

Introduction

The Payment Card Industry (PCI) Data Security Standard (DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. DNS services are a key component of network access and recent security vulnerabilities in the protocol have revealed that these systems are a perfect target for hackers trying to illegally access critical information including credit card data. Therefore it is critical that enterprises ensure that DNS servers are kept in PCI compliance.

Infoblox core network services appliances provide critical infrastructure for over 3,000 enterprises world-wide including over 125 of the Fortune 500. Recognizing the key role played by our products, Infoblox devotes significant attention to security across all phases of product design and deployment. Infoblox pays particular attention to addressing security at all of the different layers in the security model: the physical layer via a hardened appliance, the operating system via a hardened and locked down OS, the protocol services via the latest patches and versions, and in all management and intra-appliance communication via encrypted network traffic. Secure, controlled and auditable DNS and IP Address Management are critical for compliance with PCI-DSS requirements. Infoblox is the market leader in secure appliances for these core network services and helps enterprises comply with PCI-DSS requirements as detailed in this note.

PCI Requirements 2.2.1 – 2.2.4: "Implement only one primary function per server. For a sample of system components, verify that only one primary function is implemented per server. For example, web servers, database servers, and DNS should be implemented on separate servers. Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the device's specified function). Configure system security parameters to prevent misuse. Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers."

Infoblox Helps Companies Comply with PCI 2.1.1-2.2.4:

- Infoblox appliances provide a standard, well defined set of core network services on each appliance. By design, these single purpose dedicated appliances are preconfigured and the operating system is locked down at the factory. All non-essential services, libraries, binaries, and utilities e.g. Telnet, FTP, SMTP, etc. have been completely removed from the base system. Any standard Infoblox supported service (DNS, DHCP, RADIUS, TFTP, NTP etc.) that is not configured is disabled.
- Infoblox provides no root or login access to any underlying operating system preventing any user from installing additional software on any appliance. This ensures that the appliance is used only for DNS per the requirement and the functionality is not expanded.

PCI Requirement 6: Develop and maintain secure systems and applications

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches. All systems must have the most recently released, appropriate software patches to protect against exploitation by employees, external hackers, and viruses. Note: Appropriate software patches are those patches that have been evaluated and tested to determine that the patches do not conflict with existing security configurations. For in-house developed applications, the numerous vulnerabilities can create burdensome regression testing to ensure compliance.

6.1 Ensure that all system components and software have the latest vendor-supplied security patches installed. Install critical security patches within one month of release. *Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

6.2 Establish a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet). Update configuration standards as required by PCI DSS Requirement 2.2 to address new vulnerability issues.

Infoblox Helps Companies Comply with PCI Requirement 6:

The above requirements as they pertain to DNS infrastructure have three separate aspects –

1. ***Keeping your platform patched for all security vulnerabilities:*** The first key point to consider is whether your DNS platform allows easy patching and upgrading. The second key point is the frequency of patches that need to be applied.

In the case of general purpose servers e.g., Unix, Windows, AIX, Solaris etc. patches are frequent (for example, “patch Tuesday” for Microsoft) and the effort in keeping servers updated is enormous. DNS servers running on general purpose servers typically require extensive operating system patching in order to stay compliant with PCI requirements. How does an enterprise ensure it is able to keep all their DNS servers updated all the time? If they are not constantly patched, they might not be in compliance with PCI-DSS. If they keep their infrastructure updated, how much effort does it take? Does it require extensive planning and downtime? If so what are the costs borne by IT department and users?

Infoblox appliances are based on a hardened, optimized operating system and therefore do not require frequent patching. Additionally, when patching is necessary, Infoblox gathers all underlying patches, creates and tests a single bundle of code for distribution and notifies all support customers. Once

downloaded, a single click can perform system wide upgrades and make it effortless to keep your infrastructure current. This reduces operational expense while minimizing downtime. For example, Infoblox had a patch available for our customers the day the DNS "Kaminsky" vulnerability was publicly announced. Infoblox customers were able to upgrade all of the DNS servers within minutes.

2. ***Keeping your DNS software patched for all security vulnerabilities:***

The DNS software itself might have vulnerabilities and it is extremely important that patches are available immediately after vulnerabilities become public to avoid exploitation. Some key points to think about:

- a. ***What is the track record of your DNS vendor in supplying patches for critical DNS vulnerabilities?*** As evidenced by the recent Kaminsky bug (VU#800113) Infoblox was among the first vendors to provide its customers with a patch to resolve this issue. Alcatel-Lucent's QIP patches came some 28-30 days after the vulnerability was announced leaving their customers vulnerable to attacks. In the past QIP has taken even longer to release patches.
- b. ***How easy it is for you to apply patches and stay compliant?*** If it takes a lot of effort to patch your DNS systems, chances are you may not always be compliant due to the time and complexity involved in patching.
- c. ***How committed is the vendor to provide fixes?*** Core network services (DNS, DHCP, IPAM) are the primary business of Infoblox; therefore, all of the company's resources are devoted to keeping the product updated and customers compliant and secure.

3. ***Monitoring Security Vulnerabilities:***

DNS and network security are rapidly changing environments that require constant monitoring for vulnerabilities. In most cases, it requires a lot of time and effort from high-paid, security savvy individuals to monitor for potential vulnerabilities and then to ascertain the relevance to the organization's infrastructure. Does the organization have such individuals with enough time to adequately monitor all sources; is that the best use of their time?

Infoblox employs a 16 member Security Alert Response Team (with representation from Engineering, Technical Support and Product Management) that continuously monitors various sources for potential vulnerabilities. The Security Response Team is included on private security alerts distributed from key contributors to ISC BIND and other core protocols. Every reported vulnerability alert is reviewed by the Infoblox Security Alert Response Team with members on-call 24x7x365. All discovered vulnerabilities are patched or fixed prior to release. All security patches and fixes are generally made available in monthly patch releases. Serious vulnerabilities, such as the recent DNS cache poisoning vulnerability are patched immediately and customers are alerted and patches are made available on the Infoblox Support Portal. We also update the CERT Vulnerability Knowledgebase website with remediation information. Every product release is scanned with two commercial vulnerability assessment scanners before posting to the web or manufacturing.

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

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of detailed audit logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong.

For DNS servers running on a general purpose platform, it is possible for a user with a root login to make changes directly to a remote server without getting those changes reflected back in the administrative logs and thus may compromise security and compliance. In addition, most general purpose platforms don't have detailed audit logging of every DNS change made to the system. It might record that an admin edited a zone file, but it won't record the changes made. Determining the cause of a compromise is very difficult without pristine system activity logs.

Monitoring of physical access to the network resources is also critical. Many organizations find it difficult to know exactly where a particular device is plugged into the network. This becomes critical when monitoring for and tracking rouge devices.

Infoblox Helps Companies Comply with PCI Requirement 10:

Infoblox provides administrative action logging with details on when a specific change was made, who made it and details of the event for all protocols and services including DNS and DHCP. Since the Infoblox appliance is a secure, hardened platform with no OS level access, auditors can be assured that the logs are correct and can not be tampered with as is possible on general purpose servers.

The audit logs can be searched, filtered, exported and printed to allow easy analysis if there is a security event.

Infoblox also offers a method of tracking physical port connectivity and usage with its PortIQ™ appliance product. PCI means that for many retailers, they now face migrating their store networks from one to multiple VLANs, with PCI devices on their own VLANs. Healthcare providers face a similar challenge of separating infrastructure. PortIQ enables these groups to optimize their LAN infrastructure by providing a mapping of ports to VLAN to maximize port switch usage.

The PortIQ appliance also monitors port usage over time and provides historical and current reporting of which devices were connected to which VLAN and port at a specific time. In this way, administrators can audit that physical network security has been maintained on the PCI VLAN.

Summary

The Payment Card Industry (PCI) Data Security Standard (DSS) is a critical and rigorous standard that requires a secure DNS infrastructure to be fully compliant. The best, most cost-efficient way to ensure continued compliance with PCI is to deploy a robust, secure, easily-patched and auditable DNS infrastructure with Infoblox appliances.