AFFINITY Enterprises

Your Printer Is Leaving Your Network Wide Open For Security Breaches

PLUS TIPS ON HOW TO SECURE IT

Organizations today are spending hundreds of thousands of dollars on their network security, but are entirely forgetting about an important piece of the puzzle: their printers.

Printers are computers, and like computers, unsecured printers put the entire network at risk for a cybersecurity attack. Printers do more than just print, fax, scan, and copy – they have internal computing, storage, and software solutions and may handle sensitive data. Without proper security, that information can get into the wrong hands.

Once malware is installed on a printer, hackers can do some serious damage, such as:

- ***Gain access to confidential or sensitive information***
- ***Send unauthorized print jobs***
- ***Launch a denial of service (DoS) attack***
- ***Access saved copies of documents***

In 2016, there were more than 400 billion data records breached worldwide which is a 400% increase in just two years. Of those data breaches, 23.4% were government related. [1]

SECURE THE PRINTER

First off, let's secure the device itself, starting with a password. When you first get your printer, the simplest thing you can do to secure it is to change the default password. You can also deploy other options such as PIN authentications, LDAP authentication, smart cards, proximity badges, and biometric solutions as well.

Also be sure that the firmware is regularly updated. Printer manufacturers will frequently send out firmware updates as new threats are discovered, so check for them often and use them.

SECURE THE DATA

Data is most vulnerable when it travels the network wire to the printer or sits in the printer's memory or storage. If you're printing any type of sensitive information – payroll, contracts, or confidential information – it's not safe from hackers unless it has been encrypted.

Encrypt your print jobs during the travel period and when documents sit in the printer storage, waiting to be printed. The encryption converts your information into indecipherable code for hackers, making it useless to anyone who doesn't have the decryption code.

Once a document has printed, do not store the document itself or data about the document on the printer.

Before you retire a printer, wipe all the drives and storage clean. In 2010, a New York State managed care plan company returned their printers to their leasing agent without wiping the data first. It affected 344,557 individuals, whose confidential data was discovered on the hard drives of the returned copy machines. That oversight cost the company $1.2 million paid out to federal regulators for HIPAA violations.2

SECURE THE DOCUMENTS

We never think an attack could be formed inside the organization, but it can be. Documents are left in the printer tray unattended every day – how much of that information is classified? These documents can be viewed or carried off by anyone, inciting a potential security risk.

If possible, enable pull printing on your computer, where a user's print job is held on a server or workstation and released by the user at the printer. This means that nothing comes out of the printer until the authenticated user is there to retrieve it. Retrieval can be done through a smartphone, an access badge, or a PIN number.

PURCHASE SECURE PRINTERS

HP is one of the manufacturers leading the way in high-quality, secure printers. They offer printing devices with unique technologies designed to thwart potential hackers or trigger a reboot whenever an anomaly is detected, keeping your data and your organization safe from attack.

Affinity Enterprises specializes in finding the right hardware for your organization. **Contact us** to secure your printers today.

1. "Data Breaches Exposed 4.2 Billion Records In 2016", Dark Reading, January 25, 2017
2. US Department of Health and Human Services. June 7, 2017.