Empresas monitoram computadores para evitar vazamento de informações
Rafael Sigollo

Cresce a preocupação com segurança no uso da internet pelos funcionários.

Perda de produtividade já não é mais a maior preocupação das empresas quando se fala em controlar o uso da internet no ambiente de trabalho. Em um mercado cada vez mais competitivo, o vazamento de informações estratégicas e confidenciais se tornou um grande problema para os responsáveis pelos departamentos de recursos humanos e tecnologia das companhias.

Para Eduardo Godinho da Trend Micro, multinacional especializada em segurança virtual, a proteção dos sistemas serve para evitar casos de vazamento involuntário, que ocorrem por distração ou imprudência dos funcionários. "A pessoa acha normal enviar arquivos de trabalho para um e-mail pessoal ou copiá-los no pen drive para trabalhar em casa. Essa prática, porém, representa um grande risco para a corporação", alerta. Em uma pesquisa com 1.600 usuários realizada pela Trend Micro nos Estados Unidos, Reino Unido, Alemanha e Japão, cerca de 50% dos entrevistados admitiram fazer isso com frequência. Segundo Godinho, o Brasil segue a mesma tendência.

Desse modo, o monitoramento de tudo o que os funcionários fazem no computador da empresa, tanto online quanto offline, tem se tornado mais comum. E isso, vale lembrar, é legal. Apesar de não existir uma legislação específica para o tema, as organizações geralmente estão protegidas por políticas internas e pela própria CLT, que prevê punição em relação à violação de informações confidenciais e o mau uso dos equipamentos de trabalho.

"Cerca de 40% dos desligamentos de executivos intermediados pelo escritório envolvem a questão da confidencialidade de informações", afirma Letícia Ribeiro, advogada associada do Trench, Rossi e Watanabe. Segundo ela, quando há uma demissão, é preciso saber quais informações que o executivo armazenou em seu computador são propriedade da empresa e quais são pessoais. Entre as divergências mais comuns estão o direito da empresa de fiscalizar os arquivos pessoais que o funcionário armazena no computador da empresa, o direito que ele tem de guardá-los, e o dever da empresa de fornecer esses arquivos ao funcionário demitido.

Os especialistas da área, contudo, afirmam que por mais que se use ferramentas para bloquear e monitorar computadores, quem está mal intencionado sempre conseguirá driblar os mecanismos de segurança. O especialista da Trend Micro afirma, por exemplo, que cerca de 90% dos vazamentos ocorrem de dentro das companhias e não de ataques externos. "Nem mesmo o pentágono e o FBI escaparam e, recentemente, tiveram milhares de informações confidenciais divulgadas na internet", lembra.

Waldir Arevolo, consultor sênior e especialista em redes sociais da TGT, consultoria em serviços de TI, afirma que as empresas focam muito na tecnologia e pouco nas pessoas. "Não adianta proteger as máquinas e não educar os funcionários. As interações sociais ocorrem nas filas, nos restaurantes, no elevador. As pessoas conversam e, se não forem bem orientadas, podem acabar falando o que não deviam."

Na opinião de Arevolo, os gestores deveriam, por exemplo, discutir como tirar proveito das redes sociais e ensinar os colaboradores como se comportar nelas e não simplesmente bloquear seu acesso. "O funcionário pode escrever no Twitter do celular ou de casa e comprometer a empresa do mesmo jeito", explica.

Para Cássio Alcântara, gerente da Websense no Brasil, como as redes sociais têm se tornado uma ferramenta estratégica para as empresas, muitas vivem um verdadeiro dilema na hora de proibir ou não o acesso aos colaboradores. A solução mais viável, e trabalhosa, consiste em configurar as máquinas de acordo com o departamento, o cargo e as funções de cada funcionário. "É preciso haver flexibilidade por parte das companhias para não passar uma imagem antipática e centralizadora para os colaboradores", afirma.

Mesmo assim, Alcântara defende o monitoramento interno para garantir a segurança das informações, especialmente no Brasil. Segundo ele, quando existe dúvida, o americano e o europeu procuram pela norma que os autorize a fazer determinado procedimento. Já o brasileiro acha que tudo é permitido desde que não haja proibições claras. "É comum o funcionário achar que como ele levantou os dados e construiu a planilha, é o dono daquela informação. Na verdade, o direito sobre o trabalho pertence ao empregador", afirma.

O meio termo ainda é a solução adotada pela maioria das companhias. Isso significa bloquear sites inadequados ao ambiente de trabalho ou que possam trazer algum risco legal ou de segurança para a corporação, mas liberar portais de notícias e o uso do webmail. Na Caloi, por exemplo, os 180 funcionários com acesso direto à internet podem tratar de assuntos pessoais na rede em horários pré-determinados, como o do almoço. A política foi estabelecida há um ano e meio e tem dado bons resultados.

"Nossa preocupação é que o tráfego indevido prejudique os outros sistemas corporativos. Hoje, no entanto, as pessoas já têm mais consciência e não ocupam o sistema com e-mails pesados e as famosas correntes", afirma Eduardo Silva, gerente da área de tecnologia da informação da companhia. As normas de uso são as mesmas em todas as unidades da Caloi, e a liberdade varia de acordo com os cargos e os departamentos. "O pessoal da comunicação e do marketing precisa olhar as redes sociais. Já a equipe de finanças tem de conseguir acessar sites de bancos", exemplifica.

Eduardo Godinho, da Trend Micro, alerta que tentar impedir o acesso à internet e às redes sociais pode ser ainda mais arriscado para as companhias. Ele afirma que cerca de um em cada 10 funcionários contorna a segurança para acessar sites restritos no trabalho. "Os usuários procuram maneiras alternativas, aumentando a chance de exposição a ameaças."

O esforço das empresas, segundo ele, não deve ser apenas em orientar os colaboradores sobre os riscos físicos que o mau uso da internet pode trazer aos computadores e sistemas da organização. É preciso ter muito cuidado com danos com vazamento de informações e manchas em sua reputação. "O funcionário deve lembrar que é sempre possível descobrir quem fez, o que fez e quando fez", diz.

Fonte: Valor Econômico, São Paulo, 27 set. 2010, Eu & Carreira, p. D10.