Overlooked is unsecured

Best practice for secure printer configuration

brother.co.uk

Best practice for secure printer configuration

Print security has become a critical issue for business today. Due to an increased number of security threats, as well as legislation regarding privacy and data security, organisations need to focus on strategies for securing their printing functions.

According to Infosource, there were approximately 36 million printers and multifunction printing devices in use in Western Europe at the beginning of 2017. Considering most printing devices are also connected to a network, and are just as susceptible to malware and hacker attacks as computers, this equates to a significant threat to security.

Sensitive documents and information are regularly printed, and documents often remain unprotected in output trays long after print jobs have been completed. Printers may also store information that can be recalled or intercepted inappropriately, and have the potential to facilitate access to the wider network. They need to be managed and protected, just like the rest of the IT infrastructure.

Every industry is concerned about print security, but here are a few examples:

- In healthcare, secure printing and scanning is crucial due to the sensitive nature of medical data, and the importance of maintaining patient privacy and confidentiality.
- In education, staff need secure print solutions for confidential information, such as reports, test results and other legal documents related to students.
- The wider public sector handles an enormous amount of personal information and is subject to strict regulations regarding information sharing and storage.
- Small to medium businesses require secure printing and scanning solutions to safeguard business-critical information. Depending on the nature of the business, companies may also need to protect sensitive data held on behalf of their customers, such as financial or compliance information.

Legal and regulatory concerns

There are many regulations globally that mandate security controls and can impose large penalties for non-compliance, some of the most well-known examples of these are:

EU General Data Protection Regulation (GDPR)

Effective from 25 May, GDPR mandates that organisations must adequately protect private data of residents of the EU. Failure to comply can result in severe penalties of up to 4% of worldwide turnover. Many non-EU countries also enforce similar privacy legislation and associated fines.

Payment Card Industry Data Security Standard (PCI DSS)

If you store, transmit or process any payment card data, you are required to comply with PCI DSS. You need to consider how your print devices may be used in relation to card data, and ensure you meet the requirements of PCI DSS. Monthly fines can be imposed for non-compliance with the standard, and are not just limited to when a data breach occurs.

Insider trading

Many countries have insider trading laws in place, with criminal penalties including jail time for individuals involved and fines in the millions for individuals and corporates. Ensuring that data related to any sensitive corporate transactions is secured is critical to preventing your exposure to these charges.

This list is far from exhaustive, and you should check what laws and regulations are applicable to your organisation, and ensure that appropriate consideration is given to print devices within your security strategies and frameworks.

Threats

There are various kinds of threats to printing devices, including:

Document theft or snooping:

Someone could simply walk up to a printer and pick up a document that has already been printed by someone else.

Unauthorised configuration changes:

If a printer's settings and controls aren't secure, someone could mistakenly (or intentionally) alter and re-route print jobs, or perhaps reset the printer to its factory defaults.

Recovering saved copies from internal storage:

If a printer has internal storage, it can store print jobs, scans, copies and faxes. In the event that someone steals the printer, or if it's discarded or retired before the data is properly erased, it may be possible to recover the saved documents, some of which may be confidential.

Interception of network traffic:

Hackers may eavesdrop on your network traffic and potentially capture documents sent to networked printers.

Device vulnerabilities:

It may be possible to hack into a network-connected printer, especially if it's an unmanaged device with out-of-date security features or password protection, compromising the device and potentially the extended network.

Real world examples

Internet exposed devices can easily be found online, using specialist search engines, that not only give information regarding your print devices, but can give away information about insecure services and protocols available on your network, providing attackers with valuable information to plan an attack.

A grey-hat hacker printed messages to 150,000 printers that had been left accessible online. They used an automated script that searched for open printer ports and sent a rogue print job to targets' devices. the script targeted Internet Printing Protocol (IPP) ports, Line Printer Daemon (LPD) ports, and port 9100, which were left open to external connections. Luckily this was a harmless event, and warned targets of their susceptibility. However it could have easily been malicious in intent and been used to cause business disruptions.

Protecting a device involves identifying both internal and external threats

While traditionally hackers are thought of as external individuals trying to get in, recent research suggests that around a quarter of businesses noted internal threats as their most common reason for a data breach.

If a printer is accessible via the Internet, the number of potential hackers is virtually limitless. Attackers could send strange print jobs to the printer, use it to transmit faxes, change its LCD readout, alter its settings, launch Denial-of-Service (DoS) attacks against your network or against others, or even install malware on the printer itself to control it remotely or gain access to it or the wider network.

How can you create a secure printing environment? Here are some guidelines for suggested best practice.

Secure the printer

Physically protect the device

Locate the printer in an area where it is more easily observable; this alone could deter potential hackers. Situating it in an area that's accessible to many users may be better than locating it in a separate room or office, where it can't be monitored as closely. Ideally printers should not be located in areas where there is unrestricted public access, such as reception areas. Consider physically securing the printer so that it cannot be easily removed from your premises.

Increasing the physical security of printers could help prevent document theft or snooping, unauthorized access to stored documents, and misuse of the printer's Ethernet or USB connections.

Restrict access to paper stock

Access to pre-printed security paper, such as cheques and prescriptions, should be strictly controlled to prevent theft or unauthorised use.

Solutions are available to secure the paper input tray, for use in environments where control of paper stock is critical.

Segregate printing tasks

Companies should consider designating separate printers for departments which handle sensitive information, and keep those machines separate and secure from other employees.

Set a strong administrator password

Printers usually have an administration web interface that allows configuration and control of the device. A default password is usually set at the factory, so users must be diligent in setting a new, strong password upon initial configuration.

Ensure encrypted connections are used when accessing the printer administrative control panel, i.e. use HTTPS rather than HTTP. This may be configured by enabling port 443 within the Embedded Web Server (EWS) interface under HTTP Server Settings, and disabling port 80.

Note also that the administrator password often encrypted when it's saved, and the EWS will time-out after a period of 5 minutes of inactivity.

Consider whether remote administration is required. If it isn't then disable the capability and only perform administrative actions locally on the device.

Require authentication and authorisation

Access to device settings and functions should be controlled by requiring authentication and authorisation for access. Options such as PIN authentication, LDAP authentication, and smart cards could be deployed for this purpose. This won't stop a determined hacker, but every security barrier put in their way will help.

Ensure that your printer provider offers security features that allow you to restrict access to the device's settings through its control panel. This is ideal for organisations that don't want to limit the way people use the functionality but that do want to make sure unauthorised users can't change any settings.

You may also wish to prevent access to both the device's settings and certain functions. This allows administrators to decide who can do what with each machine, for instance controlling which users are able to fax and scan, or imposing monthly limits, through unique PIN numbers or NFC access cards.

Look for a provider that supports industry-standard communications protocols and encryption.

These include:

- **IEEE 802.1x:**
  Can be hardwired with a cable or via an organisation's wireless infrastructure.
- **IPsec:**
  Devices can connect directly to internal or external secure environments using built-in IPsec support.
- **SNMPv3:**
  Designed to comply with strict network security policies, devices communicate via encrypted SNMP v3 (MD5/SHA1), even during remote setup and routine maintenance.

Disable non-essential services

Many printers have insecure and non-essential services enabled by default (e.g. Telnet, FTP, TFTP, HTTP, and SNMP). Leaving these services enabled often provides attackers with the ability to access printer data directly or make configuration changes. We suggest disabling all services you do not require, and if possible, change the default port numbers, and change any additional passwords or community strings from default settings. If command line access is required, use SSH instead of Telnet to prevent eavesdropping.

A full list of supported services may be found below, together with their default port numbers where applicable. Note that supported services may differ based upon model of device; please check your device for compatibility. All the following services may be optionally disabled.

Service	Default port	Recommendation
Web Based Management (EWS)	80, 443, 631	Disable port 80
Remote Setup	-	
Telnet	23	Disable port 23
SNMP	161, 162	
LPD	515	Disable port 515 if not required
IPP	631	
AirPrint	-	
Mopria	-	
Web Services	80, 443, 631	Disable port 80
Google Cloud Print	5222	
Proxy	8080	Disabled by default
Network Scan	445	Disable port 445 if not required
POP3	110, 995	
IMAP4	143, 993	
SMTP	25, 465, 587	Disable port 25
FTP Server	21	Disable port 21
FTP Client	21	Disable port 21
SFTP	22	
TFTP	69	Disable port 69
WebDAV	445	Disable port 445 if not required
CIFS	137, 138, 139, 445	Disable ports 137-139, 445 if not required
LDAP	389	
mDNS	5353	
LLMNR	5355	
SNTP	123	
Raw Port	9100	

Disable unused device interfaces, physical ports and features

If interfaces such as Wi-Fi Direct are not required, ensure that they are disabled.

Physical interfaces such as USB may also be disabled, depending upon the product category.

If your device has other features that you do not require, disable them. Any feature has the capability to be misused, either intentionally or accidentally. Disabling anything not required minimises your risk.

Monitor and manage the print environment

Log and monitor activities on print devices. A large percentage of data breaches occur due to 'insider threats'. Having the capability to monitor and investigate user actions allows you to respond appropriately.

Monitor network traffic to and from print devices. This can alert you to unauthorized activities. For example, would it cause alarms to see activity to or from your printer from overseas, or administrative level traffic from a non-administrator device?

There are a number of tools and utilities that can monitor useage and audit printing practices such as:

- **Mass Deployment Tool:**
  This provides a configuration interface to enable management of a variety of device settings. It allows users to install and manage multiple local or network connected devices quickly and easily, without having to install additional software.

Brother supports industry-standard communications protocols and encryption (please check your device for compatibility).

These include:

- **Meter Read Tool:**
  Communicates with Brother USB or Network connected devices and reports on status via email. It collects usage information and can notify of any machine errors, or if consumables are running low.
- **BRAdmin Professional:**
  Allows system administrators to view and control the status of Brother network-connected products (as well as most other SNMP-compliant network printing devices) from a Windows computer on the same network.
- **BRPrint Auditor:**
  Allows monitoring of locally-connected Brother devices (USB & Parallel). Devices are polled on a scheduled basis set through the BRAdmin Professional software, and information is passed to BRAdmin Professional or via email. Device status such as page counts, firmware version, toner and drum status may be checked, along with notification of machine warnings and errors.

In addition, Brother devices work with leading independent Print Management solutions, including vendors such as Nuance, Papercut, Ringdale and One Q.

Update and patch firmware and software

Just like computers, printers need regular updates and patches. Check for firmware updates on all printer and network devices as part of a regular patch management schedule. Often updates add new or improved security features, patch known security exploits, and fix other problems.

Make sure you only source your software and firmware from trusted sources, and ensure the files are not tampered with prior to installation. Ensure your chosen vendor digitally signs and checks device firmware to prevent malicious code being uploaded to the device.

In addition, all associated print management software should also be part of a regular patch management schedule.

By taking the proper steps, you can help ensure the security of your printing environment, so that the printing function remains a business asset and not a liability.

Plan for end-of-life

As with all devices, hardware and software has a limited useful life. Devices will at some point run out of support and no longer be provided with updates, which can leave a device susceptible to vulnerabilities. Keep track of these dates so that you can plan in advance for asset refreshes, to ensure you have supported equipment which remains protected.

In addition, ensure you have processes in place to securely dispose of any printers when they will no longer be used, some best practices:

- Ensure any memory or storage devices are sanitised and/or destroyed.
- Ensure there is no jammed paper in the printer.
- Print multiple pages of random text with no blank areas on each printer cartridge or Multi-function Device (MFD) print drum.
- Remove any remnant toner or any visible prints from MFD print drums or image transfer rollers or destroy these if they can't be removed.
- Destroy cartridges or MFD print drums that cannot be sanitised (for example due to hardware failure).

Securely dispose of consumables

It's not only at the end-of-life stage that printer components are disposed of, but whenever any components or consumables such as cartridges or print drums are sanitised and disposed of securely when being replaced. The most common data leakage is through the loss of printed materials. Ensure that you have secure paper destruction facilities and educate staff to use these for disposing of anything sensitive.

Limit network access to the printer / segment the network

A layered approach to information security is always best practice; here are some important principles to consider:

- a properly-configured firewall should always be the first point of defence for any network.
- comprehensive network segmentation is a key component of network design.
- network administrators should ensure that devices are only allowed to communicate using necessary services or ports.
- restricting network access based upon MAC address is good practice.

Printers should not be directly exposed to the Internet. Public access should be restricted by using a network firewall. A private IP address can help secure the printer from being accessed outside of a department or institution. However, not all network infrastructure setups allow this, therefore other methods can be utilised to limit access to the printer, such as IP filtering to restrict access by IP address.

It is also possible to remove the default gateway in the IP configuration, to disable Internet routing, and making printing only available on your local network segment.

Check that your printer has features which help to securely protect data communications:

- **IP Filtering:**
  Prevents access to the device over the network, i.e. devices will only accept connections from specific IP addresses.
- **Protocol Control:**
  Allows administrators to disable protocols that aren’t required.

Avoid using administrator level usernames and passwords for network access

Whenever a printing device requires access to a network resource, ensure that a dedicated, individual network account is set up specifically for this purpose, and only grant this account sufficient rights to be able to fulfil the required function.

Additionally, where possible restrict network service accounts such as those used by printers, to deny interactive logon. This prevents anyone using these accounts for other purposes.

Ensure you can trust your supply chain

If you ever need replacement components, make sure that they are genuine parts, have come from the original manufacturer and are installed by a trusted party. Any third parties conducting maintenance on your hardware should be supervised at all times.

Secure the data

Protect printed documents

It's all too common in an office to pick up a printed document and find multiple documents left in the printer tray or sitting nearby, which may be perhaps viewed or stolen by anyone. Minimising the risk of this happening requires a security-conscious outlook within the entire organisation. It is important to remember that printer security doesn't just mean IT security.

To protect confidential data before it reaches the device tray, users should be required to authenticate themselves to the printer before any pages will print. Then, once the printing is complete, the document should not be stored on the printer for future printing.

If a printer has the capability, activate pull printing to minimise unclaimed documents. Users are then required to authenticate themselves and retrieve jobs as required.

Finally, sensitive papers should be shredded when they are no longer required.

Brother has many useful security features (please check your device for compatibility).

These include:

- **Secure Print:**
  A feature primarily designed for users who print confidential documents. It allows users to delay printing until they are physically in front of the printer, by configuring an optional pin for that user. When printing a confidential document, the user would simply assign the PIN number to that job in the print driver, which is then required to unlock the device for printing.

- **Secure Print+:**
  A feature primarily designed for users who print confidential documents. It allows users to delay printing until they are physically in front of the printer, by configuring an optional NFC access card for that user. When printing a confidential document, the user would simply assign the NFC access card to that job in the print driver, which is then required to unlock the device for printing.

- **Active Directory Secure Print:**
  This feature restricts physical access to any function on the printer by essentially locking out any unauthorised persons. To unlock the printer and collect your document, users must first authenticate themselves using their existing Windows® Active Directory username and password. In both cases the job is stored to the printer's internal memory until it's collected.
- For an extra layer of security using either Active Directory or LDAP secure print functions, administrators may specify a time limit for how long uncollected print jobs remain in the memory of the device.
- **Secure PDF:**
  Scanned documents may be turned into a PIN-protected Secure PDF.
- **Scan to SFTP:**
  Secure File Transfer Protocol (SFTP) establishes a private and safe data stream, and by controlling access to SFTP servers, organisations can help keep their whole network secure.
- **Print watermarks:**
  Ensure that confidential documents have a watermark added to every page that is printed. Watermarked documents ensure that the origin of a document is carried through any copies subsequently made of the document.
- **Add print identification:**
  Add print identification to either the header or footer of each printed page. The date and time, login user name or some personal identification may be added to every printed page, independently from the document being printed.

Encrypt print jobs to protect data communication

Sensitive data is vulnerable as it traverses a network from the source to the printer. When sending print jobs or accessing the control panel, it is possible for data to be digitally intercepted. To protect against this, you should always use an encrypted connection.

Check that your devices have built in Transport Layer Security (TLS) and Secure Socket Layer (SSL) encryption, the same technology used in e-commerce to protect bank and credit card details. Documents may therefore be encrypted at up to 256-bit during transmission over the network.

brother
at your side

Brother UK Ltd.
Shepley Street, Audenshaw,
Manchester, M34 5JD
Tel: +44 (0) 333 777 4444
Fax: +44(0)161 931 2218

brother.co.uk