

by Michael E. Smith

Protect Your Business by Avoiding Common Data Security Traps

Are You Leaving Your POS System Vulnerable to Attacks by Hackers?

In recent years the ring of yesterday's cash register has given way to the quiet whir and hum of dial-up terminals at the point of sale (POS). This evolution continues today as increasingly more business migrates toward a high-speed and wireless POS network model, in which client POS terminals connect to a central backend server or host. However, along with greater speed, functionality and efficiencies that today's enhanced POS payment systems provide come potential new vulnerabilities every card-accepting business should take steps to guard against.

For example, if a hacker breaks into the initial defensive layers of a merchant's POS network, valuable cardholder data can be stolen from both the host system and the individual POS systems.

Looking across its broad network, Visa USA has identified three of the most common areas of POS system vulnerability and has developed strategies to mitigate the risk of a data compromise.

1 Remote Access Security

Today's new dial-up terminals and highly flexible and multifunctional systems introduce greater technical complexity at the merchant storefront. Increasingly, merchants are using high-speed connections with client POS terminals that are connected to the host. This sophisticated architecture mirrors the client-server architecture of most Internet-based systems and warrants equally stringent security measures.

The availability of always-on high-speed connectivity brings a new level of efficiency to the payments industry as systems maintenance and troubleshooting can now be performed remotely. However, such capabilities introduce vulnerabilities to the POS environment if not properly secured. For example, if an intruder

Because so much information is stored or transmitted there, the host is considered to be the coveted crown jewels among hackers.



© iStockphoto.com/Duc Do

breaches the outside boundary of a merchant's POS network, both the host system and the individual terminals can be compromised and lead to a loss of cardholder data.

Many POS solution vendors, resellers and integrators have introduced remote access management products into the merchant environments they support. A wide variety of remote access products exists, ranging from command-line based to visually driven packages.

The exploitation of improperly configured and unpatched remote management software tools is the most frequent method of attack used by hackers against POS payment systems. Merchants should ask their payment application(s) vendors, resellers and integrators several key questions to ensure their systems are safely configured. It's important to know what type of remote management software is utilized, if any, who has access to it, and how it's installed and configured. It's

Networks that store, process or transmit cardholder data must be secured in accordance with the PCI DSS. Specifically, the network should have the following characteristics:

The POS system should not have direct Internet access. A firewall device can help ensure the clear separation necessary for limiting the extent of a compromise that may originate in another segment of the network.

Any wireless network must be segmented from the wired network where the POS system resides.

The strongest possible level of encryption must be enabled on any wireless network. Wi-Fi Protected Access (WPA) encryption should be used over Wired Equivalent Privacy (WEP) encryption wherever WPA is supported.

In a wireless environment the SSID broadcast function should be disabled.

Unnecessary wired network ports should be either disconnected or routinely monitored for any unfamiliar devices connected.

also critical, for example, that the software does not use default settings. Beyond making certain that any remote access features in use are in full compliance with the Payment Card Industry Data Security Standard (PCI DSS), merchants should ask what additional safeguards can be deployed to secure their system.

2 Host Security

The host is the central repository that provides authorization functionality as well as data backup and various management functions in most POS environments. Because so much information is stored or transmitted there, the host is considered to be the coveted "crown jewel" among hackers. A merchant must ensure that its host software does not store any prohibited data elements such as full magnetic stripe data or PIN data. To prevent attacks against the host, it is crucial that merchants only use

Get Control

of the Entire Employee Life Cycle

Let your managers be managers



Leave the paperwork to us

- Maintain and monitor HR information in a single, central location
- Replicate your current business process
- Eliminate interfaces between multiple systems
- ESS, MSS, employee benefits plan management, employee call center
- Payroll administration

Don't change your process to fit a system.
Choose a system that will match your process.

Applicant Tracking
Paperless Onboarding
Human Resources Outsourcing

8815 Conroy Road
Suite 156
Orlando, Florida 32835
407.244.3050
info@sequensant.com

Sequensant.com
SENTIENT HR AUTOMATION

CREDIT CARD | COMPLIANCE

payment applications that have been validated as compliant with the Visa Payment Application Best Practices (PABP). PABP-compliant payment applications do not retain full magnetic stripe data, thus limiting the extent of any possible compromise.

A list of PABP-compliant payment applications can be found at www.visa.com/cisp.

3 Network Security

Many POS environments are interconnected via wired or wireless networks. These networks may be used to manage both POS and inventory control systems. Adequate security controls must be implemented to ensure the network is properly configured and

a basic level of activity logging must be maintained in accordance with the PCI DSS.

Wireless networks can also be compromised by failing to fully encrypt network traffic.

Many network devices such as wireless routers come out of the box configured with default IDs and passwords supplied by the vendor. Failing to change the default credentials is an all-too-common cause of data breaches. Criminals are well aware that many default passwords are freely available on the Internet. In fact, their systems are frequently automated, giving them the ability to identify and attack systems

using default passwords almost as soon as they are deployed.

Wireless networks can also be compromised by failing to fully encrypt network traffic. A wireless network's signal can extend beyond a business's walls to the parking lot where it may be inconspicuously accessed by a hacker. Even if the data is encrypted, the data may still be compromised if the system uses weak encryption algorithms.

If not properly secured wired networks can be exploited through the Internet or via physical access to the merchant's systems. For example, physical access could be exploited if an individual with malicious intent were to attach a device to an open network port in order to collect data from the network as it travels between the host and the individual POS terminals. This device can be later removed from the facility along with any cardholder data that was collected. While this method requires physical access to the facility, employee collusion should not be underestimated and proper access controls should be placed around a wired network as well. Internet access can be exploited remotely if merchants do not take appropriate steps to protect their Internet-facing systems.

Unfortunately, criminals will always be among us looking for vulnerabilities to exploit. The good news is that by carefully applying sound risk-mitigation strategies to the most commonly exploited POS vulnerabilities, you can sharply reduce the risk that your customers will find your company's name associated with the next data breach news story.

To learn more about these topics, and specific steps you can take to protect your business and customers, please visit www.visa.com/cisp or contact your Visa member bank.

Michael E. Smith is senior vice president, Enterprise Risk and Compliance at Visa USA.