Multi-function Network Devices

Security for printers, scanners, copiers and fax machines

Printers, copiers, and other multi-function network devices can pose a security risk to the university if not properly configured. Similar to your everyday computer, many of these devices will have operating systems which allow network connectivity and mechanisms for storage. Consequently, these devices are subject to the ITSO standards and procedures and departments will be held responsible from the initial deployment of each device through to the point the device is either transferred to new ownership or disposal occurs.

While IT support makes every effort to mitigate risk by hardening such devices (as outlined below), the potential risk associated with a compromised printing device could still result in data leakage from logs or data recovery from internal drives. For this reason, using multi-function network devices in conjunction with sensitive data should be a considered factor and limited to necessity.

Hardening Guidelines

(This list is not exhaustive and may be updated as needed.)

1. Set a secure administrator password. (Refrain from using default credentials. Remember the longer the better, while using a combination of case, number, and special.)
2. Update firmware. (Just as software updates are a continuous effort, ensuring firmware is up-to-date whenever possible is important to help mitigate risk.)
3. Use HTTPS to manage printers across web interface. (Do not use plain HTTP.)
4. Disable any unneeded/unused services or protocols. (Whether used for management, communications, or printing the available protocols will likely exceed those that are actually being used by your department. Please disable those not in use.)
   ○ If using SNMP, ensure it is SNMPv3 for encryption and refrain from using the default community string.
5. Set Access Control Lists (ACLs) whenever possible. (Restricting access to specific subnets or machines involves additional management by support but when implemented allows added security.)
6. Disable IPv6 (if your department is not actively using such addresses).
7. Encrypt the internal HDD when available.
8. Configure generic service accounts with secure passwords for various features (i.e. print-to-file).
9. Logging should be enabled for auditing purposes.
10. Utilize a PIN/Password/Passphrase to restrict access to the configuration menu

Private Addresses

In addition to the guidelines above, the ITSO prefers each department to move printers to private addresses restricting access to those physically on campus or to those making use of the VPN.

Source URL: https://security.duke.edu/network-devices

Links
[1] https://security.duke.edu/network-devices