PCI SSC Releases Version 3.1 of Data Security Standard

On April 15, 2015, the Payment Card Industry Security Standards Council (the "PCI SSC" or "Council") released a new version of its Data Security Standard ("PCI DSS"), version 3.1, which contains numerous updates including, most significantly, a shift away from the use of the Secure Sockets Layer ("SSL") and early Transport Layer Security ("TLS") encryption protocols. Coming only three and a half months after most provisions of PCI DSS version 3.0 became mandatory, this newest version is an unusually quick follow-up for the Council. The release will require organizations to respond quickly to meet compliance requirements and avoid potential fines and other liabilities. Version 3.1 is available on the PCI SSC website here.

The PCI DSS is prepared by the PCI SSC, an organization originally formed by the major card brands, and, according to the brands, is intended to provide technical and operational requirements for all entities that store, process or transmit cardholder data. Many merchants and other entities subject to the PCI DSS have a contractual obligation to annually demonstrate compliance with the Standard's numerous requirements. Non-compliance with such requirements could result in potential liability, including the assertion of claims by the payment card brands for fines and assessments.

Under PCI DSS 3.1, SSL and early versions of TLS are no longer considered "strong cryptography." The change is described as being made in response to recent concerns that SSL and early TLS contain vulnerabilities, including what is referred to as the Padding Oracle On Downgraded Legacy Encryption ("POODLE") vulnerability. The National Institute of Standards and Technology ("NIST") similarly does not approve SSL for use in the protection of federal information due to concerns that there are weaknesses in the protocol.

As set out in revised Requirements 2.2.3, 2.3, and 4.1, "new implementations" may not use SSL or early TLS to satisfy PCI DSS requirements. In addition to the issuance of PCI DSS version 3.1, the Council has also published an Information Supplement titled "Migrating from SSL and Early TLS" that describes "new implementations" as those that "have no existing dependency on the use of the vulnerable protocols." The Information Supplement is available here. Examples of new implementations include: (1) installing a system into an environment that currently uses only protocols the Council considers secure; (2) installing an application onto a system that currently uses only protocols the Council considers secure; and (3) building a new system or network to communicate with other systems/networks that support protocols the Council considers secure. The Council recommends phasing out existing implementations of SSL and early TLS immediately. Under PCI DSS 3.1, such protocols cannot be used as a security control to satisfy PCI DSS requirements even for existing implementations after June 30, 2016. Point of Sale ("POS") Point of Interaction ("POI") terminals and termination points connected to them may continue using SSL and early TLS after June 30, 2016 if it can be verified that they are not susceptible to any known exploits for SSL and early TLS.

Under PCI DSS 3.1, protocols that are still considered "strong cryptography" include IPSEC, SSH, and some versions of TLS. In the Information Supplement, the Council states that entities using TLS must use TLS version 1.1 at a minimum, although version 1.2 is strongly encouraged. Additionally, not all implementations of TLS version 1.1 are considered secure by the Council. The Council refers to NIST SP 800-52 rev 1 for further guidance on secure TLS configurations.

Prior to June 30, 2016, if a company continues to use SSL or early TLS on existing implementations, the revised requirements provide that the company must put in place a risk mitigation and migration plan, which will require substantial organizational efforts. According to the Information Supplement, such plans should identify, among

ATTORNEY ADVERTISING

other things, the type of environment where the protocols are used, including the type of payment channel and functions for which the protocols are used, the number and type of systems using or supporting the protocols, risks to the organization's information security environment due to the use of SSL or early TLS as well as controls that will address such risks, and the process in place to monitor for new vulnerabilities associated with the protocols. The plans must require full migration to updated encryption protocols by June 30, 2016.

In addition to the changes made regarding SSL and early TLS, PCI DSS 3.1 contains several changes that the Council characterizes as "clarifications" or "additional guidance" that could potentially impact your organization. Some involve new testing procedures, while others modify the requirements themselves. Some notable changes include:

- In Requirement 3.4, which relates to rendering PAN unreadable where stored, a testing procedure is added that addresses whether hashed and truncated versions of the same payment account number ("PAN"), if both are present in the environment, can be correlated to reconstruct the original PAN;
- In Requirement 6.6, which relates to public facing web applications, the testing procedure previously providing that the assessor should verify that certain automated technical solutions are configured "to either block web-based attacks, or generate an alert" has been revised to read "to either block web-based attacks or generate an alert that is immediately investigated" (emphasis added);
- In Requirement 10.6.1, which relates to daily log review, the phrase "or that could impact the security of CHD and/or SAD" is removed from the description of system component logs covered by the requirement; and
- In Requirement 11.5, which relates to the deployment of change detection mechanisms to alert personnel to unauthorized modification of certain files, the word "modification" is now followed by the parenthetical "(including changes, additions and deletions)".

The Council has released a high level summary of the changes from version 3.0 to version 3.1 here. However, the language changes in version 3.1 itself should be carefully reviewed to determine the potential impact on your organization.

Because PCI DSS 3.1 purports to be effective immediately (although PCI DSS version 3.0 will not be retired until June 30, 2015), it is important that your organization move quickly to evaluate its potential impact. As discussed, credit card brands may try to assert claims for fines and other assessments in the event of a failure to comply with applicable PCI DSS requirements.

For more information regarding Version 3.1 of Data Security Standard or to discuss data security practices generally, please feel free to contact Jim DeGraw, Seth Harrington, David McIntosh, Doug Meal, Mark Szpak, Michelle Visser or David Cohen, or another a member of Ropes & Gray's leading privacy & data security team.

James S. DeGraw
Seth C. Harrington
David McIntosh
Douglas H. Meal
Mark P. Szpak
Michelle Visser
David T. Cohen

ropesgray.com

This alert should not be construed as legal advice or a legal opinion on any specific facts or circumstances. This alert is not intended to create, and receipt of it does not constitute, a lawyer-client relationship. The contents are intended for general informational purposes only, and you are urged to consult your attorney concerning any particular situation and any specific legal question you may have. © 2015 Ropes & Gray LLP

ATTORNEY ADVERTISING