SANDAG

2010 PCI GAP ANALYSIS

CONFIDENTIAL

Date Delivered: March 22, 2010

Performed By: Ray Zadjmool QSA
Tevora Business Solutions

Table of Contents

Foreword

Legal Disclaimer

This document (the "Evaluation") presents certain discussions and recommendations concerning systems security. The Evaluation is based upon a collection of methodologies and tests performed at a single point in time. The Internet environment is continually changing and becoming ever more complex, and security analyses and recommendations may unexpectedly become out-dated.

Tevora Business Solutions and the individual authors of this report (collectively, the "Authors") have used methodologies and software they believe to be reliable in evaluating the security issues presented, but the Authors make no representations or warranties concerning either those methodologies and software or the results obtained from their use.

While the Authors believe that the material in this Evaluation presents a fair and reasonable picture of client's security controls, nothing herein can substitute for each reader's own professional and business judgment, independent investigations, and research into the subjects covered. All information presented herein is of a general nature and may not be applicable to any particular situation. Nothing herein constitutes an endorsement of any product by the Authors.

It is important to note that not all types of penetration tools and techniques were utilized or attempted for the Evaluation. The tests executed in the Evaluation utilized penetration testing tools and techniques common to the security industry. Many penetration attempts rely on long periods of time to analyze and understand targets, utilize intermediary nodes and networks, and employ automated techniques that may run unattended for extended periods of time. Such long term testing was beyond the Scope of the Evaluation. In addition, penetration tests provide information regarding only very specific security vulnerabilities.

The Evaluation focused on technical security controls. There are additional non-technical techniques, such as social engineering, that have proven to be very effective in circumventing security controls, but were not addressed in this Evaluation.

About Tevora

Tevora is a leading security solutions specializing in the delivery of end-to-end solutions that help enterprises achieve their security and compliance goals. We offer a comprehensive portfolio of solutions and services to clients in virtually all industries and also serve institutional and government clients.

Tevora's leaders are professionals with years of experience and records of accomplishments in technology as well as business. This dual background means that we understand the importance of growth and profitability and our solutions are designed to enhance both.

As a consulting firm that has the ability to fully implement whatever it recommends, Tevora works with all of the industry's top vendors, yet is beholden to none. We are completely vendor-independent and select best-of-breed products tailored exclusively to our clients' needs. Security is our only business and our single-minded focus on anticipating and solving client problems has been described as "obsessive." We consider this a fair assessment.

Our hard work and dedication has established us as a reliable partner CTOs and CIOs can depend on to help protect against threats, both internal and external. With Tevora as a partner, business leaders can devote their energies to enhancing the overall value of information technology to their enterprise.

Tevora is a Qualified Security Assessor (QSA) and Payment Application Qualified Security Assessor (PA-QSA) in good standing with the PCI Security Standards Council. Tevora is also a DVBE (Disabled Veteran Business Enterprise) certified by the California General Services Department (Cert REF# 32786).

For more information please visit www.tevora.com.

Assessor Profile

Ray Zadjmool

As Tevora's Principal Consultant, Ray's primary role is to assist our clients in aligning their security strategies with their business goals. Ray also mentors junior consultants, manages client relationships, assists with presales and post sales activities, and oversees all projects from inception to the closeout presentation to ensure that every project exceeds our client expectations. Ray ensures that the overall Tevora consulting experience is the best available in the security industry by continuing to innovate our security consulting practice.

With more than a decade of experience in IT and security, Ray brings extensive knowledge in both business and technology to our clients. His experience in policy reviews, security assessments, security remediation, firewalls, secure network perimeter design, database security audits, messaging systems, Windows 2003 Active Directory, infrastructure management, and regulatory compliance adds astounding value to both our practice and to our client's engagements.

Notable Accomplishments

Ray has presented at various security conferences on a number of subjects including Data Loss Prevention, Identity & Access Management, Incident Response and Network Forensics. He has also been a presenter at the Gartner Mid-Size Enterprise Summits for two consecutive years providing information on the latest trends in security to C-Level executives. He has also contributed to numerous industry publications, including SC Magazine.

Certifications and Training

Ray holds the following certifications: PCI QSA, Certified Information Systems Security Professional (CISSP), and Microsoft Certified Service Provider (MCSE). Ray also served a distinguished tour of duty in the United States Marine Corps and holds a secret security clearance.

Education and Experience

Jesse is has 5 years experience with military network and computer security. His certifications include CCNA, Security+, Network+, Linux+, and Server+.

Report Conventions and Definitions

Report Sections

This report is divided into three main components per below. Each section will include a separate cover page so that it can be used separately for various parties.

A: Summary of Findings	A high-level overview of the findings, including vulnerabilities by classification. This section is meant as an overview and could also be provided to auditors.
B: Remediation Recommendations	A listing of the remediation actions we are recommending that can serve as a guide for future remediation efforts.

The following conventions and definitions will be used throughout this report.

Vulnerability Classifications

INFO	Identified information that is important to know, but does not prove any immediate concern. When warranted a greater explanation is provided but no remediation is necessary.
Non Compliant	Identified vulnerability is deemed to have a significant potential impact if exploited. Remediation or mitigation is recommended and deemed necessary.

Please note that the above classifications are given subjectively by the assessor based on both industry standards as well as the context of the vulnerability in the environment. They do NOT correspond directly to a standard score such as the CVSS score.

Additional Information References

In the Detailed Findings document, where a vulnerability or recommendation is listed, it will be accompanied by an ID number that can be referenced in the Remediation Recommendations section for additional information.

Remediation Recommendation Format

When remediation recommendations are described, they are accompanied by:

ID Number	A unique ID number for the remediation for report reference
Title	The brief description of the vulnerability or issue.
Classification	The vulnerability's classification as described previously.
Description	A more detailed explanation of the vulnerability.
Data	Details such as the vulnerable system's IP address.
Reference	A reference describing the issue.
Recommended Solution	A description of how the vulnerability can be addressed.

SANDAG

2010 PCI Gap Analysis

Section A: Summary of Findings

CONFIDENTIAL

Date Delivered: March 22, 2010

Performed By: Ray Zadjmool QSA
Tevora Business Solutions

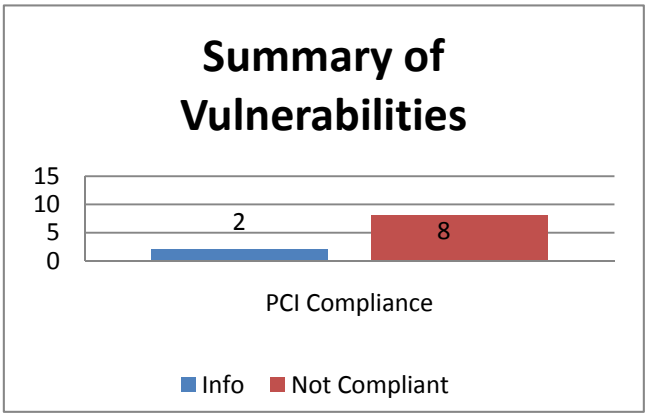
Executive Summary

The result of the March 2010 PCI GAP Analysis concludes that SANDAG should complete several non-trivial remediation projects in order to meet the requirements of the PCI Data Security Standard.

The most critical projects indentified are:

- Two Factor Authentication Solution
- Audit Logging and Log Management
- Data Retention
- Remediation of Reporting Process
- Intrusion Detection Solution
- Patch Management Proxy
- Egress Firewall Rules
- Systems Hardening
- ASV Scans and Testing

Test Snapshot	
Performed By	Tevora Business Solutions
Consultant	Ray Zadjmool, QSA
Scope	COMPASS NETWORK
Methodology	Manual Review
	Stakeholder Interviews
	Service provider Interviews



As key next steps, it is recommended that:

1. Remediation Projects be prioritized in order of risk
2. Implementation of key deficient technologies
3. Post-Remediation testing and analysis of controls

SANDAG

2010 PCI Gap Analysis

Section B: Findings and Recommendations

CONFIDENTIAL

Date Delivered: March 22, 2010

Performed By: Ray Zadjmool QSA
Tevora Business Solutions

Prioritized Recommendations

PCI-001: Two Factor Authentication

Classification: Non Compliant

Description

Two Factor authentication is required for all remote access to the cardholder network. Two factor authentication is a type of strong authentication by which a secondary form of authentication (something you have or are) is required in addition to username and password (something you know).

The purpose of all strong authentication is to increase the level of assurance associated with access authorization.

Data

The Compass network does not require two factor authentication for remote access to the cardholder network.

Reference

PCI DSS 1.2 – Requirement 8.2

> In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:
>
> - Password or passphrase
> - Two-factor authentication (for example, token devices, smart cards, biometrics, or public keys)

Recommended Solution

Implement a two factor authentication solution with VPN for all remote, administrative access into the cardholder network. Recommended solution:

- RSA SecurID with OTP Tokens

Create ACL restriction on cardholder firewall to limit access with administrative protocols to two factor authenticated VPN.

PCI-002: Audit Logging and Log Management

Classification: ☠ Non-Compliant

Description:

Audit logs of cardholder system and network components must be enabled and forwarded to a central log server. Logs must be reviewed on a daily basis. Log retention must be enabled to allow for 90 days availability online, and 1 year offline.

Data

Compass network and system components are not adequately configured to log events.

Network and system component logs are not being forwarded to a central log server and archived.

Daily log review is not being conducted.

All network and systems components are not configured to sync with a trusted NTP source.

Reference

PCI DSS 1.2 – Requirement 10.5.1
Promptly back up audit trail files to a centralized log server or media that is difficult to alter

Recommended Solution

Implement a log management solution. Recommended solution:

- Splunk (Purchased)

Enable auditing on all system components to include success, failure of authentication, policy changes, and object access.

Configure all system components, network devices, and application audit logs to forward to log management solution. Ensure that log management solution has capacity to store for 90 days online, and 1 year offline (backups).

Configure log management solution with policies for automated daily review. Configure alerts to alert personnel on policy violations.

Configure all system and network components to sync with an internal NTP source. Configure internal NTP source to sync with stratum 1 NTP servers. Ensure that ACLS are in place to limit access to NTP protocol.

PCI-003: Cardholder Data Retention

Classification: Non-Compliant

Description:

Cardholder data retention should be configured to minimize data retention and risk. Retention settings should be configured for the bare minimum required for the business. Automated purge scripts should be configured to enforce retention. Retention settings should be reviewed on a quarterly basis to ensure effectiveness.

Data

The CUBIC payment application is not currently configured to enforce business requirements for data retention of cardholder data.

Automated purge scripts have not been configured.

Retention configurations are not reviewed on a quarterly basis for effectiveness.

Reference

PCI DSS 1.2 – Requirement 3.1
Keep cardholder data storage to a minimum. Develop a data retention and disposal policy. Limit storage amount and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in the data retention policy.

Recommended Solution

Adopt a data retention policy that describes the minimum retention requirements of cardholder data for purposes of charge backs and dispute resolution. Recommended guideline:

- 90 Days for PAN storage in database

Document all cardholder storage locations and retention guidelines using the cardholder data storage spreadsheet.

Configure CUBIC data retention scripts to automatically purge or truncate cardholder data that exceeds retention requirements.

Review automated retention scripts on a quarterly basis to ensure that they are properly executing. Document quarterly reviews using the cardholder data storage spreadsheet.

PCI-004: Intrusion Detection

Classification: Non-Compliant

Description:

Network based intrusion detection or Intrusion prevention solutions should be implemented and configured to monitor all traffic in the cardholder data environment.

Data

The compass network does not have an intrusion detection or intrusion prevention solution monitoring all traffic in the cardholder data environment.

Reference

PCI DSS 1.2 – Requirement 11.4
Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic in the cardholder data environment and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines up-to-date.

Recommended Solution

Implement intrusion detection or prevention solution. Recommended Solution:

- Fortinet IPS feature-set
- Snort with subscription
- Cisco ASA w/IDS Module

IDS sensors should be configured in a way to ensure that the entire cardholder data environment is being monitor. If placement of the sensors in the cardholder data environment is not possible, configuring the IDS to monitor the inside and dmz segments of the perimeter firewall would be acceptable.

PCI-005: Patch Management Proxy

Classification: Non-Compliant

Description:

The Cardholder data network should be configured such that Cardholder system components do not have direct access to the internet. Access should be limited to servers in the DMZ.

A patch management process should be implemented such that critical security patches are deployed within 30 days of release by the vendor.

Data

Cardholder systems do not use a proxy for access to the internet for patch updates.

Cardholder systems do not use a proxy for access to the internet for antivirus updates.

The Compass network does not have a patch management process to ensure that critical security patches are deployed with 30 days of release by the vendor.

Reference

PCI DSS 1.2 – Requirement 11.4
Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic in the cardholder data environment and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines up-to-date.

Recommended Solution

Implement a patch management and antivirus distribution server in the DMZ. The recommended solution is:

- Microsoft Windows Update Server (WSUS)
- Symantec Admin server

Configure access control lists to ensure that egress access from cardholder network is limited to servers in the DMZ (WSUS).

Implement a monthly patch management procedure for all cardholder network and system components for testing and deployment of critical security patches.

PCI-006: Egress Rules

Classification: Non-Compliant

Description:

Cardholder firewalls should be configured with ingress and egress (outbound) rules to limit network traffic to only that which is required by the business.

Data

The Compass network infrastructure is not configured with egress rules for the DMZ or cardholder segments.

Reference

PCI DSS 1.2 – Requirement 1.2.1

Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.

Recommended Solution

Configure egress rules on the firewall for DMZ and cardholder segments. Ensure that rules are specific to only the hosts, subnets, and protocols required for the business.

Document all firewall rules using the firewall configuration standard spreadsheet.

PCI-007: Systems Hardening

Classification: Non-Compliant

Description:

All cardholder system and network components should be hardened using industry accepted hardening standards to limit the security footprint of systems to only that which is required for the business.

Data

Cardholder system components are not configured using industry accepted hardening standards.

Some cardholder servers are not configured with only one primary function per server in accordance with industry accepted systems hardening guidelines.

Reference

PCI DSS 1.2 – Requirement 2.2
Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.

PCI DSS 1.2 – Requirement 2.2.1
Implement only one primary function per server.

Recommended Solution

Create a systems hardening standard based on industry accepted standards. Recommended standards:

- NIST
- CIS
- Common Criteria

Ensure that separate standards are created for database servers, web servers, and infrastructure servers such as DNS and Active Directory.

Separate servers that are functioning as dual primary functions such as file transfer and Active Directory.

PCI-008: ASV Scans and Testing

Classification: ☠ Non-Compliant

Description:

Quarterly external scans should be conducted by an Approved Scanning Vendor (ASV). All critical and high classification vulnerabilities should be remediated until "clean" scan reports can be generated.

Quarterly internal vulnerability scans should be conducted on all cardholder systems. All critical and high classification vulnerabilities should be remediated until "clean" scan reports can be generated.

Annual penetration tests should be conducted on the cardholder environment. All critical and high classification vulnerabilities must be remediated until "clean" test reports can be generated.

Data

Quarterly external ASV scans are not being conducted on the Compass network.
Quarterly internal vulnerability scans are not being conducted on the Compass network.
Annual penetration tests are not being conducted on the Compass network.

Reference

PCI DSS 1.2 – Requirement 11.2

Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).
Note: Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV) qualified by Payment Card Industry Security Standards Council (PCI SSC). Scans conducted after network changes may be performed by the company's internal staff.

PCI DSS 1.2 – Requirement 11.3

Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). These penetration tests must include the following:

Recommended Solution

Conduct quarterly vulnerability scans using an Approved Scanning Vendor (ASV). Remediate and rescan until clean scan reports can be generated. Recommended vendor:

- McAfee Scan Alert
- Qualys

Conduct quarterly internal vulnerability scans on the cardholder network. Remediate and rescan until clean scan reports can be generated. Recommended vendor:

- Nessus
- Foundstone
- Tevora (Service)

Conduct an annual penetration test of the cardholder network. Remediate and retest until clean scan reports can be generated. Recommended vendor:

- Tevora (Service)

PCI-009: PA-DSS Compliant Payment Application
Classification: INFO

Description:

Utilizing a PA-DSS compliant payment application is recommended for all merchants as more and more acquiring banks are requiring them. In addition to reducing risk, PA-DSS compliant applications reduce time and effort it takes for to complete a PCI assessment.

According to Visa mandates, as of 10/1/08 PA-DSS validated payment applications are required for any newly boarded merchant[2] .

As of 7/1/10 PA-DSS Visa has mandated that all acquirers must ensure their merchants, VNPs and agents use only PA-DSS compliant applications. [2]

Data

Cubic and Webtix are not PA-DSS validated payment applications.

Reference

1. List of PA-DSS validated Payment Applications

https://www.pcisecuritystandards.org/security_standards/vpa/

2. VISA CISP mandate with regards to Payment Applications

http://usa.visa.com/merchants/risk_management/cisp_payment_applications.html#anchor_3

Recommended Solution

While it is not required to upgrade your payment application immediately, it is recommended that inquiries be made to the payment vendor as to their intent and plan towards PA-DSS validation.

Acquirers can accept other methods of validation in lieu of PA-DSS validation. From Visa:

While the use of PA-DSS validated payment applications is recommended, a payment application need not be included on Visa's list of PABP validated payment applications or PCI SSC's list of PA-DSS validated payment applications in order to comply with Phase 2, Phase 3 and Phase 5 requirements for use of PA-DSS compliant applications. Acquirers may determine the PA-DSS compliancy of a payment application through alternate validation processes, which should confirm that payment applications meet PA-DSS requirements and should facilitate compliance with the PCI DSS. [2]

Discuss with your aquirer their enforcement intent with this mandate and proper strategies for mitigation. Consider conducting a PA-DSS specific penetration test of the payment applications as a means to meet the intent of the requirement.

An upgrade to a PA-DSS validated application should be done with careful consideration to be given to ensuring that the upgrade is done in accordance with the vendors PA-DSS implementation guide.

PCI-010: Remediation of Reporting Process

Classification: INFO

Description:

Access to cardholder databases should be limited to programmatic methods such as a stored procedure executed by an application. Direct access to SQL statements, queries, and other sensitive database components should be limited to database administrators.

Data

Current reporting procedures required that raw SQL queries are posted to business partners for report generation. SQL queries can be modified maliciously to give access to sensitive data stored in the database.

Reference

PCI DSS 1.2 – Requirement 8.5.16
Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users.

- Direct access or queries to databases are restricted to database administrators.

Recommended Solution

Implement a proper reporting solution that requires an application to access the database on behalf of the user. Ensure that application is configured to prevent direct access to the database and requires proper authentication.