By Lisa Terry, Contributing Editor

POS SECURITY

SPONSORED BY hp

10 THINGS RETAILERS OFTEN MISS

As a security target, the retail POS terminal is uniquely vulnerable. Few other industries must put a computer that manages highly sensitive data out in public spaces and hand access credentials over to multiple entry-level workers.

That's one reason the retail industry is among the biggest victims of malicious attacks, and the POS terminal the most-targeted component of retail solutions. According to the *2016 Verizon Data Breach Report,* more than 70% of the prior year's retail breaches were POS incidents.

Retailers' efforts to create seamless omnichannel shopping experiences by making customer data easily accessible across channels adds to the vulnerability. In addition to credit card data, POS terminals may handle personally identifiable information (PII) including e-mails, birthdays, search and purchase histories, measurements, loyalty points, shipping addresses and more for both customers and employees — who also input access credentials into POS.

Retailers know a process-based, multi-layered security plan is the best defense against malicious attacks and even accidental exposure of data. But many are over-looking or neglecting basic block-and-tackle moves. Some of these sit available but unused on their current enterprise-grade POS set-ups, while others are part of cutting-edge solutions. Enacting these solutions can go a long way to establishing a secure environment that protects sensitive data and enables retailers to minimize impact and recover quickly from attacks.

PROTECTING THE DEVICE

Tech advancements that have made computing devices lighter and more streamlined have removed the built-in protection that enormous metal POS boxes once offered. But retailers can physically secure today's sleek devices using multiple digital and physical measures. Some underused strategies include:

Bolt down. Physically attaching a device or stand directly to the counter prevents the entire device from being stolen and hinders tampering.

Kensington locks. Keyed Kensington locks physically tether any device to a secure connection via a port lock, preventing devices from being removed or replaced with a substitute. Retailers also need a secure process to manage keys to permit add/move/change and servicing.

Location detection. Utilities enable retailers to create a WiFi- or GPS-based digital perimeter around a store and automatically disable the device if it's taken outside that area. Some retailers also use alarms.

Port protection. Most POS devices have USB ports, or some other port type. Bad actors can use these ports to insert malicious code to steal data or credentials. Sometimes this can be done innocently via a curious employee: When researchers dropped about 300

USB drives on University of Illinois Urbana-Champaign campus, 98% were picked up and 45% of them were inserted into USB ports.

Retailers often neglect to make use of Windows Active Directory as well as utilities provided by some POS companies to set rules for powering ports. Utilities can keep the port powered off permanently or until an authorized device is plugged in.

Rules can also incorporate whitelisting, so the POS will function only if a signed, trusted and approved application is attempting to operate on the POS. So if a hacker tries to insert another application via USB, it will not run.

CONTROLLING POS IDENTITY ACCESS

Retailers employ many store employees to whom they must grant access to POS terminals. Protecting access passwords is part of training, but far from foolproof: Most (85%) of IT professionals say the weakest link in security is end users failing to follow policies and procedures, according to a January 2017 Vanson Bourne study.

Hackers take advantage of this weakness. For example, PoSeidon, which has been widely used to attack POS systems, includes a memory scraper with a keylogger that can gather operator credentials on the infected system and automatically transmit them to the attacker. According to Verizon's 2017 Data Breach Report, "Use of stolen credentials to access POS environments continues to rise and is almost double that of brute force for hacking actions."

Retailers need to balance secure processes with ease of use to ensure high staff compliance. Several processes and technologies to achieve this are underused by many retailers:

HP DEVICE PROTECTION

Protect USB Ports from Tampering

RIS: POS devices sit in open, hard-to-secure areas. What are some underused tools for protecting hardware from tampering?

BRAD TRACY: There are many, but one effective but neglected step is to create true security around USB ports. Because POS typically sits out on the counter, it can be easy for anyone to insert something into the USB without being noticed. This enables a bad actor to place malicious code onto a device to exploit later on. Even consumer-grade tablets without USB ports still need to physically connect to a dock via a port, and this is vulnerable too.

HP offers multiple utilities to protect ports, providing important protections such as automatically turning them off when not in use and back on only when an authorized device is plugged in. HP's Windows 10 Device Guard, for example, lets IT managers create rules to run only signed, trusted, and approved applications on the POS to protect against walk-up and low-level attacks through USB ports.

USB protections built into HP POS devices significantly enhance their security, because even if someone plugs in a USB device with nefarious software, since that software is not on the white list of acceptable applications, it won't run. •

DAVID GOSMAN, Global Hospitality Segment Manager, HP

HP IDENTITY PROTECTION

Protect POS Access with Biometric Identity Protection

RIS: Identity protection is a big challenge for POS, with its multitude of users. What steps tend to get overlooked to control access to POS devices?

TRACY: Poor password management is a huge source of breaches. Bad habits that make POS devices more vulnerable include using the default log-in, sharing passwords, stealing credentials from another employee, never changing passwords — the list goes on and on.

Passwords alone are just too ripe for abuse to serve as the main POS access credential. Biometrics — can be combined with a username and/or password for two factor authentication — providing much stronger security to ensure that the person who is attempting entry into the system is really the one authorized to do so. The fingerprint is among the most popular POS biometrics.

HP ElitePOS' optional fingerprint reader supports secure login to ensure only authorized users gain access to the POS. Benefits include:

- **Prevents password stealing.** This circumvents common schemes such as faking discounts to steal money or transferring inventory into a black hole to steal merchandise.
- **Prevents dishonest labor.** Employees can't clock in both themselves and the buddy who hasn't yet arrived at work.
- **Prevents POI access.** Stops an employee from accessing customers' personal information or confidential information of the business, that isn't available with their login but may be with a manager's login.

Using a fingerprint reader alongside HP's Credential Guard for secure user authentication and password protection multiplies the protection as part of a layered, multi-faceted approach to POS access control. •

Biometric authentication. IDC recommends that organizations support biometric authorization to reduce fraud costs across their systems, and expects this method to become widespread. For example, the firm predicts that by 2021, 50% of online transactions will use biometric authentication, enabled by broad user acceptance, ubiquitous technology infrastructure and low implementation costs.

NFC readers. Another form of access control uses NFC readers along with a card, key or phone with NFC capability to authenticate users.

Credential guard. Enterprise versions of Windows offer this utility to allow organizations to isolate and harden key systems and user secrets against compromise, according to Microsoft. This helps minimize the impact and breadth of a pass the hash-style attack in the event that malicious code is already running via a local or network-based vector.

50% ONLINE TRANSACTIONS WILL USE BIOMETRIC AUTHENTICATION, ENABLED BY BROAD USER ACCEPTANCE, UBIQUITOUS TECHNOLOGY INFRASTRUCTURE AND LOW IMPLEMENTATION COSTS BY 2021.

SOURCE: IDC

PROTECTING DATA

Sixty two percent of intrusions affecting POS environments involve malicious remote access — a significant hazard with networked POS devices but much less common in other environments, according to Trustwave's "2017 Global Security Report."

Many strategies for protecting data go underused in the retail industry:

1) MSR encryption. Most MSR readers send data into the POS terminal, where it is briefly visible, and therefore vulnerable. A number of POS breaches would have been averted if those retailers used MSRs that encrypt data right into the device, before it travels.

Whitelisting. POS devices are required to run a limited number of applications. Locking down the device with utilities that allow only approved apps to load prevent the system from running malicious code.

BIOS security: Hackers know if they can get to the POS system's BIOS, which boots up the operating system, they can bypass a lot of the security measures that run at a higher layer. BIOS attacks are on the upswing. More than half the cyber security pros surveyed by the Information Systems Audit and Control Association reported incidents of malware-infected firmware in 2016.

Many retailers neglect to make use of the BIOS security tools offered by some POS providers, such as pre-boot authentication and administrator-implemented BIOS management controls. Other useful

tools include self-healing BIOS security, near real-time monitoring, rule-based automatic recovery, and management of "gold master" reimaging. This creates a gold master of the BIOS that is directly encrypted on the POS device. If an attacker tries to hack the BIOS, the machine will reboot itself, load the secure gold master, wipe the infected file, and alert the retailer's IT team to the attack.

Using BIOS security also strengthens downstream hardware security measures such as trusted platform module (TPM) — a dedicated industry-standard, secure crypto-processor located on the motherboard ——as well as credential guard and drive encryption.

UNDERUSED TOOLS ARE VITAL TO POS SECURITY

No retailer wants their brand associated with the exposure of customer PII or payment data. Even breaches that are quickly discovered and addressed cost retailers in customer trust. Over the next two years, 80% of consumers in developed nations will defect from a business because their personally identifiable information was impacted in a security breach, predicts IDC.

Retailers' approach to securing data and devices must be comprehensive and ever evolving. Taking advantage of security features that may already be available in current POS systems and ensuring new POS devices are designed with security top of mind are important steps to preventing breaches and keeping critical data secure. **RIS**

HP DATA PROTECTION

Use BIOS Protection to Circumvent Attacks

RIS: What technologies tend to be underused in the digital protection of POS devices?

TRACY: Hackers are known to attack POS systems at the BIOS level. The BIOS boots the computer and helps load the operating system, functioning at a level below where security software such as anti-virus does its work. The BIOS in some computers can be easier to attack than previously thought, allowing even poorly funded hackers to exploit "incursion vulnerabilities" to insert malicious code that grants them full system privileges so they can steal data. Several high-profile POS breaches have been BIOS attacks.

To minimize this threat, HP POS latest devices benefit from HP's larger security initiative by incorporating security features such as HP's BIOSphere Gen3. This provides enhanced end-to-end protection against malicious attacks and accidental errors that can compromise the BIOS, using a self-healing architecture designed to prevent, detect and repair attacks.

Then HP Sure Start works alongside HP BIOSphere Gen3 to ensure the POS is secure before initiating boot-up. If there is an issue with the BIOS, it shuts down the POS and restarts it with a clean version inaccessible to third-party software or firmware. During runtime, BIOSphere regularly rechecks the BIOS, immediately shutting down the system and restarting with a clean BIOS copy should an irregularity be detected. The system heals itself. •