ESTUDO DE CASO

PCI PIN Security (PCI PIN)

A EMPRESA

Gertec Brasil Ltda.

O PROFISSIONAL

Keren Dantas, Coordenadora de Quality Assurance

Anos na empresa: 8 anos

O que a sua empresa faz?

A Gertec desenvolve e fornece equipamentos e soluções tecnológicas para pagamentos, automação bancária e comercial em geral. A empresa está presente nas principais instituições financeiras e em todo varejo no Brasil, e em instituições financeiras na América do Sul.

O que você faz pela sua empresa?

Meu trabalho é verificar se nossas soluções atendem aos requisitos da indústria. Atuo como auditora interna antes de enviarmos dispositivos para avaliação no PCI PIN Transaction Security (PTS) Point-Of-Interaction (POI) e avaliações do PCI PIN Security por exemplo. Meu trabalho também é garantir que a operação em andamento está em conformidade, ajudando a manter o cumprimento com esforços como treinamentos, divulgação de informações atualizadas e suporte a auditorias internas.

Quais procedimentos sua empresa implementou para ajudar na segurança dos controles do PCI PIN Security?

Desenvolvemos procedimentos e estruturas de avaliação interna usados periodicamente para realizar auditorias internas. A empresa também possui um Comitê de Segurança para continuamente abordar o PCI PIN Security e outros problemas.

Como sua empresa gerenciou efetivamente a implementação dos controles de segurança do PCI PIN Security?

O primeiro desafio foi equilibrar segurança e produtividade. Nós tivemos que entender maneiras de encontrar soluções escaláveis que atenderiam aos requisitos de segurança. Geralmente, mais automação requer soluções mais sofisticadas, como sistemas de criptografia assimétrica e configuração segura de equipamentos de infraestrutura. Observamos que assessores experientes podem ajudar muito nessa fase. Recebemos ótimos conselhos de assessores e outros parceiros com mais experiência com o PCI DSS e abordagens de escopo, por exemplo.

Mesmo quando você consegue automatizar o máximo possível, outro grande desafio é manter os processos de desenvolvimento e operação em andamento. Os requisitos de segurança do PCI PIN Security nos ajudaram a entender a importância de ter os atuais procedimentos em vigor e atualizados. Isso é crucial, especialmente quando você tem mudança de funcionários ou atividades que dificilmente são executadas. Inicialmente, a Gertec possuía uma equipe técnica menor e poderíamos confiar no conhecimento de pessoas chave, mas à medida que a empresa cresce, é imperativo que você tenha procedimentos fortes, pois tudo é mais dinâmico.

Em termos de custos, o PCI PIN Security exige o uso de um HSM em instalações para injeção de chaves e um dos desafios foi encontrar uma solução que atendesse às nossas necessidades e ser rentável. Normalmente, as soluções de mercado são projetadas para grandes transações e ofereceria muito mais recursos do que realmente precisamos. Nossa abordagem foi tirar proveito de todo o conhecimento que temos com o desenvolvimento de POI e construir nossa própria solução de HSM.

Sua empresa implementou um plano de migração para blocos de chaves para aderir ao Requisito 18-3 do PCI PIN Security? Como isso foi implementado?

A implementação de blocos de chave é uma boa prática. Tinhamos uma solução proprietária e tivemos que nos adaptar aos requisitos de segurança do PCI PIN Security. O grande desafio foi executar a migração. Realizamos muitos planejamentos antecipados durante essa migração e tentamos prever quais outras mudanças futuras poderíamos esperar no futuro. Por exemplo, atualmente injetamos chaves em equipamentos versões PCI POI 4.x e PCI POI 5.x. Um novo cálculo do valor de verificação de chave foi introduzido no PCI POI 5.x, então criamos uma maneira intercambiável de lidar com os dois. Sabendo que poderemos ter migrações futuras, também implementamos mecanismos que nos ajudará da maneira mais fácil possível.

Uma migração do sistema é algo que deve ocorrer causando o menor impacto possível na operação. No entando, este foi um grande desafio. Precisávamos de muito planejamento e procedimentos de implantação para criar um script de todas as atividades a serem executadas, todos equipamentos necessários e todas as pessoas-chave que precisavam estar de plantão, para não sermos pegos despreparados.

Outro desafio foi realizar todos os procedimentos que raramente são realizados novamente, como a cerimônia de criação de chaves. Pudemos observar a importância de ter procedimentos escritos detalhados para que possamos lidar corretamente com as evidências. Simulações e treinamento também são uma boa recomendação.

Sua organização aproveitou o treinamento oferecido pelo PCI Council? Em caso afirmativo, como o treinamento beneficiou sua empresa?

Fizemos o treinamento do Avaliador de Segurança Interna (ISA) antes e foi interessante porque toda a mentalidade de conformidade com PCI DSS e PCI PIN Security é basicamente a mesma. Depois participamos do treinamento informativo do Qualified PIN Assessor (QPA), que foi muito mais preciso para os tipos de atividades que executamos.

Como você e sua empresa planejam usar o conhecimento do PCI PIN Security?

Temos que usar esse conhecimento para manter nossas operações e conformidade em andamento com auditorias internas periódicas.

Brazil Regional Engagement Board

Gertec Brasil Ltda é um membro ativo do Conselho Consultivo Regional do Brasil, que representa as perspectivas das Organizações Participantes e dos constituintes do PCI SSC no Brasil, aconselhando e fornecendo feedback e orientação ao PCI SSC sobre desenvolvimento e adoção de padrões e programas no Brasil.