Detecting PCI Upgrades

cyber security technology regulatory

Summary: New Payment Card Industry Data Security Standard requirements will go into effect June 30th. What you should know to stay compliant.

An interesting thing happened along the route of machines taking over the world. It seems an international study published in the Annals of Oncology finds artificial intelligence (AI) detected skin cancer better than dermatologists. Dermatologists accurately identified 86.5% of skin cancers during the testing vs. 95.0% for the machines and AI.

Machines handle a lot for humans in this digital world and that is certainly the case when it comes to credit cards and payments. To protect the flows, the industry is set to again move up its security standards, in hopes of making it more difficult for the bad guys to access payment networks or payment accounts.

Building off of existing mandates, new Payment Card Industry Data Security Standard (PCI-DSS) requirements will go into effect June 30, 2018. Payment card acquirers, processors, gateways and service providers worldwide are now required to discontinue the use of Secure Sockets Layer (SSL) and early versions of Transport Layer Security (TLS) in favor of a more secure encryption protocol, TLS v1.1 or higher.

For the banking and payments industry, requiring the use of these higher encryption protocols is arguably a long-time coming. SSL 3.0 encryption was introduced more than 20Ys ago and the earliest version of TLS emerged almost 30Ys ago. Over the years, both SSL and early TLS protocols have been found to have serious vulnerabilities, which exploits have utilized to compromise networks. According to the National Institute of Standards and Technology (NIST), there are no patches or repairs that can make these older protocols secure.

In this light, it is not surprising that payment processors and banks are being "strongly encouraged" to implement TLS 1.2, which was introduced merely 10Ys ago in 2008.

With the upgrade deadline close at hand, you may be wondering what community banks should do to ensure that they, their processors and their customers are compliant?

Migrate to a minimum of TLS 1.1, and preferably TLS 1.2: It is possible to implement countermeasures against some attacks on TLS 1.1, but migrating to a later version is strongly encouraged. Experts agree that this is the only reliable method to protect against the current protocol vulnerabilities.

Patch TLS software against implementation vulnerabilities: Implementation vulnerabilities, such as Heartbleed in OpenSSL, can pose serious risks, according to the PCI Security Standards Council. Banks, processors and online businesses should keep TLS software up-to-date to ensure it is patched against these vulnerabilities and have countermeasures for other attacks.

Configure TLS securely: In addition to providing support for later versions of TLS, banks and their payment providers must make sure that TLS implementation is configured securely. You need to check that secure TLS cipher suites and key sizes are supported and disable support for other cipher suites that are not necessary for interoperability, per the PCI Security Standards.

Monitor for potential suspicious activity: Banks, online businesses and their processing partners should always be on the lookout to identify unusual increases in requests to revert back to vulnerable protocols. Additionally, payments players should ensure all applicable PCI DSS requirements are also in place. It is also helpful to receive updates about new vulnerabilities.

This may seem pretty technical, but your IT team will know what to do. Check in with them to ensure that you are covered where you need to be and then let the machines do the rest.

HEDGING SERVICES FOR COMMUNITY BANKS

Community bankers seeing long-term fixed rate demand from business clients can transform payments into a floating rate on their books using Borrowers' Loan Protection (BLP). Contact us today for more information.