DRAFT- NOT FOR EXTERNAL RELEASE

Media Contacts

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

Payment Card Industry
Security Standards Council, LLC

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

PCI SECURITY STANDARDS COUNCIL PUBLISHES SUPPLEMENTAL PCI DSS SCOPING GUIDANCE

— Guidance Clarifies Scoping Principles Outlined in the PCI Data Security Standard —

WAKEFIELD, Mass., 9 December 2016 — Incorrectly identifying where and how payment data is at risk in an organization's systems continues to lead to data breaches. Today, the PCI Security Standards Council (PCI SSC) published *Guidance for PCI DSS Scoping and Network Segmentation* to help businesses address this challenge.

PCI Data Security Standard (PCI DSS) Requirement 1.1 states that organizations need to maintain a cardholder flow diagram to help identify which systems are in scope and need protection. Yet data breach investigation reports continue to find that companies suffering compromises were unaware that cardholder data was present on their compromised systems. This guidance provides a method to help organizations identify systems that, at a minimum, need to be included in scope for PCI DSS. It includes guidance on how segmentation can be used to help reduce the number of systems that require PCI DSS controls and illustrative examples of some common segmentation approaches.

"For years, we have preached the need to simplify and minimize the footprint of cardholder data," says PCI SSC Chief Technology Officer Troy Leach. "One way to accomplish this is through good segmentation. It allows an organization to focus their attention on a limited number of assets and more readily address security issues as they arise. As a result, it should also reduce the level of effort to comply with PCI DSS."

While segmentation is not a PCI DSS requirement, it is a strongly recommended practice. Segmentation of networks included in or connected to the cardholder data environment is important for organizations as it can limit the exposure of payment data in a system, can simplify PCI DSS compliance efforts and can reduce the chance of being targeted by a criminal. However, as improper segmentation can put cardholder data at risk, it's critical that organizations understand and implement segmentation properly.

The guidance was developed with industry input and collaboration in order to address common questions from PCI SSC stakeholders on scoping and segmentation.

Christian Janoff, PCI SSC Board of Advisor member and Security Solutions Architect for Cisco, works regularly with merchants using scoping and segmentation products and was a leading contributor to the guidance. "Knowing the scope of your cardholder data environment and properly segmenting to protect it has been a challenge for many organizations. By providing guidance, we hope this will help to simplify the process, making it easier to secure payment card data," he said. "We at Cisco are proud to partner with the Council and industry peers to bring additional scoping and segmentation guidance to the industry."

Guidance for PCI DSS Scoping and Network Segmentation is intended for organizations looking to understand scoping and segmentation principles when applying PCI DSS to their environments. It also provides a method for facilitating effective scoping discussions between entities, and is useful for:

- Merchants, acquirers, issuers, service providers (issuer processors, token service providers, and others) responsible for meeting PCI DSS requirements for their enterprises;
- Assessors responsible for performing PCI DSS assessments;
- Acquirers evaluating merchants' or service providers' PCI DSS compliance documentation;
- PCI Forensic Investigators (PFIs) responsible for determining PCI DSS scope as part of an investigation.

It is important to note each organization is responsible for making its own scoping decisions and that following this guidance does not guarantee that effective segmentation has been implemented, nor does

it guarantee compliance with PCI DSS. The guidance is available in the Council's document library [LINK TBD]. Chief Technology Officer Troy Leach provides additional insights on the topic on the PCI Perspectives blog.

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.

###