ROPES & GRAY

ALERT

Privacy & Data Security

May 5, 2016

PCI SSC Releases Version 3.2 of Data Security Standard

Subhead

On April 28, 2016, the Payment Card Industry Security Standards Council (the "PCI SSC" or "Council") released a new version of its Data Security Standard ("PCI DSS"), version 3.2. Significantly, the updated standard requires multi-factor authentication for all access to the cardholder data environment ("CDE") using administrative accounts, whether or not the access is remote. Other key changes in the updated standard include new requirements on service providers, revised sunset dates for the use of Secure Sockets Layer ("SSL") and early Transport Layer Security ("TLS") for encrypted data transmission, and the integration of the council's Designated Entities Supplemental Validation ("DESV"), which had previously been a separate document, into the PCI DSS itself. Version 3.2 as a whole becomes effective as of October 31, 2016, although certain new requirements will not come into effect until February 1, 2018.

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.

Attorneys

Heather Egan Sussman
Douglas H. Meal
James S. DeGraw
Rohan Massey
Seth C. Harrington
David M. McIntosh
Mark P. Szpak
Michelle Visser
Paul D. Rubin
Marc P. Berger
Laura G. Hoey
David T. Cohen
Kevin J. Angle
Matthew Coleman

As set out in new Requirement 8.3.1, the new standard requires that all non-console access from accounts with administrative access into the CDE must employ multi-factor authentication, including for access from trusted networks. Previously, multi-factor authentication had only been required for "remote" access, i.e. access from outside a company's trusted network. The new requirement for multi-factor authentication becomes effective as of February 1, 2018. Organizations required to comply with PCI DSS must still require multi-factor authentication for all accounts accessing the CDE remotely.

Version 3.2 also imposes new requirements on service providers ("Service Providers"). Service Providers are defined as business entities, other than the payment brands, "directly involved in the processing, storage, or transmission of cardholder data on behalf of another entity," including companies that "provide services that control or could impact the security of cardholder data" (emphasis added). Under the new standard, Service Providers must, among other things:

1. maintain a documented description of any cryptographic architecture used to protect stored cardholder data, Requirement 3.5.1;
2. implement a process to detect and report on failures of critical security control systems, Requirement 10.8;

3. perform penetration testing on segmentation controls at least every six months and after any changes to segmentation controls or methods, Requirement 11.3.4.1;
4. involve executive management[1] in establishing responsibility for the protection of cardholder data and PCI DSS compliance, Requirement 12.4.1; and
5. confirm quarterly that personnel are following security policies and operational procedures, including daily log reviews, firewall rule-set reviews, applying configuration standards to new systems, responding to security alerts, and complying with change management processes, Requirement 12.11.

As with Requirement 8.3.1, these new requirements will not come into effect until February 1, 2018.

Under the new Appendix A2, SSL and early TLS will no longer be accepted as valid encryption protocols for new security implementations used to protect cardholder data and/or the CDE. Entities that have existing security implementations using SSL or early TLS will have to update to a secure encryption protocol by June 30, 2018 in order to remain in compliance. Service Providers, however, must provide a secure service offering by June 30, 2016. Prior to June 30, 2018, entities utilizing an existing implementation of SSL or early TLS must have a formal risk mitigation and migration plan in place. Point-of-sale/point of interaction terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits for SSL and early TLS may continue using these protocols as a security control after June 30, 2018.

Finally, Appendix A3 integrates the DESV, which had previously been a separate document, into the PCI DSS itself. The DESV outlines a series of additional requirements applying only to certain entities designated by a payment brand or acquirer as requiring additional validation of their PCI DSS compliance.

The Council has released a high level summary of the changes from version 3.1 to version 3.2 here. However, the language changes in version 3.2 itself should be carefully reviewed to determine the potential impact on your organization.

For more information regarding version 3.2 of the PCI DSS or to discuss data security practices generally, please feel free to contact Heather Sussman, Doug Meal, Jim DeGraw, Rohan Massey, Seth Harrington, David McIntosh, Mark Szpak, Michelle Visser, Paul Rubin, Marc Berger, Laura Hoey, David Cohen, or another member of Ropes & Gray’s leading privacy & data security team.

[1] In associated guidance, executive management is defined as including “C-level positions, board of directors, or equivalent.”

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.