Web Browsers: Your Weak Link in Achieving PCI Compliance

Critical Security Gaps in Web Browsers Create Significant Risks

Does your company process credit card information via a browser? Data loss from theft or leaks, malware and Man-in-the-Browser attacks—all of the risks involved in delivering information through web browsers has led to the development of a wide range of security policies to achieve PCI compliance. Even if you believe your organisation is compliant, critical security gaps remain in the current standard technologies used to meet the requirements.

Gaps in Your Encryption

PCI Requirement 3 mandates organisations must protect stored cardholder data. Encryption is the preferred and most widely used technology for this requirement. However, if you're using a web-based processing or payment application, any credit card processing conducted in the web browser leaves the data at risk. All the encrypted data is unencrypted when it's rendered in the browser on the endpoint and in use. Data can remain in the web browser cache in clear text format, where it can be easily extracted by either malware or end users. Even simple, everyday tasks such as cut, copy, paste and screen capture put sensitive data in the system-wide clipboard, which is also rendered in clear text format and easily accessible, even after the web session has ended. In addition, stored user names and passwords from browser sessions remain available in the authentication cache and vulnerable to malware.

Does Your Antivirus Prevent Malware Infections or Zeus Attacks?

Endpoint security and antivirus effectiveness are an on-going debate; however, the use of and regular updates of antivirus software or internet security programs to prevent malware infections are still a PCI requirement. In their 2011 Banking Security Test, MRG Effitas reported that of 27 Internet Security products tested on Windows 32-bit and Windows 64-bit computers, only a handful were effective in preventing the Zeus botnet. Their report went on to conclude that, based on evidence from their research, users need to employ additional security measures on top of traditional anti-virus or internet security suites to counter threats posed by modern malware. The use of compensating controls to increase protection levels should include securing the browser session even when malware is present.

While keeping antivirus maintained and updated sounds simple, the Verizon 2011 PCI industry compliance report states that only 64% of companies they tested for PCI compliance achieved this in 2010. It's also interesting to note that of the breach incidents Verizon investigated, only 47% of those companies had complied with this requirement. Browser security that is delivered as part of the application will ensure the latest controls are always up to date and turned on as a mandatory part of the application.

Challenges to Your Web Application Security

The shift to web applications and cloud services has also created additional PCI compliance challenges. Requirement 6 states that organisations must develop and maintain secure systems and applications. Demonstrating security controls built in your own in house applications can be challenging—many are legacy systems in which comprehensive security controls likely don't exist. Many organisations are also using web-based payment applications supplied by their bank to process transactions, leaving them no control over critical security updates and patches.

Building security into the application can be impractical, expensive or simply not possible. However, it is possible to build security into the browser session, something you do have control over. Making the browser secure from local malware threats protects data from keyloggers, screen scraping and cache raiders. Encrypting and deleting data written from the browser to the local cache, preventing the cut, copy, paste, print and screen capture features and delivering this secure web browser protection as part of the application closes many of the current security gaps in meeting PCI requirements.

> ***"Quarri Protect On Q (POQ) helps clients achieve and maintain PCI compliance by addressing a variety PCI issues, including data encryption and application security, that have historically been difficult to solve. With its on demand deployment, POQ also acts as a compensating control for endpoints that don't have the latest security updates installed. And its data theft protections also ensure organisations can prevent replication of confidential data by careless or malicious end users."***
>
> **Andy Dalrymple**
> **PCI QSA**
> **PTP Consulting**

Closing Web Browser Gaps in PCI Compliance

Quarri Technologies, Inc. is a security software company that empowers organizations to keep their sensitive data secure.

Quarri Protect On Q (POQ) enables organisations to control and protect browser session content from theft or data leakage by malware and end users, both careless and malicious. POQ provides zero-hour malware defense against keylogging, framegrabbing, cache mining and other attacks that may be introduced through a user's web browser, even from malware embedded on compromised client computers. As it's not signature-based, it offers a much higher level of compensating controls than standard antivirus software. POQ is delivered on demand as part of the application browser, with no client installation. All browser session data is encrypted and digitally shredded when the session ends. In addition, central log files of all user activity enable compliance with PCI auditing requirements.

POQ also helps organizations mitigate risk by providing data leakage protection that controls the user's ability to replicate confidential data. POQ blocks users from copying, printing, screen-capturing or saving sensitive web information, including from browser-launched processes like Adobe Acrobat and Microsoft Office.

© 2011 Quarri Technologies, Inc.