A INTERNET, O E-MAIL E A (IN)SEGURANÇA DAS EMPRESAS

Sérgio Gonçalves

sergio.goncalves@clgadvogados.com.br

Data criação: 09.08.2001
Data publicação: 03.12.2001

São inúmeras as possibilidades de lucro ou, ao menos, de grande redução nas despesas das empresas que entendem e aplicam a Internet de modo adequado aos seus negócios e a sua estrutura. Neste raciocínio inicial não se pensa apenas no comércio eletrônico, mas sim na integração interna da empresa através de seus computadores (Intranet) com outras empresas e pessoas fora de sua e estrutura física (Internet). As possibilidades são muitas, mas, as vulnerabilidades aumentam e muito. Sua empresa, sua rede, seus funcionários, estão preparados para isto? No mundo atual a informação é a mais valiosa das ferramentas que uma empresa pode possuir, isso é indiscutível. Logo, se não houver uma proteção para estas informações em sua empresa, cedo ou tarde, haverá um prejuízo, seja ele moral ou material. Recente pesquisa da Módulo Security Systems com 165 empresas de grande porte (18% das quais com mais de 5.000 terminais) revelou que 40% delas já sofreu invasão em seus sistemas, enquanto 31% não souberam dizer se foram alvo de ataque aos seus dados e 29% negaram qualquer tipo de ocorrência. Estes números, embora assustadores, podem ser ainda maiores, uma vez que as empresas não tem interesse em assumir este tipo de violação aos seus dados. 8% das companhias pesquisadas calcularam seus prejuízos entre quinhentos mil e um milhão de Reais.

Uma análise nos dados divulgados revela um quadro que, embora bastante conhecido, continua a ser desconsiderado pela grande maioria dos empresários: mais da metade dos ataques aos sistemas ocorre dentro das próprias empresas e á praticado por empregados insatisfeitos ou simplesmente infiéis. Os tão temidos “hackers” são responsáveis por pouco mais de um terço das ocorrências e outros 18% delas foram fruto de espionagem industrial. Se coibir a espionagem industrial e os “hackers” parece um trabalho árduo e muito longo, a criação de políticas de segurança de dados pode eliminar mais da metade das ameaças, pois mesmo os hackers se utilizam, em geral, de uma falha interna das empresas para agir.

O aspecto técnico desta política de segurança empresarial entretanto, não pode ser implementado de modo eficaz sem um acompanhamento de medidas jurídicas capazes de garantir efetividade aos resultados. Os limites da proteção serão medidos pela interação destas duas variáveis. De nada adianta a colocação de equipamentos modernos se os funcionários puderem acessar os dados de modo indiscriminado, por exemplo. Há pouco tempo uma empresa do setor eletrônico instalada em São Paulo descobriu que dados e até projetos seus estavam sendo indevidamente enviados para fora da empresa por um funcionário que, simplesmente, todos os dias mandava (via e-mail), arquivos com até 10Mb da empresa para sua casa. Este problema, aparentemente simples, ocorre diariamente na maioria das empresas e escritórios comerciais no mundo inteiro e nos leva a procurar uma saída técnica (filtragem de e-mails) e outra jurídica: posso barrar ou monitorar os e-mails de meus empregados?

O assunto é bastante polêmico e merece considerações extensas. Porém, em síntese, diversos países do mundo já aplicam este tipo de controle nas empresas e 54% dos norte-americanos aceitam como justo este tipo de controle, havendo lá um projeto específico sobre o tema, o “Notice of Eletronic Monitoring Act”. No Brasil não há nada específico sobre este tema, nem na lei atual nem em projetos, como o dos EUA. 83% das empresas usam o e-mail como

ferramenta de seus negócios e o tráfego na rede é estimado em mais de 10 bilhões de mensagens diárias. Por estes números, vê-se que monitorar as mensagens de modo manual não é uma opção, seja pelo volume de trabalho, seja pela invasão na privacidade dos empregados. Neste caso específico, o problema é resolvido no campo técnico pela criação de um filtro (via software), impedindo uso de contas particulares nos servidores da empresa e regulando o tamanho máximo dos e-mails e arquivos anexados que podem trafegar, identificando ainda, se for o caso, mensagens que contenham frases, termos ou expressões consideradas estratégicas pela empresa. No campo jurídico, deve-se criar um termo específico sobre os limites para o uso do e-mail da empresa, incluindo um compromisso de confidencialidade sobre os assuntos internos e deixando claro que as mensagens serão monitoradas tecnicamente. Além disso, por se tratar de e-mail profissional, o nome de usuário e senha devem ser providos pela empresa, afastando o caráter de privacidade da conta, que deve ser usada apenas para assuntos de trabalho, sendo um canal da empresa e não do empregado.

Sérgio Gonçalves é advogado e conferencista, sócio da Correia Lopes e Gonçalves Advogados Associados (CLG Advogados), especialista em Direito Civil e Direito Eletrônico. Fundador e editor do Informativo Jurídico “O Neófito. Professor em curso de Pós-graduação em Direito de Informática, conselheiro do Instituto Brasileiro de Política e Direito de Informática (IBDI), do Centro de Estudos Tributários e Empresariais (CETE) e conselheiro-convidado da Organização das Nações Unidas Brasil. É também autor de diversos artigos sobre Direito Internacional, Empresarial, do Consumidor e Direito Eletrônico publicados em revistas, jornais e websites. Colunista do jornal Gazeta Mercantil sobre Direito Empresarial e co-autor dos livros "Comércio Eletrônico" (Editora Revista dos Tribunais) e "Direito Eletrônico - A Internet e os Tribunais" (Edipro).

Artigo publicado no site ***O Neófito – Informativo Jurídico*** com autorização do autor e em conformidade com a Lei nº 9.610/98. Por favor, respeite os Direitos Autorais desta obra intelectual. ***O Neófito*** não se responsabiliza pelas opiniões emitidas e/ou direitos autorais relativos aos artigos assinados. Para maiores informações sobre este texto ou para utiliza-lo, entre em contato com o autor pelo e-mail informado no início do artigo.

Copyright O Neófito 1997-2001