Canon

KEYPOINT INTELLIGENCE

MFP/PRINTER SECURITY VULNERABILITIES AND BEST PRACTICES

This information is based on a Keypoint Intelligence report, "MFP/Printer Security: Device Security Vulnerabilities & Best Practices"

57%

OF U.S. IT DECISION MAKERS CONSIDER SECURITY TO BE A TOP CRITERION WHEN CHOOSING AN OFFICE PRINTING SUPPLIER.

KEY MFP/PRINTER SECURITY RISKS

1. Breach of operating system embedded in firmware
2. Data access through network and cloud connectivity
3. Access to information on device (e.g., on hard drive)
4. DNS (denial-of-service) attack through exposed port print protocols
5. Inadequate cross-site request forgery protection for device software (leading to malicious links)
6. Routing of network credentials to hacker through security hole

MFP/PRINTER MANUFACTURER BEST PRACTICES

MFP/printer OEMs are advised to:

- Offer robust firmware protection.
- Ship devices with business secure settings.

MFP/PRINTER CUSTOMER BEST PRACTICES

MFP/printer dealers/customers are urged to:

- Look for security certified devices.
- Change unsecure default settings.
- Include printers in larger security plan.
- Proactively monitor.

FUN FACT

70% of organizations say printing will be critical or very important to their businesses over the next year.

KEY RECOMMENDED SETTINGS

- PJL (Printer Job Language) off/disabled
- HTTP port 80 disabled (and port 443 enabled)
- SNMP v1/v2 disabled (and v3 enabled with complex password)
- TCP/IP v4 disabled (and v6 enabled)
- TLS 1.2 or 1.3 and beyond
- Set complex password for embedded web server
- Front USB Port disabled
- Web services (if using HTTP, not HTTPS) disabled
- User login attempts: Limit to five or fewer

42%

of independent office equipment vendors expect devices capable of self-healing/self-maintenance to be crucial in future offices.

02/24/23-2580-9808

usa.canon.com