PROTECT

Security for Wireless Networks

INTRODUCTION

1. Wireless networks are increasingly being used by organisations. This is due to their ease of deployment, low cost compared to traditional fixed networks and to satisfy employee demand.

2. If organisations implement the security measures discussed in this document such as network segregation, changing default settings, authentication, encryption and securing devices, they will have taken significant steps towards reducing the security risks associated with the use of wireless networks.

INTENDED AUDIENCE

3. This document is intended for chief information officers, chief information security officers and other senior executives within organisations.

SECURITY CONSIDERATIONS

4. The key security considerations associated with the use of wireless networks are discussed below.

Wireless networks for public use

5. When an organisation introduces wireless networks for public access e.g. a public hotspot, such wireless networks should not be connected to any networks that communicate or store sensitive information. Allowing a connection between such networks could allow an adversary the opportunity to steal sensitive information from the organisation or disrupt their services.

Connecting wireless and fixed networks

6. When an organisation has a business requirement to connect a wireless network to their fixed network, it is important that they consider the security risks. While fixed networks are often afforded a certain degree of physical security, wireless networks due to their nature are often easily accessible outside of the controlled perimeter of an organisation. To protect against an attack originating from a wireless network against a fixed network, connections between wireless networks and fixed networks should be treated in the same way organisations would treat connections between fixed networks and the Internet.

PROTECT

Default settings for wireless equipment

7. Wireless equipment comes pre-configured with default accounts and passwords that are freely available in product documentation and online forums. To ensure default user names and passwords aren't exploited to gain access to wireless networks, they should be changed.

8. All wireless equipment comes with a default network identifier. As the default identifiers of wireless equipment are well documented on online forums, along with default accounts and passwords, the default identifier should be changed to a value that is not readily associated with an organisation, or the location of or within their organisation's premises.

Authentication for wireless networks

9. When deploying a wireless network, an organisation will need to determine whether they will deploy the network with robust security to protect sensitive information or with no security for the public to access e.g. a public hotspot.

10. If deploying a public hotspot, an organisation may opt for no authentication for devices. While this provides ease of use for the public, it also provides a number of security risks to an organisation, such as criminal misuse.

11. Organisations deploying a secure wireless network can choose from a number of authentication methods. An organisation's choice in authentication method will often be based on the size of their deployment, their security requirements and any existing authentication infrastructure they plan on utilising.

12. Each of the authentication methods for wireless networks has its own advantages and disadvantages. Organisations can choose to use simple authentication with a shared password or more secure authentication using certificates. Organisations using a certificate-based authentication method should choose a method that meets their primary motivation for authentication, be it security, flexibility and legacy support, or simplicity of use.

Encryption for wireless networks

13. As wireless transmissions are capable of radiating outside of secured areas, organisations can't rely on the traditional approach of physical security. As such, wireless networks should be encrypted using DSD approved cryptographic algorithms to maintain the confidentiality of information that is being communicated over the network.

PROTECT

Devices accessing wireless networks

14. Devices used to access wireless networks have the potential to have been exposed to viruses, malware or other malicious code. This presents a security risk as these devices could inadvertently be infecting other devices on wireless networks, being used to steal an organisation's sensitive information or impacting the availability of wireless networks. To assist in reducing this security risk, all reasonable measures should be taken to ensure the security of devices connecting to wireless networks.

15. Organisations can ensure that devices are secure before granting access to wireless networks through the use of network access protection. With network access protection, system administrators can set policies for system health requirements. This can include a check that all operating system patches are up to date, an anti-virus program is installed and all signatures are up to date, and that a software firewall is installed and being used. Devices that comply with all health requirements can be granted access to wireless networks while devices that aren't healthy can be quarantined or granted limited access.

FURTHER INFORMATION

16. Further information on security measures that can be implemented to protect wireless networks can be found in the *Australian Government Information Security Manual* (ISM)[1] and the technical companion to this document.

CONTACT DETAILS

17. Australian government agencies seeking clarification about this document can contact the DSD Advice and Assistance Line on 1300 CYBER1 (1300 292 371) or assist@dsd.gov.au.

[1] http://www.dsd.gov.au/infosec/ism/