Print security: know your risk, protect your assets

Did you know that unsecured print equals unsecured IT? Consider the thousands of potential security threats across an output fleet made up of varied devices and vendors, all of which must be managed separately to ensure they are secure. And each day with an outdated, multi-vendor fleet means in increased risk of security breaches to your organization.

For over 15 years, Lexmark has provided the highest level of security by delivering devices and solutions tailored to meet our customers' unique requirements. Our proven, secure by design methodology focuses on security as a critical component of infrastructure optimization that can significantly reduce security gaps between documents, devices, the network and all points in between.

Are your organization's devices protected against inside and outside threats? Determine your level of risk with our security checklist to help identify and close security gaps.

Policies

Many organizations are filled with aged, poorly secured print devices or with devices with firmware that have never been updated. Your best defense is to implement policies in your organization that address common gaps in securing a print environment.

- ☐ Firmware update policy for print devices

  Updating device firmware can enable new features and solve issues, but most importantly, these updates can patch common vulnerabilities and exposures (CVE). When updating firmware, use the manufacturer's website and verify the files are encrypted and digitally signed to ensure that only firmware created by the vendor can be installed on enterprise devices.

- ☐ End of life policy for unsupported devices

  Devices don't last forever and eventually manufacturers will end software, firmware and hardware support. Refreshing before that point will help devices stay current and secure. When devices are retired or moved, be sure to perform an out-of-service wipe to remove all settings, data and information stored on the hard disk or memory of the device.

Device configurations

When configuring devices, make sure you consider network communications, access controls and hardcopy security for the most secure print environment. In addition, consistent device settings deployed across your fleet will boost your defenses.

- ☐ Configuration of devices using automated tools

  Automation of device configurations can enhance your security posture by ensuring that devices match security policies and remediate automatically if a device is out of conformance to those policies.

- ☐ Secure device configuration

  To comply with the latest print security recommendations, consider disabling device USB ports, turning on hard drive encryption, disabling legacy ports and protocols, and enabling TCP/IP Address and Port filtering.

- ☐ Secure communication capabilities

  Communication with the device is protected via access controls and the latest network communication protocols including Transport Layer Security (TLS 1.2), Simple Network Management Protocol (SNMPv3) and forced HTTPS connections to the embedded web server.

- Access controls for remote management

  Individual users and groups use credentials to access the device, and authentication and authorization mechanisms can determine if a user has appropriate access to modify device settings or leverage functionality.

- Device user authentication

  Administrators can grant access to device function and apps with a PIN, simple authentication and the same magnetic stripe or proximity cards that employees use for access to physical facilities. Malicious printing and copying can be prevented on a device by configuring to only allow jobs if the user has authenticated.

- Hardcopy Security/Print Release

  Users can print jobs from anywhere including desktop, tablet or smartphone, and release jobs for printing when they are ready and from any location. A standard part of the Lexmark Universal Print Driver, Confidential Print holds your job on a specific Lexmark printer or MFP until you release it with a PIN, preventing prying eyes from viewing documents in the output bin.

Network considerations

With increased use of mobile devices and the need to support BYOD initiatives, IT departments must strike a balance between providing users with the tools they need to maximize efficiency while reducing the risk of intrusion across networks and connections.

- Secure authentication methods

  Support for a wide array of authentication protocols means the device user authentication function is compatible with an array of network environments. Secure user authentication protocols such as LDAP with SSL/TLS configured, Kerberos, LDAP+GSSAPI and NTLM protect users' credentials during the authentication process.

- Audit logging

  Tracking security-related events and device-setting changes can provide an audit trail for malicious activity. These actions can be exported to detailed logs that describe system user or activity events. These logs may be integrated with your intrusion detection system for real-time tracking.

For more information about Lexmark security features, products and services, go to lexmark.com/security or contact your Lexmark representative.

© 2020 Lexmark. All rights reserved.

Lexmark and the Lexmark logo are trademarks or registered trademarks of Lexmark International, Inc. in the United States and/or other countries. All other trademarks are the property of their respective owners.