the following phases:

- **Perimeter Survey**

The visibility of any wireless access points available to a physically external attacker will be assessed. The focus in this phase will be to establish the strength of any signal leakage to measure from how far outside the building it is possible to connect to the wireless network.

- **Site Survey**

An internal assessment will be conducted to detect the presence of any RF devices on the network. Access point visibility and mapping exercises will be conducted, together with fingerprinting of the access points and identification of potential information leakage from wireless broadcast traffic. The results gathered will be used to identify any suspicious 'rogue' or unauthorised access points accessible within the company grounds.

- **Cryptographic Analysis**

An examination of the resilience of any wireless devices discovered to typical attack techniques will take place during this phase. Further tests will be conducted to assess the network security of the wireless deployment and the authentication procedures.

- **Access to Wireless Networks**

When the consultant has gained access to wireless networks (or following the provision of access credentials by the client), a detailed examination of the wireless network in pre-authentication and post-authentication modes will be conducted to determine the level of access should the wireless network be compromised or targeted by a disgruntled employee with legitimate access.

- **Configuration Review**

A review of the access point (AP) configuration will highlight any deviations from best practices. Additionally, a review of relevant ACLs of filtering devices may be conducted to ensure that defence-in-depth principles have been observed in configuring the WLAN infrastructure.

- **Deliverables**

IRM will deliver a formal report including an executive summary, a risks and recommendations table detailing the high level results of the assessment and a detailed description of each issue discovered including remediation advice.

About IRM

Information Risk Management Plc (IRM) is a vendor-independent information security consultancy. Founded in 1998 to work alongside global enterprises in understanding the security risks inherent in an increasingly interconnected business environment, IRM has become a leader in penetration testing, risk assessment and security auditing.