Bancos reforçam sistemas contra ataque de hackers
Cibelle Bouças

Perdas no país podem chegar a US$ 100 milhões por ano

Resistir às tentativas de invasão on-line é um trabalho hercúleo para as grandes companhias de qualquer lugar do mundo. No Brasil, a tarefa não é menos extenuante. A pedido do Valor, a Kaspersky, empresa russa de software antivírus, fez um levantamento das empresas brasileiras que são os principais alvos de ameaças na internet. As cinco mais visadas são todas do setor financeiro: Bradesco, Caixa, Itaú Unibanco, Santander e Banco do Brasil, sendo que o Bradesco foi o único a constar no ranking mundial das marcas mais visadas.

O levantamento da Kaspersky considerou os casos de "phishing". São e-mails com informações falsas de uma empresa, sugerindo que os internautas acessem um site (também falsificado), com o objetivo de roubar informações sigilosas, como senhas e números de cartões de crédito. Essas mensagens também contêm vírus e outros programas nocivos, com a mesma finalidade de copiar senhas. "Os casos mais comuns são mensagens falsas se passando por um pedido de atualização de cadastro", afirma o analista de vírus da Kaspersky Lab Fabio Assolini. O especialista estima que, no Brasil, as fraudes na internet causem prejuízo aos bancos de US$ 75 milhões a US$ 100 milhões por ano.

Representantes da área de tecnologia dos bancos foram unânimes em reforçar que, embora o nome da instituição financeira seja usado para tentativas de fraude na internet, a vítima do ataque é sempre o cliente. Para reduzir riscos de perdas com esses ataques, os bancos adotam ferramentas que vão de novos sistemas de senhas a redes neurais que identificam operações incomuns feitas em nome de seus clientes.

O Bradesco registrou nos últimos 12 meses um total de 240 milhões de mensagens indesejáveis, 239 mil vírus nocivos aos sistemas do banco e 14 milhões de tentativas de invasão ao seu sistema, de acordo com o vice-presidente executivo da instituição, Laércio Albino Cezar. "É uma guerra sem trégua. Mas o alvo final do criminoso é sempre o cliente", afirma. Dos 57,4 milhões de clientes do banco, 12 milhões fazem regularmente transações pela internet.

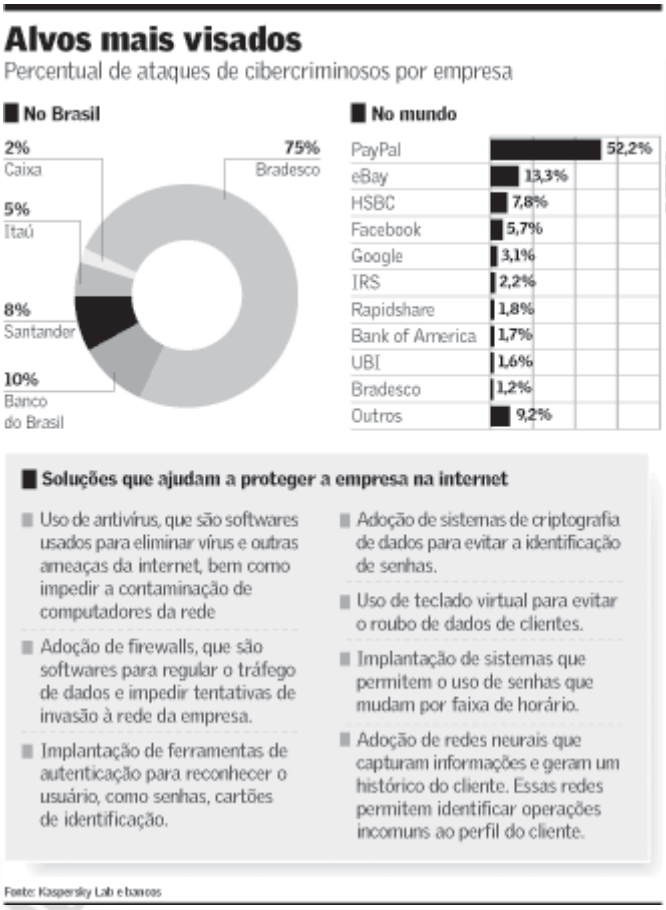
Cezar afirma que o banco já adotou uma série de medidas para que os ataques não se convertam em fraudes. As ações vão de implantação de antivírus, programas de firewall (software para regulação do tráfego de dados na rede da empresa), sistemas para criptografia de senhas, adoção de teclados virtuais e jogos de senhas que mudam por faixa de horário. Mas a estratégia que fez cair em 90% o número de ataques foi a adoção de um módulo de proteção para o cliente. Na primeira vez que o usuário acessa o serviço de internet banking, ele vê no site uma mensagem que lhe dá a opção de instalar no computador um módulo de proteção. Esse sistema contém, além do programa de senhas, um software que permite identificar se há programas nocivos no computador do usuário, como vírus e "cavalos de troia".

O Banco do Brasil, segundo principal alvo, reformulou em dezembro de 2009 o seu site, com vistas a aumentar o nível de segurança. No processo, o banco eliminou o teclado virtual e optou por acrescentar uma nova senha para cada usuário. Para fazer transações no site do banco, o cliente precisa ter uma senha para internet de oito dígitos e a senha de seis dígitos que é cadastrada no terminal de atendimento do banco. "Para ter acesso ao internet banking, um fraudador teria que roubar o cartão físico do cliente e pegar a sua senha na agência", afirma o gerente-executivo da diretoria de segurança do Banco do Brasil, Luiz Fernando Ferreira Martins. A vinculação à senha do cartão físico, diz, reduziu os riscos de ataques. O banco tem hoje 8,5 milhões de clientes do serviço bancário na internet.

No Santander, a implantação de um módulo de segurança que os clientes usam em seus computadores também reduziu os casos de fraude em 90%, afirma o diretor de tecnologia do banco, Claudio Almeida Prado. "Os mecanismos de autenticação também reduzem os riscos de fraude, mas tornam a vida do cliente mais chata. São mais senhas para guardar", observa.

Além das ferramentas tradicionais de proteção à rede da empresa, o Santander usa dispositivos de autenticação, como tokens com senhas variáveis que dificultam a captura de senhas e redes neurais, que permitem identificar o padrão de gasto de cada cliente. Se um usuário, por exemplo, paga uma conta de IPVA por ano e aparecem dez ordens de pagamento de veículos distintos, a informação fora do padrão gera um alerta ao sistema do banco. "Nesses casos, o pagamento entra em um módulo de agendamento e o gerente é acionado para tentar confirmar a operação com o cliente."

Procurados, o Itaú Unibanco e a Caixa informaram, por meio de suas assessorias, que também investem em ferramentas como cartões de segurança (com tabela de códigos), sistemas de token, programas antivírus, filtros de navegação para o site e redes neurais. O número de usuários do serviço via internet, porém, não foi informado.



Fonte: Valor Econômico, São Paulo, 01 jun. 2010, Empresas, p. B3.