COGNISYS
Smarter Cyber Security

Wireless Security Assessment

Extending the scope of your testing to include any wireless networks is crucial. Hackers generally regard wireless as an ideal route into your systems.

The convenience and accessibility of wireless technology makes it an integral part of business today. No cords or cables, just radio waves between the device of your choice and the target data.

Wireless technology is unfortunately yet another attack vector which can be compromised and used for a malicious attack if not properly secured.

Is your network properly segmented from the public access network you give to guests and clients? How easy is it to compromise your network whilst sitting outside in the car park?

01422 416 000

sales@cognisys.co.uk
cognisys.co.uk

Continued overleaf...

Wireless networks are often the primary method by which end-user devices access organisational data. It is therefore more important than ever to ensure the deployment and configuration of these networks is as secure as possible.

From flawed encryption schemes to badly configured networks, there is plenty for a malicious user to try and exploit.

Our wireless security assessments encompass all aspects of wireless infrastructure deployments and aim to uncover weaknesses that an attacker may leverage to remotely gain a foothold into the internal network.

Method

The assessment generally commences with reconnaissance to identify wireless networks, protocols used and technologies in use by the client, plus any other broadcast sources in the immediate vicinity, inside and immediately outside the premises

Cognisys' multi-faceted approach to wireless security testing assesses deployments against security best practices and can help ensure organisations adequately protect critical assets, whilst providing staff, contractors and guests the key flexibility that wireless offers.

Overview

The engagement is tailored to the client's particular topology and configuration and covers the following:

- Wireless security analysis of the premises.
- Identification of broadcast Service Set Identifiers (SSIDs).
- Identification of rogue/unauthorised wireless networks.
- Analysis of protocols and cryptography in use.
- Suitability review of authentication schema.
- Wireless radio configuration review.
- Network segregation testing.
- Analysis of wireless client protection mechanisms.
- Pre-Shared Key strength analysis including cracking exercises.

Report

Cognisys presents its findings in a comprehensive yet simple report format.

This typically comprises: an executive summary, methodology, technical findings, and prioritised recommendations for remediation.

01422 416 000
sales@cognisys.co.uk
cognisys.co.uk

INTERNAL PENETRATION TESTING | EXTERNAL PENETRATION TESTING | WEB APPLICATION SECURITY TESTING | MOBILE APPLICATION SECURITY TESTING | CYBER SECURITY REVIEW | RED TEAM EXERCISE | PHISHING SIMULATION | DARK WEB MONITORING | LOST OR STOLEN DEVICE ASSESSMENT | WIRELESS SECURITY ASSESSMENT | CLOUD SECURITY ASSESSMENT | MICROSOFT 365 TENANT REVIEW | ATTACK PATH ANALYSIS | OSINT ANALYSIS | CYBER ESSENTIALS | GOVERNANCE & COMPLIANCE | VIRTUAL CISO | MANAGED SECURITY | SMARTSCAN | SMARTVIEW