Stacked Managed Print Services: Security

An article published by Wired in February 2017 stated that;

‘In April 2015, a group of researchers from the Singapore University of Technology and Design flew a smartphone-equipped drone up to the 30th floor of an office building and waited. Loaded on the phone was an app that scanned the office's wireless network for an open printer then mimicked it, forcing local computers to connect to the phone instead. Intercepted documents were copied onto a Dropbox account and the file passed along to the real printer for output. The office workers were none the wiser.
A month earlier a cyberattack of more malicious intent by the notorious hacker, Weev, resulted in a stream of racist fliers being spewed out of the printers across 12 US universities. The January before, an unidentified hacker held a large Danish paint wholesaler to ransom by entering their network through a printer and locking the entire thing down.’

The same article details how HP is helping to re-invent security and prepare their products for the office of the future by enlisting the help of researchers, developers and entrepreneurs.

Did You Know…

64%

of IT managers state that their printers are likely infected with malware (1)

73%

of CISOs expect a major security breach within a year (2)

3.8M

is the average cost of a data breach (3)

64% of IT managers state that their printers are likely infected with malware (1) 73% of CISOs expect a major security breach within a year (2) 3.8m is the average cost of a data breach (3)

Stacked Can Help

Most businesses spend a huge amount of time, money and effort securing their file storage and computer network, but they don't always realise that their printers also offer hackers a way into their network.

The fact is that there is no point in putting an expensive alarm on every door and window in your house and then leaving the cat flap open.

It's time to develop and deploy an end-to-end imaging and printing security strategy. With the embedded security features in HP devices, a broad portfolio of HP JetAdvantage solutions and services, Stacked and HP can help give you the strategic foundation to assess, manage, and fortify security for:

- Imaging and printing fleets
- Data in transit and at rest
- Printed documents
- Cloud access
- Printing from mobile devices

The World's Most Secure Printers

HP print security features protect, detect, and recover…

The latest generation of HP Enterprise LaserJet printing devices are unique in the marketplace, because they offer three key technologies designed to thwart attackers' efforts and self-heal. These features automatically trigger a reboot in the event of an attack or anomaly.

After a reboot occurs, HP JetAdvantage Security Manager automatically assesses and, if necessary, remediates device security settings to comply with pre-established company policies. There's no need for IT to intervene. Administrators can be notified via HP management applications such as JetAdvantage Security Manager and ArcSight.

How Does It Work?

The embedded security features address three primary steps in the cycle of a HP device. HP JetAdvantage Security Manager completes the check cycle.

Automatic Reboot

Continuous Monitoring: Runtime Intrusion Detection
Detects anomalies during complex firmware and memory operations. If an attack occurs, it shuts down the device and reboots.

Check Printer Settings: HP JetAdvantage Security Manager
Checks and fixes any affected device security settings

Load BIOS: HP Sure Start
(BIOS is a set of computer instructions in firmware which control input and output operations.)
HP Sure Start validates the integrity of the BIOS code. If the BIOS is compromised, HP Sure Start defaults to a safe 'golden' copy of the BIOS.

Check Firmware: Whitelisting
Ensures only authentic, known-good HP code – digitally signed by HP – that has not been tampered with is loaded into memory. If an anomaly is detected, the device reboots.

Mind the Security Gap

Critical gaps can occur at multiple points within your imaging and printing environment. Once you understand these vulnerabilities, you can more easily reduce the risks.

1. **Capture**
   Multifunction printers can easily capture and route jobs to many destinations, potentially exposing sensitive data.
2. **Cloud Based Access**
   Unsecured cloud connectivity may expose data to unauthorised users.
3. **Control Panel**
   Users can exploit imaging and printing device settings and functions from an unsecured control panel and even disable the device.
4. **Input Tray**
   Special media for printing checks, prescriptions and other sensitive documents can be tampered with or stolen form an unsecured tray.
5. **Network**
   Printing and imaging jobs can be intercepted as they travel over the network to/from a device.
6. **Management**
   Without adequate monitoring, security blind spots across your fleet may remain undetected and increase costly data risks.
7. **Mobile Printing**
   Employees who print on the go may accidentally expose data or leave printouts unsecured.
8. **Output Tray**
   The output tray is the most common place for sensitive documents to fall into the wrong hands.
9. **BIOS and Firmware**
   Firmware that becomes compromised during start-up or while running could open a device or the network to attack.
10. **Storage Media**
    Imaging and printing devices store sensitive information on internal drives or hard disks which can be accessed if not protected.

With Stacked and HP you get security and peace of mind…

1. We help defend your imaging and printing environment
2. We help protect the data
3. We help protect documents

References

1 Ponemon Institute, “Insecurity of Network-Connected Printers”. October 2015
2 Help Net Security, “Why enterprise security priorities don’t address the most serious threats”. July 2015
3 Ponemon Institute, “Annual Global IT Security Benchmark Tracking Study”. March 2015

https://www.wired.co.uk/article/hp-re-inventors-secure-your-business