Case Study: Internal Penetration Test

- *PCI DSS*
- *Holistic Network Penetration Testing*

Subject Organization

Client: A large insurance provider subject to the Payment Card Industry Data Security Standard (PCI DSS).

About SpiderLabs

- SpiderLabs is the advanced security team within Trustwave focused on forensics, ethical hacking, and application security. The team has performed hundreds of forensic investigations, thousands of ethical hacking exercises and hundreds of application security tests globally.

About Trustwave

- Trustwave is the leading provider of on-demand data security and payment card industry compliance management solutions to businesses and organizations throughout the world.

Trustwave®
Information Security & Compliance

CHALLENGE: CRACK A HARDENED PAYMENT CARD ZONE

A national insurance provider had built a network zone to process payment card data in compliance with the Payment Card Industry Data Security Standard (PCI DSS). The insurer was confident that all regulations and best practices had been followed, and that their network was well protected against any kind of attack. As part of their compliance validation with PCI DSS, the insurer asked Trustwave's SpiderLabs to perform an internal penetration test against the network and identify any remaining vulnerabilities. When the test was complete, SpiderLabs's findings would question the security of not only the payment card segment, but of the network infrastructure as a whole.

SOLUTION: TEST WHOLE NETWORKS, NOT JUST MACHINES

SpiderLabs's penetration testing team arrived at the client's offices and was given network privileges equivalent to a restricted access employee. At first glance, the network seemed to be properly secured. Processing and storage of all payment card data occurred in segregated "red zones" consisting of hardened devices with well-secured access points, and all best practices and regulations for data encryption and handling appeared to have been followed. Anyone looking only at the payment card segment would likely be impressed by its security and issue it a clean bill of health.

The team then set aside the payment card segment and began trolling the larger network infrastructure for vulnerabilities. Eventually, this search turned up an old, forgotten server. Further probing revealed that the server's administrator password was blank—a critical mistake. The team accessed the server's account list through the hole and cracked several account passwords. They then found two other machines with the same accounts, and exploited them in the same way. This time, they discovered a single account that allowed access to a number of network machines—including the "red zone" access devices and the payment card servers themselves. The penetration testing team had not only cracked the client's "fully-secured" PCI environment, but broken it wide open.

RESULTS: TRUE LOCKDOWN OF PAYMENT CARD DATA

Starting with only basic privileges, SpiderLabs exploited a single network hole to uncover a fundamental process flaw that put the client's complete payment card data at risk. Following the test, Trustwave delivered a full report of their methods, findings and suggestions. The insurer immediately remediated the vulnerabilities throughout their network and issued new protocols for network administration.

If the penetration team had directed their tests against only a cherry picked list of the insurer's network machines, they never would have found the old server and its associated vulnerabilities. However, Trustwave's SpiderLabs knows it's not rare for a network environment to have one weakness that even an IT professional may not stop to consider. The results clearly illustrate why at Trustwave testing infrastructure means testing whole networks, and not just machines.