Security Standards Council

Payment Card Industry
Security Standards Council, LLC

401 Edgewater Place, Suite 600
Wakefield, MA 01880
Phone: 781 876 8855

Media Contacts

Lindsay Goodspeed
PCI Security Standards Council
+1-781-258-5843
press@pcisecuritystandards.org
Twitter @PCISSC

PCI SECURITY STANDARDS COUNCIL ISSUES MULTI-FACTOR AUTHENTICATION GUIDANCE

— New Resource For Payment Industry To Improve Understanding And Implementation Of Critical Security Method For Access Control —

WAKEFIELD, Mass., 9 February 2017 — Attackers continue to compromise valid credentials to access company networks and steal data. To help organizations combat this growing threat, the PCI Security Standards Council (PCI SSC) has issued guidance on the proper use of multi-factor authentication for preventing unauthorized access to computers and systems that process payment transactions.

Multi-factor authentication (MFA) is widely used across industries as a security best practice to authorize access to a network or system. In addition to identification credentials (such as a unique username), the method requires an individual to present a minimum of two separate forms of authentication credentials, such as a password plus a one-time passcode, before access is granted.

The PCI Data Security Standard (PCI DSS) has always required MFA for remote access (originating from outside a company's network). Effective 1 February 2018, MFA will also be required for administrative personnel with non-console access (administered or managed over a network) to computers and systems handling cardholder data (the cardholder data environment).

“Multi-factor authentication prevents use of a password alone to verify a user, thereby providing assurance that users are who they claim to be. As with any security control, however, it is only as good as its implementation,” said PCI SSC Chief Technology Officer Troy Leach. “This guidance will help organizations using, evaluating or upgrading an MFA solution understand how to implement it properly and securely.”

The Multi-Factor Authentication Information Supplement provides industry-accepted principles and best practices for implementing MFA securely. It also includes considerations for common implementation scenarios.

“As criminals continue to target valid credentials, authenticating the user, the payment transaction and the integrity of the payment instrument will become increasingly important to protect. The security principles in this document provide guidance to ensure payments and supporting technology are being used as intended and provide a roadmap for future security considerations,” said PCI SSC General Manager Stephen W. Orfei.

View PCI Perspectives blog post “Understanding New PCI Guidance on MFA” to learn more about this new resource.

To download the guidance, visit: https://www.pcisecuritystandards.org/pdfs/Multi-Factor-Authentication-Guidance-v1.pdf

About the PCI Security Standards Council

The PCI Security Standards Council is a global forum that is responsible for the development, management, education, and awareness of the PCI Data Security Standard (PCI DSS) and other standards that increase payment data security. Connect with the PCI Council on LinkedIn. Join the conversation on Twitter @PCISSC. Subscribe to the PCI Perspectives Blog.

###