New PCI Council Telephone Payment Guidelines supports partial de-scope

What can be done to quickly, efficiently and inexpensively remove desktops, data networks and backend systems from PCI scope for telephone payments?

DataDivider reports

Many merchants having successfully de-scoped their organisations from PCI DSS with P2PE (Point to Point Encryption) for bricks and mortar and tokenisation for e-commerce, have discovered that the Achilles heel of their PCI programme is their MOTO (Mail Order Telephone Order) payments. Suddenly from the simple act of agents and/or back office staff typing sensitive credit card data into their desktops they bring these, and their corporate networks, back into PCI scope. Until recently, options have been limited to address the challenges of telephone, snail mail, fax, email and chat payments. In the shortly to be released new Telephone Payment Guidelines the Council is supporting a partial de-scope strategy for merchants.

Voice payments

For telephone payments, much has been invested by a few merchants in implementing automated payment IVRs (Interactive Voice Response) and DTMF (Dual Tone Multi Frequency) masking solutions. Whilst these solutions, when hosted, can remove merchants from PCI scope, they have proven to be expensive and complex requiring integration into telephony infrastructure and application's architecture. Furthermore, they impact the customer journey, either forcing the customer to use their telephone keypad or converse with often frustrating voice recognition systems. Additionally, these solutions require exception handling (mobile phones whilst roaming with no DTMF tone capability, phones with pulse tone dialling only, disabled callers with no DTMF capability, etc.) which immediately brings everything back into PCI scope. These expensive investments have largely been warranted by the desire to take the telephony infrastructure out of scope, yet there have been less than a handful of telephony infrastructure breaches discovered through PCI forensic audits in the last decade. With PCI forensic audits numbering well over a thousand per annum this represents a small risk. Where the risk really lies is in the cardholder data on desktops, networks and backend systems.

So what can be done to quickly, efficiently and inexpensively remove desktops, data networks and backend systems from PCI scope for telephone payments? An alternative approach to DTMF tone masking is emerging in that of Data Capture Cloaking It is now possible to use hosted PCI Level 1 service providers that provide a SaaS (Software as a Service) security offering that affords merchants the ability for agents and back office staff to capture cardholder data without exposing the data to their local machine i.e. cloaking this data. Whilst this sounds impossible, it is achieved in a highly secure manner. Agents listen to cardholder data from customers (i.e. no change to the customer journey) and rather than typing the cardholder data into their desktops via their keyboard they access a Virtual Keypad running remotely in the PCI certified environment. Using their mouse, agents click on digits within the Virtual Keypad to enter the sensitive cardholder data. Mouse click coordinates cannot be correlated back to PAN (Primary Account Number) digits as the Virtual Keypad randomly places 0 within a circular keypad (like an old rotary dial telephone) and then again randomly rotates the keypad after each cluster of PAN digits. If preferred, digits on a Virtual NumPad can be scrambled for the same desired effect, the local session under which the Virtual Keypad/numPad runs is remotely protected to ensure that no frame images or keylogging is possible. So, even if a hacker got access to the local machine, all they could derive would be mouse click coordinates that would provide zero value.

With the sensitive cardholder data captured within the secure hosted environment this can either be directly processed through a locally hosted Virtual Terminal or can be tokenised and passed back to the merchant. By the PCI hosted service provider acting as a proxy for the Payment Service Provider (PSP) the token can be reversed for the PAN before transmitting to the PSP.

Snail mail, fax, email and chat payments

Working on the same principal it is possible to intercept cardholder data within mail, fax, email and chat and to substitute tokens within such artefacts. Again tokens can be reversed back to PAN data for entry into hosted Virtual Terminals for payment or PSP's API calls can proxy through the hosted environment for PAN substitution.

Summary

It is now possible to easily and inexpensively de-scope MOTO payments from the areas of real risk. Telephony infrastructure, whilst remaining in scope, represents a low risk which can be secured through encryption and isolation at a fraction of the alternative costs. □

For more information, please visit
http://datadivider.com

datadivider