modern office methods

Your Managed IT Partner

FSN

FULL SERVICE NETWORKING

a Modern Office Methods company

Multifunction Printers and Copiers Network Security – What You Need to Know

Contents

Introduction

Over the last decade, office technology has advanced tremendously. Networked printers and copiers have taken this technology to the next level, providing businesses and organizations with a host of advantages such as flexibility, functionality, increased efficiency, and reduced costs. These networked end-point devices also have the added benefit of expanding employee access to company resources.

Unfortunately, many organizations are not aware of the potential risks involved with networked printers and copiers. Like computers, today's networked multifunction printers and copiers are vulnerable to breaches and hacks unless they are secured and protected. A wide range of organizations, from schools to hospitals to businesses, are all putting themselves and their clients at risk with unsecured end-points running on their IT networks.

The purpose of this eBook is to provide you with an overview of the steps you need to take in securing your multifunction printers and copiers to protect your valuable data and sensitive information. Topics to be discussed include:

- **Performing an Audit of Your Networked Printers and Copiers**
- **Securing Access**
- **Disabling Unnecessary Services and Protocols**
- **Securing Data with Encryption**
- **Keeping Up with Patches and Updates**
- **Selecting Secure Multifunctional Printers and Copiers**

Performing an Audit of Networked Printers and Copiers

Depending on the size and scope of its operation, it is not uncommon for an organization to be unaware of what devices are connected to their network, or whether these devices have been configured with the proper security checks. The printers and copiers themselves can create a security risk if they are running with outdated firmware.

In addition to being a hindrance to productivity, dated printers and copiers can burden staff with an unpredictable maintenance workload and slow down business workflows.

The best place to begin a printer & copier audit is an IT network security initiative. The purpose of the audit is to:

- **Determine what, if any, firewall configurations have been set up for the network**
- **Scan to identify server, endpoint, and network vulnerabilities**
- **Develop plans for risk mitigation strategies to address each vulnerability**

A variety of network assessment tools are available for organizations that would like to do their own audit. Unfortunately, most organizations do not have the time or staff to commit to understanding the full scope of IT needs, including networked printer and copier security.

80% – Percentage of organizations reporting at least one type of security threat/breach within the past year.

Printer Network Audit Assistance

If your organization has not yet established an IT security plan due to inadequate technical knowledge, resources, or staff, qualified and experienced managed IT / print services experts are available to help. The right managed IT / print services provider will:

- **Be able to provide you with a thorough printer and copier network security audit**
- **Have knowledge and insights into current cyber threats**
- **Advise you on the best security software and hardware technology available to meet your needs**

It is important to understand that audits will continue to be needed as part of an ongoing monitoring process. Audits should be scheduled at regular intervals, depending on the complexity of your network.

78% – Percentage of companies that do not monitor their printers for security threats.

Securing Access

Many organizations with networked multifunction printers and copiers do not realize that these devices function much like computers. Like laptops, workstations and servers, networked printers and copiers must be secured.

Start the process of defending your printers, documents and data from network threats by physically securing your printers and copiers. If possible, move printers that are out in the open into a controlled access area. Access can further be controlled by disabling physical ports to prevent unauthorized use.

Access can be further secured by requiring authentication and authorization for access to device settings and functions. Taking this step has the added benefit of controlling printing costs due to unnecessary and unauthorized printer use. Printer security technology experts recommend other security solutions such as PIN authentication, LDAP authentication, smart cards, proximity badges and biometric solutions.

Printer and Copier Security Technology

Innovators of printer and copier security technology are also now developing built-in access control software and other security features. For example, some of the access control solutions include:

- **Access Control Secure Authentication** – prevents unauthorized use of printers and copiers and features while tracking use
- **Capture and Route** – Securely track and control distribution of scanned content
- **Universal Print Driver** – Replaces discrete individual print drivers, and includes special security features
- **Scanning** - Restrict scans to only go to emails on your organization's domain to prevent sensitive information from being distributed directly to personal emails

A final aspect of printer and copier access security that is often overlooked is what to do when you are through using the device. Once you are ready to retire a printer/copier or return it to a leasing agency, it is crucial that you remove any data that may be retained in the hardware's memory. Ensuring that the device's hard disk is erased, destroyed, or removed will provide you with a final added measure of security.

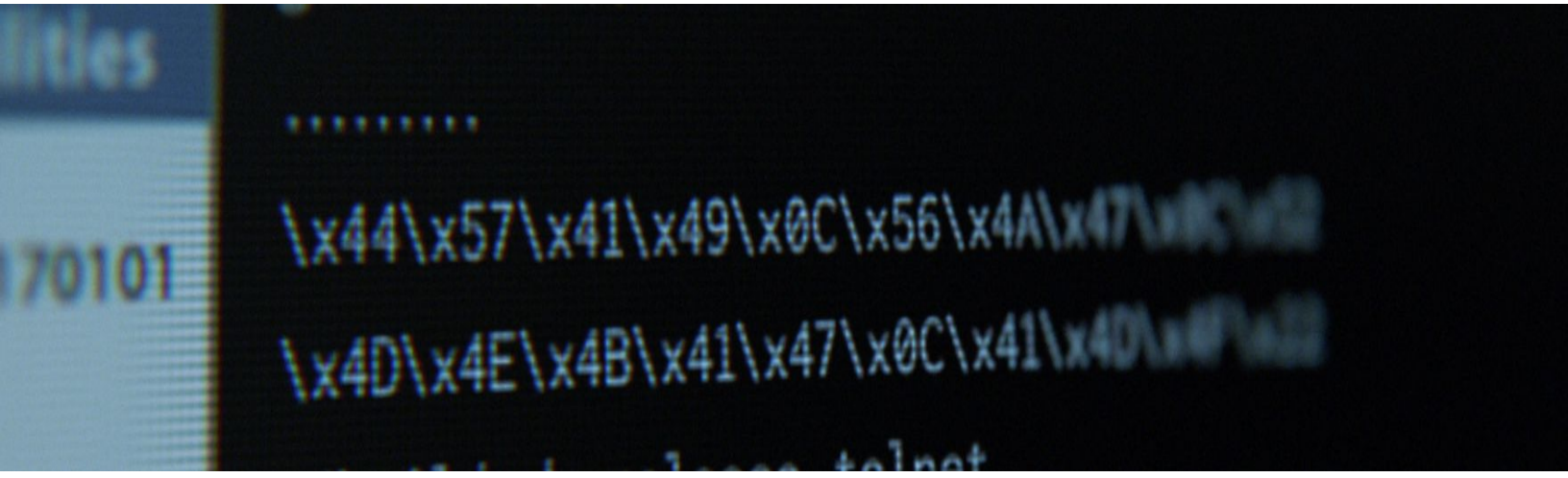
Disabling Unnecessary Services and Protocols

In an effort to provide the users of office technology with efficient, turn-key product solutions, many printer and copier manufacturers are offering models with a wide range of services and protocols built in.

Many of these enabled-by-default protocols (Telnet, HTTP, FTP) are unnecessary and not secure. Leaving these services enabled may provide attackers with the ability to access the printer/copier data directly. If breached, a hacker would have access to all the data stored on the device.

In some cases, printers and copiers utilize more than one web interface, however, if a particular web interface is not needed, the safest approach is to disable it.

29,000 – Number of printers hacker claims to have identified within minutes that were connected to the internet and could be exploited.



Zero-Day Vulnerabilities

Disabling unnecessary services and protocols is a first line defense strategy for heading off what are known as "zero-day" vulnerabilities. These are vulnerabilities that have not yet been identified, but could eventually be discovered and exploited.

Though zero-day vulnerability involves an unknown risk, the risk can still be mitigated by restricting and controlling access to your multifunction printers and copiers. While it is not possible to know every possible point of susceptibility, you can protect your network by identifying and securing every access point through which a cybercriminal may infiltrate and exploit your security.

Lastly, efficiency can also provide security. Rather than having multiple software and hardware solutions, you may be able to employ one unified solution. This solution should involve less complex code, thereby reducing the number of potential vulnerabilities.

35% – Percentage of organizations reporting an internal security threat via printers in the past year.

Securing Data with Encryption

Wireless technology has been an amazing advancement in promoting efficiency and productivity in the workplace. Unfortunately, with the benefits come risks. Your documents and data become highly vulnerable as they traverse the "wireless network" to a multifunction printer or copier. Once your information makes it to the hardware's memory or storage, it is susceptible to attack there as well.

The best way to protect sensitive data within your network is with encryption. Encrypt print and copier jobs to secure data in transit in the event of interception and use encrypted storage to protect documents in the device's queue.

Data can also be protected by authenticating users and attaching them to their specific documents. Document owners are then required to authenticate themselves to the printer or copier before their documents will print. Make sure the end-point device does not store the document or data about the printed document once the print job is completed.

In environments that involve multiple desktop printers and copiers, make sure that sensitive data is not stored on these devices. This is because desktop devices may be more vulnerable to physical theft, and with the hardware, the data could be stolen.

Keeping Up with Patches and Updates

The importance of staying on top of software and hardware firmware updates cannot be overstated. This includes the firmware used in your multifunction printers and copiers.

Firmware is the term used for the software that is embedded within devices like printers, copiers, scanners, and cameras. The role of firmware is similar to the function of a computer operating system. Like the operating system of your PC, firmware enables you to control how your printing device operates.

Firmware is installed when the multifunction printer and copier is manufactured and provides the basic control necessary to use the device. When your printer or copier requires firmware changes, manufacturers will release an update. Firmware updates typically include a combination of fixes for known issues, as well as any applicable new features and improved security.

Some printers and copiers with an internet connection will automatically check for new firmware and install it. Others will require you to periodically to visit the manufacturer website for firmware update downloads, which you can retrieve and install yourself.

Ignoring updates and patches will likely result in the development of critical vulnerability points in your network. These risks may lead to security breaches that create more headaches than the time you saved by ignoring your updates was ever worth.

Keep in mind, updated firmware can end up making changes in your security settings. Once a printer or copier is cycled through a reset, all settings return to the original factory default. After any updates or cold resets, confirm that all security controls are reinstated.

Selecting Secure Multifunctional Printers and Copiers

Without a doubt, the best way to secure your printer and copier is to invest in technology that is pre-programmed with the most up-to-date device security features. Look for multifunction printers and copiers that are designed to independently detect, protect, and self-repair damage from malware attacks.

As you upgrade outdated equipment, replace it with systems that offer built-in threat detection and software validation features, so only authorized firmware and software can be installed and executed. This will provide your network with an extra layer of security.

Are you in need of knowledgeable and experienced assistance with securing your multifunction printer and copier network? Modern Office Methods (MOM) and Full Service Networking (FSN) are here to help.

Contact Us Today!
800-345-3888
Visit Us Online at
momnet.com

Contact Us Today!
888-308-6689
Visit Us Online at
fullservice.net