IDC MARKET SPOTLIGHT

The GDPR Blind Spot: Why Printers Represent a Weakness in Compliance

July 2017

By Duncan Brown

Sponsored by HP

This IDC Market Spotlight highlights the vulnerable nature of printers in enterprise networks and, in particular, how this vulnerability impacts a compliance program focused on the General Data Protection Regulation (GDPR) and other forthcoming legislation. The paper also provides steps to reduce the risk that unsecured printers pose to the business.

Introduction

The attention given to Internet-of-Things (IoT) security grew significantly following a series of high-profile distributed denial-of-service (DDoS) attacks that focused a huge volume of malicious traffic from thousands of compromised surveillance cameras, digital video recorders, and other connected devices to bring down popular websites. What device will be targeted next?

As we look for other IoT devices that share some of the characteristics of the devices used in the latest attacks, our attention is drawn to consumer, small business, and enterprise printers. Software updates and access control, which are priorities on traditional IT products, are often overlooked on printers. Printers may be the next vector for a large IoT attack but could also pose new dangers to business operations because they reside inside the corporate network, offering the potential for data theft and DDoS on the internal portion of a network. With the business consequences of personal data breaches elevated by GDPR and other incoming rules, the network printer is the forgotten endpoint that needs urgent attention.

Your Printer Is an Endpoint

Consider the following scenario: An unknown device is placed into an enterprise network, behind perimeter defences such as firewalls, intrusion prevention systems, and other IT infrastructure, so that the device has unfettered access to all the corporate network resources. A web server is embedded into the device to maximise the device's functionality. All the ports will be set as "open" by default and enable the connectivity with as much as a gigabit of Ethernet connectivity to make the device accessible. The device will have a rich OS such as Linux to maximise functionality. It will not be examined on an ongoing basis using the enterprise's vulnerability scanner as the embedded web server will likely light up the organisation's security information and event management (SIEM) tools with false positives. The vulnerability scanner will be configured to ignore the device, leading to the conclusion, depending on the brand, that the device will not be updated, maintained, or patched during its 5- to 10-year useful life. Device protection will consist of a default password, and unvetted third parties will maintain the device. The device will be core to organisational productivity, so there will be one of these devices for every 10 employees. These employees not only will use this device but also will actively send sensitive personal data to it, where it is stored. Worse, that data can be output to the casual bystander, with no authentication or access control.

Some might call this a nightmare; some might call this a printer.

A very important point needs to be clarified. "Print security" is a mature security discipline, driven for the most part by the need for data security. As one may assume, compliance standards play a

strong role in driving the print security discipline. In EMEA, this means GDPR but also extends to the Network and Information Systems Security Directive (NIS), as well as the ePrivacy Directive update and the Revised Payment Services Directive (PSD2). These standards provide the basis for security *outcomes*, without specifically setting out the technical details for compliance.

The Essentials of GDPR

GDPR is a welcome and long overdue refresh of Europe's data protection laws. It replaces current legislation that dates to 1995, predating the dot-com boom, Twitter, Facebook, and the cloud. GDPR updates the law to account for these and future developments that create and use personal data.
An additional benefit of GDPR is that it applies to all European Union (EU) member states.

GDPR was signed into law in April 2016 and becomes effective on May 25, 2018. Organisations have less than one year to ensure compliance; the penalties for noncompliance could reach 4% of global annual revenue or €20 million, whichever is greater. GDPR also introduces mandatory breach notification, the consequences of which concern executive boards that worry about reputational damage.

Note that the United Kingdom's prospective exit from the EU (aka Brexit) does not materially affect the broad GDPR landscape:

- U.K. firms that process EU personal data will have to comply with GDPR anyway because GDPR applies extra-territorially to the personal data of any person in the EU.
- The United Kingdom is likely to implement local laws such as GDPR to facilitate data transfers from the EU, as governed by "adequacy" rules.

GDPR is more than a security issue. It contains a raft of new measures including data portability, consent and revocation, age verification, and the right to be forgotten. However, a large part of achieving compliance comes down to good security. What does GDPR say about this specifically?

GDPR is remarkably nonprescriptive about defining security measures. Of its 99 articles, only Article 32 talks specifically about security. The requirement is that organisations take "appropriate technical and organisational measures to ensure a level of security appropriate to the risk." In other words, it is up to each company to assess the risk associated with its personal data and implement security controls it deems necessary.

One aspect of this consideration is what GDPR terms "state of the art." Firms are not obliged to implement state-of-the-art technology. However, they must know what this means and defend their position. A situation for firms to avoid is trying to justify why they did *not* implement a particular security control or technique, which then led directly to a data breach.

One of the key tests likely to be applied by GDPR regulators is what IDC calls the "How hard did you try" test. Not knowing about a vulnerability is bad. Knowing about a vulnerability and doing nothing about it is worse. Purposely ignoring a vulnerability on a printer estate will cause an organization to fail the test and may be considered a breach of several GDPR principles such as "purpose limitation," "data minimisation," "storage limitation," and "integrity and confidentiality" (see Article 5).

Importantly, the material scope of GDPR is "the processing of personal data wholly or partly by automated means, and to the processing other than by automated means, of personal data which form part of a filing system or are intended to form part of a filing system." In other words, data doesn't need to be in electronic format to be in scope. Paper will do nicely.

The Network and Information Systems Security Directive

The EU understands that, in an era of increasing cyberattacks, important services need protecting, especially those deemed critical to economic or societal functioning. To achieve consistency across all member states with regard to protection against cyberattacks, the EU passed the NIS Directive.

NIS is surprisingly light on detail when it comes to security requirements. There is a broad focus on protecting infrastructure, including physical assets, and there is a primary emphasis on resiliency (incident management, business continuity management, etc.). It includes a mandatory breach notification clause (see Article 16), but there are no prescribed fines for noncompliance.

Because NIS is a directive, it needs to be transposed into law by a member state and ratified by its legislature. NIS took force in August 2016. Member states will have until May 10, 2018, to transpose the directive into their national laws and six months more to identify operators of essential services.

The Benefits of Printer Security

Printer security, as opposed to print security, is solely focused on physical devices associated with printing and is a network security discipline. Printer security views the printer as an endpoint, treating it with the same care as any other endpoint such as notebooks, servers, and mobile devices. Although they share a common vernacular and have some related areas of concern, print security and printer security are unique disciplines.

Just how vulnerable are network printers?

Printers are recipients of considerable volumes of data, some of which will be personal data. Few users, compliance professionals, or IT administrators consider the security of such data as it is transmitted to, and stored on, printers. Data resident on printers remains subject to compliance requirements: a core principle of GDPR (see Article 5.f) mandates "appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures." But few organisations give any consideration to the security of data on a printer.

Further, it is common to see printed documents forgotten on printer paper trays. In light of GDPR, pull printing solutions, which require users to be at the printer to authenticate themselves and collect the document, can become a real requirement for companies that permit printing of personal data.

Printers are a juicy target for cybermiscreants in part because they are not considered part of IT and thus do not command much attention by security personnel. Printer management is often considered part of the facilities function. When printers became networked devices, as long as the devices were behind the enterprise firewall, they were largely considered "low risk." The vulnerability of print endpoints remained underidentified.

Combination printer/scanner/fax machines are also increasingly sophisticated, and they have general-purpose computers installed inside to control all the action. Windows and Linux systems are often built into many modern printers. Because these computer controllers get little hardening and patching attention, they are often vulnerable. In addition, functionality requires connectivity, which results in many printers being shipped with a multitude of open ports to support usability.

A lack of attention combined with powerful computing power and a potpourri of connective options means that attackers can access printers in several ways, such as through a modem, wireless access point, or a jump-off from spyware-infected desktops. After gaining access, attackers can use this power to hit other machines on your internal network or participate in a distributed denial of service. Most printers have unfettered access to an internal network. An attacker who compromises a printer can scan all over for exploitable systems.

As with other endpoint devices requiring protection, printers are not only a "gateway" but also a target for cybermiscreants. Printers often store sensitive documents in their print spool. They are often combined with a document scanner, too, and documents are often stored in the scanning archive for far longer than most people expect.

Considerations

If printer security has not been a focus for your organisation, IDC has some recommendations for where to start.

It All Begins with Visibility

As with any endpoint requiring security, start with the basics: Step one is always visibility. Compile a complete inventory of all printers, including brand, model, features, and configurations. Creating such a list can be problematic because individual initiative often places printers in unidentified places (shadow IT). Labs, executive offices, or field service offices will often place a printer on the network for convenience, or connect it directly to a PC, regardless of the security implications.

Ideally, an endpoint inventory that includes printers will be derived from a network access controller (NAC) or asset management tool, which has device discovery as core functionality. Achieving truly comprehensive visibility of printers is extremely difficult without a NAC. Granted, some printer models can provide for autodiscovery when they are connected to the network. If your network environment is not fortunate enough to include a homogeneous installed base of such printers, a NAC is the way to go.

Harden Your Printer Endpoints

Printers within the organisation must be managed just as any other connected endpoint. Shut off any unneeded services that the printer offers, such as FTP. Most organisations do not need FTP access to their printers, and it can often cause more harm than good. For instance, some printers allow an attacker to make FTP requests and take jobs off a print spool anonymously. Also, many FTP services on modern printers are subject to FTP bounce attacks. With a tool such as Nmap (Network Mapper), an attacker can obscure the source of a port scan, convincing a compliant FTP server to allow
proxy FTP connections. While such FTP bounce scans are old techniques, a remarkable number of brand-new print servers are susceptible to such attacks.

However, the single most important activity in hardening printer endpoints is password management. The most egregious mistake made by organisations is failing to change the default passwords. According to Verizon's *2016 Data Breach Investigations Report*, 63% of confirmed data breaches involved leveraging weak, default, or stolen passwords. If printers are managed by facilities or third-party vendors, convenience is paramount (for them). When a device needs to be maintained, finding a password can be an issue. When there is one printer for every 10 employees, an organisation with 10,000 employees can have 1,000 passwords to maintain. Security, thus, gives way to convenience. Password management is not just a failing of nontechnical staff. The second most egregious mistake made is having the username and password freely accessible in unencrypted text, available to anyone with an http:// connection.

Maintain and Patch

Most breaches occur because of a lack of hygiene. According to Verizon's *2016 Data Breach Investigations Report*, the top 10 exploited vulnerabilities in 2015 accounted for 85% of successful exploit traffic. The most exploited vulnerabilities are known and publicly disclosed. Cybermiscreants will use what works and maximise the investment that they have made in their malware tools.

Maintaining and patching printer endpoints will make you a harder target, pushing cybermiscreants to use their tools on organisations that have not maintained their systems.

When it comes to patching, not all printers are created equal. Some manufacturers offer management tool sets that allow you to monitor, manage, and patch some makes and models of printers. Such tool sets are extremely valuable because an enterprise's vulnerability scanner will likely have issues with printers because of the embedded web server. If you happen to have such printers with robust management tool sets, you are in luck. If not, you may have to manually patch each printer because cobbling together an automated solution may be difficult.

In addition, to prevent "noise" from being imported into the SIEM tools, organizations often configure vulnerability scanners to ignore printers. This is as much an issue with SIEM and vulnerability management tools as it is with printers. It may be complicated to configure such tools to accept only certain messages from printers, but in the short term, this effort will help protect the network from printer-borne infections.

Secure the Connection

Shore up the management protocols used for the printer. Most modern printers support some sort of management via HTTP and/or HTTPS, and a few even support Telnet or Secure Shell (SSH). Carefully choose a management protocol that provides encryption, such as HTTPS or SSH, and disable weak or broken ciphers such as SSLv3.

Last, make sure that your printers do not have wide-open access to the rest of your internal network. Segmenting enterprise networks is a network security best practice, and printers need to be included in the effort. Certificates can be used to logically segment access to network resources and to encrypt traffic. However, be aware that these additional security measures can impair printer functionality, such as restricting access to directory services (e.g., Active Directory) and cloud-based management and monitoring. Getting the balance between tightly securing printers and preserving business functionality is always a matter of judgment and assessment of business risk.

Conclusion

Printers have not received the attention given to other cybersecurity threat vectors. The vulnerability and the corresponding threat are very real. Organisations of all sizes must take steps to address the concern and address it quickly. Cybermiscreants are voracious copycats. Once a threat vector has been exploited for gain by one malicious actor, others follow quickly.

The financial and reputational consequences of ignoring printer security are about to escalate to board-level status with GDPR. It would be unfortunate to see an otherwise compliant organisation, which has worked hard on its information governance processes and technologies, let down by a printer blind spot.
