Out-Law.com
Legal news and guidance from Pinsent Masons

Payment card data security rules presenting a challenge to management of 'firewalls', says IT security specialist

Meeting the requirements of a global standard on payment card data security is putting pressure on IT teams and may be preventing them from protecting businesses' commercially sensitive information and customer data, an IT security expert has said.

11 Mar 2015

Online businesses handling payment card details must do so in a way that corresponds with the Payment Card Industry Data Security Standard (PCI DSS). Jody Brazil of FireMon told Out-Law.com, however, that many IT professionals believe the PCI DSS regime's requirements on 'firewall' management are counterproductive.

Firewalls are network security systems used to control the flow of information to and from an internal network and within that network.

"For many years, practitioners have complained that PCI DSS commands so much time and attention that it actually detracts from their ability to improve overall management of network security," Brazil said.

The problem lies in the fact that the PCI DSS framework "requires organisations to analyse and document all of their firewall access

http://www.out-law.com/en/articles/2015/march/payment-card-data-security-rules-presenting-a-challenge-to-management-of-firewalls-says-it-security-specialist/

policies on a frequent basis", he said. The PCI DSS framework was updated in 2013, although many of the changes only took

effect earlier this year. Brazil said that the changes mean that compliance, including in relation to firewall policies, is now measured on a more "continuous" basis, presenting a resourcing issue for online retailers.

"While some experts and the PCI Council maintain that this advancement has served to make the standard more practical and effective, many others have argued that it has only made compliance more difficult," Brazil said.

"While meant to improve the implementation of firewalls at large, the process of striving to maintain compliance with PCI DSS, including related analysis triggered by every policy change event, has become a significant challenge and drain on already limited security management resources," he said.

Brazil said that "firewall management" is an important tool in preventing unauthorised access to businesses' internal systems and the potential loss of data or service interruption that can result from such an intrusion.

The "proper design and oversight" of network security policies is "the most significant challenge of implementing and managing firewall technologies", he said.

"As organisations advance their network access requirements, such as to launch new applications meant to increase the speed and efficiency of their operations, they must determine the safest manner to create new connections into and out of their environments," Brazil said. "This sounds straightforward, but

http://www.out-law.com/en/articles/2015/march/payment-card-data-security-rules-presenting-a-challenge-to-management-of-firewalls-says-it-security-specialist/

most often a single firewall policy is constructed from hundreds of underlying rules that serve to dictate access controls, creating a tremendous degree of related complexity."

"As a result, the process of safely changing access, and ensuring that network defences are always properly aligned, becomes even more difficult over time. One of the most significant issues today is the overwhelming amount of undocumented, out-of-date and overly permissive access that results from long-term operation of firewall systems, creating a lack of visibility into the real-world alignment of controls and the opportunity for unseen gaps in defence," he said.

http://www.out-law.com/en/articles/2015/march/payment-card-data-security-rules-presenting-a-challenge-to-management-of-firewalls-says-it-security-specialist/