decisionpoint systems, inc.™

Secure Thermal Printing:

Part of Every Comprehensive Security Strategy

ZEBRA

Security Must Be Top of Mind

Cybersecurity is an ever-changing landscape: As technology evolves, hackers keep looking for new weaknesses to exploit. It's hard to miss the headlines of high-profile supply chain and ransomware attacks across all industries, from Colonial Pipeline and leading meat processor JBS Foods to computer manufacturers Quanta and Acer. Additionally, smaller companies should never make the mistake of thinking it will not happen to them.

When investigators look at the root cause of security incidents, they sometimes discover a vulnerability in an unexpected place: enterprise printers. Endpoints — including thermal printers, such as barcode, wristband, receipt, and shipping label printers — are becoming targets. It only takes one vulnerability to give hackers access to your network, where they can download or corrupt data or hold the system for ransom. To strengthen your security posture, your cybersecurity strategy must not overlook thermal printers.

Why Enterprise Thermal Printers Are Targets

Networked printers give businesses several advantages:

- Centralized printer management
- Distributed access for employees
- Mobile printers optimize worker productivity

However, because they are on the network, connected devices can give hackers a way into the system. CyberNews white-hat hackers performed an experiment in 2020 to understand the extent of vulnerable printers connected to networks. They were able to hijack about 28,000 printers out of the 50,000 they targeted, providing an indication of how many unprotected devices are connected to networks worldwide.

Printers have historically been difficult to protect. They are more like Internet of Things (IoT) devices than other types of endpoints on the network — and IoT devices have become popular targets for hackers. Additionally, the 2018 Government Procurement Device Security Index from International Data Corporation (IDC) reports that printer security is a challenge for businesses because it is more difficult to "harden" printers or make them less vulnerable to attack after they've shipped. Compounding the problem is the fact that businesses don't include printers in their security policies: 89% of IDC survey respondents said they consider desktop PCs in their endpoint security strategies, but only 52% said they consider printers.

The Cost of a Security Vulnerability

Unfortunately, enterprise and thermal printers with inadequate security can lead to data breaches. Printers can be an open door that hackers exploit to steal customer data (including sensitive financial or healthcare data) or company logins and passwords that give them access to corporate applications, systems, and accounts.

According to the 2021 Cost of a Data Breach Report from IBM and the Ponemon Institute, the average cost of a data breach has grown to $4.24 million, which is a 10% increase from the cost in 2020. The average cost of a ransomware breach is even higher: $4.62 million. These costs come from the event itself and the aftermath, including:

- Downtime
- IT remediation
- Fines and legal fees
- Customer or patient notification and monitoring

However, the biggest cost — 38% of total data breach costs on average — is lost business. Furthermore, this factor can impact a company long after the cyberattack and data breach remediation. The loss of consumer trust and goodwill causes long-term harm to a business.

Make Security a Priority When Selecting a Thermal Printer Solution

Hackers will consider every potential endpoint vulnerability — and so should you. Think through more than just connecting a printer to your network. You need to know more about the device you plug in. Investigate the printer manufacturer's commitment to security, including whether security is built in from the ground up rather than addressed as an afterthought. Overlooking these questions during procurement is a common problem: according to the IDC study, requests for proposals (RFPs) for printers were 72% less likely to specify security requirements than RFPs for PCs.

Then, once you select a thermal printer, you need to take your responsibility to secure it seriously. However, visibility and management can be challenges with most printing solutions. You need to be aware of your printer's capabilities and know what you want it to do — or not do. For example, many printers can now store the information you've printed, which could be risky. You need a printer that is reliable, performs in your environment, and delivers ROI. But you also need a printer solution that you can monitor and manage to avoid data loss and malware that causes downtime or denial of service.

Legacy thermal printers lack those capabilities; however, today's state-of-the-art intelligent printer solutions, such as LinkOS printers from Zebra, give you the management capabilities and visibility you need to keep printers — and your network and your business — safe from cyberattacks.

The Advantages of a Security-First Thermal Printing Solution

Look for an thermal printer solution that is not only user-friendly but also offers management and control features (such as the ability to delete information from the printer's hard drive).

You should be able to engage the security features you need for your user case, including user authentication, password protection, and encryption. Your printer solution should also give you the ability to control and monitor which applications or devices can connect to your printer, and to manage printers remotely to quickly change settings or upload security updates.

How Secure Is Your Printer?

According to the IBM report, the chances of experiencing a data breach in 2019 were 29.6% and rising. With those odds, cybersecurity must be a priority. If you are using older printer solutions without security features, it's time to consider an upgrade. If you've recently deployed new thermal printers, you may need assistance to familiarize yourself with their security features. In either case, DecisionPoint Systems can help. Contact us today for a security assessment to identify and remedy any gaps in your thermal printing solution security.

Through our partnership with Zebra Technologies, DecisionPoint Systems helps organizations migrate from legacy mobile devices to modern, purpose-built mobile solutions that increase the connectivity, productivity, and security of your mobile workforce.

About DecisionPoint Systems, Inc.

DecisionPoint Systems believes that your mobile workforce is the face of your company, and that the customer impressions it makes are lasting. For over 25 years, DecisionPoint's reason for being has been to empower these workers to make better and faster decisions. Utilizing the industry's best mobile computing technologies, DecisionPoint designs, develops, deploys and maintains enterprise-class mobile computing solutions that connect your mobile workforce to one another and to your enterprise systems. Whether your mobile workforce consists of retail store associates, truck drivers, field service/sales associates or delivery personnel, DecisionPoint understands their unique mobile needs and can provide a mobile solution that enhances customer satisfaction and accelerates your business growth.

decisionpoint systems, inc.

Phone: 949.465.0065
Email: info@decisionpt.com
Website: www.decisionpt.com

ZEBRA