Perigo na web

Sofisticação dos ataques virtuais exige que empresas, inclusive as de pequeno porte, redobrem a atenção e invistam em softwares, processos e na conscientização dos profissionais para evitar perdas financeiras e prejuízos relacionados à imagem

ROBERTA FILLA revista@supervarejo.com.br

Quem se imagina andando à noite calmamente, sozinho, em uma rua escura, com algum objeto de valor? Nos dias de hoje, em que o índice de criminalidade é elevado, torna-se difícil visualizar uma cena como essa. Já no mundo virtual, esse tipo de situação é muito comum. Alheios aos perigos da web, usuários ao redor do mundo, inclusive dentro de muitas empresas, navegam tranquilamente por sites perigosos, colocando em risco suas informações pessoais, dados da companhia e até de clientes da empresa.

Isso acontece por que muitos desconhecem as ameaças da internet ou apenas subestimam o impacto que elas podem causar. Mas a verdade é que, assim como é preciso ter cautela no mundo real, no espaço virtual também é melhor prevenir do que remediar.

O número de pragas virtuais pode dar uma pista da dimensão que o problema atingiu nos últimos anos. De acordo com a McAfee, fornecedora de soluções de segurança, diariamente são criadas quase 6 mil ameaças na web. Dados do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (Cert.br) indicam que o total de incidentes notificados ao órgão avançou mais de 60% entre 2008 e 2009, passando de 222,5 mil para 358,3 mil.

Um levantamento da empresa especializada em sistemas de segurança Trend Micro, divulgado no ano passado, apontava o Brasil como o quarto colocado no ranking mundial de PCs infectados por vírus. O estudo mostra que, de 2007 para 2008, o número de infecções de PCs verificados pela Trend Micro cresceu 360%, com 1,5 milhão de máquinas contaminadas. Das cinco maiores ameaças na América Latina, quatro são específicas para o Brasil. O país já é o primeiro em volume de spam, respondendo por 20% desse tipo de mensagem em todo o mundo.

Outro dado preocupante refere-se à mudança no perfil do criminoso digital, também conhecido como hacker. Há alguns anos, esses especialistas invadiam sistemas e difundiam vírus e outras pragas motivados pela fama. Eles se envaideciam de quebrar barreiras de segurança e deixar a marca de sua capacidade técnica. Os tempos mudaram e hoje os hackers atuam com foco em ganhos financeiros. O objetivo deles é acessar dados que os permitam ganhar dinheiro, seja realizando fraudes bancárias com dados roubados, seja vendendo cadastros furtados.

Todos esses perigos podem trazer muitos danos para a companhia não apenas do ponto de vista financeiro, mas para suas operações e para sua imagem. "Se a empresa é atacada e todos ficam sabendo, isso pode assustar os clientes e fazer com que deixem de confiar nela", comenta a gerente de Consultoria da IDC Brasil, empresa especializada em tecnologia, Célia Sarauza.

As pragas da internet também podem causar paradas no sistema, afetando a operação e muitas vezes trazendo perdas pela impossibilidade de registrar compras ou realizar rotinas internas do negócio.

Quem pensa que essas ameaças estão restritas às grandes corporações se engana. Hoje os criminosos virtuais buscam ampliar seus ganhos pelo volume de máquinas afetadas, por isso internautas e principalmente as pequenas empresas estão na mira deles. "Como os criminosos buscam o lucro, as empresas menores se mostram mais atraentes do que os usuários domésticos. Já as grandes companhias costumam investir mais em segurança, dificultando o trabalho dos criminosos", alerta o gerente nacional de Vendas da Symantec, empresa provedora de soluções de segurança, Fabiano Tricarico.

Redes sociais na mira

O uso cada vez mais intenso da internet e o avanço de novas formas de comunicação via web, como redes sociais e serviços de mensagens instantâneas, impõem novos desafios e geram muita polêmica. Há os que defendem o bloqueio do acesso a esses canais, enquanto outros alegam que não é possível evitar que os funcionários utilizem esses novos meios digitais.

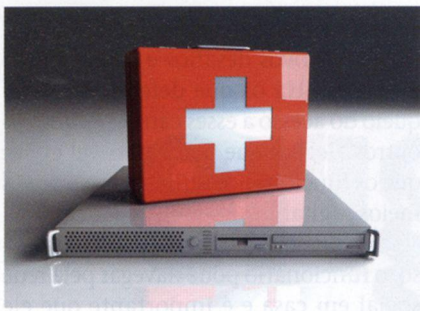
"Mesmo que a empresa proíba o acesso, o funcionário pode navegar pela rede social em casa e é importante que ele saiba que não deve colocar informações de negócios nesses canais, pois dados muitas vezes considerados irrelevantes pelo funcionário podem fornecer subsídios a pessoas mal-intencionadas", alerta o consultor e professor da Faculdade de Informática e Administração Paulista (Fiap) Edison Fontes, diretor do Comitê de Segurança da Informação da Associação Brasileira de Profissionais de Segurança (Abseg), além de autor de livros de segurança da informação.

Outro agravante são os perfis falsos. "É difícil saber quem está enviando algo por e-mail. Às vezes chega uma mensagem anunciando uma promoção que só é válida se a pessoa clicar no link, e fica complicado definir se o remetente é quem realmente diz ser", comenta o especialista em ameaças virtuais da Trend Micro, Eduardo Godinho.

Os comunicadores instantâneos, como MSN, Gtalk, ICQ e tantos outros, também são motivo de atenção, pois, uma vez contaminados, podem disparar mensagens infectadas para o grupo de contatos do usuário, difundindo as pragas virtuais. "Uma indicação é não clicar no link recebido e perguntar ao suposto remetente se ele de fato encaminhou a mensagem", afirma o gerente de Suporte Técnico da McAfee para a América Latina, José Matias.

Para se proteger dos perigos da web, o Emporium São Paulo adotou diversas

ATUALMENTE EXISTE UMA AMPLA GAMA DE SOLUÇÕES TECNOLÓGICAS QUE AJUDAM AS COMPANHIAS NA ÁRDUA TAREFA DE PROTEGER O SISTEMA



Para proteger a empresa

- Ter proteção técnica eficiente, com pessoal especializado (próprio ou por meio da contratação de empresa terceirizada)
- Definir regras para os usuários utilizarem recursos de informação da organização
- Informar periodicamente a política e as normas de segurança da informação a todos os usuários (empregados, estagiários, prestadores de serviço, conselheiros, clientes)
- Estabelecer um processo de sensibilização, conscientização e treinamento para os usuários
- Assegurar o apoio da alta administração para que o processo de segurança da informação seja verdadeiro e eficaz. As chefias (em todos os níveis) devem dar o exemplo
- Fazer e manter cópias de segurança com frequência adequada para a organização, de maneira que se ocorrer perda de dados, elas minimizem essa situação
- Garantir a continuidade das ações relacionadas à segurança
- Atualizar os programas (softwares antivírus, firewall, antispam etc.)

soluções tecnológicas e processos, entre eles o bloqueio no acesso a determinados sites, como os de redes sociais. "Temos uma lista de sites cujo acesso não é permitido e, portanto, o firewall bloqueia", explica o gerente de TI, David Ronco.

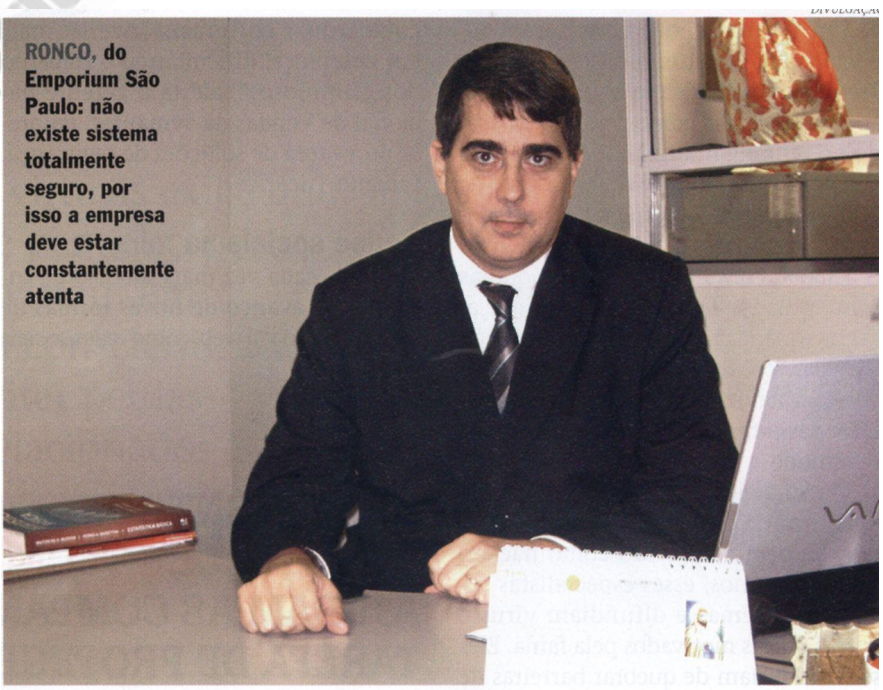
O executivo também busca acompanhar o que está sendo divulgado sobre a empresa na web. Para isso, Ronco utiliza um sistema de alerta de um site de buscas e recebe e-mails notificando toda vez que algum comentário sobre o Emporium São Paulo é feito na internet. "Tentar obter dados da empresa por meio dos funcionários é uma estratégia dos hackers. E isso não se aplica apenas no mundo virtual: em uma conversa no café o funcionário pode revelar informações importantes e que colocam a empresa em risco", alerta.

A política de segurança do Emporium contempla essa questão, por isso, ao ser contratado, o profissional recebe orientações sobre os cuidados que deve tomar com as informações corporativas. As normas envolvem ainda a troca periódica de senha e o uso de combinações diferentes e mais complexas.

Do ponto de vista da infraestrutura, o supermercado conta com sistemas preparados para minimizar o risco de invasões ou infecções. O Emporium possui duas camadas de firewall, software responsável por controlar a entrada e saída dos dados, bloqueando acessos não autorizados. O antivírus possui atualização automática; o recurso de autoexecutar, que possibilita a instalação automática de um software, é desabilitado e os usuários não têm acesso a determinadas áreas do sistema operacional. "Algumas configurações do sistema operacional podem deixar o ambiente tecnológico mais vulnerável", explica Ronco, lembrando que, como não existe sistema totalmente seguro, a empresa deve estar constantemente atenta para aprimorar os cuidados.

Muito além dos vírus

Atualmente existe uma ampla gama de soluções tecnológicas que ajudam as companhias na árdua tarefa de proteger o sistema. A oferta dos fornecedores é extensa e inclui desde softwares gratuitos até pacotes voltados a empresas de todos os portes, que reúnem as principais ferramentas tecnológicas destinadas à segurança. Outra opção é a contratação dessas soluções como serviço. "Uma empresa pequena que não possui equipe dedicada à segurança pode buscar uma companhia especializada, que fica responsável pela administração dessa questão", afirma Matias.



RONCO, do Emporium São Paulo: não existe sistema totalmente seguro, por isso a empresa deve estar constantemente atenta

DIVULGAÇÃO

MATIAS, da McAfee: uma empresa pequena, que não possui equipe dedicada à segurança, pode contratar uma companhia especializada

Entre as ferramentas consideradas imprescindíveis para garantir um nível básico de segurança, a mais popular delas é o antivírus. Ele evita a entrada e propagação dos vírus, que podem agir de diversas formas, como destruir arquivos do computador ou tentar capturar dados do usuário. Mas é preciso ficar atento, pois, apesar de essencial, o antivírus só protege contra determinados perigos. "No Brasil temos um problema de conceito, pois muitas pessoas acreditam que qualquer ameaça é vírus e acham que apenas o antivírus é capaz de proteger o computador. Isso cria uma falsa sensação de segurança. Há muitos outros riscos que exigem sistemas de proteção diferenciados", afirma Tricarico, da Symantec.

O executivo cita como exemplo o phishing. Trata-se de uma mensagem que, fingindo ser proveniente de uma instituição conhecida, seja banco ou empresa, induz o usuário a fornecer dados pessoais ou instalar um programa, o que permite ao criminoso ter acesso à máquina e às informações do internauta. Outra ameaça é o chamado download não autorizado: ao entrar em um site infectado, o programa é instalado sem que o usuário perceba. "Soluções de proteção mais básicas não bloqueiam esse tipo de ameaça", alerta Tricarico.

O firewall, que evita acessos não autorizados, e o antispam, que barra mensagens não solicitadas enviadas para um grande número de pessoas, também devem fazer parte da estrutura básica das empresas. "Se a empresa recebe muito spam, a rede fica lenta e a produtividade do profissional é abalada", observa Matias, da McAfee, comentando que estudos apontam que entre 76% a 82% do tráfego de e-mails na web é motivado por spams.

A lista do que não pode faltar inclui ainda o antispyware, software que inibe a ação de um sistema que tem o objetivo de monitorar atividades da máquina e enviar as informações coletadas para terceiros.

O papel do funcionário

ALGUNS CUIDADOS SÃO ESSENCIAIS PARA AMPLIAR A SEGURANÇA NO ACESSO À INTERNET

- **Atenção com as pessoas com as quais se relacionar. Checar se elas são quem dizem ser**
- **Evitar a navegação em sites desconhecidos**
- **Utilizar as ferramentas de proteção que a empresa disponibiliza**
- **Nunca emprestar identificação pessoal ou senha**
- **Jamais fornecer informações a pessoas ou sites antes de se certificar da sua autenticidade**
- **Atenção com as informações no ambiente virtual: um simples comentário em um e-mail pode vazar uma informação confidencial**

DIVULGAÇÃO

FONTES, da Fiap: funcionário não deve disponibilizar informações sobre os negócios nas redes sociais

Outra ação simples, mas que ajuda a reforçar a segurança, é a atualização constante do sistema operacional. Basta configurar a máquina para que realize, de forma automática, as atualizações feitas pelo fabricante. "Essa rotina viabiliza ter acesso aos ajustes de segurança e isso também se aplica às demais soluções, como antivírus, firewall etc", afirma Godinho, da Trend Micro.

Segurança começa com o funcionário

A batalha constante contra os criminosos digitais passa por outros aspectos além da infraestrutura. Não menos crítico é o comportamento do usuário. Por mais sofisticadas que sejam as ferramentas, dificilmente elas serão suficientes se não houver colaboração dos profissionais. "Muitas vezes a informação vaza porque saiu da empresa, e isso pode ocorrer em função do comportamento dos profissionais sem que eles tenham intenção de prejudicar a companhia", comenta Célia, da IDC. Dados encaminhados para e-mails particulares ou gravados em pen drives podem chegar às mãos de pessoas mal-intencionadas.

"A empresa deve ser transparente e explicar a função das regras de segurança. O funcionário pode até não gostar, mas ele tende a entender e cooperar", acredita o consultor Fontes. Na opinião dele a equipe responsável pela segurança deve agir em conjunto com a área de Recursos Humanos para conscientizar as pessoas. "As ações de conscientização devem ser periódicas, do contrário acabam sendo esquecidas", destaca Matias.

Para isso, algumas empresas investem em cartilhas e atividades lúdicas, capazes de ajudar a memorizar as normas. "Conforme os usuários adotam comportamentos seguros no trabalho, eles reproduzem essas práticas na vida pessoal, o que é positivo para a segurança em geral", garante Célia.

"MUITAS PESSOAS ACREDITAM QUE QUALQUER AMEAÇA É VÍRUS E QUE O ANTIVÍRUS SOZINHO É CAPAZ DE PROTEGER O COMPUTADOR. ISSO CRIA UMA FALSA SENSAÇÃO DE SEGURANÇA"
FABIANO TRICARICO (SYMANTEC)

> FONTES DESTA MATÉRIA

Abseg: (11) 3255-6573
Cert.br: www.cert.br
Emporium São Paulo: (11) 5538-4600
IDC Brasil: (11) 5508-3400
McAfee: 0800-8915846
Symantec: (11) 5189-6230
Trend Micro: (11) 4003-2129

Fonte: Supervarejo, São Paulo, ano 11, n. 114, p. 56-62, maio 2010.