Networked Multi-function Systems

Security Standards

NDSU Information Technology Division
July 2009

Multi-function systems (printer, copier & fax which can be one unit or separate units) are devices with embedded operating systems such as Windows that interact with the network. These systems often deal with confidential information. As such, these systems must be secured and in compliance with all NDSU policies and procedures.

Checklist to multi-function systems

- All multi-function systems must have a static IP address. Printers connected to desktops and used by one individual are not required to have a static IP number.
- If multi-function system will be used for copying, faxing, and/or printing confidential data, it must be located in an area of the office or department that is not available to the public.
- Allow use only to those employees that have a definite need to use the device.
- Disable unneeded or unused services on the device e.g., “Document Server”.
- Change default login and passwords.
- Turn off Web connections unless a need can be justified for them.
- Use strong authentication for remote administration of devices.
- Vendor support must allow for configuration information and login and password information to be shared with NDSU IT personnel.
- The vendor must provide security patches in a timely manner. Any vulnerability left unpatched for more than thirty days would require the device to be shut down until the patch is available from the vendor and installed on the multi-function system.
- The administrator login and password must be changed from the default and is one that is within standards established by NDSU policy 158 and NDUS policy and procedure 1901.2.
- If computer support is administered remotely or via the Web, the administrator login and password must be encrypted in transfer and storage. If encryption cannot be used, then Web administration is not allowable and only the local console should be used.
- The device will be scanned for the latest vulnerabilities at least quarterly using SANS Top 20 tests. If the scanning causes performance issues for the printer/copier, it should be powered off until the vendor can fix or replace it.
- Multi-functions systems must be restricted from offsite Internet access. Users can not remote to system to print documents from off campus.
- E-mail sent and received from the printer/copier must be within the @ndsu.edu domain.
- If SSL certificates are used, the device must use certificates as approved by NDSU.
- Devices must support 801.1x network authentication, or have planned upgrade (by vendor) to support it.
- Devices must support IPv6, or have a committed upgrade path from vendor for IPv6.
• All services must be configurable and must allow complete disable (i.e., SMTP, NTP, FTP, HTTP, NFS, IPX, Appletalk, etc.)

• Disable the Telnet daemon. If a remote shell is needed, it is recommended to use SSH or OpenSSH.

• Disable anonymous FTP access.

• Disable support for HTTP Trace method.

• Disable NetBIOS Null sessions.

• SNMP community name string must be changed from the public default name string.

If you would like more information ITS Desktop Support has an informative Website that can provide you with more information.

http://its.ndsu.edu/help_desk/desktop_support/printing/securing_your_network_printer/