Tracy Reed
treed@tracyreed.org

Whitepaper on PCI Compliance

Table of Contents

Introduction

The Payment Card Industry Data Security Standard (PCI DSS) is the security standard for protecting payment card data. While navigating the requirements of the PCI DSS and implementing the technical security controls can be quite complicated, ACME is here to help guide you through the process.

If your systems touch credit card data in any way your bank and the major card brands require you to be PCI compliant. Hardened systems managed by experienced security professionals who know how to implement the PCI DSS are the key to avoiding audit failures or, worse, breaches and expensive fines and reputational damage. ACME has the security and system administration resources to get the job done right.

Your specific PCI compliance needs depend on exactly what you do with the card data (is card data stored or does it only pass through on the way to a payment gateway, etc.) as well as how many card transactions your company processes. This determines your verification requirements (whether you can self-assess or whether a third party auditor must attest to your compliance) and exactly what you must do to become compliant (which Self Assessment Questionnaire) must be completed. It could be as simple as satisfying a dozen requirements or as complicated as several hundred. Speak to a ACME PCI specialist to review the specifics of your situation and determine your PCI obligations. Useful resources:

Official PCI Compliance website:

https://www.pcisecuritystandards.org/

Complete PCI DSS security standard:

https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf

Compliance vs Security

All companies who have a compliance obligation must remember that the point of compliance is to impose a certain level of security. Security is the ultimate goal, not necessarily compliance. Compliance comes as a result of having a good security program. ACME will help you to avoid the "Checkbox security" mentality by ensuring effective security controls which not only meet the compliance requirements but provide practical and effective security measures to meet the actual need, not just the compliance need. Remember that the PCI DSS is the minimum acceptable practice for protecting payment card data.

ACME pulls in additional security resources such as NIST, CIS, and other security standards and benchmarks to enhance the security of our service offering beyond the minimum required by PCI DSS.

Being compliant does not mean you are secure. It merely means you have "checked the boxes". There are many things which could still result in a compromise such as an employee accidentally leaking his passphrase by getting his computer infected with malware, a bug in a web application exposed directly to the Internet, etc.

Occasionally it becomes necessary to go beyond the security requirements spelled out in the letter of the law. Compliance requirements should be considered "minimal acceptable practice" and not strictly "best practice".

Security is a process, not a product.

Both compliance and security are ongoing efforts. There is no "We're PCI compliant, we're secure, we're done." There are always new vulnerabilities discovered, new versions of software coming out, and advances in the state of the art in terms of attacking and defending. The work is continuous and never-ending.

It has been said that compliance is not a checkmark, it is a culture. This is demonstrated in companies who have successfully implemented a PCI compliant security program.

Prevention, Detection, Response

ACME's PCI security program has 3 main components: Prevention, detection, and response. Each of the security controls described herein can generally be classified as one of these.

Using secure passwords (Requirement 8.2.3), keeping systems patched up (Requirement 6.2), and even employee background checks (Requirement 12.7) are considered prevention. These seek to avoid trouble in the first place.

But despite best efforts, since there is no such thing as 100% security: prevention cannot always be successful. We must also plan to detect problems such as intrusions or situations which could lead to intrusion and limit damage. Firewall egress rules, intrusion detection systems, and auditing/logging are all examples of critical methods of detection.

And finally, a plan must be in place to respond to an intrusion to prevent the situation from getting worse and to ultimately resolve the issue. This plan must be drafted taking the needs of the business into account. Responses involve, for example, isolating the trouble area, notifying the appropriate people, and taking proper remedial action.

Exposed web applications: Statistically the greatest weakness

The Verizon Business "2009 Data Breach Investigations Report" found that of the 285 million compromised records from the 90 breaches studied, 79 percent were compromised via Web applications. http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf

Between SQL injections, path traversals, cross-site scripting, and many other attacks, web applications must be written very carefully and undergo thorough penetration testing and security review. Any application which has not yet had security review is practically guaranteed to have fatal flaws. This security review must be done on a recurring basis because added features and code changes can have a serious effect on the security of the application. If there were an SQL injection vulnerability (among many other possible flaws) in the web app it would allow data to be stolen, deleted, or corrupted, possibly leaving no trace at all. The Client must ensure web application security.

Web application penetration testing is a necessity (Requirement 11.3). It is not further discussed in this document but is a necessary part of PCI compliance for an organization offering a custom built web application on the Internet. ACME can help arrange for penetration testing to happen.

Keep in mind that when no vulnerabilities are found it does not mean there are none. All it takes is an attacker slightly more clever than whoever does the security testing to cause a serious problem.

Risk mitigation is the name of the game

There is no such thing as perfect or complete security. Each security control implemented is designed to reduce the probability of having an incident in some way. Sometimes it may seem that any one particular security control may not be terribly critical but remember that probabilities add up and anything that can be done to reduce the probably by even 1% can be worth it. To be able to mitigate risk an assessment must be done to identify the risk.

PCI DSS Scoping

The “scope” of a PCI Card Data Environment (CDE) environment, explained very simply, is any system which contains payment card data and any system which touches or is directly accessible by a system which contains payment card data. There are some additional rules also but this covers the general idea. The PCI DSS is applicable to any systems which are “in scope” and all such systems must be secured per the PCI DSS. ACME can help you analyze your systems, determine the scope, and most importantly **minimize** the scope. To minimize the scope of the CDE is to reduce risk, reduce expense, and reduce the burden of maintaining a compliant environment.

Security Controls

A security control is anything which reduces risk. ACME will conduct a risk assessment of your environment and identify the risks. Each risk identified in the risk assessment must be addressed by a security control which is intended to reduce or mitigate that risk.

In addition to the PCI DSS ACME uses publications such as NIST SP-800-53 for additional guidance in implementing security controls.

Technical Safeguards

Information systems housing payment card information must be protected from intrusion. In our PCI compliant hosting environment ACME implements many hardening measures to prevent and detect intrusion. This area is ACME's greatest strength and value. It is also the largest and most complex area of security controls requiring exceptional skills to implement and maintain.

The Requirements of the PCI DSS

The PCI DSS itself is a list of things that you are required to do in order to secure your Card Data Environment (CDE). While the PCI DSS has only 12 major requirements, each of those 12 can have a dozen or more sub-requirements resulting in hundreds of requirements. Exactly which of these requirements your company must meet depends on what you do with the card data. It is based on risk: If you store card data you will have to meet every one of the requirements. If you don't actually store the data and only have it momentarily as it passes through your systems on the way to the payment gateway you must only comply with a subset of the requirements. In the following pages we take a quick look at the 12 major requirements and a few of the sub-requirements.

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Firewalls must be configured with both ingress and egress filtering. Most people are familiar with the idea of firewalls blocking inbound connections but blocking unusual outbound connections is necessary also to prevent many kinds of attacks from working as well as exfiltration of data. Firewalls logging blocked outbound connections is an excellent source of information as to unusual things happening within the network.

Network segmentation is key in reducing the PCI scope of the CDE. The Client's environment will be maintained on its own private network separated from non-client systems via firewalls using VLANs. Web application servers, database servers, and development servers will all reside in their own separate VLANs and be protected from each other to the greatest extent practical. The CDE will reside in its own isolated subnet or subnets separate from other systems which are not involved in the processing of payment card data.

The firewall blocks access to ssh on all of the internal servers. No direct connections can be allowed. An SSH bastion host with public key only authentication (effectively two-factor authentication when used with passworded private keys) is provided to facilitate SSH access to internal production servers. The bastion host will be hardened/locked down to the greatest extent practical.

As it is generally the only way into the environment (VPN is a possibility for some customers) special attention will be paid to SSH. Too many failed login attempts will cause the IP address of the user/attacker to be banned for a fixed amount of time to mitigate password guessing/brute force attacks.

Personnel who have never worked in a secured environment may be unfamiliar with the practice of using public key authentication, relaying their SSH connection through a bastion host, or not being able to make outgoing connections from the servers. These developers will require training. SSH, particularly the OpenSSH implementation, is not only the industry standard but is a very powerful tool for providing remote access and has facilities to make working among these restrictions easy.

Requirement 2: Do not use vendor supplied defaults for system passwords and other security parameters

This requirement covers not only using default passwords (which attackers frequently use to attempt access) but also ensuring that each system performs one task, disabling unused services, etc. ACME automation disables unnecessary services and enforces strong authentication methods. We can help you design your environment such that each server provides only one service per requirement 2.2.1.

Requirement 3: Protect stored cardholder data

ACME can help to analyze the need to store cardholder data, what forms of data are permissible to store and what are not, and implement strong encryption or other security controls as required to meet Requirement 3. Proper key management is a big part of keeping encrypted data secure and Requirement 3 has a number of sub-requirements in this regard.

Requirement 4: Encrypt transmission of cardholder data across open, public networks

When payment card data flows over open networks encryption must be utilized: ACME uses SSH for administrative functions, GPG for email, and SSL for webserving of such information. Standard Linux whole disk encryption is also available although generally only recommended for mobile devices such as laptops. ACME makes extensive use of SSH and SSH configurations to ensure confidentiality and integrity of data as well as requiring public key authentication for all external system access. ACME does not use any wireless technology in the datacenter (Requirement 4.1.1) and ensures all of our staff receive training on how to handle payment card information properly (Requirements 4.2 and 4.3).

Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs

ACME uses automation to ensure that anti-virus is installed on all systems, is up to date, is configured to scan properly, generate audit logs, etc. Furthermore, systems are in place to provide monitoring and alerting to the discovery of viruses or malware on servers via a centralized log collection system.

Requirement 6: Develop and maintain secure systems and applications

ACME goes to great lengths to harden our systems to ensure they are as secure as possible. Our Linux host hardening program is based on the NSA Linux Hardening Guide also known as the NSA Systems Network Attack Center (SNAC) hardening guide:

http://www.nsa.gov/ia/_files/os/redhat/rhel5-guide-i731.pdf

Chief among our hardening measures is the use of an automated configuration management system known as Puppet. This system automatically applies many config changes to a stock Linux server. It currently consists of over 3000 lines of code and covers automatic configuration and maintenance of security controls such as:

- File integrity monitoring (SNAC-2.1.3.1.1)
- System audit logs (file accesses, changes, etc) (SNAC-2.6.2.1)
- Secure automount configuration (SNAC-2.2.2.3)
- Disable avahi autoconf (SNAC-3.7.1.1)
- Configure warning banner (SNAC-2.3.7.1)
- Enforce secure bootup (SNAC-2.3.5.3)
- Enforce secure console permissions (SNAC-2.3.1.1)
- Disable coredumps to minimize chances of information leakage (SNAC-2.2.4.2)
- Disable atd, ensure proper cron file permissions (SNAC-3.4)
- Ensure execshield is enabled to thwart buffer overflow attempts (SNAC-2.2.4.3)

- Ensure proper mount permissions such as noexec etc. in fstab (SNAC-2.2.1.[1,2])
- Ensure proper home directory permissions (SNAC-2.3.4.2)
- Configure various kernel parameters, enable no-exec stack, disable hazardous drivers (SNAC-2.2.4.4.2)
- Ensure proper log rotation so as not to lose log data (SNAC-2.6.1.5)
- Disable certain esoteric kernel modules from loading, reducing attack surface (SNAC-2.2.2.5)
- Ensure NFS related services are disabled (SNAC-3.13.1.1)
- Enforce strong passwords, set lockouts, etc. (SNAC-2.3.3.1.1)
- Set password lockouts, hash algorithm, file permissions. (SNAC-2.2.3.1)
- Ensure root's $PATH is safe and sane (SNAC-2.3.4.1.[1,2])
- Configure postfix to not listen on network (SNAC-3.11.1.1)
- Regularly scan the system comparing rpm checksums with installed files (SNAC-2.1.3.2)
- Ensure sendmail is off and uninstalled (SNAC-3.11.1.1)
- Ensure a number of undesirable/unsafe services are disabled (SNAC-3.3.15.2)
- Set global umask settings (helps ensure safe file permissions) (SNAC-2.2.4.1)
- Disable wireless kernel modules (SNAC-2.5.2.2.3)
- Ensure proper SSH config, distribution of pubkeys, etc. (SNAC-3.5.2)

ACME also implements SELinux on all of our security hardened servers. This is a system of mandatory access controls (MACs) developed by the NSA: http://selinuxproject.org

SELinux is indispensible in preventing security flaws in things such as web applications from accessing/changing other parts of the system as well as preventing many other classes of security problems. ACME will configure SELinux to run in enforcing mode and confine processes to least privilege to the greatest extent practical while still allowing normal operation.

We review a number of sources of security information on a daily basis (Requirement 6.1)

Security patches will be applied within 30 days (Requirement 6.2), Client permitting (reboots are usually required).

Requirement 6.3 calls for the development of secure web applications. While ACME ensures our own web applications are secure it is up to the customer to secure the applications they wish to install, particularly as it pertains to web applications. ACME will support the client in this on a best-effort basis.

Requirement 7: Restrict access to cardholder data by business need to know

Using standard access control methods provided by the operating system such as users, groups, etc. The systems will be configured to allow access only to those who have a business justification. Two factor authentication, public key authentication, etc. will be used as appropriate.

Requirement 8: Identify and authenticate access to system components

This requirement basically says each individual user must have a unique user ID (no shared IDs) to ensure personal individual accountability (Requirement 8.1.1). It also calls for good account management practices, strong passwords, lockout after a particular number of failed authentication attempts, etc. Systems are configured implement all of this using automation to ensure consistent enforcement of these rules.

Requirement 9: Restrict physical access to cardholder data

The ACME datacenter facility is audited annually to SSAE 16 Type II and has a 24/7 manned physical presence. The datacenter has extensive video camera coverage (Requirement 9.1.1) and visitors are logged by required sign-in (9.4.4) etc. ACME logs all equipment as it physically enters and leaves the datacenter. When equipment is retired it is disposed of properly to ensure that card data is not compromised including the secure wiping or physical destruction of media (Requirement 9.8).

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

Regular analysis of system log files is an important means of detecting intrusions, intrusion attempts, and software misconfigurations. It is critical to get the system log files off the server on which they are generated and onto a separate secured system where they cannot be tampered with. System log files will be sent in real-time to a central log server where they can be subjected to weekly audit log reviews per requirement 10.6.

The following regularly scheduled audits will be conducted:

- Daily log file analysis
- Quarterly system audits to check for any unusual processes, accounts, etc.
- Quarterly physical security audits
- Quarterly internal and external vulnerability scans and remediations

Proof of audit log reviews, audits, findings, etc. will be retained.

The Linux audit system (auditd) logs access to critical files and various important events and is automatically configured by Puppet.

Centralized logging aggregates all of this information and provides a platform in which to investigate issues and detect intrusions.

Netflow monitoring logs network traffic making it possible to detect unusual network traffic.

This combined IDS provides accountability for employees by tracking their network activity. It provides a quick clue regarding unauthorized host access for rapid response to CDE access, alteration and/or destruction and detects malicious and suspicious network activity and works in conjunction with third party devices to mitigate or remediate security policy violations. IDS excels as an incident response tool and serves as a first responder technology that provides notification of potential issues.

Requirement 11: Regularly test security systems and processes.

Requirement 11.4 calls for intrusion detection systems for information system monitoring, near real-time alerting of issues, etc.

One of the best ways to monitor network activity and detect network attacks is to use a Network Intrusion Detection System (NIDS). Such a system inspects all traffic going into and out of the network and applies rules and heuristics to network traffic to attempt to detect attacks and alert security personnel of potential issues. Data coming from the NIDS must be reviewed regularly and in a timely manner to ensure early detection of issues.

Requirement 11.5 calls for File Integrity Monitoring (FIM) to detect changed system files. This is automatically deployed by Puppet configuration management. Changed files are logged and appear in the periodic system log review.

Requirement 12: Maintain a policy that addresses information security for all personnel.

The security policy is a required document which ensures that all personnel with access to the card data environment know their responsibilities with respect to security. It lays out the policies and procedures that personnel are expected to follow. A copy signed by each individual with such access must be kept on file. There are many risks for which there is no technical solution as the risk is due to individual behavior and actions. An example might be the sharing of passwords. This is addressed in the security policy by prohibiting the sharing of passwords. Employee education, security awareness training, etc. are all covered under Requirement 12. Monitoring the PCI compliance of service providers is another big one in this section. Many companies have been compromised because a trusted provider with access to the CDE failed to live up to its security obligations resulting in a compromise.

Conclusion

The major points of PCI compliance have now been covered and we hope you have a better understanding of exactly what a PCI compliant hosting solution looks like with ACME. While implementing all of the above ACME will be keeping records of such activities so as to be able to prove compliance to you or auditors. We will happily work directly with auditors to prove your compliance.

This document demonstrates that ACME has the skills and resources to provide your company with a complete PCI compliant hosting solution. We have pre-existing processes and procedures and technological infrastructure in place to ensure your hosting environment is hardened and monitored so that you can sleep well at night knowing your valuable card data is safe.

PCI compliance is a team effort and we look forward to working with you as we help your company move towards obtaining and maintaining PCI compliance.

Contact us now to discuss your specific PCI needs!