

Cliente: PATRÍCIA PECK P. ADVOGADOS  
Veículo: DECISION REPORT  
Data: DEZ/2009 - Nº 17  
Cidade: SÃO PAULO  
Coluna: RISK  
Marca: PATRÍCIA PECK P. ADVOGADOS

17/02/10  
SP  
Pág: 29 A 34  
05

# Risk

## REPORT

SEGURANÇA DA INFORMAÇÃO E GESTÃO DE RISCO

NÚMERO 7/2009

SANDRA TURCHI,  
SUPERINTENDENTE  
DE MARKETING  
DA ACSP



**Os dois lados  
da moeda nas  
redes sociais**

# Riscos e oportunidades nas redes sociais

SEJA PARA RELACIONAMENTO OU DIVULGAÇÃO INTERNA, O USO DAS FERRAMENTAS WEB 2.0 PODE SER A PORTA DE ENTRADA PARA AMEAÇAS. A VULNERABILIDADE AUMENTA QUANDO A EMPRESA DESCONHECE A NAVEGAÇÃO DE SEUS FUNCIONÁRIOS NO AMBIENTE CORPORATIVO **POR PAULA ZAIDAN**

**O**s sites de Web 2.0, que permitem conteúdos gerados por usuários, estão no topo da lista de ataques dos cybercriminosos e spammers. Essa é uma das conclusões do relatório semestral Websense Security Labs, State of Internet Security, produzido pela Websense. O estudo revelou que 95% dos comentários gerados por usuários em blogs, salas de bate-papo e mensagens contém spams maliciosos.

Outra constatação é o fato de que os esforços realizados para a autoproteção das propriedades de Web 2.0 são ineficazes. A Websense revelou que ferramentas de segurança utilizadas em sites como YouTube e Blogspot tem 65% a 75% de ineficiência na proteção do usuário contra riscos de segurança e conteúdos suspeitos.

Por isso, à medida que crescem os ataques e a maior adesão de usuários em redes sociais, muitas organizações bloquearam os acessos às ferramentas Web 2.0 pelos seus funcionários. De acordo com estudo da empresa de segurança Sophos, 63% das empresas se preocupam com as informações pessoais que seus funcionários compartilham online. Em média, 50% das empresas bloqueiam o acesso às redes sociais analisadas – Facebook, LinkedIn, MySpace e Twitter. A segunda maior preocupação em relação aos sites é a perda de produtividade durante o expediente. Mas existem outros riscos, como roubo de informações estratégicas.

“As empresas mais conservadoras como bancos acabam se protegendo e fecham o acesso. É muito comum em alguns bancos não ser permitido nem o acesso ao linkedin”, observa Paulo Prado, gerente de marketing de produto da Symantec para a América Latina.



SANDRA TURCHI,  
SUPERINTENDENTE  
DE MARKETING  
DA ACSP

**PREVENÇÃO.** Diante do crescimento no número de usuários que usam as ferramentas sociais seja para fins corporativos ou pessoais, a política de segurança nas empresas leva a TI a tomar duas atitudes: bloquear o acesso às ferramentas ou utilizar meios de proteger a infraestrutura da empresa com ações de conscientização e monitoramento constante da rede. Em ambientes em que os sites são importantes para o trabalho, o bloqueio não é uma opção. Resta seguir à risca as melhores práticas da segurança e implantar uma cultura entre os usuários.

“A primeira providência que a empresa deve tomar é ter uma norma sobre qual o tipo de site de rede social pode ser acessado pelos funcionários e a sua finalidade. A segunda medida é treinamento, Isso significa não clicar em URLs duvidosas, baixar jogos ou sites que tenham um conteúdo de convite para comparecer em um órgão ou estabelecimento comercial por problemas com cartão de crédito, por exemplo. É fácil ser enganado no twitter, por exemplo, onde ocorre os maiores índices de envio de códigos maliciosos”, orienta Marcus Moraes, VP da Arcon.

Segundo Moraes, outra maneira de proteger os dados empresariais é ter filtros de conteúdo e de URL, capazes de apontar se aquela informação recebida é um site de baixa reputação ou duvidosa. Prado, da Symantec, reforça que as companhias que optam em abrir um canal de comunicação por meio de redes sociais devem manter essas soluções constantemente atualizadas. “Além disso, é preciso obrigar o uso de senha forte, fazer com que esses microlinks do twitter, por exemplo, sejam avaliados pela área usuária em conjunto com a Segurança”, recomenda Prado.

## As teias sociais no comércio

A ASSOCIAÇÃO COMERCIAL DE SÃO PAULO INAUGURA A ERA DIGITAL DE COMUNICAÇÃO COM BOAS PRÁTICAS DE SEGURANÇA

**E**star presente no mundo online é fundamental para proporcionar a exposição rápida de informações, expandir negócios e conquistar novos espaços. Considerando essas premissas, a Associação Comercial de São Paulo (ACSP), nos últimos meses, investiu fortemente em sua presença digital nas mais variadas redes sociais, além de sites de compartilhamento de dados.

Blog, Twitter, Slideshare, Flickr e Web Forum. Esse é o arsenal de relacionamento lançado pela ACSP (Associação Comercial de São Paulo). As ferramentas são monitoradas e gerenciadas pelas áreas de marketing e comunicação da entidade. Esse é o primeiro ponto para a administração do conteúdo e cuidado de a oportunidade de disseminar e divulgar a marca não vire um risco.

A instituição pretende disseminar informações sobre as suas principais frentes de trabalho. Isso pode ser realizado pela representação dos empresários de todos os setores ou portes e por meio de seu principal produto: Serviço Central de Proteção de Crédito (SCPC), que apresenta o maior banco de dados

de pessoas e empresas do País. Com isso, os usuários das redes sociais poderão acessar em tempo real as principais notícias da ACSP e do SCPC, as novidades de produtos e serviços, os últimos lançamentos e a promoção dos eventos.

Segundo Sandra Turchi, superintendente de Marketing da ACSP, a concepção do projeto se vale de publicar apenas informações que não sejam sigilosas e estratégicas. Não dá para colocar o banco de dados da ACSP na nuvem porque é um risco deixar em cloud aquilo que é estratégico.

Mesmo com todos os cuidados praticados, a executiva diz ainda que a Associação também utiliza o protocolo de segurança denominado Secure Privece, responsável pelos dados do Sistema de Proteção ao Crédito (SPC). “As empresas devem avaliar o que é possível abrir para fora e, ainda assim, analisar muito bem os níveis de serviços dos fornecedores, quem está oferecendo ferramentas que mostrem maior segurança”, aponta Sandra.

O webforum foi criado para levar conhecimento principalmente no tocante ao e-commerce e disseminar informações sobre as compras na internet. Em parceria com a Câmara enet, A Associação tem levado conhecimento e apresentado possibilidades de parcerias para que os empresários adquiram elementos críticos sobre os assuntos abordados. “A partir do cadastro deles em nosso portal, receberão informações sobre políticas de segurança no e-commerce, por exemplo. Também atuamos com serviços de utilidade pública com os consumidores finais, por causa do SPC, levando conteúdo sobre educação financeira”, explica Sandra. ■

**ENDEREÇOS WEB** em que os internautas podem conferir as novidades ACSP são:

- ▶ **Blog (diário virtual):**  
[www.acsp.com.br/blog](http://www.acsp.com.br/blog)
- ▶ **Slideshare (site de compartilhamento de arquivos):**  
[www.slideshare.net/acspdigital](http://www.slideshare.net/acspdigital)
- ▶ **YouTube (vídeos):**  
[www.youtube.com/acspdigital](http://www.youtube.com/acspdigital)
- ▶ **Flickr (galeria de fotos):**  
[www.flickr.com/acspdigital](http://www.flickr.com/acspdigital)
- ▶ **Twitter (novidades em tempo real):**  
[www.twitter.com/acspdigital](http://www.twitter.com/acspdigital)
- ▶ **Webforum de e-commerce para PMEs:**  
[www.acsp.com.br/e-commerce](http://www.acsp.com.br/e-commerce)



## Segurança na palma da mão

O USO DE DISPOSITIVOS MÓVEIS NOS AMBIENTES CORPORATIVOS AVANÇAM NA MESMA VELOCIDADE EM QUE AUMENTAM AS VULNERABILIDADES. DECISION REPORT MEETING DEBATE A QUESTÃO POR PAULA ZAIDAN

Cada vez mais as empresas optam por dispositivos móveis para comunicação, acesso às informações estratégicas e transacionais, a exemplo de CRM e força de vendas. Na contramão, o risco de roubo de dados confidenciais aumenta numa proporção maior que o crescimento do mercado, seja porque os aparelhos ainda possuem baixo grau de proteção, dificuldade de gerenciamento e treinamento das equipes. “Recentemente avaliamos que muitas empresas não consideram o uso desses dispositivos em suas políticas de segurança”, revela Célia Sarauza, consultora da IDC Brasil.

Somente no primeiro semestre de 2008, foram vendidos mais

smartphones do que no ano inteiro de 2007, totalizando 1,3 milhão de equipamentos vendidos no País nos primeiros seis meses do ano passado. Segundo Vinícius Caetano, analista sênior de Telecomunicações da IDC Brasil, esse número continuará crescendo porque as pessoas que estão substituindo os telefones celulares preferem os smartphones e, recentemente, os iPhones.

“A segurança será sempre uma briga de gato e rato. O fato é que nenhuma empresa deixará de investir em mobilidade por conta da insegurança da informação”, reflete Paulo Biamino, gerente de informática da Kimberly-Clark. Entretanto, não será um impeditivo para a evolução da mobilidade,

## O QUE ELES DIZEM

### **GISELE TRUZZI, advogada especialista em crimes digitais da PPP Advogados**

*"Independente de onde o profissional praticante de pedofilia esteja, se ele usar um dispositivo móvel da companhia, juridicamente o acesso de armazenamento de dados é de responsabilidade dela. E será penalizada caso não encontre quem usou um de seus ativos para atos criminosos".*

### **MANUEL BARBOSA, CSO do Banco Standard de Investimentos**

*"Temos uma disciplina de gerenciamento de risco, mas qual o impacto que causa a vulnerabilidade? Isso deve ser levado à área de negócio?"*

**SOB CONTROLE?** Em setembro, a IDC e a Accenture divulgaram um estudo sobre a maturidade da infraestrutura das 150 maiores organizações do País. A pesquisa baseou-se nas melhores práticas de TI, das quais a biblioteca ITIL foi a espinha dorsal da análise, além de metodologias como COBIT. Foram 54 questões que pontuavam o quão maduro está o País conforme níveis entre 1 a 5.

De acordo com a pesquisa, uma das menores pontuações foi a Segurança da Informação. Isso significa que ainda estamos engatinhando porque os brasileiros são bons para implementar políticas de segurança, mas não controlam. Pior. Célia comenta que o instituto também tem realizado outros levantamentos e algumas empresas não consideram os dispositivos móveis em suas políticas de segurança.

"Aproximadamente 50% das organizações estão em adaptação ao mundo móvel. Além de garantir que a infraestrutura física (desktops, servidores e rede) da empresa esteja segura, a companhia deve levar em consideração que o funcionário está fora da empresa e precisa seguir as mesmas regras de quando está dentro dela", enfatiza a consultora da IDC.

Victor Murad, presidente da Prodest, compartilha da mesma reflexão da IDC. "Acessamos o nosso webmail de qualquer lugar, mas não nos preocupamos se vamos abrir uma conexão segura". Entretanto, César Cadota, diretor de Segurança da Net Serviços, defende um meio termo. "A Net possui algumas aplicações por meio de celular para facilitar a instalação do Virtua. Para tanto, muitas foram as questões abordadas pela área usuária: qual o celular, qual o dispositivo adotado que tornasse a comunicação segura, quanto isso aumentará o valor do projeto?"

como soluções de Prontuário Eletrônico e o e-payment.

Diante desse cenário de explosão no uso de dispositivos móveis, outros dois aspectos devem ser considerados especialmente em 2009 para o crescimento desse mercado. A crise financeira global e a gripe suína aceleraram o processo de trabalho remoto. Como controlar aquilo que você não vê? Esse foi o tema abordado no debate "Mobilidade Segura", promovido pela Conteúdo Editorial, em agosto, com a participação de CIOs e CFOs de diferentes setores do mercado.

Renato Opice Blum, advogado especialista em crimes digitais, afirma que é importante desenvolver nas pessoas boas práticas de segurança e fazer com que os usuários sigam as regras corporativas do uso da informação seja no ambiente empresarial ou fora dele.

"Ainda assim não é possível garantir o acesso seguro dos dados. Hoje é possível encontrar esses equipamentos em acessórios de uso pessoal, como relógios de pulso, com chips e USB embutido. Quem pode detectar isso durante uma visita na minha empresa?", indaga Célia quando, durante o debate, refere-se ao relógio de pulso de Fábio Leto, presidente da Abrasinfo.

Por isso, Carlos Eduardo da Fonseca, consultor de TI, conhecido como Karman, acredita que a vulnerabilidade não impedirá o avanço da mobilidade corporativa. Para ele, segurança é uma corrida permanente. De um lado, as empresas querem se proteger e do outro, hackers querem invadir. “É importante ter a consciência do cenário atual. Existe uma postura um pouco promíscua porque quando se trata de mobilidade, a primeira coisa que visualizamos é o celular. Contudo, esses equipamentos aumentam cada vez mais o poder computacional a ponto de armazenar mais informações e operar como um computador”.

“Portanto, a Segurança da Informação não é um entrave, mas algo que deve ser considerado. O problema da interoperabilidade vem antes da segurança. A sociedade brasileira e a global usará a TI em alta escala e considerará os entraves

qual o impacto que causa a vulnerabilidade? Isso deve ser levado à área de negócio?”, indaga. “Pode ser que o custo que a empresa pagará na compra daquela solução de segurança não cubra o prejuízo do vazamento de informação”, reflete.

Erlen Ângelo Abatayguara, gerente de TI da Tejofran de Saneamento e Serviços Ltda, confessa ser paranóico. Mas faz um contraponto com Barbosa quando acredita ser da responsabilidade da TI estar alinhada com o negócio. “As áreas usuárias precisam de uma solução, mas nem sempre a tecnologia é consultada, o que pode acarretar em riscos de segurança. É como se uma empresa resolvesse abrir uma nova filial e não se preocupasse com uma área jurídica”.

Mesmo frente a um cotidiano paranóico, de olho no roubo da informação corporativa, os CSOs e CIOs enfrentam desafios dentro de casa: a prática da pedofilia. Os criminosos di-



DA ESQUERDA PARA A DIREITA: CÉSAR CADOTA, DIRETOR DE SEGURANÇA DA NET SERVIÇOS; GISELE TRUZZI, ADVOGADA ESPECIALISTA EM CRIMES DIGITAIS DA PPP ADVOGADOS; MARCELO NORONHA, GERENTE MÉDICO DA HOME DOCTOR; E RENATO MARTINI, DIRETOR PRESIDENTE DO ITI

de segurança. Sempre haverá fraudadores e reagiremos contra o crime digital”, complementa Renato Martini, diretor presidente do ITI.

Marcelo Noronha, gerente médico da Home Doctor, analisa a Segurança da Informação como a descoberta de um novo vírus na medicina. “Ele sofre mutação constante, as vacinas são produzidas sempre depois da sua aparição. Quando o paciente é diagnosticado com gripe suína ele tomará o remédio. Porém, se houver os cuidados necessários com a higiene, ele consegue prevenir a infecção”, observa.

**DIREITOS E DEVERES, QUAL O LIMITE DO MOBILE?** Se por um lado, as empresas escrevem as suas políticas de segurança e ainda não as controlam, elas gerenciam o ambiente de segurança com uma certa dose de paranóia. Entretanto, Manuel Barbosa, CSO do banco Standard de Investimento, avalia que o executivo de Segurança acaba tomando decisões que nem sempre são de sua responsabilidade nem da TI.

“Temos uma disciplina de gerenciamento de risco, mas

giciais continuam empenhados na criação de grandes teias de bandidos por trás de máquinas e com um arsenal tecnológico. Entretanto, os pedófilos encontraram na internet um meio de praticar o ato e isso pode acontecer dentro das empresas.

Por isso, Gisele Truzzi, advogada especialista em crimes digitais da PPP Advogados, alerta: “independente de onde o profissional praticante de pedofilia esteja, se ele usar um dispositivo móvel da companhia, juridicamente o acesso de armazenamento de dados é de responsabilidade dela. E será penalizada caso não encontre quem usou um de seus ativos para atos criminosos”.

Gisele ilustra ainda com outro exemplo, envolvendo uma cadeia de responsáveis por práticas ilícitas na internet que comprometem a imagem corporativa. “Estamos desenvolvendo um trabalho de mobile banking para uma instituição financeira em que a agência não será física. A sua operação será em cloud computing. Se a transação bancária ocorre por dispositivos móveis, as empresas de telefonia também serão penalizadas”. ■