CASE STUDY

PCI PIN Security (PCI PIN)

THE COMPANY

Gertec Brasil Ltda.

THE PRACTITIONER

Keren Dantas, Quality Assurance Coordinator

Years at company: 8 years

What does your company do?

Gertec develops and provides equipment and technology solutions for payments, banking and commercial automation in general. The company is present in the main financial institutions and in all retail in Brazil, as well as financial institutions in South America.

What do you do for your company?

My job is to verify that our solutions meets the industry requirements. I act as an internal auditor before submitting PCI PIN Transaction Security (PTS) Point-Of-Interaction (POI) submission and PIN Security assessments for instance. My job is also to ensure that the ongoing operation is compliant helping to enforce compliance with efforts such as trainings, dissemination of updated information and internal audits support.

What procedures has your company put in place to help with PCI PIN security controls?

We developed internal evaluation procedures and framework used periodically to conduct internal audits. The company has also a Security Committee to continuously address PCI PIN Security and other issues.

How has your company effectively managed the implementation of PCI PIN security controls?

The first challenge was balancing security and productivity. We had to understand ways of finding scalable solutions that would comply with security requirements. Usually more automation requires more sophisticated solutions such as asymmetric cryptography and hardening of infrastructure equipment. We observed that experienced assessors can help a lot during this phase. We got some great advice from assessors and other partners that were more experienced with PCI DSS and scoping approaches, for instance.

Even when you manage to automate as much as possible, another great challenge is to keep the development and operation processes ongoing. The PCI PIN Security requirements helped us to understand the importance of having the actual procedures in place and up to date. This is crucial especially when you have personnel change or activities that are hardly performed. Initially Gertec had a smaller technical team and we could rely on the knowledge of key people, but as the company grows, it is imperative that you have strong procedures since everything is more dynamic.

In terms of costs, PCI PIN Security requires the use of an HSM for Key Injection Facilities and one of the challenges was finding a solution that would fit our needs and be cost effective. Usually market solutions are designed for great transactions load and would offer much more features than what we actually needed. Our approach was to take advantage of all the knowledge we have with POI development and build our own HSM solution.

Has your company implemented a key blocks migration plan to adhere to PCI PIN Security Requirement 18-3? How was this implemented?

The implementation of key blocks is a good practice. We had a proprietary solution and we had to adapt to PCI PIN Security requirements. The great challenge was to perform the migration. We performed a lot of planning ahead during this migration and try to predict what other future changes we could expect in the future. For instance, currently we inject keys to equipment in both PCI POI 4.x and PCI POI 5.x versions. A new key check value calculation was introduced in PCI POI 5.x so we designed an interchangeable way to deal with them both. Knowing that in the future we might have future migrations, we also have implemented mechanisms in place that will assist that in the most frictionless way as possible.

A system migration is something that should occur causing as little impact as possible in operation. This was a great challenge, though. We needed a lot of planning and implantation procedures so to create a script of every activity to be performed, all equipment needed and every key person that needed to be on call, so not to be caught unprepared.

Another challenge was to perform all those procedures that are rarely performed once again, such as key creation ceremony. We could observe the importance of having detailed written procedures so we could handle everything properly with the right evidences in place. Simulations and training are also a good recommendation.

Has your organization taken advantage of training offered by the Council? If so, how has the training benefited your company?

We did the Internal Security Assessor (ISA) training before and it was interesting because the whole mindset for PCI DSS and PCI PIN compliance are basically the same. We later participated in Qualified PIN Assessors (QPA) informational training, which was much more precise for the kind of activities we perform.

How do you and your company plan to use the knowledge of PCI PIN Security?

We have to use this knowledge to keep our operations and compliance ongoing by periodical internal audits.

Brazil Regional Engagement Board

Gertec Brasil Ltda is an active member of the Brazil Regional Engagement Board, which represents perspectives of PCI SSC Participating Organizations and PCI SSC constituents in Brazil, advising and providing feedback and guidance to the PCI SSC on standards and programs development and adoption in Brazil.

Payment Card Industry Security Standards Council, LLC
www.pcisecuritystandards.org