BLINDE OS DADOS

Além de investir em tecnologias de gestão de risco, RH e TI devem treinar os colaboradores para o uso cauteloso da internet

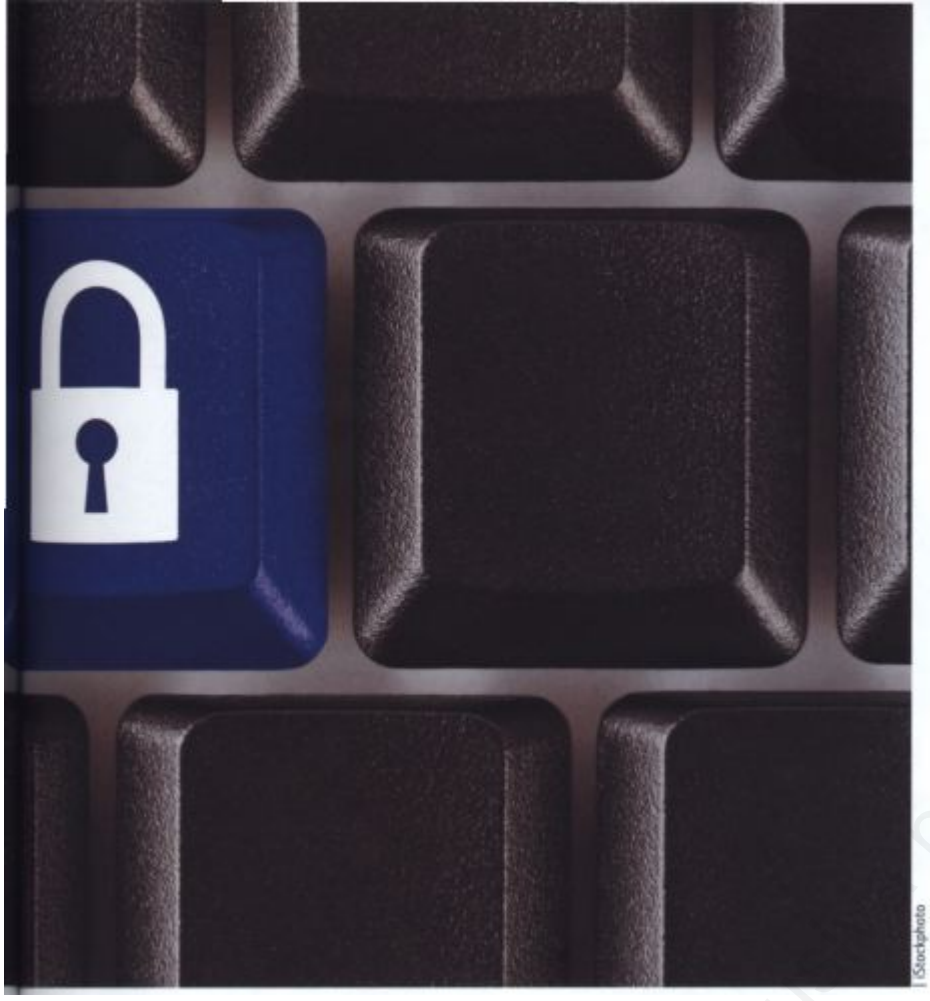
Por Felipe Falleti

A imagem do espião industrial que monitora telefonemas e e-mails corporativos para vender informações secretas aos concorrentes da companhia observada pode não ser totalmente falsa, mas certamente é uma exceção no mercado de TI. Apesar dos casos pontuais em que uma grande empresa se descobre diretamente espionada por um rival, a imensa maioria dos dados sensíveis perdidos ou expostos aos funcionários, fornecedores, à imprensa e, sobretudo, aos competidores escapam do controle da empresa por erros simples dos colaboradores e falta de treinamento para armazenar e proteger informações confidenciais. A advogada especialista em direito digital Lívia Andrade conta que atendeu um cliente que acusava seu principal concorrente de espionagem. 0 argumento central da acusação era o fato de a empresa rival possuir uma planilha com seus dados financeiros e contatos dos clientes mais importantes. "Na audiência, a acusada mostrou que esses dados não foram obtidos de forma escusa, mas tomados públicos pela companhia que a acusava", lembra Lívia. Nesse caso, a defesa mostrou um post no Twitter de um dos contadores da empresa que fez acusação. No texto, ele dizia: "Após uma semana de trabalho, consegui concluir esta planilha".

O episódio pode soar ridículo, mas de acordo com o professor de segurança em redes de dados da escola politécnica da USP, Guilherme Ortellado, falhas grosseiras na manipulação de dados corporativos respondem por mais de 98% dos episódios de perda de dados sensíveis. "Quando analisamos as crises nas empresas por perda, furto ou exposição indevida de dados, constatamos que a imensa maioria dos episódios ocorre por erros bobos e apenas 2% dos casos em função do uso de uma engenharia social ou exploração de vulnerabilidades técnicas de segurança", diz.

Nível básico de segurança

Para o especialista da USP, a primeira tarefa que as empresas devem realizar para melhorar seus níveis de segurança é reunir os técnicos da TI com os gestores de RH e o pessoal do financeiro. "É preciso traçar um plano em torno de quais são suas atuais vulnerabilidades, qual o nível de conhecimento técnico que seus funcionários têm e quanto sua empresa considera adequado



investir para melhorar esse quadro", diz. Um plano básico pode incluir apenas uso de antivírus e uma política de sofisticação de senhas pessoais. Planos ambiciosos podem exigir o desenvolvimento de redes privativas (VPN) para tráfego de dados sensíveis e engenhosos sistemas de alertas.

Ortellado alerta para o fato de não existir um ambiente com 100% de segurança em redes conectadas à web, mas diz que é possível definir padrões muito exigentes de proteção de dados. "Sua empresa talvez não precise ter o mesmo esquema contra hackers e vazamentos de dados que possuem a Nasa ou o FBI, mas certamente há dados gravados nos computadores das firmas que seus gestores não gostariam de ver nas mãos de concorrentes ou fornecedores", analisa.

Uma pesquisa realizada pela consultoria de TI Gartner aponta que as falhas mais comuns responsáveis pela perda de dados são o uso de senhas simples, o compartilhamento destas senhas e o mau manuseio de hardwares, como notebooks, pen drives e smartphones. "Usuários que criam senhas como 123456 ou usam nomes de bichos de estimação e datas de aniversário expõem suas empresas", diz Edvaldo Santos, analista do Gartner. Senhas simples podem ser quebradas por hackers que façam uso de softwares que tentam várias combinações até acertar a senha. 0 cenário ideal é o sistema de TI só aceitar a criação de senhas com mais de 8 caracteres e a combinação de números, letras e caracteres especiais. Uma senha como "caRRe8eto1", por exemplo, combina tantas variáveis (números, símbolos e letras) que não pode ser quebrada por softwares de tentativa e erro. "Isso não vale de nada se o colaborador contar sua senha para seu vizinho de mesa, e este pegar um arquivo em seu computador ou, ainda, se o funcionário deixá-la anotada num bilhetinho colado no PC", lembra Santos.

Com o advento da mobilidade nas empresas e a disseminação de notebooks, pen drives e smartphones, o manuseio de hardware tornou-se também uma preocupação para TI. "O ideal é que dados altamente sensíveis, como listas de clientes e planilhas de salários, nunca possam ser acessados fora da rede interna ou copiados para estes tipos de dispositivos", diz Santos. Quando for necessário transportar esses dados em notebooks, por exemplo, isso só deve ser feito em máquinas protegidas com sistemas de encriptação. Ou seja, caso o notebook seja perdido, nenhuma informação dentro dele poderá ser acessada sem o uso da senha correta, que deve ser composta de uma combinação de alto nível de dificuldade.

Políticas de uso da rede

Definido o treinamento para uso de senhas e hardware, o segundo passo, dizem os especialistas, é blindar as ameaças que chegam aos computadores das empresas pela internet. Vírus, spam e a disseminação de códigos maliciosos nos PCs têm basicamente duas portas de entrada, os e-mails e as ferramentas de troca de mensagens e arquivos, como MSN Messenger e aplicações P2P

para baixar músicas e filmes. "Não conheço nenhuma empresa que libere o uso de P2P na rede corporativa. Além das ameaças de segurança, essas aplicações consomem muita banda e tornam a internet de todos mais lenta. No entanto, devem existir softwares de monitoramento para identificar se há algum colaborador usando P2P de forma clandestina, bloqueá-lo e orientá-lo a não fazer mais uso desse tipo de ferramenta", conta Ortellado.

Treinamento eficaz

Já o uso de aplicativos tipo MSN e Gtalk são muitas vezes liberados para facilitar a comunicação dos colaboradores. Além disso, e-mail é inevitavelmente permitido, ainda que apenas o e-mail corporativo. Para bloquear a contaminação dos PCs, a regra elementar é o uso de antivírus, que deve estar necessariamente atualizado. Além disso, os colaboradores precisam ser treinados a não baixar anexos suspeitos e conhecer as extensões mais comumente maliciosas, como arquivos com final ".exe". Atualmente, hackers exploram complexos mecanismos de engenharia social que buscam ludibriar o usuário de internet. No caso das empresas, elas precisam treinar seus colaboradores para saber reconhecer esses golpes. "Foi-se o tempo em que um hacker mandava uma mensagem do tipo 'veja as fotos daquela festa' ou outros truques parecidos. Muita gente já percebe que isso é um golpe e nem abre o e-mail", diz professor Ortellado.

0 método mais avançado consiste em monitorar, por exemplo, os contatos do usuário nas redes sociais e enviar-lhe um e-mail com nomes e situações reais, induzindo-o a clicar na mensagem maliciosa. Se o software hacker reconhece, por exemplo, que "João" esteve no churrasco de "Pedro" no último domingo, ele pode disparar a mensagem, "muito legal nosso churras no final de semana. Olhe só as fotos que o Pedro tirou". A mensagem torna-se muito mais crível. 0 usuário mais atento verá, no entanto, que o emissor do e-mail não é nenhum de seus amigos e poderá notar inconsistências no texto enviado. Em caso de dúvida, a orientação é nunca baixar arquivos anexos, especialmente em PCs sem antivírus ou com este software desatualizado.

Políticas sofisticadas

Grandes companhias ou médias empresas que trabalham com muitos dados sensíveis podem adotar ferramentas mais avançadas de gerenciamento de segurança. Uma delas é chamada de Identity Management, solução que traça perfis dos usuários e emite alertas quando alguma operação suspeita é efetuada. Um exemplo de uso dessa tecnologia é o colégio Bandeirantes, em São Paulo. Após enfrentar problemas com alunos que espionavam professores para lhes furtar senhas e, assim, tentar alterar suas notas, o colégio adotou uma solução que emite alertas quando uma operação fora do comum é efetuada. "Se um professor que só dá aulas às quartas-feiras acessar nosso sistema às quintas, algo está errado e vamos investigar", diz Sérgio Bórgio, diretor de TI do colégio. Outra tecnologia que melhora os níveis de segurança são aplicações chamadas DLP (Data Loss Prevention). Esse tipo de software faz backups automáticos e evita, por exemplo, que fotos de um evento importante ou relatórios especiais sejam perdidos caso um notebook ou cartão de memória seja roubado ou destruído em um acidente. Em quaisquer dessas hipóteses, haverá uma cópia de segurança gravada nos servidores da empresa. O uso de soluções de encriptação e chaves físicas de identificação, por fim, complementam um plano de elevado nível de segurança. A encriptação serve para tornar quaisquer dados de um dispositivo inacessíveis sem o uso da senha correta e a chave de identificação, que pode ser um token como esses que os bancos distribuem a seus clientes, assegura que só o usuário devidamente autorizado acessará o sistema. "Se alguém descobrir sua senha do banco, não poderá fazer muita coisa se não tiver o token em mãos para digitar uma segunda senha, randômica. Muitas empresas usam esses recursos também para liberar acesso à sua rede corporativa", diz Ortellado, da USP.

| iStockphoto

Fonte: Melhor: gestão de pessoas, Especial Tecnologia, São Paulo, p. 28-30, 2011.