QUICK REFERENCE

SECURING WIRELESS NETWORKS

Objective

Set up a robust and secure 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.

Target recipient: Network administrators

Last update: 2017-06

The basics

Wireless technology relies on a radio link with waves that are subject to interception and interference (accidental or intentional). There are many reasons why a wired connection should be used, but if not possible, the confidentiality of the information should be ensured by using additional encryption measures, such as IPsec or TLS.

The security and robustness of wireless networks generally depend on:

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

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

Recommendations

All types of terminals:

- Turn off the wireless interface when not using it.
- Systematically disable the automatic connection to wireless access points configured in the terminal to maintain control of connectivity.
- Keep the operating system and wireless network drivers up to date.
- Where possible, don't connect to unknown or unverified networks.
- Use the local firewall settings to block incoming connections via the wireless interface.

Professional terminals:

- Comply with the company's security policy, especially in terms of encryption authentication and protection of information confidentiality and integrity.
- Don't connect a personal terminal to the company network.
- If out of the office, 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).
- Set up a specific security protocol, such as TLS or IPsec, when sensitive data is being transmitted over a wireless network.

Wireless hotspots:

- Set up hotspots with strong encryption. The WPA2 security mode that uses the AES-CCMP encryption algorithm is highly recommended. For personal access points, use the WPA-PSK (WPA-Personal) authentication mode with a long and complex password (e.g., around 20 characters), especially since the password is saved and doesn't need to be memorized by the user.
- When access is only protected by a password (WPA-PSK), it's essential that the password be changed regularly and its distribution be controlled. Specifically, you should:
    - not communicate the password to unauthorized third parties (e.g., service providers)
    - not record the password using a medium that can be seen by an unauthorized third party
    - change the password regularly and when compromised
- For wireless networks in professional environments, set up a WPA2 using a centralized authentication server based on WPA Enterprise (802.1x standard and EAP protocol) and robust authentication methods.
- Configure the private VLAN guest in isolated mode when the wireless access point takes over this functionality.
- Don't use a generic network name (SSID) that is proposed by default. The SSID used should not be too explicit in terms of professional activity or personal information.
- Systematically disable the WPS function of access points.
- 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 access to wireless users
    - using strong administration passwords
- 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 supervisory infrastructure.

Network architecture

- Wireless network coverage should be limited to zones that need the coverage.
- In a professional environment, isolate the wireless network from the wired network and put in place network filtering equipment that allows for strict rules 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.
- If a visitor 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

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