05 – Junho de 1999

Pequenos detalhes, grandes vulnerabilidades

Imagino e torço para que você esteja acompanhando esta coluna desde sua inauguração. Assim, poderei ir direto ao assunto sem ter que falar da tendência de migração dos negócios para ambientes informatizados e da manipulação de informações críticas nas redes corporativas.

É preciso termos uma visão macro do que vem a ser segurança da informação. Fazendo uma analogia, a segurança seria uma corrente composta por diversos elos, que seriam os pontos vulneráveis merecedores de atenção. Neste conceito de corrente, existe a preocupação de mantermos o mesmo nível de segurança para cada elo, pois de nada adiantará elos extremamente fortes, se um único estiver fraco e vulnerável.

Será que sua empresa pensou em todos os elos da corrente?
Provavelmente não. São pequenos detalhes, que muitas vezes passam desapercebidos ou recebem pouca atenção - e podem comprometer todo o investimento em segurança realizado - representando grandes vulnerabilidades.

Façamos um exercício. Sua empresa tem uma grande malha de rede, interligando departamentos, prédios e até filiais. Centenas de estações de trabalho, que acessam a Internet. Um grande volume de correspondência impressa e eletrônica, muitas vezes, documentos importantes e sigilosos, trafegando entre as unidades de negócio. Um ambiente moderno de fácil circulação, formado por divisórias baixas.

Para analisar os elos deste ambiente, comecemos com o cabeamento. Um elemento fundamental para o funcionamento dos recursos computacionais e com um grande potencial de gerar problemas. Se desestruturado ou mal administrado, pode tornar a informação – tão importante para seu negócio – inacessível.

E o material impresso? Será que está sendo manipulado, armazenado, transportado e descartado corretamente? Lembremo-nos que possuir um eficiente fluxo de informações – agregando agilidade e qualidade ao negócio – sem os devidos cuidados com a sua segurança, pode representar um enorme perigo. É preciso desenvolver regras claras e explícitas para classificação das informações, que possibilitem aos usuários manipulá-las adequadamente, transportá-las em material apropriado, descartá-las em fragmentadoras de papel e armazená-las em local seguro.

E o acesso à Internet, esqueceu? É uma porta de entrada e saída de informações, um ponto muito vulnerável. Para garantir o nível de proteção adequado contra ataques e invasões, deve estar, no mínimo, protegido por um *firewall.* Imagine quando o acesso discado acontece através de um modem instalado em uma das centenas de máquinas dos usuários conectados à rede. Ameaças como os atuais “vírus” ou “cavalos de tróia” potencializam este tipo de vulnerabilidade, permitindo ao invasor adquirir o domínio total da estação e

capturar toda e qualquer informação armazenada, inclusive a senha de acesso aos servidores da mesma rede. Uma catástrofe!

Lembrou-se do email?
Este também é merecedor de atenção. A atual realidade das empresas, quanto à privacidade e proteção na utilização do correio eletrônico, nos leva a associá-lo a um cartão postal enviado pelo correio convencional. Sistemas específicos e soluções de Identidade Digital permitem a troca de mensagens criptografadas – garantindo o sigilo e integridade no trajeto e na armazenagem – além de assegurar sua entrega ao interlocutor.

E os backups?
Falta de luz, defeito de hardware e até mesmo sabotagem podem ser a causa de uma forte dor-de-cabeça. É preciso definir os procedimentos conforme o perfil das informações manipuladas, garantindo a disponibilidade dos dados em casos de contingência. Backup não se resume apenas em manter uma cópia das informações importantes, mas em uma política completa e adequada, contemplando estratégias de rodízio incremental – por exemplo – utilizando-se diversas unidades de fita, e um esquema de armazenamento de acesso controlado. Manter as fitas de backup fora do prédio ou em um cofre blindado, são algumas das técnicas mais utilizadas.

O usuário também é um elo da corrente, você sabia?
Mesmo que o servidor esteja bem configurado, o email seguro, o lixo informático fragmentado, e os backup realizados com exatidão, é necessário ainda uma política de segurança que sirva como bússola, definindo diretrizes, responsabilidades, normas e procedimentos para a melhor utilização do ambiente informatizado.

A essa altura, já falamos de diversos elos da corrente da segurança e com certeza faltam muitos outros, um verdadeiro leque de vulnerabilidades. Mas esses serão assunto para as próximas colunas.

Marcos Sêmola *é MBA em Tecnologia Aplicada e Analista de Segurança da Módulo Security Solutions S.A.*
msemola@modulo.com.br