Security at the Edge: Protecting a Network Must Include Endpoints

"Attackers are always looking for an easy way into the network."

– LEE KIM
DIRECTOR OF PRIVACY AND SECURITY
HIMSS

On Feb. 3, 2017, some 150,000 internet-connected printers worldwide generated a printout notifying owners that their machines had been compromised. According to news reports, the text-based notes were the work of a teenager in the United Kingdom who exploited a vulnerability in the printers.[1]

Although that instance turned out to be an innocuous prank, it surely caught the attention of network administrators in healthcare organizations, who have come to view edge devices as security nightmares. In the rapidly expanding Internet of Things, every printer, PC workstation and mobile device that connects to a hospital's networks has become a potential "open door" for cybercriminals looking to steal valuable personal health information or to lock up critical data for ransom.

"Attackers are always looking for an easy way into the network," said Lee Kim, Director of Privacy and Security at HIMSS. "What's always optimal is for them to find an entry point where they don't have to authenticate and can get an extremely complex root or administrative password with relative ease."

Connected computing devices on the edge of a network – such as a tablet or PC workstation – can have their own IP addresses exploited to a hacker's advantage. That can make networks vulnerable to a variety of cyberthreats, including malware attacks, advanced persistent threats and DDoS attacks.

That's also true of networked printers. "It's too often the case that the credentials to access the printer – such as username and password – have not changed. So, hackers will use that printer as the point of entry into your system," Kim said.

Once they gain access, the damage to healthcare organizations is enormous. Last year, breaches cost up to $355 per healthcare record – compared to $158 for other pilfered confidential data, according to a 2016 Ponemon Institute report. Another estimate pegged the healthcare industry-wide cost of breaches and prevention efforts at nearly $6 billion. Experts say healthcare records are particularly enticing to cybercriminals because they provide rich, holistic data for identity theft, fraud or phishing scams, as opposed to financial data, such as credit card or bank records, which can be changed.

In 2015, Ponemon partnered with HP to gauge endpoint security among 2,000 IT security practitioners in the Americas, EMEA and Asia-Pacific. Among Ponemon's key findings was a lack of employee awareness (at least among non-IT staff) that printers, PCs and other devices posed an intrusion threat, especially among executives, sales and human resource departments.

> We have seen anywhere between a 50 to 60 percent increase in attacks on the ends points in the last few years. That's because hackers have realized that's a vulnerability that we have not put enough guardrails around."

– GAGAN SINGH
VICE PRESIDENT OF PREMIUM PRODUCT MANAGEMENT,
SECURITY, INNOVATION AND SOFTWARE
HP

"So much of what we do in the business world is to take functionality for granted and not think about security," Kim said. "Unfortunately, I don't think healthcare organizations will take to heart the need for better printer security or IoT security unless and until regulators step in and try to enforce against some kind of deficiency."

Gagan Singh, Vice President of Premium Product Management, Security, Innovation and Software at HP, agreed that PCs and printers are not top of mind when healthcare providers think of IT security. "We have seen anywhere between a 50 to 60 percent increase in attacks on the ends points in the last few years," he said. "That's because hackers have realized that's a vulnerability that we have not put enough guardrails around."

Without a carefully designed security solution, the sheer number of end points can quickly grow beyond the IT department's capacity to keep tracking, keep patching and keep protecting. Putting "guardrails" around centralized servers is one thing, but ensuring the security of every PC and device that connects to the network – especially in the BYOD era – is of another order of magnitude in difficulty using only traditional network tools. But it is essential to ensure that policies are being adopted and implemented at every endpoint.

"If you block one point of entry, they will look for another one," Singh said. "And it is more likely to be a printer because it has an embedded operating system and a BIOS (below the operating system). It also mostly likely has no firewalls or anti-malware software to help protect it."

Healthcare IT leaders should look for security solutions that enable easily managed, multiple layers of security. Start with protecting the BIOS, which is the operation that kicks in from the time someone presses the power button to when the operating system is fully launched. Then make sure there are multiple authentication factors to both verify and limit access to printers, PC workstations and other IT devices that connect to the network. For busy clinicians, this can be a smart card and/or biometric authentication that minimizes login effort and doesn't interrupt clinical workflows.

"Many times, enterprises will spend an inordinate amount of money on things like firewalls and malware protection, and then nothing on authentication," Singh said. "Map out the threats in all the ways you can be attacked, and make sure those devices have coverage. Always remember: If you close 10 doors but leave one open, it won't matter that you closed 10 doors; only that someone still got in."

[1] Iain Thomson. "Hacker: I made 160,000 printers spew out ASCII art around the world," The Register, February 6, 2017, https://www.theregister.co.uk/2017/02/06/hacker_160000_printers/

About HP:

HP is a recognized leader in computing, imaging, and printing technology and services around the world. For more than 50 years, HP has been working to help make healthcare more inclusive, and responsive. Today, we leverage the latest advances in mobility, cloud, and security to help enable providers and empower patients with intuitive solutions that securely access relevant data, applications, and services to deliver better care and patient experiences.

The depth and breadth of the HP healthcare portfolio, backed by a full suite of HP support services, make it easy for small practices and big health systems to get everything they need from a single source.