What Do I Really Need To Do To STAY PCI DSS Compliant?

By Dr. Anton Chuvakin - http://www.chuvakin.org/

Lately, a lot of security industry discussions have been focused on PCI DSS (Payment Card Industry Data Security Standard). The conversation ranges from practical advice on “how to get compliant” all the way to branding PCI as a devilish invention (Google for “PCI is the devil”). Fiery debates aside, PCI DSS guidance helped countless organizations to see the light of security where there was none before. It goes without saying that it didn’t magically make them “become secure” – no external document can.

One of the frequent criticisms of PCI focuses on the misguided view that “PCI is all about passing an ‘audit’.” Many people would be surprised to find out that PCI DSS lists specific tasks that you have to be doing all the time – NOT just before the assessment. This article focuses on the exact steps organizations must take to actually stay compliant and not just pass validation via scanning, on-site assessment or self-assessment questionnaire (SAQ).

del.icio.us

Discuss in Forums {mos_smf_discuss:/root}

Indeed, very few experts will actually tell you how to STAY compliant and not just how to GET compliant. Recent cases of massive card data breaches at companies that were at one point validated as PCI DSS compliant show that staying compliant is much harder than getting compliant. Security benefits of PCI DSS are not realized just because an assessor in a fancy suit tells you that are “validated as compliant.” Such benefits are there if you are “doing PCI” and “doing security” every day (yes, PCI does include daily tasks for you to do!). By the way, if you are trying to use PCI DSS to launch your security program, this resource would be a useful guide: http://chuvakin.blogspot.com/2009/10/my-fun-pci-webcast-on-oct-27-2009.html

Despite the above focus on “getting compliant,” some security vendors preach the theme of “ongoing compliance.” In fact, they’ve been doing that literally for years. Of course, the “ongoing compliance” theme is awesome. Sadly, a majority of the same vendor customers don’t do it like this (to their own loss – this why it is sad). They still have assessment-time rush, “pleasing the QSA” approach and a “checklist-oh-we-are-DONE” mentality. We can conclude that before one wants to “sell” a continuous compliance concept, one needs to educate the audience first.

To top it off, achieving 100% PCI compliance for validation gets much more resources at corporations compared to maintaining 100% PCI compliance.

In light of the above discussion, a lot of people are surprised that the PCI DSS document itself contains a list of tasks to perform to maintain compliance between assessments. The table below shows these periodic tasks:

PCI DSS Requirements Version 1.2.1

Period

3

3.6.4 Periodic cryptographic key changes

§ As deemed necessary and recommended by the associated application (for example, re-keying); preferably automatically

§ At least annually

1/year

6

6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods:

§ Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes

§ Installing a web-application firewall in front of public-facing web applications

1/year

9

9.5 Store media back-ups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. Review the location's security at least annually.

1/year

9

9.9.1 Properly maintain inventory logs of all media and conduct media inventories at least annually.

1/year

12

12.1.2 Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment

1/year

12

12.1.3 Includes a [security policy] review at least once a year and updates when the environment changes

1/year

12

12.6.1 Educate employees upon hire at least annually

1/year

12

12.6.2 Require employees to acknowledge at least annually that they have read and understood the company's security policy and procedures.

1/year

X

On-site QSA assessment (Visa L1, Amex L1, MC L1-2, etc) or self-assessment (Visa L2-L4, Amex L2-3, MC L3-4, etc)

1/year

1

1.1.6 Requirement to review firewall and router rule sets at least every six months

1/6 months

11

11.1 Test for the presence of wireless access points by using a wireless analyzer at least quarterly or deploying a wireless IDS/IPS to identify all wireless devices in use

1/quarter

11

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).

1/quarter

11

11.5 Deploy file integrity monitoring software to alert personnel to unauthorized modification of critical system files, configuration files or content files; and configure the software to perform critical file comparisons at least weekly.

1/week

10

10.6 Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS).

1/day

12

12.2 Develop daily operational security procedures that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures).

1/day

A lot of other processes require to "maintain", "ensure", etc - as well as procedures mentioned in item 12.2

As needed

Source: PCI Data Security Standard

Your Easy to Follow To-Do List

What do we learn from the above on how to stay compliant? We can come up with the following lists of periodic tasks:

• Every year

- o Review security of web application
- o Review security policy
- o Perform security awareness training
- o etc

• Every six months

- o Review firewall and router configurations

• Every quarter

- o Perform external and internal vulnerability scanning

• Every week

- o Run integrity checking on critical files

• Every day

- o Review logs from the systems in scope for PCI
- o Perform other daily operational procedures defined in security policy

To conclude, while getting compliant gets more attention, staying compliant is where a lot of mistakes and faults (leading to data breaches) are made. As you are working on PCI DSS compliance related initiatives, make sure that staying compliant is taken just as seriously as getting to that first validation.

ABOUT THE AUTHOR:

Dr. Anton Chuvakin (http://www.chuvakin.org/) is a recognized security expert in the field of log management and PCI DSS compliance. He is an author of books "Security Warrior" and "PCI Compliance" (second edition coming in November 2009!) and a contributor to "Know Your Enemy II", "Information Security Management Handbook" and others. Anton has published dozens of papers on log management, correlation, data analysis, PCI DSS, security management (see list http://www.info-secure.org/) . His blog http://www.securitywarrior.org/ is one of the most popular in the industry.

In addition, Anton teaches classes and presents at many security conferences across the world; he recently addressed audiences in United States, UK, Singapore, Spain, Russia and other countries. He works on emerging security standards and serves on the advisory boards of several security start-ups.

Currently, Anton is developing his security consulting practice, focusing on logging and PCI DSS compliance for security vendors and Fortune 500 organizations. Dr. Anton Chuvakin was formerly a Director of PCI Compliance Solutions at Qualys. Previously, Anton worked at LogLogic as a Chief Logging Evangelist, tasked with educating the world about the importance of logging for security, compliance and operations. Before LogLogic, Anton was employed by a security vendor in a strategic product management role. Anton earned his Ph.D. degree from Stony Brook University.