O que fazer diante de golpe ou fraude na emissão de passagens no sistema de Agências de Viagens?

O que fazer diante de golpe ou fraude na emissão de passagens no sistema de Agências de Viagens?

As companhias aéreas que operam no Brasil possuem hoje poderosas e rígidas normas de segurança da informação. No entanto, é sabido que o atacante foca comumente nos usuários e consumidores que utilizam os portais e sistemas de compras de passagens.

No que tange às agências de viagem ou turismo, outro problema grave. Comumente estas celebram contratos com Companhias aéreas, que fornecem acesso ao portal para agências ou mesmo sistema de reservas, onde estas possuem algumas vantagens, como faturamento mensal, descontos, reservas de ultima hora, dentre outros.

É neste ponto que reside um grande perigo que tem prejudicado e lesado inúmeras agências que utilizam sistemas eletrônicos de reservas de passagens. O risco de um furto de credenciais, que será utilizado para emissão de passagens fraudulentas ou questionadas.

As agências normalmente não adotam regras mínimas de compliance e segurança da informação, não estão dispostas a investir em blindagem de seus equipamentos e manter um padrão de segurança alinhando com normas como COBIT, ITIL ou mesmo da família ISO 27000. O resultado, recebem da companhia aérea um acesso “MASTER” para cadastro de usuários que poderão emitir passagens, não gerenciando estas contas, não aplicando senhas fortes, não revogando permissões, dentre outras omissões que

custam caro.

Como se sabe, criminosos hoje podem usar técnicas, que vão desde *pishinhg scam* até engenharia social para conseguirem estes acessos. Alguns até conseguem sniffar o tráfego da agência, capturando senhas. Desde modo, o ataque normalmente permite que centenas de passagens sejam emitidas, em curto espaço de tempo, para inúmeros passageiros, alguns que voam, outros *no show.*

Seja como for, ao final do mês a agência, se não adotar mecanismos de segurança e não contratar uma perícia em informática para identificar origem da fraude e forma de atuação, receberá uma fatura elevadíssima da operadora e logicamente que será cobrada a pagar, considerando que "deu causa" às emissões fraudulentas.

Assim, diante de uma fraude de compras de passagens, o primeiro passo é preservar o ambiente da agência para uma perícia que possa constar se está seguro e se não, como se deu a infecção. Após, o caminho é a buscar um advogado especializado em crimes na internet ou direito digital, para que possa, diante da ausência de fraude, acionar a operadora para revisão dos valores cobrados.

Importante destacar que se trata de uma medida onde a perícia e a assistência técnica em informática são essenciais, do mesmo modo em que um advogado especializado em direito digital é desejável, pois será necessário compreender questões envolvendo token, certificado digital, transações via API, banco de dados, sistemas específicos e outras áreas.

Deve se destacar, conforme diversos julgamentos no Brasil, que a companhia aérea não será responsabilizada caso demonstre que ofereceu instruções à agência, recursos para sua proteção e que seu ambiente é seguro, demonstrando ainda culpa exclusiva da vítima, em ceder ou negligenciar com suas senhas ou não utilizar os controles disponibilizados para aprimoramento da

segurança. De se destacar que a quebra de sigilo que indique inúmeros Ips, inclusive fora da sede da agência, por si só, não é motivo para se atribuir a responsabilidade à companhia, considerando que é da essência do negócio que seja permitido à agência emissões de qualquer localidade e horário.

Um perito em informática poderá avaliar o ambiente da agência, assegurar adoção de boas práticas e até mesmo constatar inexistência de vulnerabilidades, em laudo técnico forense, de uso em juízo, importante prova e que reforçará judicialmente o entendimento sobre quem deu causa ou permitiu a efetivação da fraude.