4 Ways To Improve
The Security Profile of Your Print Environment

With all the recent advances in—and focus on—cybersecurity, we could be forgiven for assuming that data breaches are occurring less than ever before. Unfortunately, the opposite is true. The constantly increasing complexity of technology and the speed with which it evolves means that data breach incidents, both accidental and intentional, continue to rise.

Through our interactions with thousands of IT professionals across a wide range of industries and business sectors, we've learned four specific strategies to improve the security of print environments. While many approaches to more secure printing were identified, these four continued to bubble to the top of conversations. They are:

- Prevent print data loss
- Integrate AAA with printing
- Reduce attack surface
- Employ hardened management solutions

Why be concerned about print security?

The short answer is: because up to this point most organizations have NOT been concerned with it. "Printers are a culturally trusted technology because they're perceived as not being new," says Kayne McGladrey, director of information security services at Integral Partners.[1]

Hewlett-Packard reports that almost 90 percent of enterprise businesses have suffered at least one data loss specifically because of unsecured printing![2] A Gartner report identifies printers as among the first Internet-capable devices to be incorporated into enterprise networks, but points out that awareness of the accompanying security risks of these IoT printers is still lagging.[3]

Here's an example of what they mean. In January 2017, a white-hat hacker in the U.K. compromised more than 150,000 printers and multifunction devices (MFDs) around the world and forced them to print rogue documents. The hacker also used an undisclosed remote command execution in the web interfaces of certain devices to access print data stored on them.

Additionally, the U.S. Federal Trade Commission (FTC) updated its document titled Digital Copier Data Security: A Guide for Businesses to warn organizations to secure their MFDs. In the previous editions of this guide, the FTC had stated clearly, "Digital copiers are computers." But its 2017 edition, the commission went a step further, recommending that organizations understand the impact of adding and using MFDs on their networks and to treat them as they would a PC or server because they're vulnerable to the same security risks.[4]

Michael Howard, the Worldwide Security Practice Lead at Hewlett-Packard, recently said "the biggest mistake companies make when it comes to securing sensitive data is…"not securing their printing fleet."

And those breaches are expensive, Howard says, with an average cost of $5.4 million per incident and $136 per compromised record.2 That's in addition to costs associated with loss of corporate reputation.

Here's more on the top four ways that our conversations with IT professionals have determined to improve printer security.

1. Prevent Print Data Loss (Print DLP)

No organization wants sensitive files and information to walk out the door in a worker's or contractor's bag. User-level print monitoring that tracks every print document to its originating workstation and printer can deter this kind of document exfiltration by allowing admins to see who printed what, when and where. In the event of an actual data breach, a database of print job histories can help identify the devices and persons who printed the affected files.

Compliance regulations and security best practices already require many businesses to have in place procedures for regularly reviewing records of system activity. By storing an audit trail of all print activity, compliance can be validated and any out-of-compliance situations can be quickly identified and corrected.

2. Extend AAA into Printing

Organizations are quick to think of AAA for logical and physical access. But perhaps because print resides in a gray area that lives in the "analog-digital divide," it's often ignored. Organizations must remember to extend current Authentication, Authorization and Accounting controls into their printing space. Failure to extend these safeguards can leave printing as an open avenue for data breaches. Users should be authenticated before accessing printers and sending print data. All printers should have an authorization policy defined and only be accessible to authenticated users. All printing should be accounted for, no matter the source or destination of a print document.

Additional security can be integrated by enforcing authentication at the printer before a document prints. Users can leverage their identification badges, or other method of identity authentication, in order to initiate and retrieve a print job while physically at the printer. This prevents unintentional breaches when documents containing sensitive data may be left unattended on the printer for long periods. It also deters malicious actors from engaging in "visual hacking," which includes snatching sensitive documents from the output tray.[5]

3. Reduce Attack Surface

A typical business printing environment includes print servers to support and synchronize printers on the network. These print servers also centralize queues and temporarily spool print jobs as they await printing. The unintended effect of storing and routing print documents through a server is to increase the attack surface for a malicious actor to exploit and gain access to restricted data. By snooping or exploiting one server, a malicious actor can gain insight into all print data that passes through it.

By consolidating print servers, or perhaps removing them completely and transitioning to a centrally managed direct IP printing model, the attack surface is reduced. In addition, the removal of a single point of exploitation provides a more secure print environment against any malicious actor. Configuring print infrastructure to avoid the local storage of any document on a printing device before the document is printed also eliminates an attack vector.

4. Employ Hardened Management Solutions

Because of the nature of their mission, IT departments typically have high demands placed on them by organizations. It's no wonder that IT often seeks tools or solutions that can help ease their burden by delivering better and more efficient internal services. However any IT management solutions that trade security for efficiency, or introduce risk in the name of streamlining a process, should be avoided.

All new platforms and toolsets should be held to security standards defined by trusted and reputable governing bodies like the International Organization for Standardization's ISO/IEC 27002 or the National Institute of Standards and Technologies' Common Criteria Certification and FIPS 140-2. Before any new toolset or platform enters the organization's environment, it should be evaluated to comply with these frameworks, standards, and security best practices.

Conclusion

The cost of preventable data breaches, whether accidental or the result of a cyber attack, continues to grow. It's critical for organizations to take immediate action to minimize risk by securing their print infrastructure. The four strategies identified here come directly from our conversations with thousands of IT professionals. Any of the four represents a good place to start.

Consultants at PrinterLogic are available to help you with these and other secure printing approaches. Please visit our website at **www.printerlogic.com**.

1. https://www.csoonline.com/article/3229907/security/are-you-doing-all-you-can-to-protect-your-confidential-documents.html
2. https://digitalguardian.com/blog/expert-guide-securing-sensitive-data-34-experts-reveal-biggest-mistakes-companies-make-data#Howard
3. Market Insight: IoT Security Gaps Highlight Emerging Print Market Opportunities Published: 31 October 2017 ID: G00336890 Analysts: Kristin Von Manowski, Deborah Kish
4. https://www.ftc.gov/tips-advice/business-center/guidance/digital-copier-data-security-guide-businesses
5. https://news.3m.com/press-release/company-english/new-global-study-reveals-majority-visual-hacking-attempts-are-successf