11 – Outubro de 1999

E-mail: como controlar sem infringir?

Correio eletrônico ou e-mail, como preferir, é o nome da mais nova preocupação da empresa moderna. Este recurso computacional, que existe há anos – sendo um dos primeiros associados às redes –, está assumindo o papel de ferramenta essencial para a comunicação corporativa.

Contudo, os recursos de TI que representam o alicerce para sustentação da agilidade e competitividade nos negócios, podem ao mesmo tempo serem uma das grandes dores de cabeça dos executivos.

Mas como o e-mail pode oferecer tanto risco?

Não é difícil entender. A empresa automatizada tem sua gestão apoiada por informações estratégicas armazenadas em grandes bancos de dados digitais. Estes, por sua vez, estão sendo compartilhados localmente, e também através de Extranets e do acesso remoto. Nesse contexto, com a conexão à Internet feita pela rede corporativa, o correio eletrônico torna-se uma porta aberta para saída e entrada de qualquer informação.

Então, muitas corporações se perguntam: como controlar o tráfego dos dados veiculados por e-mail, impedindo o vazamento de informações, sabotagens ou até mesmo perda de produtividade e recursos financeiros, sem infringir a Lei maior que reza sobre a inviolabilidade das comunicações?

A Lei nº9.296 de 24 de Julho de 1996, sancionada pelo Presidente da República, é clara quando determina: "Art. 10º: Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei."

Porém, nem todos os caminhos estão fechados para se administrar o uso da comunicação em meio digital sem ir contra a legislação. A prática aconselhável está diretamente ligada ao controle parcial do tráfego de informações e da conscientização dos usuários. Esta estratégia pode se converter em diversas ações, que juntas, trarão mais segurança à empresa:

- Termo de Sigilo assinado pelo funcionário, comprometendo-o a somente utilizar os recursos a ele disponibilizados para o exercício da sua atividade, com pena de multa e/ou demissão por descumprimento.

- Seminários de conscientização, que esclareçam a importância do uso correto da tecnologia no ambiente de trabalho e o impacto que o mau uso pode acarretar à empresa.

- Software de controle do uso da Internet nas estações de trabalho, atuando como Firewall Pessoal, protegendo as máquinas e ao mesmo tempo coletando dados que irão subsidiar a auditoria.

- Monitoramento generalizado e impessoal dos acessos aos recursos da rede corporativa e da própria Internet, gerando estatísticas de utilização veiculadas em uma campanha de divulgação interna.

- Regras e critérios técnicos de uso, como: o volume máximo permitido para o tráfego de informações por e-mail, a inibição de acesso a determinados serviços da rede/Internet e ou endereços web.

- Política de Segurança personalizada, com diretrizes, normas, procedimentos e instruções que norteiem os usuários quanto ao uso da infra-estrutura tecnológica.

Todas essas ações são ótimos exemplos para se iniciar o controle e potencializar o uso dos recursos de informática, sem pôr em risco as valiosas informações que sustentam o negócio. E o mais importante... sem esquecer de garantir o direito do principal bem das empresas modernas: o capital intelectual.

Marcos Sêmola *é MBA em Tecnologia Aplicada, Bacharel em Ciência da Computação, Coordenador de Segmento de Mercado e Analista de Segurança da Módulo Security Solutions S.A.*
msemola@modulo.com.br