PrinterLogic™

Improving Print Security in Government Agencies

Six ways to harden your print environment and avoid preventable data breaches.

PrinterLogic™

Introduction

This white paper describes common security risks in network print infrastructures and explains how to secure your environment and reduce or eliminate vulnerabilities associated with print servers and multifunction devices (MFDs) or printers. We explain the importance of securing your print network, present recent data on breach activity, and make the following six recommendations to better secure your print environment:

1. **Eliminate print servers as an attack vector.**
2. **Centrally audit print activity.**
3. **Enforce role-based access control.**
4. **Apply FIPS 140-2 standards.**
5. **Implement secure print release.**
6. **Digitally sign print jobs to ensure document integrity.**

Data Breaches

The Ponemon Institute works with IBM Security to identify costs, causes, and trends associated with data breaches. Ponemon defines a data breach as an event in which an individual's name along with personally identifiable medical or financial information is put at risk or exposed to unauthorized personnel—regardless of intent. In 2018, the firm released its thirteenth annual study on the cost of data-breach incidents, *2018 Cost of Data Breach Study: Global Overview.* The study brings up several notable statistics:

Global study at a glance

> Average total cost of a data breach:
$3.86 million

> Average cost per lost or stolen record:
$148

> Likelihood of a recurring material breach over the next two years:
27.9%

> Average total one-year cost increase:
6.4%

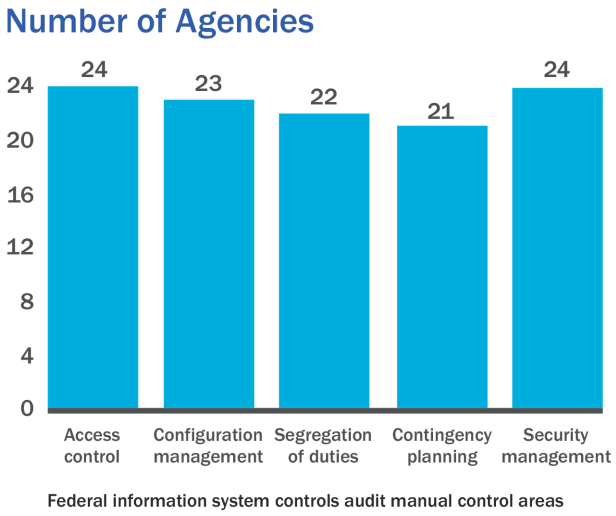
> One-year increase in per capita cost:
4.8%

> Average cost savings with an incident response team:
$14 per record

Given the many recent advances in cybersecurity, one might assume that the prevention of both types of data breaches, accidental and intentional, is improving. Unfortunately, the increasing complexity of technology and the rate at which it is evolving means the opposite is true. Data-breach incidents are not only a frequent occurrence—they are on the rise.

In its September 2017 report titled *Federal Information Security: Weaknesses Continue to Indicate Need for Effective Implementation of Policies and Practices*, the U.S. Government Accountability Office stated, "During fiscal year 2016, federal agencies continued to experience weaknesses in protecting their information and information systems due to ineffective implementation of information security policies and practices. Most of the 24 Chief Financial Officers Act agencies had weaknesses in five control areas—access controls, configuration management controls, segregation of duties, contingency planning, and agencywide security management." Access control and security management were cited as the top two priorities.

The 24 CFO Act Agencies with Information Security Weaknesses in the Major Information System Control Categories, Fiscal Year 2016



Source: GAO analysis of agency, inspectors general, and GAO reports on the 24 Chief Financial Officers Act agencies' information security practices and policies for fiscal year 2016. |

In the healthcare industry, for example, the U.S. Department of Health and Human Services (HHS) currently has more than 4,000 cases of breach activity under investigation.[1]

Nor are government agencies themselves immune. In 2016, the GAO documented that government agencies reported 30,899 information-security incidents, 16 of which met the threshold of being a major incident.

One example of an accidental release of sensitive military information was reported in November 2017. UpGuard, a cybersecurity company, discovered in September 2017 that an Amazon Web Services S3 cloud storage bucket contained data belonging to the U.S. Army Intelligence and Security Command (INSCOM),[2] including details of the DoD's battlefield intelligence platform and a virtual system used for classified communication. This was a publically accessible repository.

Public embarrassment is only the mildest repercussion. Often the consequences are much more severe. In 2011, a security breach within TRICARE, the U.S. Department of Defense healthcare

program, impacted 4.9 million individuals and resulted in at least three class-action lawsuits worth a total of $4.9 billion. These lawsuits represent only a small portion of the direct cost. Total costs were far greater.[3]

Overlooked or Ignored Infrastructure Threats

In planning and implementing their print infrastructure, IT departments and contracting managers too often focus on convenience at the expense of security. Gartner reports issued in late 2017 and early 2018 confirm this. Despite a widespread awareness of data breaches, and a corresponding increase in endpoint security budgets, "...print devices, paper documents, and users inappropriately handling digital and paper documents will continue to be sources of major data breaches across all global regions, vertical industries, and market sectors." [4,5]

50%
increase in endpoint security budgets in 2016

YET

LESS THAN 20%
of enterprises will have an end-to-end print security strategy by 2021

Best practices suggest that to eliminate security weaknesses and compliance gaps, the print environment must be "hardened" by addressing the two most serious vulnerabilities: print servers and printers/MFDs.

Print servers

Centralized and distributed print servers pool all print data in a single location, thereby creating a weak link in the print network. Even with security measures in place to protect data at rest (more on this topic below), print servers that utilize a shared document file store, a print job repository, or print queues can become a high-value target for malicious actors.

Historically, most documented instances of unauthorized access have been unintentional, but this should not downplay the possibility of malicious unauthorized access, which can be initiated surreptitiously within the secure network by authorized users with detailed system knowledge. Typical print-server architectures are vulnerable because they allow actors to access large amounts of sensitive or classified print data through a single breach. It then follows that even a single document breach means all print data may have been compromised.

Printers and MFDs

In January 2017, a white-hat hacker in the U.K. compromised more than 150,000 printers and MFDs across the globe and forced them to print rogue print jobs. Additionally, the hacker used an

undisclosed remote command execution (RCE) in the web interfaces of certain devices to access print data on the devices.

Later that same year, the Federal Trade Commission (FTC) updated its document *Digital Copier Data Security: A Guide for Businesses*. In the previous iterations of this guide, the FTC had not strayed from its very clear statement: "Digital copiers are computers." The newer report took this concern one step further. It introduced recommendations that organizations take steps to understand the impact of adding and using MFDs on their network and to treat them as they would a PC or server, given they are vulnerable to the same security risks as that of a computer.

Protecting a secure print infrastructure

Every time a document or form is copied or printed, sensitive data can be accidentally exposed or intentionally compromised. PrinterLogic, a leading provider of advanced printer-management and access-control solutions, has developed a secure software solution that allows government agencies to secure their print network infrastructure and reduce their total cost of ownership. PrinterLogic offers a single integrated package that includes device-agnostic printer and driver management, as well as CAC/PIV authentication.

Recommendations

1. Eliminate print servers as an attack vector

In a typical printing environment, an IT administrator deploys and provisions a print server to support and synchronize printers on the network. These print servers and any related software often rely on a centralized document repository and print queues to hold print jobs that are awaiting execution. As detailed above, the risk inherent in this infrastructure is that it creates a single attack vector that a malicious actor can exploit to gain access to some or all of the print data. Even if those repositories are encrypted or protected in other ways, print servers still create a single point of failure and a weak link in the IT chain.

Our recommendation is to remove this vulnerability by removing print servers from the environment and transitioning to the centrally managed direct-IP printing model that PrinterLogic offers. The elimination of print servers—and concomitantly their centralized document repositories—creates a more secure environment in which a malicious actor would need to compromise each workstation to gain access to the same amount of print data. This hinders the scale of any breach by limiting its impact to precisely targeted workstations.

2. Centrally audit print activity

Centrally auditing print activity means establishing a system in which printers store information on their respective print-job history in a common database. In the event of a breach, this database can facilitate the identification of any printing device and user affected by the breach.

Compliance and security standards already require that most businesses implement procedures that include a regular review of records of system activity. By storing an audit trail of all print activity, compliance can be validated and out-of-compliance scenarios can be remedied quickly.

PrinterLogic's print-management solution tracks all print data across the network by default. This enables administrators to pinpoint print-related network events that involve a specific user or device. This feature also allows administrators to generate reports by department, device or user. With this easily attainable, taxonomic data, reports can be assembled and distributed in a way that is useful and actionable to customers, including managers and decision-makers.

3. Enforce role-based access control

Every network user should be a part of a centrally managed system that defines user rights and privileges such that areas of the network have limited access. Granularized access control over the entire organization is an accepted practice.

It's critical from a security perspective that the same granularized access control is applied to MFDs and printers. This means the printing devices must likewise support the restriction of features and capabilities of an authenticated user on the basis of group-policy membership.

PrinterLogic recommends the implementation of strict role-based access control—along with print-management software and print devices—that natively support this practice. Enforcing stringent access control at the device prevents unauthorized execution or release of printed documents. Furthermore, every print device should be equipped with an authentication mechanism and, where possible, physical access to the printer should be controlled.

4. Apply FIPS 140-2 standards

Printers often have storage mechanisms (e.g., hard drives, flash memory) that are used to cache printed documents. Non-volatile memory on these devices should use an automated data-erasure method to protect data in accordance with U.S. National Institute of Standards and Technology (NIST) *Special Publication 800-88*.

The Cryptographic Module Validation Program (CMVP) is a well-established program jointly managed by NIST and the Canadian Communications Security Establishment (CSE) for the certification of cryptographic modules that meet the Federal Information Processing Standard FIPS 140-2

cryptography-based standards. The U.S. government requires the use of CMVP-validated cryptographic modules for all unclassified uses of cryptography.

In the U.K., these standards are managed by The National Cyber Security Centre, an organization within Government Communications Headquarters that offers guidance on products that are cryptographically secure. In Australia, the Defence Signals Directorate (DSD) is tasked with this objective and the corresponding Canadian entity is the Communications Security Establishment (CSE).

PrinterLogic meets the security requirements for cryptographic modules defined by FIPS Publication 140-2. This is accomplished by employing specific accredited encryption methods for data in motion (DIM) and data at rest (DAR).

For our purposes here, data in motion applies to communication between printers and PrinterLogic. Data in motion is transferred over TLS V1.2. Supported printers can utilize FIPS 140-2 accredited Open SSL/TLS FIPS Object Modules, including AES and RSA.

Data at rest applies to jobs held in the print queue. Encryption is enabled directly on the Windows operating system and not within the PrinterLogic software. Data at rest is stored using single or dual-layer data encryption by leveraging two Windows OS encryption methods: the Windows Encrypting File System (EFS; NT file system) and BitLocker Drive Encryption (whole disk). Both methods depend on FIPS 140-2 validated cryptographic libraries.

5. Implement secure print release

Given the high cost of security breaches involving personally identifiable or personal health information, documents should only be available to the authorized user who originated the job. With secure print release, the print job is released only when the authorized user is physically present at the printer. This helps to ensure that documents are not left unattended in the output tray.

Devices that are properly configured for secure print release will print only those documents that are associated with the authenticated user, and during this process the print job itself should not be stored on the print device before printing. Print jobs should not be stored on a centrally managed server where they are vulnerable to a single attack.

PrinterLogic's coupling of secure print release functionality with its direct-IP printing paradigm avoids local storage on both printers and servers. A malicious actor would need an extremely complex multi-vector attack plan to gain access to the organization's print jobs.

6. Digitally sign print jobs to ensure document integrity

For true end-to-end print security, PrinterLogic recommends that all print jobs are digitally signed at the point of print. When a user securely releases the job (following Recommendation 5 above),

the PrinterLogic software validates the print job by comparing hash values and the digital certificate obtained from the smart card prior to releasing the job. This ensures the print job has not been tampered with. This increases the security profile of the print job and provides non-repudiation of the print data and print user.

Conclusion

Given the increasingly high cost of preventable data breaches, it is critical for organizations to take immediate and active steps to minimize risk by controlling and protecting potential access points on their print networks. The costs of penalties and settlements as well as indirect repercussions that stem from failing to secure printers can be significant, even catastrophic.

PrinterLogic facilitates printing compliance by adding a layer of security and control that uses robust, automated security protocols that cannot be circumvented. It has the ability to authenticate users, restrict access to printing devices and print jobs, monitor real-time print activity, and compile and maintain a comprehensive audit trail of historical user print activity. As a result, PrinterLogic reduces the risks inherent in existing print infrastructures, corrects non-compliance, and helps companies and agencies avoid the penalties and other costs of data breaches.

By implementing PrinterLogic, your organization can follow the essential security recommendations laid out in this document. In doing so, you will join the many government agencies and enterprise-scale companies worldwide that trust and depend on PrinterLogic's unique solutions to help secure their print data.

Footnotes

[1] HHS Active Case Breach Report, available at https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

[2] Dan O'Sullivan, "Black Box, Red Disk: How Top Secret NSA and Army Data Leaked Online," UpGuard, November 28, 2017: https://www.upguard.com/breaches/cloud-leak-inscom (accessed December 4, 2017)

[3] Howard Anderson, "TRICARE Breach Affects 4.9 Million: Incident Involves Theft of Backup Tapes," available at https://www.inforisktoday.com/tricare-breach-affects-49-million-a-4105

[4] "Market Insight: Cloud and Security Concerns Create New Pull-Print Market Opportunities," available at https://www.gartner.com/doc/3847477/market-insight-cloud-security-concerns

[5] "Predicts 2018: Print Solutions Become Intelligent, but Customers Struggle to Become Secure," available at https://www.gartner.com/doc/3835765/predicts--print-solutions-intelligent

PLWP_GVT_PRINT_SECURITY_FV1_101518