SEGURANÇA DA INFORMAÇÃO – UM CAMINHO ESTRATÉGICO PARA A CONTINUIDADE DE NEGÓCIOS

CESAR BASTA
Livre-Docência e Doutorado em Ciências – UNESP;
Mestrado em Engenharia Elétrica – UFRJ;
Graduação em Matemática – USP.
basta@uninove.br

WALDIR ANTONIO DA SILVA
Aluno da Pós-Graduação em Administração Profissional – UNINOVE.

Resumo

Com a proliferação e expansão de novas plataformas, o risco de exposição dos dados aumentou de forma exponencial, o que exige maior rigor para assegurar a continuidade dos negócios, minimizar as perdas financeiras ocorridas por meio de acessos não autorizados, permitir o uso compartilhado da informação de forma segura, manter a confidencialidade, a integridade, a disponibilidade, a autenticidade e a irrevogabilidade das informações. Essas questões são algumas das razões do desenvolvimento deste trabalho que busca conscientizar os administradores quanto à importância da Segurança da Informação. Destaca-se o fato de que as organizações multinacionais têm enfatizado mais o problema da segurança que as nacionais. Assim, pretendemos fornecer àqueles que desejam implantar um plano de segurança uma fonte de pesquisa e de apoio para o início do projeto.

Palavras-chave: *Segurança da Informação. Plano de Segurança.*

Abstract

The present work intends to be one of the awareness sources to administrators concerning the importance of the Information Security in an organization, regardless its dimension. To achieve the proposed aim, many devices used in information networks are presented, being analysed their advantages, disadvantages and failure points through which data security can be violated resulting in irreversible losses to companies. It's also carried out an analysis about reports presented by the media related to the subject with the intention of pointing out the biggest omissions inside organizations to administrators.

Key words: *Information Security. Security Plan.*

Introdução

A partir de 1995, o computador entrou na linguagem, na cultura e na própria vida do brasileiro médio, não em termos de recursos financeiros, e sim como elemento da vida nacional, infiltrando-se nos assuntos do dia-a-dia do cidadão. Se, à época, apenas 1% da população do país, tinha um micro em casa, atualmente ele se encontra entre os eletrodomésticos à venda em supermercados, constituindo mais um instrumento, entre outros, inserido em nossa vida, educação e cultura. No entanto, seu impacto tem causado mais dúvidas do que respostas para o povo brasileiro.

No século passado, viveu-se a era industrial. O mundo começava a experimentar a aventura da linha de montagem, que mesclava os elementos humanos e mecânicos para produzir bens em quantidades impensáveis; hoje, século virado, vive-se uma outra realidade: a era da informática. O que mudou, nesse período, foi a maneira como o homem passou a olhar para a máquina. Ela foi despida de sua roupagem de mero robô para revestir-se de um papel menos servil e, portanto, mais polêmico: o de agir, além de fazer.

A indústria da informática, que tem no computador seu principal componente e movimenta mais de 400 bilhões de dólares por ano, só perde em faturamento para a indústria do petróleo e a do automóvel. Enquanto estas já esgotaram sua capacidade de transformação da sociedade, o potencial do computador ainda está na primeira infância, fato que se opõe ao que tantas vezes ocorreu na história da inventividade humana, não pela complexidade das máquinas e dos sistemas de redes disponíveis, mas pelas diferenças entre as diversas plataformas de *hardware*[1] e *software* existentes no mercado. Essa situação parece caminhar para uma solução quase total, graças ao modelo de comunicação cliente/servidor. Esse modelo permite que pessoas, em sua estação de trabalho, entrem em diferentes bancos de dados em qualquer parte do mundo, sem preocupação com a marca da máquina ou do *software* que estão sendo usados. É a democratização da informação e a transparência para o usuário final, que pode acessar *online* os servidores de bancos de dados existentes, tanto no mercado corporativo quanto no doméstico.

Sabe-se que as empresas, por longo tempo, efetuaram suas transações comerciais – compras, pagamento de faturas, envio de orçamentos, análise de propostas ou assinatura de contratos – por meio da comunicação, utilizando muito papel, datilografia, fax, correio e trabalho de conferência, o que resultava em demora, erros, atrasos e desencontros.

Os computadores e as redes vieram, portanto, para minimizar o trabalho, os transtornos e, principalmente, para garantir a agilidade e a flexibilidade que a comunicação sempre exigiu das organizações. Pedidos de compra, avisos de entrega, notas de débito, propostas, tudo flui por meio do *Eletronic Data Interchange – EDI*, com qualidade e velocidade, atingindo o coração da empresa e transformando aquilo que era transtorno-trabalho em diferencial competitivo.

A era do processamento centralizado, que vigorou do fim dos anos 60 até meados da década de 80, caracterizou uma fase da tecnologia de redes, batizada pelos especialistas como a 'primeira onda', datando dessa época o início do processamento interativo com o uso de terminais. A 'segunda onda', iniciada na década de 80 com a difusão dos sistemas distribuídos, decorreu da proliferação dos mini e microcomputadores,

[1]Serão marcadas em itálico todas as palavras e abreviações ou siglas em língua inglesa que fazem parte da linguagem utilizada pela informática.

utilizando as redes locais e os conceitos do modelo cliente-servidor. Estações cada vez mais poderosas e novas tecnologias de transmissão, aliadas ao uso de fibra óptica, estão mudando os padrões exigidos na implantação das novas redes de computadores. Nos próximos anos, os ambientes acadêmicos, comerciais ou mesmo residenciais, exigirão recursos de infra-estrutura de rede, o que implicará mudança radical dos atuais modelos, evoluindo para as redes chaveadas (*switched networks*), dando início, assim, à 'terceira onda'.

Na época da primeira onda, o processamento era concentrado no Centro de Processamento de Dados – CPD, para garantir a confidencialidade, integridade, disponibilidade e autenticidade dos dados armazenados. Aos administradores eram dadas garantias quanto à sua segurança porque apenas as pessoas treinadas e autorizadas tinham acesso às máquinas e, de maneira geral, eram as únicas que sabiam como o equipamento funcionava. O risco de exposição dos dados, portanto, estava concentrado no próprio CPD. Com a proliferação e expansão de novas plataformas, esse risco aumentou de forma exponencial, exigindo maior rigor para assegurar a continuidade dos negócios, minimizar as perdas financeiras ocorridas por meio de acessos não autorizados, permitir o uso compartilhado da informação de maneira segura, manter a confidencialidade, a integridade, a disponibilidade, a autenticidade e a irrevogabilidade das informações.

Essas são algumas das razões deste trabalho, cujo objetivo é conscientizar os administradores da importância da Segurança da Informação.

Segurança nos negócios

Com o advento da *internet* e a proliferação das redes corporativas, as informações sensíveis, em acessos remotos, não estão mais seguras atrás da barreira de um CPD, ficando, pois, vulneráveis à destruição, alteração ou furto. Residindo em servidores ou estações (clientes), permite um acesso fácil a uma vasta gama de informações. Conectando-se a rede ao *mainframe*, fornece-se uma capacidade de acesso e cópia ainda maior. *PCs* do tipo *palmtop*, *notebook*, *laptop*, apesar de convenientes, permitem que as informações sejam levadas para fora da empresa, aumentando o risco de exposição dos dados.

Segundo Caruso (1991, p. 83),

> a informação confidencial da empresa não está mais sob a proteção da segurança tradicional associada ao CPD, devido ao grande risco de exposição dos dados. Quando as informações residiam apenas nos *mainframes*, os administradores tinham mais garantias quanto à sua segurança porque apenas as pessoas treinadas e autorizadas tinham acesso às máquinas e, de maneira geral, eram as únicas que sabiam como o equipamento funcionava, e o risco de exposição, portanto, estava concentrado no próprio CPD.

Hoje, nem as grandes corporações estão imunes às ações de criminosos digitais, pois todos os dias temos, em nível mundial, notícias de um caso de quebra de segurança de sistemas ou de descoberta de algum novo vírus eletrônico. Assim, com o crescimento da informatização nas organizações, existe a crescente necessidade de segurança. Mesmo aqueles que, numa empresa, reconhecem a necessidade de segurança aqui discutida e encontram um produto adequado para efetuá-la podem supor que esse tipo de segurança é uma tarefa impossível; outros entendem que pode ser opressiva a segurança numa plataforma múltipla que tenha *mainframes*,

minirredes e computadores *stand-alone*. Os funcionários, por sua vez, podem não considerar interessante participar de um plano de segurança que lhes proíba o acesso a muitas informações, pois estas deverão ser cadastradas e permitidas somente àqueles que possuem autorização.

Como o crescimento da microinformática foi muito rápido, as empresas não se preveniram quanto ao trato de seus bens de informação. O modo de corrigir tal problema consiste em reconhecer e utilizar planos específicos de segurança que sejam amplos, flexíveis e seguros.

A segurança da informação, de fato, é uma questão ampla e complexa; cabe analisar vários aspectos, sendo primordial iniciar, para toda a organização, o plano de segurança por meio de uma padronização consistente, pois sua implantação pode ser cara e ineficaz se a comunidade de usuários possuir visões diferentes sobre segurança e produtos decorrentes. Portanto, assegurar a continuidade dos negócios, minimizar as perdas financeiras ocorridas por meio de acessos não autorizados, permitir o uso compartilhado da informação de maneira segura, manter a confidencialidade, integridade, disponibilidade, autenticidade e irrevogabilidade dos dados fazem parte dos objetivos da Segurança da Informação. Sem sistemas de segurança que utilizem esses controles, a organização não pode ter a garantia de que seus dados sejam confiáveis, conforme define a *Internacional Standard Organization – ISO,* que inclui ainda outros controles como autenticação, acesso e não-repulsão. Tais objetivos serão atingidos só se a organização tiver uma política de segurança consistente, pois ela será responsável pela distribuição dos sistemas, pelas diretrizes e normas estabelecidas, bem como pela padronização e procedimentos no ambiente de tecnologia da informação.

Em face dos aspectos apresentados, a Segurança da Informação deve ser uma atividade preventiva e não corretiva; as informações devem ser selecionadas para possibilitarem o controle, e os dados confidenciais, armazenados em ambientes computacionais seguros, porque são muito importantes tanto para a organização quanto para seus concorrentes. Assim, é necessário saber quem está acessando o quê... e quem controla tais acessos. De todo modo, devemos observar que nenhuma organização está totalmente imune a ataques ou seqüestro de informações.

Política de segurança

A política de segurança é a diretiva de gerenciamento que estabelece as metas comerciais da organização, fornece uma estrutura de implementação para alcançar os objetivos dessas metas e atribui responsabilidades e domínios ao processo. Ela é projetada para gerenciar os riscos que a organização pode ter ao buscar seus objetivos comerciais, havendo, então, a necessidade de avaliação desses riscos.

Para Ribeiro (1997, p. 70),

> É uma espécie de cartilha que identifica os recursos da rede (*hardware* e *software*) e seus pontos vulneráveis; define o grau de sigilo de cada informação e quais dados estarão disponíveis; determina quem de dentro da companhia pode ter acesso aos dados; como será feito esse acesso nos diferentes níveis hierárquicos e departamentais; como serão configurados os sistemas operacionais e as estações de trabalho, e a forma como o funcionário poderá se conectar à rede e à *internet*, dispõe sobre os direitos e os deveres do usuário e cria punições para casos de violação interna.

Toda informação deve ser tratada de forma profissional, isto é, o fato de um usuário manipulá-la diariamente pode dar-lhe a impressão de que é insignificante; porém, para um usuário de outro departamento, é possível que se torne crucial para a continuidade dos negócios e, se cair nas mãos de um concorrente, poderá significar uma perda irreparável.

É fato que a *internet* oferece uma grande economia de custos e excelentes ganhos de produtividade, além de muitas oportunidades significativas à geração de receita para uma organização. Em contrapartida, a segurança de suas redes fica ameaçada. Tais ameaças exploram os pontos fracos de um sistema relacionados com a tecnologia ou a política de operação, tais como fraquezas tecnológicas, fraquezas na política de operação, rede interna, interceptação, repudiação, *replay*, disfarce, roteadores, 'Cavalo de Tróia', vírus e *internet* aos funcionários.

Fraquezas tecnológicas são as deficiências nos produtos de *software*, *hardware* e as falhas no material de comunicação. Fraquezas na política de operação são as regras pelas quais se operam os sistemas de computadores e, de acordo com Bernstein (1997), "o projeto de um sistema seguro é tão importante quanto ter uma política de segurança eficiente." A ameaça só é eliminada quando os dois estão presentes. Logo, para ter segurança de seu patrimônio, a organização deve compreender essas ameaças e tomar as providências necessárias à proteção das informações, recursos e redes.

Apesar de a conexão com a *internet* ser muito vantajosa para a organização, em razão de o trâmite e a troca de informações serem mais ágeis, é possível criar pontos vulneráveis e difíceis de ser controlados. Se houver falhas na segurança, não visualizadas na implementação das soluções, pode-se permitir o acesso de intrusos como os *Hackers* (que invadem o computador, apenas para violar a segurança) e os *Crackers* (que entram no computador para roubar arquivos ou destruir dados, além de acionar outros componentes como vírus e 'Cavalo de Tróia') (VASCONCELLOS, 1998).

Com relação à rede interna, os levantamentos de segurança feitos pelo Instituto de Segurança de Computadores do *Federal Bureau of Investigation – FBI* (*Computer Security Institute – CSI*) mostram que quase 50% de todas as invasões de rede vêm de dentro da própria organização.

A interceptação pode ocorrer por meio de correio eletrônico, transação da *web*, *downloads* de arquivos etc. Por isso, é importante que se disponibilizem recursos especiais para diagnosticar suas tentativas de realizar tal procedimento.

A 'repudiação' ocorre quando o participante de uma transação *online* nega que ela tenha realmente ocorrido, isto é, que tenha participado da comunicação. Esse repúdio será crítico especialmente para transações financeiras e acordos contratuais eletrônicos.

O disfarce se verifica quando o usuário A assume a identidade do usuário B, tendo, portanto, autorização para utilizar os privilégios e o direito de acesso do usuário B. São os chamados ataques de *spoofing* ao *Internet Protocol – IP*, nos quais os intrusos criam pacotes de dados com endereços de origem falsificados. Esses ataques exploram aplicações que utilizam a autenticação baseada em endereços e permitem o uso não autorizado do sistema destino com todos os seus privilégios.

O *replay* é uma seqüência de eventos ou comandos observados e reproduzidos para efetivar alguma ação não autorizada. É uma das ameaças que exploram as falhas em esquemas de identificação em conjunto com a falsificação de servidores de autenticação. A manipulação consiste em danificar a informação durante o armazenamento ou a transmissão, sem que isso seja detectado.

Os roteadores são computadores ou equipamentos que controlam e direcionam o tráfego na *internet* ou em uma rede: uma mensagem roteada de um usuário A para um usuário B pode ser interceptada. As instruções de controle de roteamento não autorizadas ocorrem devido à falta de proteção ou pela configuração inadequada das redes, linhas de comunicação e outros dispositivos do sistema. Os roteadores incorretos podem ser usados com disfarces, manipulações e *replays*.

O 'Cavalo de Tróia' é um processo não autorizado que pode executar um programa como se fosse um processo autorizado. Um programa aplicativo ou de sistema é substituído por outro que contém uma seção adicional alterada, permitindo algum tipo de atividade mal-intencionada que pode não ser detectada.

A contaminação por vírus, considerada muito crítica, é uma ameaça constante e consiste em códigos de programa que se auto-reproduzem, podendo destruir completamente todos os arquivos armazenados.

As organizações, ao oferecerem a seus funcionários acesso direto à *internet*, podem ter a segurança de suas informações ameaçada porque, se estes podem fazer o acesso, a *internet* também pode acessar a organização. Esse problema pode ser evitado, utilizando-se dispositivos como o *firewall*. Há ainda outra ameaça relacionada com o acesso direto à *internet* pelos funcionários: a produtividade. Sendo a *internet* um repositório aparentemente infindável de informações sobre os mais variados temas, não é difícil imaginar que alguns de seus serviços possam ser utilizados pelos funcionários para finalidades incompatíveis com os objetivos e atividade da organização, por exemplo: jogos, trabalhos escolares e sites de piadas.

Dessa forma, para que se tenha, nos negócios, uma política de segurança ampla, flexível e atualizada constantemente, deve-se levar em consideração as ameaças relatadas.

Conclusão

É importante salientar que o assunto aqui discutido é objeto do Decreto nº 3505, de 13.6.2000, sancionado pelo então Presidente da República Fernando Henrique Cardoso. Seu artigo 1º dispõe sobre o que segue: "Fica instituída a Política de Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal." Assim, tomando-se como base o decreto assinado, comprova-se que o governo está consciente da importância de suas informações e da necessidade de protegê-las e guardá-las de forma segura, utilizando, para isso, todo o aparato tecnológico e todos os conceitos e objetivos da Segurança da Informação.

Espera-se, portanto, que os administradores se preocupem com as informações de suas organizações, avaliem-nas, prevejam seus custos e, finalmente, percebam o que e quanto eles poderiam perder caso alguma informação fosse 'saqueada' de seu ambiente computacional ou seu *site* invadido, pois a Segurança da Informação mostra ser um caminho estratégico para a continuidade dos negócios.

Referências

BERNSTEIN, Terry (Coord.). *Segurança na Internet*. São Paulo: Campus, 1997. 461p.

CARUSO, Carlos A. A. *Segurança em Microinformática e em Redes Locais*. Rio de Janeiro: Livros Técnicos e Científicos, 1993. 60p.

CARUSO, Carlos A. A.; STEFFEN, Flavio Deny. *Segurança da Informação*. Rio de Janeiro: Livros Técnicos e Científicos, 1991. 274p.

RIBEIRO, Gisele. *As suas Informações Estão Seguras?*, v. 6, n. 11, p. 66-74. São Paulo: Byte Brasil, 1997.

VASCONCELLOS, Marcio José Accioli de. *A Internet e os Hackers – Ataques e Defesas*. São Paulo: Chantal, 1998. 336p.