



Identifying and Detecting Security Breaches

August 17, 2011

Payment System Risk Data Security Webinars Overview



- Encourage greater adoption of and adherence to the Payment Card Industry Data Security Standard (“PCI DSS”), Payment Application Data Security Standard (“PA-DSS”) and PCI PIN Transaction Security (“PTS”) Requirements
- Promote security awareness
- Disseminate frontline information and latest data security trends
- Create transparency and clarity around PCI rules, roles and responsibilities

Controlling Fraud: A Layered Approach



Maintaining and enhancing stakeholder trust in Visa as the most secure way to pay and be paid

Agenda



- Global System Compromises
- Common Vulnerabilities and Malware
- Signs of an Incident
- How to Detect a Security Incident
- Implementing and Reviewing Logs
- Logs and PCI DSS Compliance
- Basics of Incident Management
- Top Challenges
- Visa's "What To Do If Compromised" Procedures
- Resources
- Questions

Web-based exploits

- SQL injection
- Misconfigured web applications that allow remote execution

Network-based exploits

- Payment systems accessible from the Internet
- No segmentation on internal network
- Single domain implementation
- No strict firewall configuration
- Remote access
- Use of RDP/Terminal services on internal network

Host-based exploits

- Excessive permissions
- Use of shared and/or default credentials
- Administrative accounts not protected (e.g., domain accounts, DBAs, SAs)
- Databases not hardened (e.g., direct-SQL queries, stored procedures)

Payment application-based exploits

- Unauthorized user able to modify application to do following:
 - Troubleshooting
 - Capture full track data
 - Take advantage of risky protocols allowed by application

Malicious Software



Malicious Software – Configured to damage and infiltrate computer systems

- Packet sniffers
- Key loggers
- Backdoors
- Password crackers

Signs of an Incident



Understanding where and how payment data flows through the environment is essential to the early detection of malicious activity

- What networks are traversed?
- What systems are touched?
- Where is data stored?



In 2010, most reported data compromises found payment card data **outside** of the payment network environment

- On non-payment network systems directly connected
- In temporary files on test systems
- In archive files (e.g. *.rar, *.zip, *.tar) on internet-accessible systems

Signs of an Incident



Before an organization is able to effectively detect malicious activity on the network, some preliminary work is required:

For each network in the environment:

- Identify all connections in the network
- Identify dependencies and shared resources
- Document network connections and shared resources
- Audit network connections regularly and eliminate unnecessary/outdated connections
- Harden networks – remove or disable unneeded services; ensure network devices are patched and kept current
- Utilize incident readiness and assessment tests to improve environment security posture

Signs of an Incident



Once data flow maps and network diagrams have been created or updated, a security baseline can be established

Security baselines can help an organization by:

- Concentrating focus on actual incidents
- Establishing “norms” for data channels and network traffic
- Determining peak and valley traffic volumes
- Understanding network bottle-necks, choke points or other traffic patterns that might derail incident containment or investigation
- Targeting system and file integrity efforts

Signs of an Incident



Once an organization's environment is prepared, its processes, people and tools can be placed to detect malicious activity

Visa recommends adoption of a layered approach

Layered security offers several levels of protection and harder to circumvent for attackers – more traces left behind

A robust Security Information and Event Management (SIEM) is highly recommended

Robust SIEM includes:

- Capability to provide log and event correlation and analysis across multiple platforms and disparate devices
- A balanced mix of trained professionals and technology
- Flexibility to adapt to changing trends and threats

Signs of an Incident



Indicators of a compromise can be as diverse as the methods used to perpetrate malicious activities. Some examples include:

- Excessive login attempts in system authentication and event logs
- Unexplained modification or deletion of data
- Presence of unexpected IP addresses or routing
- Unknown or unexpected services and applications configured to launch automatically on system boot
- SQL injection attempts or strange code in web server logs
- Unexpected file lengths, sizes or dates, especially for system files
- Unexplained new user accounts
- Presence of archived/compressed files in system directories
- Variances in log chronology or timestamps

How To Detect A Security Incident



Examine security event logs on:

- Web
- Application logs for SQL injection
- Firewall
- Intrusion detection (host and network)
- VPN servers
- Third-party remote access

How To Detect A Security Incident



Where and what to look for:

- Inspect recent vulnerability scan reports and remediate immediately
- Look for suspicious error and usage trends across your web servers
- Monitor user accounts (root level privileges) for unusual local and remote access dates, times and locations
- Look for unusual outbound traffic
- Review registry settings where malicious code is known to hide

Implementing and Reviewing Logs



Implement third-party security log management tool

- Centralized logging
- Analyze logs
- Disseminate alerts
- Keep a history of logs
- Protect logs from unauthorized access
- Companies should have standard procedures for log management

Implementing and Reviewing Logs



Logs are useful when performing:

- Forensic analysis
- Auditing
- Internal investigations
- Operational trends
- Long-term problems

Routine log review is useful in identifying:

- Security incidents
- Policy violations
- Operational problems

PCI DSS Requirement 10:

Track and monitor all access to network resources and cardholder data.

Objective:

To ensure controls are implemented:

- To adequately monitor and track all network resources and all access to cardholder data
- To identify and alert in the event of anomalous behavior indicative of a network, system, or data compromise

PCI DSS Requirement 10: Track and monitor all access to network resources and cardholder data

Establish a process for linking all access to system components to an individual user

Implement automated audit trails to reconstruct the following events, for all system components:

- All individual user access to cardholder data
- All actions taken by any individual with root or administrative privileges
- Access to all audit trails
- Invalid logical access attempts
- Use of identification and authentication mechanisms
- Initialization of the audit logs
- Creation and deletion of system-level objects

PCI DSS Requirement 10: Track and monitor all access to network resources and cardholder data

Record at least the following audit trail entries for each event, for all system components:

- User identification
- Type of event
- Date and time
- Indication of success or failure
- Origination of event
- Identity or name of affected data, system component, or resource

Basics of Incident Management



Preparation

- Organizations should have policies and procedures in the event of a compromise
- Computer Incident Response Team (“CIRT”) should include information security, legal, PR, executive management
- Incident handlers should have proper software / hardware
- Know who to call

Detection

- Gather evidence
- Take good notes
- Make sure to answer the four W’s: Who, What, When, Where, and for extra credit “How and Why”

Basics of Incident Management



Containment

- Remove compromised system from the network
- Do not access or alter compromised system
- Create a binary copy of the compromised system
- Store original drives in a safe place

Eradication

- Rebuild infected systems
- Rotate passwords
- Implement strict inbound and outbound filtering
- Implement up-to-date security patches and anti-virus signature files
- Disable ports / services

Basics of Incident Management



Recovery

- Restore systems from clean backups
- Validate the systems have been restored
- Monitor systems closely

Follow-up / Lessons learned

- Identify areas for improvement, such as:
 - Procedures
 - Security
 - Communication

Top Challenges



1. Failure to report or ask for help
2. Incomplete / non-existent notes
3. Mishandling / destroying evidence
4. Failure to create working backups
5. Failure to contain or eradicate
6. Failure to prevent re-infection
7. Failure to apply lessons learned

Visa's What To Do If Compromised Procedures



Compromised entities must:

- Immediately contain and limit the exposure
- Notify their merchant bank
- Notify law enforcement
- Work with Visa on forensic investigation
- Provide compromised Visa, Interlink, and Plus accounts to your merchant bank
- Provide an incident report to your merchant bank

*For more info, please refer to the “What To Do If Compromised” document available at Visa Online (“VOL”) or www.visa.com/cisp

Visa's What To Do If Compromised Procedures



Acquirers must:

- Ensure compromised entity cooperates with Visa on the investigation
- Perform an initial investigation and provide documentation to Visa
- If Visa deems necessary, an independent forensic investigation must be conducted by a PCI Forensic Investigator (PFI)

*For more info, please refer to the “What To Do If Compromised” document available at Visa Online (“VOL”) or www.visa.com/cisp

Visa's What To Do If Compromised Procedures



Acquirers must:

- Provide at-risk account numbers to Visa
- Ensure the compromised entity has contained the incident
- Perform a PIN security assessment (If PINs are at risk)
- Provide forensic report to Visa
- Ensure the compromised entity achieves PCI compliance

*For more info, please refer to the “What To Do If Compromised” document available at Visa Online (“VOL”) or www.visa.com/cisp

Visa

- www.visa.com/cisp
- “What To Do If Compromised” document
- “Responding To A Data Breach: Communications Guidelines for Merchants” document

PCI Security Standards Council

- www.pcisecuritystandards.org
- PCI Data Security Standard (“DSS”)
- PCI Forensic Investigator (“PFI”) program

Questions?

