SEÇÃO INTERATIVA: TECNOLOGIA Quão segura é a nuvem?

A empresa de investimentos bancários e serviços financeiros Cowen and Co., com sede em Nova York, transferiu seus sistemas de vendas para a nuvem por meio da Salesforce.com. Até agora, Daniel Flax, CIO da empresa, está satisfeito. A utilização de serviços da nuvem ajudou a Cowen a diminuir os gastos iniciais com tecnologia, diminuir o *downtime*, e oferecer serviços adicionais. Contudo, ele está tentando lidar com as questões de segurança. A segurança na computação em nuvem é, de fato, turva, e essa falta de transparência é preocupante para muitos. Um dos maiores riscos da computação em nuvem é que ela é altamente distribuída. Aplicações da nuvem e combinações de aplicações residem em bibliotecas virtuais de grandes centros de dados remotos e em fazendas de servidores que oferecem serviços empresariais e gestão de dados para diversos clientes corporativos. Para economizar dinheiro e manter os custos baixos, os provedores de computação em nuvem costumam distribuir o trabalho por centros de dados ao redor do mundo onde o trabalho pode ser executado de modo mais eficiente. Quando você usa a nuvem, pode não saber ao certo onde seus dados estão hospedados, nem sequer saber o país onde eles estão armazenados.

A natureza dispersa da computação em nuvem dificulta o rastreamento de atividades não autorizadas. Quase todos os provedores de nuvem utilizam criptografia como SSL (*secure sockets layer*) para proteger os dados que gerenciam enquanto são transmitidos. Mas, se os dados estão armazenados em dispositivos que também guardam arquivos de outras empresas, é importante garantir que esses dados também são criptografados.

Indian Harvest Specialtifoods, uma empresa de Bemidji, Minnesota, que distribui arroz, grãos e legumes para restaurantes de todo o mundo, utiliza o provedor de software para nuvem NetSuite a fim de garantir que seus dados enviados à nuvem estejam totalmente protegidos. Mike Mullin, diretor de TI da empresa, diz que utilizar SSL para criptografar os dados lhe confere certo nível de certeza de que os dados estão seguros. Ele também observa que sua empresa e outros usuários dos serviços da nuvem precisam estar atentos a suas próprias práticas de segurança, em especial aos controles de acesso. "Seu lado da infraestrutura é tão vulnerável, senão mais, quanto o lado do provedor", comenta ele.

Uma maneira de lidar com esses problemas é usar um fornecedor de nuvem que seja uma empresa pública, obrigada por lei a informar como gerencia as informações. A Salesforce.com é uma empresa desse tipo, com processos e diretrizes estritos para a gestão de seus centros de dados. "Sabemos que nossos arquivos estão nos Estados Unidos e sabemos exatamente em qual centro de dados estão localizados", diz Flax.

Outra alternativa é utilizar um provedor de nuvem que ofereça aos assinantes a possibilidade de escolher onde será realizado o trabalho de computação em nuvem. Terremark Worldwide Inc., por exemplo, oferece a um de seus assinantes, a Agora Games, a opção de escolher onde suas aplicações vão funcionar. A Terremark possui instalações em Miami, mas está abrindo outras unidades. No passado, a Agora não tinha como escolher onde a Terremark hospedaria suas aplicações e seus dados.

Mesmo que seus dados estejam totalmente seguros na nuvem, pode ser que você não consiga provar. Alguns provedores de nuvem não atendem aos atuais requisitos de conformidade relacionados à segurança, e alguns desses provedores, como a Amazon, já afirmaram que não pretendem seguir essas regras e não irão permitir auditorias locais.

Existem regras que restringem onde as empresas podem enviar e armazenar alguns tipos de informação — informações pessoalmente identificáveis na União Europeia, trabalho do governo nos Estados Unidos, ou aplicações que utilizem determinados algoritmos de criptografia. Seja nos Estados Unidos ou na União Europeia, as empresas das quais se exige o cumprimento dessas regras relacionadas à proteção de dados não poderão utilizar provedores públicos de nuvem.

Algumas dessas regras exigem provas de que os sistemas são gerenciados de modo seguro, o que pode demandar confirmação por parte de uma auditoria independente. É possível que os grandes provedores de nuvem não permitam que auditores de outra empresa inspecionem seus centros de dados. A Microsoft encontrou uma maneira interessante de lidar com esse problema. A empresa reduziu 26 tipos diferentes de auditoria a uma lista de 200 controles necessários para cumprimento dos padrões de conformidade aplicados aos ambientes e serviços de seus centros de dados. A Microsoft não permite o acesso de todos os clientes ou auditores aos centros de dados, mas sua estrutura de conformidade permite que auditores selecionem testes a partir de uma lista e recebam seus resultados.

As empresas esperam que seus sistemas funcionem em tempo integral, mas os provedores de nuvem nem sempre conseguem oferecer esse nível de serviço. Milhões de consumidores da Salesforce.com sofreram 38 minutos de pane no início de janeiro de 2009 e outras paradas alguns anos antes. A parada de janeiro de 2009 impediu que mais de 900 mil assinantes acessassem aplicações e dados cruciais para transações empresariais com seus clientes. Usuários dos serviços de nuvem da Amazon vivenciaram inúmeras quedas em 2008. (Em julho de 2008, o serviço ficou interrompido por oito horas.)

Acordos para serviços como o Amazon EC2 e o Microsoft Azure definem que essas empresas não podem ser responsabilizadas por perdas de dados, multas ou outras penalidades legais quando as empresas usam seus serviços. Ambos os fornecedores oferecem instruções sobre como usar suas plataformas de nuvem de modo seguro, e ainda podem proteger seus dados de maneira mais segura do que as instalações locais.

A Salesforce.com vem construindo e replanejando sua infraestrutura para garantir serviços melhores. A empresa investiu 50 milhões de dólares na tecnologia Mirrorforce, um sistema de espelhamento que cria um banco de dados duplicado em um local separado e sincroniza instantaneamente os dados. Se um banco de dados não estiver disponível, o outro assume seu lugar. A Salesforce.com abriu dois novos centros de dados nas Costas Leste e Oeste, além de suas instalações no Vale do Silício. A empresa distribuiu por esses centros o processamento de seus grandes clientes de modo a balancear a carga de seu banco de dados.

Fontes: John Edwards, "Cutting Through the Fog of Cloud Security". *Computerworld*, 23 fev. 2009; Wayne Rash, "Is Cloud Computing Secure? Prove It". *eWeek*, 21 set. 2009; Robert Lemos, "Five Lessons from Microsoft on Cloud Security". *Computerworld*, 25 ago. 2009; Mike Fratto, "Cloud Control". *Information Week*, 26 jan. 2009.

PERGUNTAS SOBRE O ESTUDO DE CASO

1. Que problemas de segurança e controle são descritos neste caso?
2. Que fatores pessoais, organizacionais e tecnológicos contribuem para esse problema?
3. Quão segura é a computação em nuvem? Explique.
4. Se fosse responsável pelo departamento de sistemas de informação de uma empresa, quais pontos gostaria de esclarecer com os possíveis fornecedores?
5. Você confiaria seus sistemas corporativos a um provedor de computação em nuvem? Justifique.

Seção Interativa sobre tecnologia detalha algumas questões de segurança da nuvem que devem ser consideradas.

Usuários da nuvem precisam confirmar que, independentemente do local onde seus dados estejam armazenados ou para onde sejam transferidos, eles estão protegidos em um nível que atende a seus requisitos corporativos. É preciso exigir que o provedor da nuvem armazene e processe os dados em jurisdições específicas segundo as regras de privacidade da jurisdição em questão. Clientes da nuvem devem descobrir como o provedor separa os dados de sua empresa dos arquivos das outras e solicitar provas de que o mecanismo de criptografia é seguro. É importante também saber como o provedor da nuvem responde em caso de desastre: se consegue restaurar completamente os dados e quanto tempo essa operação leva. Usuários da nuvem devem questionar ainda se os provedores da nuvem são submetidos a auditorias externas e certificações de segurança. Esses tipos de controle podem ser escritos no acordo de nível de serviços (*service legal agreement* — SLA) antes de contratar um provedor de nuvem.

Segurança em plataformas móveis

Malwares direcionados a dispositivos móveis não são tão comuns quanto aqueles direcionados a computadores, mas, ainda assim, estão se espalhando através de e-mail, mensagens de texto, Bluetooth e cópias de arquivos da Web por meio de redes sem fio ou celulares. Se os dispositivos móveis estão executando muitas das funções dos PCs, precisam, como os desktops e laptops, estar seguros contra *malware*, roubo, perda acidental, acesso não autorizado e tentativas de invasão. Dispositivos móveis que acessem sistemas e dados corporativos demandam proteção especial.

As empresas devem se certificar de que sua política de segurança corporativa inclui os dispositivos móveis, com detalhes adicionais sobre como esses dispositivos devem receber suporte e proteção e de que modo devem ser utilizados. As diretrizes devem estipular softwares e procedimentos necessários ao acesso remoto de sistemas corporativos. Por enquanto, a segurança dos *smartphones* não está tão bem desenvolvida quanto a dos dispositivos maiores. Esses dispositivos podem não conseguir proteger integralmente informações sensíveis, em especial os dados transmitidos via anexos de e-mail e aqueles armazenados localmente nos dispositivos.

Garantia da qualidade de software

Além de implantar segurança e controle eficientes, as empresas podem melhorar a qualidade e a confiabilidade dos sistemas através de métricas e testes rigorosos de software.