Avecto Whitepaper

Compliance series

Guide to meeting the requirements of PCI DSS 3.2

Payment Card Industry Data Security Standard

The Payment Card Industry Data Security Standard (PCI DSS) is a compliance mandate that has wide-reaching implications for organizations that handle credit card data – specifically card numbers, expiry dates and the card holder name – either during a transaction or at any point thereafter. This whitepaper examines the directives of PCI DSS that impact endpoint security and how the access control requirements can best be achieved.

> “Organizations found to breach PCI DSS regulations can be fined and be required to meet the costs of fraudulent activity.”

Introduction to PCI DSS

Designed to protect consumers from credit card data theft, the PCI DSS consists of 12 requirements to encrypt or remove sensitive data, protect networks, secure applications and provide security through auditing, monitoring and access control. Putting these measures in place can help prevent denial of service attacks, data theft, and systems from being infected with malicious code.

American Express, Discover, MasterCard, Visa and JCB formed the Payment Card Industry Security Standards Council (PCI SSC) in 2004 to develop a mandate to enforce a minimum level of security, to which all merchants processing credit card data should comply. The first version of the standard was published in June 2005, and updated to version 2.0 in October 2010. PCI v3.0 came into force in January 2014 and companies were given one year to implement it.

It’s a legal requirement to comply with PCI DSS if your organization stores, processes or transmits cardholder data. Banks regularly report the compliance status of merchants to the credit card companies, which then select businesses to investigate. If found to be in breach of the regulations, organizations can face fines of up to $500,000 and be required to meet litigation costs brought as a result of fraudulent activity. If any part of the payment process is outsourced to a third-party, it must also be PCI DSS compliant and you should ask to see a compliance certificate annually.

Merchants are categorized by four levels according to the number of credit card transactions they process. Level 1 merchants process six million or more transactions annually and are required to have a yearly onsite security assessment, and a quarterly network scan if involved

in ecommerce. Level 4 merchants are at the bottom end of the scale and can comply by completing a self-assessment form.

The 12 PCI DSS mandate requirements are divided into six areas and the remainder of this whitepaper will focus on implementing strong access controls and monitoring networks.

PCI DSS aims to make sure organizations:

- Build and maintain a secure network
- Protect cardholder data
- Maintain a Vulnerability Management Program
- Implement strong access controls
- Regularly monitor and test networks
- Maintain a policy that addresses information security

What's new in PCI DSS 3.2

Released as a draft document in April 2016, the PCI DSS 3.2 standard will be considered a best practice until January 31st 2018, and from 1st February 2018 a requirement, although the PCI DSS 3.1 mandate will still be active for six months after that. While there are some changes to the technical requirements in PCI DSS 3.2, the need to implement strong access control remains unchanged, including restricting access to cardholder data according to business 'need to know', identifying and authenticating access to system components, and restricting physical access to cardholder data.

The key technical change in PCI DSS 3.2 is the requirement (8.3.1) to enforce the use of multifactor authentication, either at the network or system level, for all users with administrative access to systems in the cardholder data environment (CDE). This doesn't apply to server application or system accounts. Furthermore, multifactor authentication must be used when accessing the CDE network from remote locations outside the entity's network (8.3.2).

Appendix A3 now includes the Designated Entities Supplemental Validation (DESV) requirements, previously a separate document, which necessitates that designated entities prove they are truly maintaining compliance with PCI DSS. DESV doesn't add any additional technical requirements to PCI DSS.

Most other changes in the draft are procedural, such as the requirement to perform penetration testing on segmentation controls every six months (11.3.4.1), and the requirement to include verification that any PCI requirements aren't impacted in requests for change (6.4.6).

What follows is a summary of the key requirements in PCI DSS and, where necessary, more detail pertaining to the principle of least privilege security and identity management.

Build and maintain a secure network and systems

Hackers can find backdoors via untrusted networks using different techniques, including exploiting browser zero-day vulnerabilities or from a partner's business network.

1. Install and maintain a firewall configuration to protect cardholder data

PCI DSS deems any network that is not under review, and/or not controlled directly by the entity (organization), to be untrusted. And as such, network security must be maintained to ensure systems are protected from unauthorized access that might be gained through untrusted networks.

2. Do not use vendor-supplied defaults for system passwords and other security parameters

Default configurations are often insecure, or at best provide only a basic level of protection. PCI DSS requires that organizations reduce the attack surface of systems by enabling only the necessary services and protocols required by business applications. Systems should be appropriately hardened to prevent misuse and unnecessary features removed, and root and administrator account passwords changed

from their factory defaults. The removal of administrative privileges is important to make sure users can't reverse configuration changes designed to secure systems.

Protect cardholder data

Even if a malicious attacker gets past other security defenses, when cardholder data is encrypted, the data cannot be read without access to the cryptographic keys.

3. Protect stored cardholder data

In the same way as access to accounts holding domain administrator privileges should be limited, access to cryptographic keys must also be restricted to the fewest number of systems and custodians.

4. Encrypt transmission of cardholder data across open, public networks

Data must be encrypted across open networks, or other networks that might be easily accessed by malicious actors.

Maintain a vulnerability management program

Hackers often take advantage of known security vulnerabilities to compromise systems.

5. Protect all systems against malware and regularly update antivirus software or programs

Antivirus should be installed that can detect all types of malicious software, and measures taken to make sure users cannot disable malware protection or change policies. The removal of administrative privileges from end users can help achieve this goal. Policies and procedures designed to protect business systems must also be documented.

Definition-based antivirus isn't always able to defend against zero-day vulnerabilities, and can fail to provide protection if not kept up-to-date. But a defense-in-depth endpoint security solution, including least privilege security and application whitelisting, can provide protection where traditional AV solutions might fail.

If your organization uses legacy software that is either known to be vulnerable or is no longer updated, such as unsupported versions of Internet Explorer, Windows XP, or applications developed in house, a comprehensive endpoint security solution can help protect against vulnerabilities in line-of-business software.

6. Develop and maintain secure systems and applications

Change control is critical in maintaining secure and functional systems, and managing user privileges plays a key part in ensuring that unwanted changes can't be introduced into production systems without approval for all concerned stakeholders. OS and application security patches should be installed in a timely manner to protect against known vulnerabilities, and the change process used to install them, including any software modifications, documented.

Security patches should be applied in a timely manner. But in situations where patches fail to apply or aren't available for critical business applications, endpoint security (in addition to a network or host-based Intrusion Protection System (IPS)) and real-time monitoring of security and operating system event logs, can help to mitigate exploits, while vulnerabilities in software or the operating system remain unpatched.

OS Command Injection is a technique used by hackers to run commands on an OS via a compromised application. PCI DSS requirement 6.5.1. necessitates that these types of attacks be considered when securing systems, and limiting access rights, use of application whitelisting and isolating untrusted content can help mitigate zero-day vulnerabilities in applications.

> "Requirement 7.1 – Limit access to system components and cardholder data to only those individuals whose job requires such access."

Implement strong access control measures

Restricting use of privileged credentials, and generally who can access what, is a key principle of information security.

7. Restrict access to cardholder data by business 'need to know'

To comply with the access control requirements of PCI DSS 3.2, merchants must restrict access to cardholder data by business need-to-know (Requirement 7), assign unique user IDs to each employee (Requirement 8), and limit physical access to cardholder data. PCI defines business **need-to-know** as when access rights are granted to only the least amount of data and privileges needed to perform a job.

Users' roles for access to system components and data resources should be defined and documented, including the level of privilege required to access each resource. PCI DSS states that employees issued with privileged user IDs, such as root or administrator accounts, must be limited to the least set of privileges necessary to perform their job responsibilities (Requirement 7.1.2). IT staff are commonly given full administrative permissions to systems on a permanent basis, because at some point unrestricted access will be required to perform a particular task. Instead, it's preferable to implement a privilege management solution that assigns administrative access to a limited set of applications or operating system executables. Providing IT staff with full administrative access to endpoints and servers significantly increases the risk of data theft and malicious code entering sensitive systems.

Similarly, standard users should be assigned privileges based on job classification and function (Requirement 7.2.2). Employees are sometimes given Power User or Administrator privileges to facilitate performing certain restricted operating system tasks, such as defragmenting the hard drive or adding hardware. This is especially prevalent amongst notebook users, who are often given elevated privileges as they are considered more difficult to support when away from the office.

> "Requirement 7.2.2 – Assignment of privileges to individuals based on job classification and function."

But this is a double-edged sword, as although notebook users with administrative privileges can perform some tasks that would otherwise require intervention from IT, they can also change critical operating system settings, and are more likely to become victim to malicious code; resulting in downtime, system slowdowns and potential data theft. A privilege management solution can deliver secure and compliant desktops while at the same time providing all the functionality users need to perform their job functions.

> “Requirement 8.1.1 – Assign all users a unique ID before allowing them to access system components or cardholder data.”

8. Identify and authenticate access to system components

Windows Vista (and later) has a basic privilege management feature in the form of User Account Control (UAC), designed to encourage programmers to code software that doesn't require elevated privileges and to protect consumers from themselves. But UAC requires users to have two accounts, one with standard user privileges and the other with full administrative access, permitting users to elevate privileges whenever they see fit.

Using a third-party privilege management solution is the only way to provide users with the flexibility afforded by UAC and the security required for PCI DSS compliance, including Requirement 8.1. PCI DSS also makes a special point of requiring that all access attempts made using administrative privileges be logged (Requirement 10.2.2).

The creation and modification of user accounts should be strictly controlled to ensure that users are only granted the minimum privileges required to undertake job responsibilities (8.1.2). A password or passphrase is the minimum protection requirement for non-consumer users and administrators on all systems (8.2), but smartcards or biometric security can also be implemented to further protect user accounts.

9. Restrict physical access to cardholder data

Physical access should be restricted to systems that store cardholder data. This can be in the form of entry control facilities to restrict only authorized personnel.

Regularly monitor and test networks

Security is an ongoing process that must be reevaluated as threats and systems change.

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

An audit trail should be kept of each individual user's access to every system. In addition, access to cardholder data, actions performed using root or administrator accounts, access to audit logs, invalid login attempts, use of identification and authentication mechanisms, and changes to audit trail recording systems, must be separately recorded.

Log data should contain information about the user account, action performed, date and time, indication of success or failure, the location from where the action was executed, and information about the modified component. This information should be reviewed on a regular basis so that any suspicious activity can be identified, and must be kept for a minimum of one year.

11. Regularly test security systems and processes

Quarterly vulnerability scans should be performed, and any weaknesses identified rectified to ensure systems remain secure. After remedial work has been carried out, systems should be rescanned to confirm vulnerabilities have been removed from systems.

> "Using a third-party privilege management solution, such as Defendpoint, can help organizations meet compliance needs faster and more easily than using native tools."

Maintain an information security policy

End users are often the weakest link in security.

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

When new employees are hired, they should undertake security awareness training, and this training should be updated and repeated at least annually. Making users aware of the dangers posed by social engineering and misuse of administrative privileges can help improve an organization's security posture.

Windows User Account Control (UAC) alerts cannot be customized, but a third-party privilege management solution can be used to provide custom and branded messages to users to help them understand the risks of overriding corporate security policy when attempting to launch applications with elevated privileges or access untrusted content.

Defendpoint helps businesses meet PCI DSS compliance

Defendpoint allows organizations to implement privilege management from a central location using Active Directory and Group Policy. Users can be assigned unique IDs that have standard user privileges, but still use legacy applications or operating system features that require additional rights. Individual processes can be run with elevated privileges without requiring a second user account, while ensuring that all other processes are protected by the user's limited access token. Defendpoint can save significant time and resources when implementing and maintaining strong access controls for PCI DSS 3.2, including comprehensive audit trails and customization of elevation consent dialogs.

Avecto's application whitelisting works across all supported versions of Windows, starting from Windows 7 and the equivalent server editions, and has a flexible rule set making it easy for administrators to limit users to only approved applications based on different criteria.

Both the privilege management and application whitelisting features of Defendpoint can be used with **challenge/response authentication**, where if a user is required to launch a process with elevated privileges, or a blocked application, a quick call to the IT helpdesk can provide users with an authorization code that allows them to carry out the required task. Additional features include the ability to sign policies, ensuring they haven't been modified, and other tamper-proof measures that prevent Defendpoint from being intercepted or disabled. Additionally, Defendpoint's unique sandboxing feature operates transparently to users and utilizes default Windows security mechanisms to give protection against zero-day vulnerabilities.

No compromise on security or usability

As noted by security professionals, many organizations are PCI DSS compliant but not secure. Using a third-party privilege management solution, such as Defendpoint, helps organizations meet compliance needs faster and more easily than using native tools, and go beyond the basic mandate requirements with little extra effort.

About Avecto

Avecto is an innovator in endpoint security. Founded in 2008, the company exists to protect businesses from cyber attacks.

Its endpoint security software, Defendpoint, is a multi-layered prevention engine that stops malware at the endpoint. It takes a proactive approach, uniquely integrating three core capabilities of privilege management, application control and content isolation in one lightweight agent.

This unique and award-winning combination makes prevention possible, allowing businesses to build solid security foundations that protect over 6 million endpoints at many of the world's most recognizable brands. This proactive strategy is advocated by analysts, industry experts and security professionals alike.

Avecto's simpler and smarter approach to security makes organizations more secure from day one. For more bespoke requirements, an experienced and qualified team of consultants is available to guide the implementation and ensure project success.

Deloitte. Technology Fast50 UK 2014

UKtech awards 2015

winner Cyber Security Awards

intel Security Innovation Alliance

Microsoft Partner Gold Application Development

Russell Smith

Russell Smith is author of Least Privilege Security for Windows 7, Vista and XP published by PACKT, Contributing Editor at the Petri IT Knowledgebase and a regular contributor to leading industry blogs and journals. With over 15 years' experience securing and managing Windows Server systems for Fortune Global 500 companies and SMEs, Russell is also an experienced trainer. You can contact Russell at rms@russell-smith.net.