Deficiências na Legislação

A LEGISLAÇÃO E OS CRIMES NA INFORMÁTICA

No dia 25 de junho a edição do Jornal Nacional mostrou uma matéria sobre os roubos bancários através dos cartões magnéticos em caixas automáticos.

Mostrava que os clientes de um determinado banco estavam sendo cobrados por retiradas de valores das suas contas, que os mesmos alegavam não ter feito.

O delegado ante sua impotência e ignorância sobre o assunto, limitou-se a fornecer sugestões ineficazes como: intensificar a instalação de câmeras de vídeos para fiscalizar os caixas eletrônicos e o aumento de guardas de segurança próximos aos citados caixas, como se tais medidas resolvessem o problema.

Por outro lado, os bancos imputavam aos clientes o ônus do débito das somas retiradas.

Isto me fez lembrar a minha experiência de 26 anos de auditor, e de 6 anos gerenciando a Auditoria de Sistemas Informatizados em uma grande empresa bancária nacional.

Com base nas informações do noticiário, comecei a questionar o quão limitada e frágil é a segurança das informações que trafegam através das mídias modernas do país.

Os princípios básicos e elementares da Auditoria de Informática ensinam que quaisquer informações consideradas críticas como: passwords (senhas), números de contas, etc., devem ser criptografadas a fim de evitar a intromissão de terceiros.

Existe uma gama infindável de algoritmos de criptografia. Sabemos também que a prática da plugagem de linhas telefônicas já não é mais ficção científica.

Os marginais estão acompanhando velozmente a evolução tecnológica.

O que antes ocorria nos EUA e era considerado ficção aqui, hoje para nós é realidade.

Portanto, por que não acompanharmos preventivamente a tecnologia, a fim de evitarmos o pior?

Os bancos, principalmente os seus parques de informática possuem profissionais experientes e conscientes da responsabilidade que têm quanto ao fator segurança, nos seus sistemas e bancos de dados.

A legislação também, embora tímida, garante a proteção dos clientes de tais empresas.

A prova é que são elas.

2023 - www.conjur.com.br - Todos os direitos reservados.
Felipe Vilasanchez
07/07/1999

Analisando a questão específica, questionamos o seguinte: Será que o cliente é realmente responsável pelo saque fraudulento, ou será o banco responsável pela negligência quanto à segurança dos dados que trafegam em linhas telefônicas ou de dados?

Sabemos que qualquer profissional de telefonia mais dedicado, pode interceptar uma conversa telefônica.

Nessas circunstâncias, imagine uma interceptação em linhas de dados, o que já é feito por técnicos e auditores de informática em algumas empresas, porém com objetivos bem diferentes.

Um equipamento chamado Data Analyzer (algo como analisador de dados) permite ao técnico a observação do comportamento dos dados trafegando nas linhas como se fosse um letreiro automático.

Acredito não estarmos preparados para enfrentar tais problemas, não por questões técnicas, mas por uma simples questão de vontade – de circunstância.

A legislação carece de meios mais eficazes de proteção ao usuário, embora o Código de Defesa do Consumidor preveja, como já dissemos em parágrafo anterior, tímidos mecanismos de defesa.

Pergunta-se: o que fazer então?

a) Inicialmente, atualizar a legislação no que se refere a estas responsabilidades, buscando com isto, definir o alvo de tais imputações, evitando assim a injusta peja de culpabilidade do consumidor;

b) Exigir dos bancos e demais empresas de crédito, maiores cuidados em seus mecanismos de transmissão e tratamento de dados, estabelecendo regras de controle das informações;

c) Atualizar a legislação criminal, visando a imputação penal nestes delitos;

d) Aliar aos legisladores, quando da elaboração de tais leis, profissionais experientes em consultoria de segurança de dados.

Dessa forma, acredito que poderemos adentrar ao novo século, usufruindo das maravilhas da tecnologia da informação sem o receio da perda de controle do nosso rumo de crescimento.

Date Created
07/07/1999
Author
felipe-vilasanchez

2023 - www.conjur.com.br - Todos os direitos reservados.