REFERENCE SHEET

SECURING YOUR WIRELESS NETWORK

Purpose of the document

Set up a secure, robust wireless access point.

Wireless, or Wi-Fi, networks are often vulnerable and can be hacked by people trying to intercept sensitive data (personal information, payment card PIN codes, business data, etc.).

The issue of securing wireless networks is not always well understood, and the risks are often overlooked.

The basics

Wireless technology relies on a radio link with waves that are subject to interception and interference, whether accidental or intentional. In many situations, a wired connection should be used. However, if that's not possible, information confidentiality should be ensured by using additional encryption measures, such as IPsec or TLS.

The strength and security of wireless networks generally depend on:

- network accessibility, i.e. the range of the electromagnetic signals that transmit the wireless signal
- authentication mechanisms used to identify users of the network uniquely and securely
- cryptographic mechanisms put in place to protect wireless communications, which are often derived from authentication mechanisms
- administrative and monitoring mechanisms of the network access points and terminals using the network
- other configuration aspects for wireless access points

Implementation and use of wireless networks should be covered by a security policy that's validated by the company's senior management.

The basics

All types of terminals

1. Turn on the wireless interface only when it needs to be used.
2. Systematically disable automatic connection to wireless access points configured in the terminal to maintain control of connectivity.
3. Keep the operating system and wireless network drivers up to date.
4. Whenever possible, don't connect to unknown or unverified networks.
5. Use the local firewall settings to block incoming connections via the wireless interface.

Professional terminals

6. Comply with the company's security policy, especially for authenticating encryption and protecting information confidentiality and integrity
7. Don't connect a personal terminal to the company network.
8. Working remotely: When connecting to unverified wireless access points (e.g. hotels, train stations or airports) and before exchanging any data, always use additional security measures (e.g. IPsec VPN).
9. Set up a specific security protocol, such as TLS or IPsec, when sensitive data has to be transmitted over a wireless network.

Wireless hotspots

10. Set up hotspots with strong encryption. WPA2, which uses AES/CCMP encryption, is highly recommended. For personal access points, use WPA-PSK (WPA-Personal) authentication mode with a long, complex password (e.g. about 20 characters), especially since it's saved and doesn't need to be memorized by the user.
11. When access is only protected by a password (WPA-PSK), it's essential to change the password regularly and control its distribution. Specifically, you should:
    - not share the password with unauthorized third parties (e.g. service providers)
    - not store the password on a medium that can be seen by an unauthorized third party
    - change the password regularly and whenever it has been compromised
12. For wireless networks in a professional environment, set up a WPA2 using a centralized authentication service based on WPA Enterprise (802.1x standard and EAP protocol) and robust authentication methods.
13. Configure the private VLAN guest in isolated mode when the wireless access point takes over this functionality.
14. Don't use a generic network name (SSID) proposed by default. The SSID used should not be too explicit in terms of professional activity or personal information.
15. Systematically disable the WPS function of access points.
16. Secure administration of the wireless access point by:
    - using secure administration protocols (e.g. HTTPS)
    - connecting the administration interface to a secured administration wired network to at least prevent wireless users from accessing it
    - using strong administration passwords
17. Configure the access point so that security events can be monitored. In a professional environment, it's preferable to redirect all events generated by access points to a central monitoring infrastructure.

Network architecture

18. Wireless network coverage should be limited to zones that need coverage.
19. In a professional environment, isolate the wireless network from the wired network and put in place network filtering equipment so that strict rules can be applied in line with the company's security objectives. Like the access point, the filtering equipment should be set up so security events can be monitored.
20. If a guest wireless network needs to be set up, it's recommended to use a separate infrastructure isolated from the other networks that does not allow access to any resource in the internal network. This network should have its own more restrictive security policy.

Active directory environment

21. Install the GPOs required by the security policies to control the wireless configurations on Windows clients' workstations so that the recommendations in this document can be applied.
22. To avoid disclosing information to users, use GPO to deploy network connection information on Windows workstations (network name, access key, certificates that may be required by the EAP method, etc.).