Office of the NEW YORK STATE

COMPTROLLER

Local Government Management Guide

Wireless Technology and Security

New York State Comptroller

THOMAS P. DiNAPOLI

OCTOBER 2019

Table of Contents

Wireless Technology and Security

Wireless technology has changed the way people use computers and devices to communicate and access the Internet. Wireless networks are often easier and less expensive to manage and maintain than traditional wired networks. They are also more convenient for users, who expect to connect laptops, tablets and smartphones without being highly restricted by physical location. The convenience offered by wireless networks has also introduced additional security issues that don't exist in wired networks.

Wireless networks are exposed to many of the same types of threats and vulnerabilities as wired networks, including viruses, malware, unauthorized access and loss of data. However, they are considered inherently less secure than wired networks because their information-bearing signals are broadcast or transmitted through the air. These traveling signals can potentially be intercepted and exploited by individuals with malicious intent. Since wireless networks are used as extensions of wired networks, even minor flaws in the configuration and implementation of a wireless segment can impact the security of an entire network. The decision to use wireless technology should be supported by a valid business purpose and undertaken only after careful consideration of the costs and benefits.

Since wireless networks are used as extensions of wired networks, even minor flaws in the configuration and implementation of a wireless segment can impact the security of an entire network.

There are a number of steps that local governments and school districts can take to help mitigate the risks of wireless technology. Although wireless environments can be quite complex, government personnel can implement effective controls with relative ease and without incurring additional cost.

Basic Wireless Technology Concepts

The purpose of this guidance is to provide a basic overview of wireless technology and security. It is focused primarily on wireless local area networks (WLANs)[1] as opposed to other types of wireless communications, such as radio systems or cellular networks. WLANs differ from traditional, wired local area networks (LANs) in that WLANs move data using radio waves instead of network cables. Radio waves have characteristics that make them well-suited for wireless communication – specifically, they can travel long distances and pass through solid objects.

> Radio waves can travel long distances and pass through solid objects.

When a WLAN is used to extend a LAN, wireless access points (APs) are physically connected to the LAN and each AP broadcasts a signal that can handle traffic from any number of laptops, tablets, smartphones and other types of devices operating within its broadcast area.

Alternatively, two or more devices (e.g., laptops, tablets, smartphones) can communicate with each other wirelessly without use of an AP as an intermediary. In some cases, home or small office networks operate in this manner to share files without the need for Internet or other network connections.

Best Practices

There are several steps that local governments and school districts can take to better secure their wireless networks.

Adopt written policies and procedures.

Local governments and school districts should have written policies and procedures regarding wireless technology and security. Even when wireless technology is not in use, a policy should be established to ensure that users are aware that wireless communications are prohibited, especially when sensitive and/or critical data is involved, and that users must not install unauthorized APs or connect the organization's devices to public WLANs (such as those provided by hotels and cafes). Wireless policies and procedures should be maintained and updated as technologies and trends evolve. They should also be communicated to employees to increase awareness of security threats and strengthen their understanding of their responsibilities for protecting the organization against these threats.

Consideration should be given to who might be accessing the WLAN, and the policies and permissions that govern access should be developed accordingly. The wireless policy should explicitly identify if WLANs are available to business partners, customers, taxpayers, and other guests. It should also identify the information resources that should and should not be available to WLAN users (e.g., guests are allowed to use the government's Internet connection, but not to access its internal database servers). The policy should further identify who is responsible for installing, configuring, and maintaining WLAN equipment. Procedures should be established to guide individuals in completing those responsibilities in a manner that meets the entity's security needs.

Determine the optimal number, physical location and broadcasting power of wireless access points.

The physical location of APs is the foundation on which a secure environment is created. APs and other supporting wireless devices should be placed in a physically protected location that minimizes opportunity for theft, damage or unauthorized access. Local governments and school districts should have the minimum number of APs necessary to meet their needs, as every additional AP represents another entry point into the organization's network. To minimize the ability of unauthorized users to gain access to the network, AP coverage should radiate out to the windows but not beyond. To accomplish this, personnel should consider locating APs toward the center of the building rather than near windows. In addition, the broadcast power level on most APs can be adjusted to the minimum required for adequate coverage (this does not affect the quality of the connection or the speed at which data is transferred). The goal is to avoid broadcasting where it is not necessary for legitimate use and thus minimize the risk of unauthorized access.

Maintain an inventory of and monitor wireless access points.

Local governments and school districts should maintain an inventory record of authorized APs. It is the basis for identifying unauthorized APs and can be helpful for a variety of support tasks, including identifying security patches that should be applied. Personnel should periodically conduct site surveys to determine if unauthorized APs are in use. By performing a site survey, personnel can determine the presence of wireless signals in and around the municipality's facilities. The survey should include monitoring for full coverage of wireless signals in the appropriate areas and confirming no signal in areas outside of designated coverage areas; identifying all wireless signals in coverage areas, including those belonging to outside entities; verifying encryption on organizational APs (see discussion below that addresses encryption); assessing the physical security of all APs; and monitoring for unauthorized APs.

Change the service set identifier.

The name of the wireless network, known as the service set identifier (SSID), is used to differentiate wireless networks from one another. When devices detect a wireless network, the name displayed is that wireless network's SSID. Most APs come with a default network name and similar models from the same manufacturer typically have the same default network name (e.g., the default network name for most Linksys brand APs is "linksys"). The default SSID may give information about the hardware and/or software in use to potential attackers, who could attempt to exploit any vulnerability identified in that hardware or software. Similarly, an SSID that identifies the AP as belonging to a particular entity makes it easier for an unauthorized user to identify a potential entry point into a specific target network. Personnel should change the SSID and use a naming convention that excludes identifiable information about the entity (e.g., the SSID of the wireless network in the Town of First should not be "townfirst" or even "townwireless"), location (e.g., Server-Rm-WiFi), technology, manufacturer and type of data traversing the network.

The default SSID may give information about the hardware and/or software in use to potential attackers, who could attempt to exploit any vulnerability identified in that hardware or software.

Require an access password and enable the most secure encryption available.

Generally, an AP can be set up as Open, where no password is required to connect and wireless communications between connected devices are sent in readable cleartext, or Secure,[2] which requires the use of an access password (different from the administrative password discussed below) and wireless communications between connected devices are encrypted. When configuring a Secure AP, there are two primary encryption types available: Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). WEP was the first encryption method available to wireless networks. It is no longer considered a secure method of encryption due to significant weaknesses for which there are free tools available on the Internet that allow attackers with minimal skill to determine the password and then convert wireless communications back into readable cleartext. WPA encryption addresses these weaknesses, providing for stronger protection over wireless communications. Since WPA's initial development, two enhanced versions, WPA2 and WPA3, have been released.

Users should be required to enter a strong password when attempting to connect to the wireless network.

Users should be required to enter a strong password when attempting to connect to the wireless network. This password should not contain any portion of the network name nor any words identifying the organization, as these passwords could be easily guessed by unauthorized users. Whenever feasible, enable the most secure encryption option available (currently WPA2 or WPA3).

Change the default administrative password.

The administrative password, different from the password used to connect to the wireless network that was discussed above, allows the administrator (the person setting up the AP) to change configuration settings as necessary. In most cases, APs come with a preconfigured default administrative password. In other instances, no default password is provided and an administrative password must be created during the initial configuration process. Attackers can find the default administrative username and password for almost any wireless product on public websites. Further, anyone can access the AP's configuration settings as long as he or she is connected to the same network, wired or wirelessly, and knows the administrative username and password. This means that APs can be accessed from outside the building within which the AP resides, reducing the likelihood that an unauthorized individual would be noticed prior to causing damage to the AP.

If a default password is supplied with the device, it should be changed upon installation. A complex administrative password should be created, safeguarded and periodically changed. Complex passwords contain a combination of upper- and lower-case letters, numbers and special characters and are at least eight characters in length. Complex passwords are not simple words or names, nor do they include any part of the associated user name or entity name. To prevent a compromised password from having much wider consequences, entities should not use a common administrative password for multiple APs.

Update and patch in a timely manner.

All software and hardware devices need occasional updates for improved performance, compatibility and security. Unlike most operating systems and applications that users interact with on a regular basis, network devices (including APs) do not notify users when updates are available, nor do they facilitate downloading and installing updates. Manufacturers will typically post security bulletins regarding threats, vulnerabilities and exploits targeted at specific equipment along with any related upgrades, hotfixes or patches. However, administrators must search manually for those updates and patches that affect the devices on the networks they manage. Any vulnerability that remains unpatched on an AP could be exploited in an attempt to gain unauthorized access to the wireless network, modify or corrupt wireless communications to and from connected devices, or otherwise disrupt legitimate wireless communications. To remain informed of security vulnerabilities that exist in the devices used on the local government or school district's wireless network, personnel should regularly visit manufacturers' websites for updates and security bulletins. Updates or patches for those devices should be downloaded and installed as soon as it is practical.

Any vulnerability that remains unpatched on an AP could be exploited in an attempt to gain unauthorized access to the wireless network or disrupt legitimate wireless communications.

Consider other security controls.

Personnel responsible for information technology and data security should consult reputable sources such as those listed in the Additional Resources section of this guide for additional wireless security configuration and monitoring options and recommendations.

Additional Resources

Multi-State Information Sharing & Analysis Center (MS-ISAC)
http://cisecurity.org/ms-isac/

National Institute of Standards and Technology (NIST)
http://nist.gov

New York State Office of Information Technology Services (NYS ITS)
http://its.ny.gov

United States Computer Emergency Readiness Team (US-CERT)
http://us-cert.gov

Notes

[1] A wireless local area network connects two or more devices (e.g., laptops, tablets, smartphones, access points, servers, printers, etc.) within a limited physical area (such as a municipal building or school district) using wireless communications.

[2] As with many security settings, this does not mean the AP is inherently secure.

Contacts

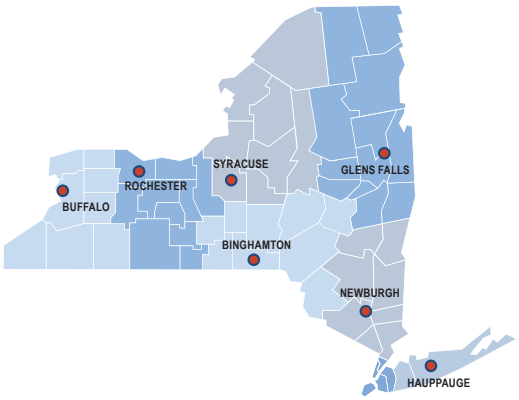
Office of the NEW YORK STATE
COMPTROLLER

New York State Comptroller
THOMAS P. DiNAPOLI

Division of Local Government and School Accountability

110 State Street, 12th floor, Albany, NY 12236
Tel: 518.474.4037 • Fax: 518.486.6479
Email: localgov@osc.ny.gov

www.osc.state.ny.us/localgov



Executive • 518.474.4037
Elliott Auerbach, Deputy Comptroller
Tracey Hitchen Boyd, Assistant Comptroller
Randy Partridge, Assistant Comptroller

Audits, Local Government Services and Professional Standards • 518.474.5404
(Audits, Technical Assistance, Accounting and Audit Standards)

Local Government and School Accountability Help Line • 866.321.8503 or 518.408.4934
(Electronic Filing, Financial Reporting, Justice Courts, Training)

Division of Legal Services
Municipal Law Section • 518.474.5586

New York State & Local Retirement System
Retirement Information Services
Inquiries on Employee Benefits and Programs
518.474.7736

Technical Assistance is available at any of our Regional Offices

BINGHAMTON REGIONAL OFFICE
Tel 607.721.8306 • **Fax** 607.721.8313 • **Email** Muni-Binghamton@osc.ny.gov
Counties: Broome, Chenango, Cortland, Delaware, Otsego, Schoharie, Sullivan, Tioga, Tompkins

BUFFALO REGIONAL OFFICE
Tel 716.847.3647 • **Fax** 716.847.3643 • **Email** Muni-Buffalo@osc.ny.gov
Counties: Allegany, Cattaraugus, Chautauqua, Erie, Genesee, Niagara, Orleans, Wyoming

GLENS FALLS REGIONAL OFFICE
Tel 518.793.0057 • **Fax** 518.793.5797 • **Email** Muni-GlensFalls@osc.ny.gov
Counties: Albany, Clinton, Essex, Franklin, Fulton, Hamilton, Montgomery, Rensselaer, Saratoga, Schenectady, Warren, Washington

HAUPPAUGE REGIONAL OFFICE
Tel 631.952.6534 • **Fax** 631.952.6091 • **Email** Muni-Hauppauge@osc.ny.gov
Counties: Nassau, Suffolk

NEWBURGH REGIONAL OFFICE
Tel 845.567.0858 • **Fax** 845.567.0080 • **Email** Muni-Newburgh@osc.ny.gov
Counties: Columbia, Dutchess, Greene, Orange, Putnam, Rockland, Ulster, Westchester

ROCHESTER REGIONAL OFFICE
Tel 585.454.2460 • **Fax** 585.454.3545 • **Email** Muni-Rochester@osc.ny.gov
Counties: Cayuga, Chemung, Livingston, Monroe, Ontario, Schuyler, Seneca, Steuben, Wayne, Yates

SYRACUSE REGIONAL OFFICE
Tel 315.428.4192 • **Fax** 315.426.2119 • **Email** Muni-Syracuse@osc.ny.gov
Counties: Herkimer, Jefferson, Lewis, Madison, Oneida, Onondaga, Oswego, St. Lawrence

STATEWIDE AUDIT
Tel 315.793.2484

Contact

Office of the New York State Comptroller
Division of Local Government and School Accountability

110 State Street, 12th floor
Albany, NY 12236
Tel: (518) 474-4037
Fax: (518) 486-6479
or email us: localgov@osc.ny.gov

www.osc.state.ny.us/localgov/index.htm

Like us on Facebook at facebook.com/nyscomptroller
Follow us on Twitter @nyscomptroller

Released January 2016
Updated October 2019