



ESTUDO DE CASO PCI Data Security Standard (PCI DSS)

A EMPRESA:



A Decolar/Despegar é uma empresa de viagens on-line na América Latina. Com 20 anos no mercado, opera em 20 países e oferece através de seu site ou aplicativo móvel uma oferta completa de voos, pacotes de viagem, hotéis e produtos relacionados ao turismo e entretenimento em todo o mundo.

Como o PCI Data Security Standard (PCI DSS) beneficia sua empresa?

Usamos nosso conhecimento do PCI DSS de várias maneiras. Primeiro, aplicamos isso em campanhas de conscientização, onde educamos nossos funcionários da central de atendimento. Isso faz com que eles entendam a importância das informações que estão lidando ao atender ou lidar com casos de atendimento ao cliente. Também aplicamos o conhecimento do PCI DSS às nossas políticas de segurança, bem como aos nossos planos de resposta a incidentes e planos de continuidade. Mesmo que estejam focados nas informações do cartão de pagamento, o PCI DSS é um dos padrões de segurança mais abrangentes do setor e pode ser aplicado em várias áreas.

Qual tem sido o principal desafio da sua empresa na implementação e manutenção dos controles do PCI DSS?

Uma de nossas tarefas mais desafiadoras foi trabalhar com um provedor de nuvem terceirizado (CSP) e manter os controles do PCI DSS em nosso ambiente de nuvem. Foi equivalente a reiniciar a certificação do zero.

Como a empresa lidou com esse desafio?

Criamos um novo ambiente de rede, que é uma tarefa muito difícil de realizar porque envolve a instalação e configuração de todos os dispositivos de comunicação e todos os dispositivos de segurança baseando-se no PCI DSS, bem como a documentação relacionada que suporta essa nova zona em nossa infraestrutura.

Quais resultados foram obtidos?

Com a implementação de um CSP agora temos um plano de recuperação de desastres também no ambiente de nuvem, o que nos permite recuperar os serviços essenciais da organização, incluindo a segmentação do ambiente de dados do portador do cartão (CDE).

Que principais aprendizados você pode compartilhar para ajudar outras empresas que podem enfrentar desafios semelhantes?

O CSP oferece muitos serviços para garantir que a infraestrutura seja adequadamente protegida. Nós somos responsáveis, em última análise, pela segurança dos dados, bem como pela configuração dos serviços em execução na rede. Recomendamos ter um contrato por escrito que cubra as responsabilidades da sua empresa e as responsabilidades do CSP.

Para cumprir o requisito de filtragem por firewalls, decidimos usar grupos de segurança como componentes que permitem a rastreabilidade de conexões estabelecidas. Além disso, usamos túneis VPN IPSec para criptografar as comunicações entre nosso ambiente no CSP de e para nosso datacenter local, além de usar protocolos criptografados dentro desses túneis.

Conselho Consultivo Regional do Brasil

A Decolar/Despegar é um membro ativo do [Conselho Consultivo Regional do Brasil](#), que representa as perspectivas das Organizações Participantes e dos constituintes da PCI no Brasil, aconselhando e fornecendo feedback e orientação ao PCI SSC sobre desenvolvimento e adoção de padrões e programas no Brasil.