Desvio de dinheiro de conta é a fraude mais cometida na internet

04/08/2009

Uma pesquisa feita com mil consumidores virtuais de São Paulo pela Fecomércio apontou que a fraude mais conhecida e sofrida pelos entrevistados é o desvio de dinheiro em conta corrente (37%). Em seguida, vem compras indevidas com cartão de crédito (24%) e uso de dados pessoais (19%). Enquanto o Congresso cria meios de acelerar a aprovação do Projeto de Lei 89, que regula os crimes praticados na internet, advogados, empresas e tribunais estudam a melhor forma de se proteger na web e garantir que criminosos modernos sejam culpados. Acordos entre governo, servidores, redes sociais e campanhas de conscientização da população são armas que andam juntas, quando o assunto é Justiça na internet, segundo especialistas que participaram do Congresso *Crimes Eletrônicos*. O evento termina nesta terça-feira (4/8), na Fecomércio, em São Paulo.

O deputado federal Julio Semeghini, atual relator do projeto, informou que para acabar com as idas e vindas do texto, ele espera que se faça um acordo entre a Câmara e o Senado para que o projeto seja aprovado em conjunto. Há mais de dez anos em tramitação no Congresso, as inúmeras alterações feitas impossibilitam a aprovação da lei. Para Coriolano de Almeida Camargo, presidente da Comissão de Direito na Sociedade da Informação da OAB, toda a comunidade jurídica tem feito um excelente trabalho em fazer valer a legislação atual para os crimes virtuais, mas há brechas na lei que facilitam a ocorrência de crimes e atrapalham a investigação. “Nos Estados Unidos, por exemplo, é possível que o servidor ‘congele’ uma informação até que se consiga um mandado judicial que apóie a busca destes dados”, explica.

Para ele, o maior desafio hoje é conseguir provas que realmente valham para o processo. “As leis terão de ficar cada vez mais técnicas para que não se perca o direito de ampla defesa. A Polícia Federal e outros órgãos que investigam crimes na internet criaram até manuais próprios de procedimentos para ter acesso a dados sigilosos no mundo virtual”. Ele explica que um passo errado no acesso às informações pode tornar a prova inválida e ainda ultrapassar a barreira de sigilo do suspeito investigado. “A prova pode ser impugnada pela defesa”. Na opinião de Renato Ópice Blum, presidente do Conselho Superior de Tecnologia da Informação da Fecomércio, não há o que reclamar da Justiça brasileira quando é preciso um mandado judicial para apreender computadores ou captar provas na internet. Ele diz, porém, que a polêmica é sobre o tempo em que o servidor deve armazenar os dados na internet.

Outro consenso entre os palestrantes foi o fato de que é preciso conscientizar melhor os usuários sobre os cuidados ao acessar a internet, além de como se defender de atos ilícitos. Segundo Ópice Blum, a criação de novas leis sempre criam um efeito cultural. “Sabendo da nova lei, as pessoas correm atrás da informação e aumentam os processos. Por outro lado, os criminosos ficam mais cautelosos para cometer os crimes”, afirma.

Já Coriolano reforçou, em sua exposição sobre os crimes de pedofilia que os pais devem estar atentos aos costumes dos filhos na internet. “Os pais devem negociar com os filhos. Eles devem

ter o direito de acessar o histórico para ver por onde as crianças “tem andado na internet”, afirma. Na mesa, os convidados citaram diversos casos de sequestros falsos, reais e atos de pedofilia que foram planejados a partir de informações extraídas do redes sociais como o Orkut. “Pelas redes sociais, os criminosos constroem um verdadeiro dossiê da vítima sobre onde ela frequenta, o que fez no final de semana, quem são seus amigos”, conta.

Insergurança virtual

A compra feita em uma máquina de doces com cartão de crédito, a nota fiscal eletrônica emitida ou um livro que o internauta adquire na web faz com que seus dados viajem por um sistema virtual. E essa vulnerabilidade já é sentida pelos usuários de internet. Foi o que mostrou a pesquisa feita pela Fecomércio e apontou que a fraude mais conhecida e sofrida pelos entrevistados é o desvio de dinheiro em conta corrente.

Essa constatação reforçou entre os especialistas a necessidade de parcerias constantes entre governo, empresas e usuários para garantir a segurança dos dados que trafegam pela web. Representantes de empresas de tecnologia como IBM, Microsoft e Cisco concordam que hoje os *hackers* agem por dinheiro e tem grandes esquemas montados, que desafiam os sistemas de segurança diariamente. “O criminoso na internet hoje não é mais aquele estudante querendo desafiar os sistemas. Ele está em busca de dinheiro e age por oportunidade”, explica Ricardo Marques, especialista em segurança da IBM e ISS.

Para Ghassan Dreibi Junior, da Cisco, os criminosos não precisam saber mais sobre os sistemas. Basta saber mais que os usuários. Segundo pesquisa da empresa, este ano foram detectadas mais de 7.400 novas vulnerabilidades na rede. Para mostrar o quanto o crime eletrônico está avançado, os especialistas mostraram formatos em que os *hackers* invadem computadores comuns pelo próprio navegador. Há ainda organizações que vendem programas de clonagem de cartão de crédito prontos. “São verdadeiros kits”, ele conta. O “serviço” contratado chega a fornecer assistência por telefone e e-mail e garante que se o “cliente” for pego por algum antivírus, ele disponibiliza uma atualização do programa.

Há quadrilhas que transferem sua base na internet para os Estados Unidos para aperfeiçoarem seus sistemas. Para se ter uma ideia da participação norte-americana, o Brasil é responsável por 4% dos e-mails spams, que na maioria das vezes, trazem links em forma de armadilha. Os Estados Unidos está em primeiro lugar com mais de 170% dos spams distribuídos pelo mundo.

As grandes empresas devem contratar sistemas de segurança e atualizá-los sempre, segundo recomendação dos representantes das principais empresas de tecnologia presentes no evento. Já para os usuários comuns, a melhor forma de garantir a segurança é atualizar o software periodicamente, o que depende da utilização de programas pagos e licenciados. De acordo com Opice Blum, este é o risco de softwares livres. “A diferença de ter um Linux é que você não terá quem processar, caso algo grave aconteça”.

Fonte: https://conjur.jumps.com.br/2009-ago-04/desvio-dinheiro-conta-fraude-cometida-internet/