How to close hidden cybersecurity gaps in printing environments

Security managers must be mindful of so many outside threats that it's easy to overlook the inside threat from poorly managed multifunction products. Fortunately, the latest generation of devices and the help of expert service providers can successfully address this gap.

Malware, ransomware, social engineering. Diligent IT managers and chief information security officers guard against a wide range of threats to critical corporate data. But there's one area that often falls under the security radar, and it lies within even the most hardened network perimeters. Inadequately managed multifunction products (MFPs) attached to these networks pose a significant security threat—both from enterprising hackers and from inadvertent data leaks by employees. The reason: Fully securing these devices requires a multifaceted approach that considers more than network configurations and the strength of cloud services.

Fortunately, a combination of the latest technology, managed services, and best practices can plug these security holes without impairing the productivity of end users. Here are the must-haves to look for when evaluating MFPs and analyzing the security expertise of potential managed services providers.

Select devices engineered for security

Data security should be built into MFPs from the start rather than enabled with add-on hardware and software. How can you determine this? Start by focusing on a unit's hard drive, which is "ground zero" for data protection. The drive should support federal government-backed data encryption protocols for data in transit and at rest. Examples include the Advanced Encryption Standard used for the government's classified documents.

Additionally, the MFPs should include software for wiping data from hard drives to ensure that sensitive information doesn't linger after print jobs are completed or when the unit is decommissioned. Just having data wiping is not enough because if a job is interrupted or the disk cleaning is disabled, the data is still at risk.

Encryption protocols protect data when it's at rest or traveling across the network, but it's vulnerable at other times as well. Don't overlook risks related to output trays. If an MFP processes a print job before the sender finds time to retrieve it, financial data, personnel files, and other sensitive information are exposed to any unauthorized person who happens by. To prevent this, follow-me printing options in MFP software keep the print job on hold centrally until the rightful recipient scans an ID badge, enters a password, or does both, depending on corporate policy.

Authorizations can be most effectively managed by administrators when they're centrally stored in the company's Active Directory rather than on the device itself. Care should be taken to secure connections between the enterprise's Active Directory and badge readers on the devices. Direct connections that encrypt communications are the most secure way to enable these transmissions. Additionally, by managing the print documents centrally, security is enhanced because information is not stored on device hard drives.

To further bolster security, IT managers may consider sending files directly from PCs to printers without pooling jobs on print servers. This is important because many organizations don't encrypt files waiting on print servers, potentially making the information accessible to hackers. Encrypting pooled files is an option; however, this may limit an organization's ability to enable follow-me printing. Thus, decision makers must balance the various alternatives based on the criticality of the data being processed and productivity considerations to ensure that each solution meets their specific requirements.

> *To further bolster security, IT managers may consider sending files directly from PCs to printers without pooling jobs on print servers.*

MFPs may fail to comply with corporate security standards when installers don't adjust the default settings of the units. Thus, the configuration process should include settings that determine whether to limit scan-to-email, faxing, printing, and copying activities for certain workgroups and individuals.

For devices that handle particularly sensitive information, such as medical records and Social Security numbers, consider data loss prevention (DLP) utilities that can alert administrators and even block print jobs that include such data.

Finally, another configuration consideration is the role of end users associated with individual devices. For example, not every unit will process files that warrant DLP or two-factor authentication. Forcing people to follow unnecessarily tough protocols invites them to circumvent established procedures in the name of productivity, which then creates additional vulnerabilities.

Keep security in mind when evaluating managed print providers

Providers of managed print services perform an important role for large organizations. They routinely service and maintain each unit to avoid mechanical problems and incidents where productivity comes to a standstill because a printer ran out of toner or paper. These specialists can also maintain proper security settings and install software patches to keep hackers from exploiting known bugs. The key is determining which providers have the security depth necessary to protect corporate information.

Since service providers perform many of the management tasks remotely, get details about how a candidate's network connects to the printer fleet. Analyze how these links are secured, including whether the provider uses dedicated tunnels and VPNs to communicate with devices.

And because each workgroup requires tailored device settings—neither too loose nor too onerous—make sure that a potential service provider doesn't offer one-size-fits-all security solutions.

Case Study: Army facility gets tough with security

A training facility that serves the U.S. Army provides tough, realistic instruction—which sometimes involves live firearms—for ground and aviation brigades. Realism is a prime focus, and so is security.

The organization uses a wide variety of communications and technology, including networked printers and MFPs that support mission-critical strategies. In the past, many of the organization's networked, single-function printers and copiers were largely unprotected. Documents could be printed and accidentally left on the printer, for example, bringing the possibility that confidential information could be retrieved by an unauthorized recipient. In addition, people weren't required to enter authentications before being able to fax, copy, or scan information on the devices, raising the chance that critical data could leave the facility and bypass its security protocols. Similarly, documents could be scanned and anonymously sent to any email address from these unsecure output devices, which violates U.S. Department of Defense policy.

The facility's Information Assurance Division chief understood that the organization required a new solution to ensure compliance with government mandates. To more fully protect sensitive information, the facility needed a solution to verify identity and security classifications each and every time a user attempted to use the print, copy, fax, or scan features of networked output devices on the network.

After a test of possible solutions, the organization chose to implement Lexmark MFPs equipped with a print-release capability. Now, users authenticate themselves using smart cards called common access cards (CACs) to ensure that the proper recipient is at the MFP to immediately clear the output tray. The authorizations contained in the CAC credentials also control who is allowed to use other MFP capabilities, such as the scan-to-email function.

Lexmark's authentication software enables the training facility to validate CAC credentials and PINs from its Active Directory. This approach obtains the certificate chain for each print, copy, fax, or scan request.

"Other vendors couldn't provide the level of security we needed," says the organization's Information Assurance Division chief. "Lexmark listened and created a simple solution that directly addressed our requirements."

> *Security managers must be mindful of so many outside threats that it's easy to overlook the inside threat from poorly managed MFPs.*

Close the gap

Security managers must be mindful of so many outside threats that it's easy to overlook the inside threat from poorly managed MFPs. Fortunately, the latest generation of devices and the help of expert service providers can successfully address this gap. The outside world may not become a safer place, but at least CIOs and chief information security officers won't have to lie awake at night worrying about their MFPs.

About Lexmark

Lexmark International, Inc. (NYSE: LXK) is uniquely focused on connecting unstructured print and digital information across your enterprise with the processes, applications, and people that need it most.

Insight®

Work smarter.

At Insight, we'll help you solve challenges and improve performance with Intelligent Technology Solutions™.

Learn more