The new PCI DSS version 2 is effective. What now?

Released on: January 24, 2011, 08:02 am
Author: QueryCLick LTD
Industry: Computers

The PCI Security Standards Council (PCI SSC) is a global, open industry standards body providing management of the Payment Card Industry Data Security Standard (PCI DSS), PIN Transaction Security (PTS) requirements and the Payment Application Data Security Standard (PA-DSS). The PCI SCC has released the new version 2 of its PCI Data Security Standard (PCI DSS) which has become effective on 1st January 2011.

The new standard begins the three year lifecycle that allows for validation against the previous version of the standard (1.2.1) until 31st December 2011. This provides stakeholders time to understand and implement the new version of the standard as well as provide feedback. The PCI SCC encourages organizations to transition to the updated version as soon as possible.

The changes in version 2.0 introduce no new major requirements. The majority of changes are modifications to the language to clarify the meaning of the requirements and make understanding and adoption easier. Many of the revisions reinforce the need for a thorough scoping exercise prior to assessment in order to: understand where cardholder data resides; reduce the infrastructure and applications subject to the standard; allow organizations to adopt a risk-based approach when assessing; prioritizing vulnerabilities based on specific business circumstances;

commissum’s Principal Assurance Consultant André Coner commented that many organisations fail to adequately segment the cardholder data environment from the remainder of it’s network and therefore are significantly increasing the complexity and cost of their PCI DSS compliance. Because, without adequate network segmentation the entire network is in scope of the PCI DSS assessment. Segmentation is therefore strongly recommended as it will reduce the scope and cost of the PCI DSS assessment. It also reduces the cost and difficulty of implementing and maintaining the PCI DSS controls.

The commissum information security managed services, provides services for PCI DSS
Requirement 11: “Regular test security systems and processes” which include:
Quarterly security scanning.
Penetration testing: network and application.
Host configuration reviews of firewalls and network infrastructure.
Web Application Security Assessment (WASA).
Wireless Security Assessments.
Securing the software development lifecycle.
Code review.
Recommendation of compensating controls.

About commissum
With 20 years of experience, commissum is adept at offering practical advice and recommending cost-effective solutions, to deliver a joined-up, coherent approach to protecting an organisation's information assets.

Contact Details: Quay House,
142 Commercial Street,
Leith,
Edinburgh,
EH6 6LB,
Scotland,
United Kingdom

t: 0845 644 3217

f: 0845 644 3218

~~~~~

Press release distributed via EPR Network (http://express-press-release.net/submit-press-release.php)
~~~~~