HOSTED PAYMENT PAGES

Joshua Knopp, CISSP MasterCard Worldwide

Merchants have many options to consider when evaluating how to best comply with the Payment Card Industry Data Security Standard (PCI DSS) requirements. One option that is becoming increasingly popular, especially among smaller merchants, is using hosted payment pages. Merchants use these hosted payment pages with the goal of reducing or removing their environments from scope of some PCI DSS requirements.

BACKGROUND

Web-based payment applications that allow a cardholder to enter payment card information to complete an online checkout process are commonly referred to as a payment page. When these payment pages are outsourced, or hosted, a merchant is then relying on a third-party service provider to securely manage the application, accept the cardholder data, and authorize the transaction. For example, when the cardholder is ready to checkout when making an online purchase, he or she is redirected from the merchant's own web site and handed off to a service provider's payment page. The cardholder then enters his or her payment card information directly into the service provider's page. Once the service provider authorizes the transaction, the cardholder is sent back to the merchant's web site to receive any final information or to continue shopping. In many cases, this process often is seamless to the cardholder.

Per that scenario, the merchant's web application is no longer transmitting, storing, or processing cardholder data since the cardholder provides that information directly to the service provider via the payment page. While these hosted payment pages may help the merchant in reducing PCI DSS scope, it does not remove the need for a robust information security program to be implemented around the merchant's web environment to mitigate data security vulnerabilities.

Based on the current compromise and attack trends, hosted payment pages may pose the following data compromise security vulnerabilities.

REG RISK: MAN-IN-THE-MIDDLE (MITM) AND REDIRECTION ATTACKS

A MITM attack occurs when an unauthorized party is able to insert itself between the origin and destination of a communication channel. In respect to hosted payment pages, attackers are compromising the merchant's web environment causing the cardholder to be re-directed to a malicious site at time of checkout when payment card information is provided to complete a transaction. By using what appears to be a legitimate payment page to the cardholder, the attacker tricks the cardholder into exposing his or her payment card information by either harvesting the data or, acting as a proxy by collecting the data and passing it on to the service providers web site to complete the order. The latter situation is particularly seamless since the cardholder may be able to complete the checkout process without any knowledge that he or she was re-directed through a malicious site.

FRAUD MITIGATION ACTION: STRONG SECURITY CONTROLS & MUTUAL AUTHENTICATION

1) Merchants should employ strong security controls that follow industry best practices on their web-based environment, even if the environment is not in scope of PCI DSS requirements.

   Specifically: Secure Application Development, Regular Vulnerability Scans and Penetration Testing, Robust Patching, Intrusion Detection, Monitoring, and Network Security Controls (such as Firewalls)

   If a merchant's web environment has strong security controls in place, the risk of an attacker successfully compromising the environment can be greatly limited.

2) In some cases, it may be possible to employ Mutual Authentication to prevent redirection attacks. In Mutual Authentication, both ends of the communication channel must trust each other. In common web applications using SSL-based encryption, only the authenticity of the remote server is validated; the source of the connection is not validated. When using Mutual Authentication, the authenticity of both the source and destination must be validated. When applied to this scenario, the merchant's web application would not share data with any entity whose authenticity had not been validated. Likewise, the service provider would not accept information from any source that was not validated as authentic.

PHISHING ATTACKS

Some common malware has begun targeting these types of scenarios by harvesting credentials directly from the cardholder's computer. A high-profile example of this is the Zeus Trojan malware. Also, malware now has the ability to identify when popular service providers are referenced in a merchant's application. When this happens, malware hiding on the cardholder's computer activates and harvests payment card information at time of checkout.

FRAUD MITIGATION ACTION: CONSUMER BASED SECURITY

Unfortunately, in these situations there is often little that can be done besides educating cardholders about proper data security practices. The end user should employ anti-virus software and personal firewalls as well as regular operating system and application patches to minimize the risk presented by new and existing malware.

.

SUMMARY

While a merchant may be able to reduce or remove the scope of its environment's applicability to comply with PCI DSS requirements by using hosted payment pages, it does not remove the merchant's risk of being involved in, or even the source of, an account data compromise event. Merchants still have a duty to employ security controls based on industry best practices to their web based environment to protect payment card data.