August 16, 2016

PCI DSS Version 3.2 is Here!

RISK ADVISORY/INTERNAL AUDIT
BY SCHNEIDER DOWNS PROFESSIONAL

The latest version of the Payment Card Industry Data Security Standard (PCI DSS) – version 3.2 – was released earlier this year, and it includes some fairly significant changes. This latest version comes outside of the normal cycle, as the PCI Security Standards Council (PCI SSC) typically releases new versions in the fourth quarter each year. According to an interview with Troy Leach, Chief Technology Officer for PCI SSC, he does not expect another version to be released later this year.[i] From a compliance standpoint, the new requirements introduced in version 3.2 will be considered best practices until January 31, 2018, after which (starting February 1, 2018) they will be effective as requirements. However, if you start planning now, and can get these changes in place earlier, it will improve your payment card security and keep you ahead of the compliance curve.

The summary of changes, as well as the entire PCI DSS can be found on the PCI SSC website at https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss. Below is a summary of the key changes in PCI DSS version 3.2.

1. **Change in timing to upgrade from SSL and early TLS.**

For those of you already wondering what SSL and TLS are, I'll give you a quick overview. Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are encryption protocols used primarily in web browser-based transactions. Both are commonly used on websites that have addresses starting with "HTTPS" (instead of "HTTP"). SSL has been in use for over 20 years, which is an eternity in the IT world! Essentially, SSL and TLS encrypt (or "scramble") the signal being sent between two endpoints, such as a customer's web browser and a web server, to provide security over the data as it makes its way across the internet.

PCI SSC has determined that that all versions of SSL (v1.0, 2.0, and 3.0), as well the earliest version of TLS (v1.0), no longer meet minimum security standards because of vulnerabilities that do not have fixes available. To remain in compliance, organizations must upgrade to TLS v1.1 at a minimum, although PCI SSC states that "entities are strongly encouraged to consider TLS v1.2." This implies that a future version of PCI DSS will likely require TLS v1.2, so it would be a good idea to upgrade to that version now if possible. The PCI SSC originally announced this requirement as part of PCI DSS version 3.1 with a deadline of June 30, 2016. However, PCI DSS version 3.2 has given organizations a bit of a break, moving the deadline for compliance out to February 1, 2018.

What does this mean for you? If you are collecting or transmitting cardholder data (e.g., credit card numbers, expiration dates, verification codes) via a web-based

application, you should make sure that the website is using TLS v1.1 at a minimum, preferably v1.2. If you outsource your website, shopping cart, or other payment transaction functions to a third party, you should ensure that your service provider is in compliance with the standards. There are limited cases where an earlier version of SSL/TLS may still be used, but you must have a formal Risk Mitigation and Migration Plan in place to address the risks.

2. Multi-factor Authentication for Administrative Access.

Another change with version 3.2 is that "non-console" administrative access to systems within the cardholder data environment (CDE) now requires multi-factor authentication, as well as **any** remote access to the CDE from outside the environment. Let's break this down into the key terms of this requirement:

The cardholder data environment (CDE) includes the people, processes and technology that store, process, or transmit cardholder data or sensitive authentication data for credit card transactions. For purposes of this requirement, think of the CDE as any servers, routers, switches, or storage devices that store, process, or transmit such data.

Non-console access occurs when someone logs in to a system component over a network interface (e.g., Remote Desktop connection) rather than on the physical server itself (via mouse and/or keyboard connected directly to the server). Non-console access includes access from within local/internal networks as well as access from external, or remote, networks. In other words, this access can originate from either inside or outside the firewall.

Multi-factor authentication is the use of two or more independent methods of verifying access (i.e., factors) for an individual. These factors include something you **have** (e.g., smart card or token), something you **know** (e.g., password, passphrase, or PIN), or something that represents who you **are** (e.g., fingerprint, palm scan, or retina scan). In order for it to count as multi-factor authentication, it has to include two *factors*. In other words, having two passwords (or a password and a PIN) is **not** multi-factor authentication. Additionally, the National Institute of Standards and Technology (NIST) recently announced that receiving a PIN/code via SMS message (i.e., text message) is no longer considered secure, because recent vulnerabilities may allow an attacker to intercept the text message. PCI SSC has not yet ruled-out SMS messages as an acceptable authentication method, but stay tuned.

Remote access occurs whenever an individual accesses data within the CDE from an endpoint that is outside the CDE (i.e., outside the firewall). For most organizations, this equates to Virtual Private Network (or VPN) access to the network. If you allow such access from outside the network, and users have the ability to touch cardholder data this way – even if they are not administrators, you are required to use multi-factor authentication.

What does this mean for you? Take a look at how your users and administrators access servers within the CDE. If any of your users have VPN access and can access the CDE remotely, even with read-only access, the multi-factor authentication requirement applies to their access. If your administrators can access a server within the CDE through any remote administration tools, Secure Shell (SSH), or Remote Desktop

Protocol (RDP) – and almost all of them can, this requirement also applies.

3. **Changes to Penetration Testing Requirements.**

One of the keys to successful PCI compliance is segmentation of your network. Through segmentation, you are able to significantly limit the scope of your network that is considered to be the CDE. Without proper segmentation, your entire network can essentially become your CDE.

Previous versions of the PCI DSS already required organizations to conduct quarterly penetration tests of the network as a whole. However, under version 3.2, penetration tests must also be conducted against the segmented CDE every six months, to validate security around the segmentation.

What does this mean for you? Hopefully you have already segmented your network to limit the scope of PCI compliance as much as possible, and you're already conducting routine penetration tests against your network. If this is the case, all you need to do to meet the additional penetration testing requirements is add the firewalls/devices protecting the PCI segment(s) into your recurring penetration testing plans, and resolve any issues noted during the testing.

Contact us if you have questions about the latest version of the Payment Card Industry Data Security Standard and visit our Risk Advisory Services webpage to learn more about other services that we offer.

---

[1] PCI SSC Blog, Preparing for PCI DSS 3.2: What to Expect in 2016, February 17, 2016

You've heard our thoughts... We'd like to hear yours

The Schneider Downs Our Thoughts On blog exists to create a dialogue on issues that are important to organizations and individuals. While we enjoy sharing our ideas and insights, we're especially interested in what you may have to say. If you have a question or a comment about this article – or any article from the Our Thoughts On blog – we hope you'll share it with us. After all, a dialogue is an exchange of ideas, and we'd like to hear from you. Email us at contactSD@schneiderdowns.com.