Segurança na Internet aumenta produtividade do usuário

A web possui um grupo único de assuntos relacionados à segurança para mercados online. Os consumidores irão fornecer suas informações pessoais, como números de cartão de crédito, apenas se estiverem convictos de que as informações irão permanecer seguras.

Mas o Brasil está ameaçado de ter suas mensagens bloqueadas em outros países por possuir um grande número de hackers anarquistas, de acordo com reportagem não tão recente publicada no Caderno de Informática do jornal Folha de São Paulo:

“O Brasil está prestes a ser filtrado no mundo todo, ou seja, ter seu acesso impedido, por conta dessa falta de credibilidade da segurança brasileira na Internet”, disse Raphael Mandarino Junior, presidente da Associação Nacional dos Usuários da Internet (ANUI).

Com ou sem alarmismos, sabe-se que, de posse de ferramentas específicas – muitas vezes acessíveis na Internet em sites especializados (as chamadas “receitas de bolo”) – um hacker mal-intencionado (em muitos casos menor de idade) pode tomar completamente o controle de um servidor e, remotamente, obter acesso a senhas gravadas na memória do sistema e executar outras ações danosas e irresponsáveis.

No mundo ainda deviante do ciberespaço, consumidores e comerciantes virtuais devem lidar com novas espécies de ameaça – o perigo anônimo, sem identidade. Temos as seguintes situações ou condutas:

* Acesso não autorizado: alguém fazer uso indevidamente de um sistema de computadores para interceptar transmissões e se apropriar de informações de terceiros;

* Alteração de dados: o conteúdo de uma transação virtual – nome do usuário, número de cartão de crédito, e quantias monetárias – pode ser alterado localmente ou durante a própria transferência de dados;

* Monitoramento: Um hacker infiltrado no sistema acessar e acompanhar a troca de informações confidenciais;

* *Spoofing*: um vândalo virtual cria um site falso, fazendo-se passar pelo verdadeiro site, podendo furtar informações do consumidor inocente, ou apenas atrapalhar o negócio original;

* Serviço negado (*deny of service*): um sabotador pode tirar do ar ou bloqueia o site, impedindo o acesso aos visitantes;

* Repúdio: o participante de uma transação online nega a sua ocorrência, ou sua autorização.

Estas atitudes exaltam o perigo de uma fraude, as conseqüências de um serviço interrompido, vendas perdidas, furto de informações confidenciais, e o mais importante de tudo: a perda da confiança do consumidor.

Os negócios e novos mercados estão se direcionando cada vez mais para a Internet. Torna-se necessário o conhecimento e análise dos riscos e vulnerabilidades a que se está exposto, caso a caso, de modo que

os mecanismos adequados para a segurança sejam determináveis.

Como princípios básicos da segurança plena, a confidencialidade, a integridade e a disponibilidade das informações. Os benefícios são evidentes: redução dos riscos com vazamentos de dados, fraudes, erros, uso indevido, sabotagens, roubo de informações e diversos outros problemas que possam comprometer estes princípios básicos.

A segurança também intensifica a produtividade dos usuários , por meio de um ambiente mais organizado, de um maior controle sobre os recursos de informática, viabilizando a execução de aplicações críticas das (e nas) empresas.

A segurança tornou-se uma preocupação importante na Internet (1). Talvez uma das mais importantes. A maioria das pessoas hesita em distribuir seu número de cartão de crédito ou suas informações pessoais, com medo de interceptação e/ou uso indevido e não-autorizado.

Existem, porém, mecanismos tecnológicos que poderão proteger essas informações, e as empresas estão ansiosas para disponibilizar tais mecanismos, para que então o comércio eletrônico possa prosperar.

Tais mecanismos de proteção tecnológica servirão também para melhorar a qualidade e a quantidade das informações disponíveis na Internet, bem como facilitarão as transações online garantindo a autenticidade das mensagens. E o respeito à Lei.

Editores da Web e também os particulares estão hesitantes em transmitir certas informações na Internet. Autores, artistas gráficos, fotógrafos, músicos e outros muitas vezes não publicam e divulgam seus trabalhos na web com medo de que seus trabalhos caiam em mãos de usuários não autorizados.

Por exemplo, qualquer pessoa pode fazer o download de um artigo ou fotografia para seu computador pessoal e depois republicar essa informação em qualquer lugar do ciberespaço, negando crédito ao autor.

Qualquer violação de direitos autorais passível de ser cometida no mundo “real” pode ser ocorrer na Internet, com uma violação especialmente difícil de ser detectada diante do reino sem fronteiras do ciberespaço. Além disso, é muito mais difícil rastrear e deter um pirata virtual do que um pirata “real”, diante da habilidade de alguns usuários de mascarar sua identidade através de contas anônimas de correio eletrônico ou de “spoof” do endereçamento IP.

As ramificações deste problema são óbvias quando vistas da perspectiva da utilidade da web do ponto de vista do comércio eletrônico, que é perdida pelo internauta típico, bem como os procedimentos potenciais que são também perdidos pelos editores e divulgadores virtuais.

Na tentativa de se contornar esses obstáculos, pesquisadores e programadores desenvolveram algo chamado de “sistema confiável” (*trusted system*), uma proteção tecnológica que poderá ajudar a garantir que certos materiais não possam ser reproduzidos ou que apenas os consumidores que previamente adquiriam a licença possam acessar determinadas informações.

Outra implementação visando à segurança é a adoção da assinatura digital. Um e-mail ou outro documento online pode, assim, ser autenticado e garante, por exemplo, que a mensagem não foi

modificada durante ou após a transferência. Tais assinaturas digitais, aumentando a confiabilidade das transações virtuais, poderão, da mesma forma, facilitar as transações, servindo de método válido para o envio e recebimento de documentos.

Mas ainda paira a dúvida: como será a recepção de tais inovações no ordenamento jurídico atual? Serão absorvidas naturalmente ou criarão mais um entrave burocrático? A resposta nos guia para o futuro. Um futuro de inovações tecnológicas, e um excesso de informações disponíveis, mas cada vez mais individualizadas.

Nota de rodapé:

[1] http://eon.law.harvard.edu/property/introtech/techprotect.html

Revista **Consultor Jurídico**, 20 de março de 2001.

Date Created
20/03/2001