Print Devices:

An Overlooked Network Security Risk

Print devices are significantly overlooked in most IT security strategies, despite clear evidence they are an easy target for cyber criminals.

START ▶

hp | IDG STRATEGIC MARKETING SERVICES

Print devices are not getting enough attention in the enterprise's IT security strategy. Only 30% of IT professionals recognize printers as a high security risk, according to a May 2018 Spiceworks survey.

And yet 59% of organizations have reported a print-related data loss in the past year, according to a 2019 Quocirca analysis and trend report.

Cyber threats targeted toward printer and Internet of Things (IoT) devices have increased more than 200%, according to the 2019 SonicWall Cyber Threat Report.

The writing is on the wall: As an endpoint device attached to the network, the print device is a significant security risk. Just like IoT sensors, today's modern, intelligent, programmable print devices are routinely connected to the internet and the corporate network—in turn expanding the enterprise cyber attack surface.

"With the universe of connected devices growing exponentially, so is the sophistication and volume of cyber attacks and data breaches; this includes an increase in focus on enterprise printers, which tend to be the more sophisticated devices on the network comparable to PCs," Shivaun Albright, Chief Technologist of Print Security at HP, told *Forbes*.

Cyber threats targeted toward printer and Internet of Things (IoT) devices have increased more than 200%

This paper examines why print devices make easy targets for cyber criminals, and how organizations can better address print device security to manage and help reduce risk.

Only 30% of IT professionals recognize printers as a high security risk

Printers Are a Target

Even more so than a PC, a print device can be an easy target for cyber criminals to gain access to the network. Many enterprise printers are not hardened, have no access controls or authentication policies in place, don't use encryption, and/or are running outdated firmware, based on HP Security Advisory Service risk assessments.

Hackers look for these under-secured, unmonitored endpoints to gain entry to the network. By infecting a print device, hackers can then move laterally through a network and cause damage while they remain hidden.

"We've compromised a number of companies using printers as our initial foothold. We've moved laterally from the printer, find the Active Directory, query it with an account from the printer and bingo, we hit gold," writes Peter Kim in his book *The Hacker Playbook 2: Practical Guide to Penetration Testing.*

How do hackers exploit vulnerabilities and gain entry to print devices? There are several methods:

Remote attacks. The hacker runs execution code via a multi-function print device's telephone line. Or they send weaponized Postscript or Office files as a phishing attempt. These strategies bypass firewalls and can be used to then move across the network for further exploits.

Physical attacks. The attacker physically plugs in a USB drive to the print device. If this maneuver is not discovered, the criminal can move through the network to exfiltrate sensitive data.

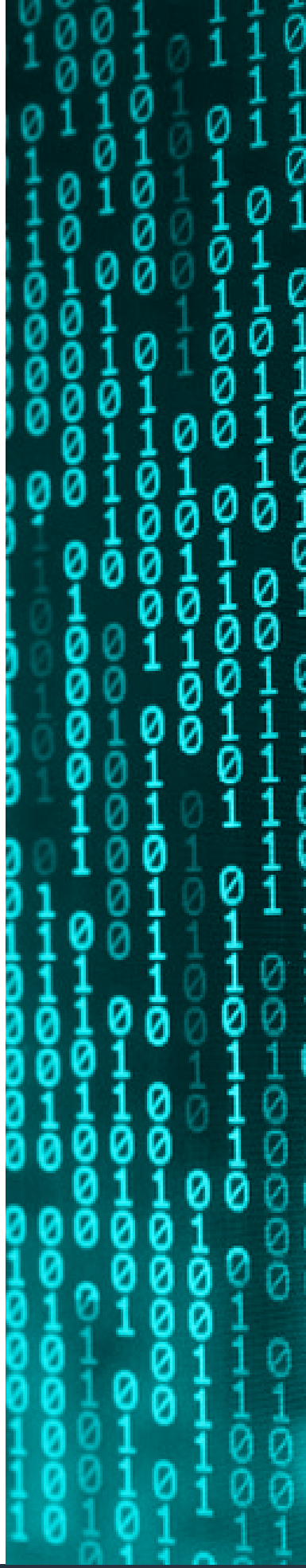
Wireless hacking. A smartphone with stolen credentials can send malware to local printers. Taking it a step further, Singapore researchers attached a mobile phone to a drone, and then demonstrated how the device could intercept data to or from an open, wireless print device.

The use of hacking tools such as Metasploit or Mimicatz allow hackers to scan the printer and local subnets for data such as user information and admin credentials that can provide access to different networks.

Exploit old protocols or system services typically available on printers to run malware.

Take advantage of misconfigured devices, especially those set up with default accounts or passwords.

Once attackers are in, they can remain hidden on the network, and cause serious damage (see Printer Exploits box below).



Sophisticated Technology—But Often Overlooked

Today's modern print devices are sophisticated, vulnerable pieces of network technology. For example, printers are similar to IoT devices with built-in proprietary software; they are intelligent, programmable, and internet-connected. In addition, multi-function print devices use powerful capabilities to process and transmit data, as well as scan to USB and email.

In addition, today's print devices are built with connectivity functionality such as remote management and smart application access. They are often connected across multiple network subnets with varying trust levels, making them a viable source for hackers to move laterally through a corporate network.

Each print device comes with its own set of proprietary software that must be configured, patched, updated, and monitored. Like other providers of software and proprietary systems such as IoT devices, the print device manufacturer has the responsibility to patch and provide security features such as malware detection.

Also, IoT manufacturers often lag in incorporating security features. As described above, there are numerous ways that attackers take advantage vulnerabilities, especially in off-the-shelf devices, making it critical for enterprises to take printer security seriously.

So, why are these sophisticated pieces of technology overlooked?

A significant part of the issue is a general lack of IT visibility and/or a lack of risk prioritization. For example, print devices are often installed, managed, and/or connected to the network by individual business teams in a very decentralized manner; thus, the enterprise has zero visibility. Or print devices are deployed by

IoT manufacturers often lag in incorporating security features

facility and procurement departments as a continuation of legacy processes established originally for copiers and fax machines. Often, IT has no knowledge of these print devices, meaning their configuration management database of devices on the network is outdated and incomplete. This is the case for 55% of companies[1], according to HP security risk assessments.[2]

Another reason print devices are overlooked: Companies think existing protections like firewalls are sufficient. However, in its threat investigations, SonicWall found cyber criminals are using malicious PDF and Office files to get around these security controls—to greater effect. That's because it takes only one user to send a print file with a weaponized Postscript file to initiate a stealth attack.

In addition, it's common for the IT staff to neglect print devices due to the sheer volume of devices across the enterprise. The typical organization has deployed multiple print device brands, each with its own set of proprietary software to configure, patch, update, and monitor. For example, a multi-function print device can have up to 250 security settings that must be configured. The Spiceworks survey found that many IT departments simply don't have the time and knowledge to keep up.

Cyber criminals are using malicious PDF and Office files to get around security controls

[1] Based on data from 1.2 million printers, using the HP firmware tool.
[2] Stats are calculated by HP using an internal HP database of results from assessments conducted by HP Print Security Advisors (78 assessments in the database, as of February 2019).

What's more, in some scenarios IT professionals view security monitoring for print devices as a nuisance. These tasks are given low priority because print logs are complex to interpret; staff suffer threat-alert fatigue from false positives; or there is an inaccurate attitude that other intelligent, programmable, and connected devices such as PCs pose a greater security risk. Each of these reasons is evident from HP Security Advisory Service risk assessments[2]:

of companies do not periodically review logs

of companies' print and scan jobs are not encrypted while in motion

of companies' printer logs are not enabled to identify logon attempts or changes to access control

of companies do not produce or regularly review print security compliance reports

of companies have not enabled anti-malware on print devices

of companies do not have security awareness training around IoT and printers

of companies have insufficient audit event log storage space needed for security investigations

of companies use generic accounts for print fleet management solutions and servers

All of these examples make it clear that organizations need to address print device security

5 Steps Toward Print Device Security

There's a better way to ensure print device security, including starting with an assessment and looking to your managed print services (MPS) provider to take on IT security tasks.

Print devices must become part of the organization's overall IT security strategy. To that end, analyst firm Quocirca offers some of the following recommendations:

1. Assess security and risk. Organizations must treat print devices like any other IT endpoint and build them into the overall security strategy. Start by evaluating the existing fleet to discover potential vulnerabilities and develop a foundation for ongoing device monitoring.

2. Buy with security in mind. During the procurement process, evaluate printers for built-in security features such as intrusion detection, white-listing, and syslog data collection with links to security information and event management (SIEM) tools.

3. Strengthen printer use and maintenance. Change default passwords for print devices to complex ones, as advised by the National Institute of Standards and Technology. Use encryption services and protocols to ensure secure transfer of print jobs. Also, consider automating the process of firmware updates for easier management.

4. Continuously monitor. Network monitoring and alerting tools track devices to provide a secure view of the entire print environment. Use the data generated by multi-function printers, for example, to identify and respond to security incidents.

5. Consult with experts. MPS providers offer a wide range of services, including full assessments of the print environment and evaluation of potential vulnerabilities. They can also take on a wide variety of security tasks, such as training users on the need to protect sensitive information, thus reducing the burden on IT teams.

5 Steps to Button Up Print Device Security

The Bottom Line

At the end of the day, print devices must be included in any IT security strategy. Just like PCs, they carry multiple vulnerabilities and risks. And just like IoT devices, they are an endpoint entry onto the network, where the potential for damage multiplies.

According to a 2019 report by Quocirca by analyst Louella Fernandes: "Print security is becoming a greater concern to businesses with 59% reporting a print-related data loss in the past year... It is imperative that businesses become more print security conscious, particularly as they look to close the paper-to-digital gap in their business processes."

Fernandes goes on to advise, "By using the appropriate level of security for their business needs, an organization can ensure that its most valuable asset—corporate and customer data—is protected. Managed Print Service providers are well positioned to provide the support and guidance needed. There is no room for complacency, given the far-reaching repercussions—legal, financial and reputational—of print related data losses."

The Growing List of Print Exploits

The seemingly innocuous printer has become a prime target for hacks and attacks. Vulnerabilities and examples include:

- A print device was the entry point for an India bank heist. Even IT administrators initially thought it was simply a device error, and rebooted the system.
- Print devices at the Norwegian Parliament had to be taken out of commission due to alleged Russian espionage.
- Researchers discovered thousands of 3D printers had no password protection, leaving 3D model plans and webcam feeds exposed.
- A vulnerability in a multi-function printer enabled a hacker to compromise the device—by sending a fax.

Get Print Security Help From the Experts

Commit to assessing your enterprise's print situation. The HP Print Security Advisory Service helps companies develop a cohesive strategy to protect the business. The Service includes an in-depth security risk assessment, including a detailed security risk report down to the device level, security policy guidance, and solution recommendations. **Download a brochure here.**

4AA7-5851ENW, July 2019