

by Michael E. Smith

Top 3 Data Breach VULNERABILITIES And How to Avoid Them

An organized workforce keeps a focused eye on the hospitality industry using advanced skills and technology. The hours are long and the research is tedious but the potential for enormous payoffs keeps them highly motivated. Their business objective is to steal payment card information.

Hackers frequently look to hotels and restaurants for payment environment vulnerabilities. In fact, Visa found that approximately half of known compromises in 2007 involved restaurants.

From its investigations, Visa has identified the top three vulnerabilities that have led to data compromises. By carefully heeding the following risk-mitigation strategies and by making compliance with the Payment Card Industry Data Security Standard (PCI DSS) a 24/7 priority, your company may avoid uncomfortable conversations with regulators, reporters, attorneys and most importantly your customers.

1 Storage of Track Data and Other Sensitive Data

Track data is the information encoded and stored on two tracks located within the magnetic stripe on the back of payment cards. The storage of the full contents of the magnetic stripe once the authorization process is completed is explicitly prohibited by Visa rules and PCI DSS requirements. Unfortunately, many merchants and service providers may be unknowingly storing this data because a number of commercially available point-of-sale (POS) payment systems and custom-designed payment applications retain this data by default without any action by the user. Visa regulations and the PCI DSS also prohibit the storage of the card verification value 2 (CVV2) and personal identification numbers (PINs) or PIN blocks.

The value of full track data to hackers is significant. With little effort, a duplicate

Hackers frequently look to hotels and restaurants for payment environment vulnerabilities. In fact, Visa found that approximately half of known compromises in 2007 involved restaurants.



© iStockphoto.com/Duc Do

card can be created that will appear indistinguishable from the original card during the authorization process. Storage of this data by merchants and agents exposes this sensitive information to potential compromise and can make it easy for hackers to commit fraud that is difficult to detect. CVV2s and PINs are also highly sought after by hackers.

2 SQL Injection Attacks

Structured Query Language (SQL) injection attacks on e-commerce Web sites and Web-based reservation systems have become more prevalent. Criminals continue to use techniques, including SQL injection attacks to exploit Web-based applications integrated with databases that use client-supplied data. SQL injection attacks can occur at a hospitality merchant mainly due to unpatched Web servers, improperly designed applications or poorly configured Web and database servers.

These SQL injection attacks pose a serious risk to cardholder or personal data stored or transmitted within these systems

Risk Mitigation Strategy: Storage of Track Data

- Ensure payment applications do not store track data or other sensitive data by using a payment application that has been validated as compliant with Visa's Payment Application Best Practices program. A list of Payment Application Best Practices (PABP) compliant payment applications can be found at www.visa.com/cisp. The PCI Security Standards Council (SSC), an entity that manages security standards globally for the five major card brands, adopted Visa's PABP and on April 15, 2008 released it as the Payment Application Data Security Standard (PA-DSS). In late 2008, the PCI SSC will assume management of the list of validated payment applications.

- Merchants that discover track data or other sensitive data in their systems should immediately delete this data and take steps to upgrade or replace any software vulnerable to this security flaw.

- Custom-designed solutions should also be carefully evaluated for any evidence of magnetic-stripe data storage. If track data or other sensitive information is stored subsequent to an authorization, the data should be eliminated immediately and the solution modified to no longer store this data.

(e.g., Microsoft and UNIX-based) and networks connected to the affected environment. Criminals have successfully exploited SQL injection vulnerabilities to compromise cardholder and personal data and perpetrate fraud.

Risk Mitigation Strategy: SQL Injection Attacks

2

To minimize the possibility of a SQL injection attack and mitigate the risk of a data compromise, hospitality merchants should, at a minimum, take the following actions:

- Use an information security company to test susceptibility to SQL injection utilizing automated tools or manual techniques.
- Disable programmatic functions that execute operating system (OS) commands through stored procedures or SQL statements. (e.g., xp_cmdshell).
- Adopt secure coding practices that include independent code reviews and regular testing against SQL injection if your organization utilizes proprietary or custom applications.
- Use only secure Web and database servers. Please refer to the product vendors' Web sites for instructions on hardening Web and database servers (e.g., visit <http://www.microsoft.com> for instructions on hardening IIS Web servers and SQL database servers).
- Consult an information security company to ensure all systems are updated (including Web and database servers) routinely with the most current security patches and your firm is prepared to address emerging vulnerabilities.
- Routinely check for and purge any sensitive cardholder account data (i.e., full magnetic stripe data, CVV, CVV2, PIN data) that is not needed for business purposes.

3 Packet Sniffers and Network Security

A packet sniffer, also known as a network analyzer or protocol analyzer, captures and interprets a stream or block of data (referred to as a packet) traveling over a network. Packet sniffing is the practice of using computer software or hardware to intercept and log traffic passing over a computer network. Therefore, securing the network and monitoring network traffic for unauthorized access is the foundation for a secure environment. Consequently, the network is often a target for security breaches and is the main vehicle for transmission of malicious code between systems. It is critical that proper firewall rules configuration and management of network devices are adopted to prevent unauthorized access. To minimize the threat of data compromise, it is essential internal networks and devices are properly managed and not susceptible to known vulnerabilities.

This threat can be incredibly detrimental to a hospitality merchant's network as recent investigations have uncovered evidence of packet sniffers being used by network intruders to capture sensitive data—even as it was being transmitted over the network.

Webinar and Further Information

Visa regularly offers data security focused webinars. For a list of current scheduled webinars, please visit <http://visa.webex.com>. For more information on Visa's Cardholder Information Security Program and training seminars focused on cardholder data security, please visit <http://www.visa.com/cisp>.

Michael E. Smith is the head of payment system risk at Visa Inc.

Risk Mitigation Strategy: Packet Sniffers

3

Although packet sniffing is often difficult to detect, the following essential security practices should be utilized to mitigate the risk of exposure to systems where cardholder data resides:

- Utilize host-based intrusion detection systems (IDS).
- Monitor firewalls for suspicious traffic, particularly outbound traffic to unknown addresses.
- Ensure security of any wireless network in use, to include encryption (WPA at a minimum).
- Implement file integrity monitoring to detect and alert security personnel of unauthorized file changes.
- Secure user workstations to ensure that packet sniffers or other malware cannot be installed.
- Encrypt sensitive data to protect and render sniffed data unreadable.
- Utilize packet sniffers legitimately to understand and detect network intrusion attempts or suspicious activity on the network.
- Ensure operating system, POS applications, antivirus, anti-spyware, anti-malware and all critical software is up to date.
- Examine systems and networks routinely for newly added hardware devices.
- Identify normal data flows for cardholder information into and out of the network. Configure firewall rules to deny all inbound traffic from non-trusted external networks to protected networks and systems. Larger networks should implement internal proxy servers for Web traffic. This will consolidate all World Wide Web (WWW) traffic (i.e., HTTP, typically port 80 and HTTPS, typically port 443) outbound to the Internet through one server and allow for less complex firewall rules. In addition, this practice allows for inspection of outbound WWW traffic to detect malicious activity and the possible leakage of sensitive cardholder data.
- Ensure default, easily guessable and well known passwords and default settings on firewall and other network devices are not used, this can deter hackers from gaining remote administration of the device.
- Ensure system administrators block direct remote connectivity to the database on the firewall (e.g., for Microsoft SQL Server, typically TCP port 1433, UDP port 1434, etc.). Additionally, hospitality merchants should consider limiting or blocking all non-console administrative connectivity to the internal network.