CANON SOLUTIONS AMERICA

healthcare informatics CUSTOM MEDIA

HEALTHCARE'S SECURITY GAP:

A GUIDE TO MULTIFUNCTION PRINTER RISKS AND SOLUTIONS.

SMART CHANGE STARTS HERE.

CANON SEE IMPOSSIBLE

CONTRIBUTING EXECUTIVES

Matthew Junod
Chief Information Security Officer
University of Toledo

Sean Murphy
Vice President, Chief Information Security Officer
Premera Blue Cross

Shane Pilcher
Administrative Director of Information Services
Siskin Hospital

Mark Sinanian
Senior Director, Marketing Solutions
Canon Solutions America

TABLE OF CONTENTS

INTRODUCTION

In computer networking, hacking is any technical effort to manipulate the normal behavior of network connections and connected systems. A hacker is any person engaged in hacking. The term hacking historically referred to constructive, clever technical work that was not necessarily related to computer systems. Today, however, hacking and hackers are most commonly associated with malicious programming attacks on networks and computers over the internet.

As computer networking and the internet exploded in popularity, data networks became by far the most common target of hackers and hacking. Hardly a day goes by that you don't hear something about a hack or a hacker in the news. Now, however, hacks affect millions of computers connected to the internet, and the hackers are often sophisticated criminals.

Common Network Hacking Techniques

Hacking on computer networks is often done through scripts and other network software. These specially designed software programs generally manipulate data passing through a network connection in ways designed to obtain more information about how the target system works. Many such pre-packaged scripts are posted on the internet for anyone—typically entry-level hackers—to use. Advanced hackers may study and modify these scripts to develop new methods. A few highly skilled hackers work for commercial firms, hired to protect that company's software and data from outside hacking.

Healthcare chief information security officers (CISOs) take the threat very seriously. For example, Matthew C. Junod, CISO of the University of Toledo (Ohio), which includes a healthcare system, says that his organization regularly conducts internal and external security assessments of all data facilities, including printers. His biggest worry about printer security is that a printer will be used as a vector to bypass security controls and invade the rest of the network.

Source: What is Hacking - June 2019
https://www.lifewire.com/definition-of-hacking-817991

In a Ponemon Institute survey, the average cost of a data breach in healthcare is $6.45M.

The average cost per record in healthcare is $429. The average size of a US data breach included 26,523 records.

51% of breaches were malicious attacks – 24% were caused by human error and 25% were due to system glitches.

Source: 2019 Cost of a Data Breach Study by the Ponemon Institute and IBM Security

Sean Pilcher, administrative director, Information Systems, at the Siskin Hospital for Physical Rehabilitation, Chattanooga, TN, acknowledges that it is possible to hack data in transit to or from a printer. His hospital has begun to encrypt data in transit, he says, and it is implementing a new solution that enables central control of all printers in the organization.

Sean Murphy, vice president and CISO of Premera Blue Cross in Seattle, has had a long career in health IT. Asked whether hackers could intercept documents in transit to or from printers or take over a printer and intercept data there, he says, "Both scenarios are likely and have been done in various capacities."

MULTIFUNCTION PRINTERS

Single-function printers attached to PCs are less vulnerable to hacking and malware than are multifunction printers (MFPs) that have full-fledged CPUs, hard drives, and operating systems, notes Mark Sinanian, senior director, Marketing Solutions for Canon Solutions America.

"MFPs, by their nature, have more features and functionality and integration scenarios than their print-only cousins," Sinanian explains. "Because of those capabilities, there are a lot more systems embodied in that product, and as a result there's more opportunity for a security breach if the device is not secured properly."

Of the 29 million printers in the U.S., 88% are single-function printers, Sinanian says. Although they may not have any exposure to the web, these printers have their own security vulnerabilities, he says.

"Depending on when those devices were put into service, they may or may not have the security features you see in today's devices. The single-function printers, in particular, stay out in the fleet for a very long time, longer than MFPs."

This paper explains why health IT professionals should be concerned about printer security and what they can do to protect both their printers and their networks.

> "Chances are that organizations are going to have printers that don't have the security features of modern printers. The same is true of older MFPs."
>
> —*Mark Sinanian*

HACKING

Security breaches are dangerous in any organization, but in healthcare organizations they can be even worse. Much of the data that flows through care providers is PHI, which these organizations must protect to comply with the Health Insurance and Portability and Accountability Act (HIPAA). Failure to provide adequate data security could result in fines and bad publicity. Moreover, if a hacker uses a printer to take over a provider network, operations that are essential to patient care could be severely compromised. Malicious software, such as ransomware, could shut down the entire system.

Cyber thieves have many routes to steal the data sent to and consumed by printers, especially MFPs. Hackers have their choice of intercepting data in transit, seizing control of printer software, or even gaining control of a print server. If a printer runs a web service, Junod says, and there's a security hole in that service, hackers could use that vulnerability to create a botnet to intercept data sent to the printer.

MFPs are especially at risk because they can send and receive information over the internet, notes Murphy. He suggests giving MFPs private IP addresses or creating virtual local area networks (VLANs) to make sure they're not directly interfacing with the internet. Unless they have a business requirement to connect to the web, these printers should be locally routable, he says.

Sinanian agrees. "Our security experts believe that it's never a good idea to connect a printer IP to the public internet, especially with older printers that lack security features or even other MFPs where the security features aren't configured," he says. Instead, Sinanian believes they should be sequestered behind a firewall with proper security settings.

ENCRYPTION

Pilcher's department at the Siskin Hospital has begun encrypting data in transit, and highlights this as a particularly effective strategy. "If somebody penetrated our system, they wouldn't be able to grab encrypted data flying across our network," he says.

Encryption makes it very difficult to snatch print jobs being transmitted to printers, Junod agrees. "You'd have to be on our network to do that. You'd have to control some path between the asset and the printer."

Sinanian similarly believes that encryption is essential to printer security. Canon's printer systems, he says, can be used to encrypt not only the print job but also the transmissions to and from the device, including the "send" protocols.

In Murphy's view, encryption is the best defense organizations have against hackers, but it's still limited. If someone has the key to decrypt a print job, he notes, they can steal whatever is in it, and purloined network identification can provide that key. Murphy further clarifies that intrusion protection devices which sit at the perimeter of a system are only as good as the rule set used in that software. "By and large, it's a good defense mechanism to weed out generalized attacks," he says. The same is true, he adds, of antivirus software.

The University of Toledo has installed intrusion detection software at its perimeter to monitor traffic in and out of the system, Junod says. The application, which includes specific rules to detect printer attacks, notifies administrators of any traffic that doesn't match certain signatures; but it's just one among many security tools that the organization uses. Other safeguards include audit trails and aggregated logs that monitor activities across the network, he says.

MALWARE

Many malware attacks rely on human fallibility. Phishing attacks, in particular, depend on endpoint users downloading attachments that contain malware. However, Junod says, it is unlikely that someone could infect a printer with a malware attachment they opened and sent to that printer.

> "Most of the time, the attachment is being opened by something like Microsoft Word, and Word is calling an API in the computer to print," he explains. "There's a device in the printer that takes that raw input and turns it into something the printer can understand."

However, some printers have features that allow authorized users to email jobs to them from an outside computer or mobile device. "Some of them have network shares or FTP (File Transfer Protocol) servers," Junod notes. "And there could be a vulnerability in the printer's interpretation engine."

At the University of Toledo, most printing is done at local sites. Junod says that if a physician needs to send information from his office to the hospital, for example, or to another physician office, he or she would normally fax it or transmit it electronically, which means that emailing print jobs from one site to another is not an issue.

Pilcher says he has never considered the possibility of malware being transmitted to a printer from outside the system. However, Sinanian and Canon recognize this as a real possibility. Sinanian says Canon Solutions America has such threats covered with a security feature that can detect if there's a virus in the email attachment or even in the body of the text. If the printer finds a difference between the normal format of an attachment and an attachment with malware in it, it immediately deletes the job.

The University of Toledo and Siskin Hospital both use print servers. Pilcher points out that Siskin's print server has a security feature that can detect malware before a job is routed to a printer. But, he admits, "nothing is 100%."

As with a singular printer, it is also possible for an attacker to take control of a print server. "That's another vector you could use to intercept a print job," says Junod. "In fact, if a server were to be compromised, theoretically you could intercept all the data flowing through it. But if you were in a position to do that, there would be easier ways to access PHI. If you've already compromised the server and the environment, you're going to go after a database server or an application server."

AUTHENTICATION

Healthcare organizations authenticate network users to ensure that they're authorized to access the network. For printers, there are some MFPs that offer more advanced forms of access management which can improve security while enhancing productivity and lowering cost.

An advanced MFP can authenticate users using a proximity badge, smart card, magnetic swipe card, PIN, fingerprint, or username and password. In addition, a user could be asked to select his or her own photo on a screen and then to enter a PIN. If a proximity badge is used, it would normally be the same one that the employee uses to enter a building or go through doors in the facility.

Multi-factor authentication provides an effective way to deter hackers from impersonating authorized users, Murphy says. However, he notes that PINs are not terribly effective because they can be stolen. A hard or soft token, a device in which the authentication numbers keep changing, is better for this purpose, he says.

The advanced type of access management is deployed for other purposes besides authentication of a user's identity. First, because authentication is controlled on a central server rather than individual printers, authorized users can access not only the first printer they encounter, but also every other printer in the facility during a shift. Second, this type of solution requires a printer to hold a print job until the person who sent that order shows up at the printer to release the job. That capability safeguards PHI by ensuring that the copies are not left in a tray and are not retrieved by someone else who may or may not be authorized to see the information.

Pilcher likes the "hold job" feature, not only because it improves HIPAA compliance, but also because it reduces cost and increases productivity. "If a printout is never picked up, that adds to cost," he points out. "If the job is never released, it's deleted and never goes to print."

An MFP that includes this type of authentication can also provide role-based access to individual users, depending on their function in the organization. For example, some users might be allowed to copy documents, but may not be permitted to scan them into the EHR or to send scanned documents to other departments or organizations. This could have a security benefit if it prevents someone who is not familiar with security rules from scanning documents and sending them to the wrong place by accident.

Pilcher also sees a cost advantage in this feature. "In the past, we controlled cost by controlling access to the device, making it inconvenient as much as possible," he says. "Now we're controlling cost by controlling a user being able to use it in a certain way. We don't have to make it inconvenient for the user, and we can control it a lot more effectively."

CONTROL

The CISOs and experts emphasize the need to control all aspects of printer management. A big part of that is keeping track of the printers in an organization and discouraging users from adding their own. For example, the University of Toledo has about 4,000 printers, including around 1,000 MFPs, says Junod. The MFPs are found in the hospital and the ambulatory clinics as well as across the university. The IT team has been trying to consolidate those printers and limit them to a few models, but because departments have their own operating budgets and spending authority, "things slip in, especially in the research areas," he notes.

Nevertheless, no one in the organization can connect to the network without IT being involved. So, even if somebody buys a printer on their own, IT can stop it from being networked and creating a potential security hole. Even if individually purchased printers are hooked up only to single PCs, Murphy points out, they still have security vulnerabilities. Even further, Junod says that his department is trying to control the variety of devices on the network.

> "We also do vulnerability scanning every two weeks against every IP address across the entire university," he notes. "So we're scanning printers for security holes. That could be default passwords, holes in the secure code revisions, and a number of other potential risk factors."

As for the scenario where print jobs are emailed in, Junod says, "You'd have to route them. You couldn't hit the printer directly." He recommends using a print server as a routing device to "keep the bad guys out."

Organizations can also protect their printers by building a rule set for intrusion detection software, Junod notes. Such a rule set, according to Junod, should include "the IP addresses the printer is supposed to talk to and the protocols you should be using."

A printer is a peripheral and doesn't do a lot of different things, he observes. "You should be able to at least predict what kind of communication it's going to engage in. If all of a sudden your printer tries to communicate out of an unassigned port, you might have an infection. You might have somebody exfiltrating data."

CENTRAL SERVER

Another method of centralizing control, Pilcher says, is to adopt a solution that allows IT administrators to manage all of their printers on a single server. This is the kind of solution that Siskin Hospital is now installing, he reveals.

As Pilcher explains, the organization has 34 MFPs and will replace them all with products from a single vendor. In addition, Siskin is adopting a solution that will change how users are authenticated on these MFPs. Network authentication for printers will now be controlled on a secure server rather than on individual printers, Pilcher says.

The MFP solution will include role-based authentication, the "follow me" system that allows users to access any printer in the facility, and the "hold jobs" feature that withholds copies until the user appears and is authenticated. Unlike the University of Toledo, which has turned on the "hold jobs" function only in selected printers, Siskin Hospital plans to use this feature throughout the facility.

From a security/privacy standpoint, Pilcher notes, his organization could have limited "hold jobs" to unsecured areas like nurses' stations. But from a cost standpoint, he argues, requiring controls on the release of documents drives down printing costs.

Overall, Pilcher is not very satisfied with the security features that are built into some MFPs.

> "But some of the add-on solutions, such as controlling software, increase my satisfaction significantly," Pilcher clarifies, "because now I'm able to control the security at a granular level that I didn't have without it."
>
> *- Shane Pilcher*

FAXING

Health IT security professionals don't like faxes, partly because they generate paper that sits in the trays of fax machines and MFPs. This can create a HIPAA problem if they're not picked up or if they're picked up by someone other than the intended recipient. In addition, MFPs save faxes to their memories, making that data vulnerable to hacking. Outgoing faxes also present HIPAA issues because they can't be encrypted, they can be sent to the wrong phone number, and even if they're sent to the right number, it's impossible to know who is receiving those faxes.

"Encryption provides not just confidentiality but often authenticates the recipient," Junod notes. "In an encrypted transmission, you generally know who's on the other side. But with a fax, you just know you've sent it to a phone number. It's a lot harder to authenticate the remote sender. I don't like fax technology for that reason, but it's not likely to go away anytime soon in a clinical environment."

Both Junod and Pilcher say their organizations use fax servers, which can detect malware. In addition, Pilcher says, Siskin Hospital makes special efforts to ensure that fax numbers are as accurate as possible. "We try to do most of our faxing from an approved, pre-programmed fax directory so that it diminishes the ability to mistype the number," he says.

Inbound faxes can also be routed to a secure location, perhaps through a fax server, Sinanian points out. They could go to a secure mailbox on the MFP that the user can unlock only after they authenticate themselves.

MFPs that interact with fax servers or document management solutions can ensure that faxes never sit in a paper tray, he says. "They're always secured in a location, whether that's on the hard drive that's on the device itself, or routed to a fax server, or to a content management solution where it's indexed, archived—that way you have an audit trail around it."

SCANNING

The security features that Siskin Hospital is putting in place for scanning are similar to those for printing under its new centralized solution. The ability of users to scan documents is controlled by their role-based access to that feature. Scanning also goes through specific servers that have their own security mechanisms, Pilcher says.

Pilcher's main concern about scanning is that a scanned document, like the aforementioned faxing concerns, could be sent to the wrong place. For example, a clerk scanning in a clinical document might place it in the wrong patient's electronic health record. To prevent that, Siskin Hospital requires that scanned documents go to a data repository before entering the EHR. They can also go to shared drives with user permission or to secure personal file stores that are made available to certain users, but they can't go to an unsecured open access folder on the network, he says.

Physicians often wish to scan documents themselves, usually to send them to other doctors. Pilcher says they have the right to scan because this is a task that is part of their job, but if they want to attach a document containing PHI to an email, both the document and the message must be encrypted. With the new solution that requires everyone to "badge in" for authentication, the physicians can scan directly from the printer to email. They can do that because the new system allows administrators to track who sent that email and whether they had the right to scan, Pilcher says.

> "When you scan to an electronic format, you have to pay close attention to the security controls around your file server," Junod continues. "Whatever technology it's using to save that scanned document, you want to have a security control on that."
>
> *- Matthew Junod*

Junod also emphasizes the importance of authenticating users who scan documents. Beyond that, he says, the big questions are where the document is going and how it's being transferred. "Is the MFP dropping it into a file share, or is it sitting in an email?" he asks. "And if it's going by email, is it being sent outside your organization or within?"

Sinanian views scanning security as a function of authentication, which can be used to configure workflows on Canon's MFPs. "When you authenticate, your scanning workflows follow you from machine to machine," he explains. "You can only scan to the destinations you're supposed to scan to. It's another way of controlling access and ensuring documents and images go to the right location."

The same process can be used with doctors and other casual users of scanning, Sinanian says. "You set up the screens so that they're easy to navigate and they send you only to the destination you need to go to. So authentication unlocks the possibilities of the [MFP] machine. When the machine knows who you are, you can customize the user experience however you need to, including the functions the individual has access to."

If organizations really want to take document scanning security to the next level, they can implement enterprise digital rights management (EDRM) into the scan workflow. Here's how it works: once the document is scanned on the device, it is routed to a cloud-based destination where an encryption wrapper is attached to the file before it moves on to its final destination. Because the encryption key resides in the cloud, the document owner can control access to the document anywhere it travels to or resides.

The document owner can grant or revoke access in real-time as well as monitor the file usage. The owner can also restrict the use of the document relating to printing, copying, scanning or even preventing screen shots. This can be a very positive contributor towards compliance with HIPAA guidelines and to protect PHI. It can also be an added security measure in the unfortunate event of a data breach.

PHYSICAL SECURITY

The physical security of printers should not be taken for granted. To begin with, printers should generally be in a back room out of public view, and that room should be locked up after hours, Murphy says. Otherwise, maintenance people could walk away with a hard drive or an entire printer. Security cameras set up in a printer room or other printer locations can help security personnel keep a close eye on the printers.

> "It is possible for someone to insert a USB stick into a printer and infect it with malware," Murphy notes. "Even if people are prohibited from using the USB drives in printers, maintenance people could come in and plug in a dongle."
>
> —*Sean Murphy*

Before an organization removes a printer from a facility, it should ensure that the device's hard drive is pulled out and destroyed. Pilcher explains that some of Siskin Hospital's printers are leased, and the organization has the right to retain hard drives under an agreement with the leasing company.

Murphy stresses the importance of working with "good solid vendors that have good security practices in terms of bringing in the device, maintaining it, and disposing of it." He further advises a regular audit of these vendors and to make sure they destroy the hard drives of decommissioned printers if the organization is not doing that on its own.

A vendor worth their weight in salt, so to speak, will also offer to assist a customer with recommendations for hardening the device. Hardening is the process of limiting the exposure of the device to the outside through port management and network settings utilizing IPsec and advanced encryption transport protocols. The golden rule of security professionals when it comes to device hardening and port management is: if you don't need it, turn it off!

Training employees on printer security practices is also essential, our experts say. At the University of Toledo, Junod notes, "It's generally part of technology training. Every employee at the university, including in the clinical area, gets basic training when they're hired. Clinical employees get mandatory training every year, usually delivered electronically with video. The topics include the physical security of technology. All high-level stuff, but most people would be able to absorb it."

CONCLUSION

From a security standpoint, not all MFPs are created the same. Some have better security features than others. And, even if they have advanced features like network authentication and encryption, those might not be easy to configure. "The problem is that printers generally don't come secure out of the box, and they're also hard to manage in a secure fashion," Junod says. Moreover, he believes that vendors need to test their devices better. "We see devices that have security flaws which don't get fixed," Junod states.

Nevertheless, the best MFPs—which provide features such as role-based access and "hold jobs" functionality—represent a significant advance over previous models, our experts agree. Moreover, individualized printer workflows can improve productivity and reduce printing costs while enhancing security.

No security approach is foolproof, and cyber thieves are always devising new ways to attack healthcare organizations. But health systems and organizations that pay attention to printer security are closing a significant loophole in their overall security strategy.

"You have to incorporate printers in your enterprise security strategy so you have the protections in place and the compensating controls to either identify those risks, protect against them, or detect any injections of malware," Murphy declares.

Part of that strategy is to incorporate printers into vulnerability scans like the ones that the University of Toledo does for all of its IT assets. At the end of the day, an MFP is a computer like any other computer on an enterprise network. It has many of the same vulnerabilities to cyber-attack that any desktop or workstation has.

Sinanian advised, "The good news is they have a lot of security features and functionalities built into them that, if leveraged correctly, can mitigate a lot of the risk. You need to treat printers just like you do your servers and your workstations and secure them in the same regard."

> "Look at today's MFPs the same way you would any network device that's handling confidential information," Sinanian says. "These devices have all the same capabilities as a regular PC. They've got CPUs, hard drives, RAM, and in some cases they're running operating systems similar to the ones on your desktops. Confidential information is flowing through them every day, and they have similar vulnerabilities."
>
> *—Mark Sinanian*

Canon

CANON SOLUTIONS AMERICA

1-800-815-4000 CSA.CANON.COM

Canon Solutions America does not provide legal counsel or regulatory compliance consultancy, including without limitation, regarding Sarbanes-Oxley, HIPAA, CCPA, GDPR, GLBA, Check 21 or the USA Patriot Act. Each customer must have its own qualified counsel determine the advisability of a particular solution as it relates to regulatory and statutory compliance. Canon products offer certain security features, yet many variables can impact the security of your devices and data. Canon does not warrant that use of its features will prevent security issues. Some security features may impact functionality/performance; you may want to test these settings in your environment.