**Computação em nuvem: os desafios de segurança**

*Gestores de TI contam como acreditam que as empresas devem lidar com os riscos inerentes ao modelo de cloud computing e quais as possíveis alternativas*.

Ao considerar os custos que implicam na manutenção da infraestrutura de hardware e software no ambiente corporativo, a ideia de adotar a computação em nuvem (cloud computing) e arcar apenas com os custos de um provedor desse tipo de serviço parece ótima. Entregar tudo a um terceiro, não precisar de uma equipe para gerenciar data centers e ter todos os serviços entregues por meio da web é, sem dúvida, o sonho de muitos gestores de TI. No entanto, quando acordam, esses executivos são obrigados a encarar a principal barreira do modelo de cloud computing: a segurança dos dados armazenados e transacionados.

Como em todo novo serviço de tecnologia, o número de facilidades é proporcional aos problemas. No caso de cloud computing, grande parte das dúvidas dizem respeito à proteção das informações armazenadas na nuvem. Baseado nesse cenário, seguem as opiniões de alguns gestores de TI sobre como as companhias devem lidar com a segurança nesse novo ambiente.

Matt Schneider, consultor e arquiteto de redes da fabricante de veículos automotores Ford Motor Company

“Atualmente estamos desenvolvendo um aplicativo web para hospedar ferramentas de segurança que garantam mais proteção aos dados movimentados por e-mail, chats, plataformas internas de colaboração. A ideia é criptografar todas as informações e exigir senhas de acesso, de acordo com os níveis de importância de cada dado transacionado.

Ainda estou fazendo contatos com colegas que já implementaram projetos de segurança na nuvem, mas ainda não tenho pleno conhecimento da área. Entretanto, penso que alguns conceitos já conhecidos de todos devem ser aplicados nessa situação. Seria muito irresponsável apenas dizer que estou fazendo todo o possível para garantir a segurança de meus usuários sem que eles também tivessem consciência das ameaças às quais estão expostos.

Grande parte da população mundial utiliza a internet como data center e armazena ali – no Gmail, Facebook, Orkut, LinkedIn, Twitter – informações pessoais e profissionais de grande valor. Essas pessoas correm os mesmos, ou mais, riscos do que uma empresa que aposta em cloud computing. No entanto, as companhias sabem dos problemas que podem estar assumindo e devem calcular se os benefícios obtidos com a tecnologia em questão superam as ameaças.

Eu mesmo uso o cartão de crédito milhares de vezes na internet e sei que algum hacker pode burlar o sistema de segurança dos sites de bancos e das lojas. Porém, o benefício de comprar online é tão maior do que os possíveis estragos que aconteceriam no caso de um incidente, que continuarei com a mesma postura.

É óbvio que há questões legais que precisam ser definidas com fornecedores no que diz respeito à custódia de dados e ferramentas de proteção, mas, assim como qualquer outra plataforma, o modelo de cloud computing oferece riscos e vantagens. Cabe a cada um tentar equilibrar essa equação da melhor maneira.”

Michael Versace, consultor de segurança da comunidade global que reúne especialistas e pesquisadores dedicados a melhorar a relação entre TI e negócios, The Wikibon Project: “Algumas pessoas estão fazendo os modelos de proteção em cloud computing parecerem mais complexos do que realmente são. Naturalmente baseada em riscos, a segurança da informação é uma disciplina que envolve ameaças.

O papel dos gestores de TI é mitigar ao máximo os perigos desse padrão, de modo a torná-lo viável ao negócio. Na prática, isso significa que os CIOs devem criar políticas de proteção consistentes o bastante para tornar viável, operacional e financeiramente, a adoção da computação em nuvem.

George Moraetes, consultor da organização que promove discussão sobre os temas de segurança em TI entre clientes e fornecedores Cyber Warfare: “Cloud computing é, nada mais, do que uma terceirização de data center a provedores terceirizados e, como todos os outros modelos da mesma natureza, não é infalível e 100% seguro.

As principais questões de segurança na computação em nuvem devem, portanto, girar em torno das práticas para garantir que os fornecedores cumpram os requisitos necessários à proteção dos dados de clientes.

É preciso avaliar a credibilidade do parceiro e definir contratualmente questões como a custódia dos dados em caso de quebra de contrato, cumprimento das normas regulatórias vigentes no segmento de atuação da empresa contratante e onde as informações ficarão armazenadas – no mesmo país da matriz da companhia ou em outros. Neste último caso, é preciso estar ciente das leis que regem tal nação também.

Se os dados forem de uma empresa norte-americana, por exemplo, e armazenados em países “não-amigo” dos Estados Unidos, é possível que fiquem mais expostos a riscos que não existiriam se estivessem hospedados em território estadunidense.”

Venkatesh Ravindran, gestor de segurança da empresa de investimentos KVH: “Como sabemos, a segurança da informação é composta fundamentalmente por disponibilidade, integridade e confidencialidade dos dados.

Assim, o modelo de cloud computing precisa de ferramentas que garantam esses três quesitos a suas operações e isso se dá por meio de controle de perímetros (monitoramente do que entra e sai do sistema em nuvem), blindagem dos meios de comunicação utilizados para contatos entre cliente e fornecedor (e-mail, ligações telefônicas, conversas por meio de comunicadores instantâneos), integração da plataforma de segurança do parceiro à do contratante, bloqueios de acesso e movimentação de dados sigilosos e cumprimento de normas regulatórias.”

COMPUTAÇÃO em nuvem: os desafios de segurança. **CIO**. São Paulo, out. 2009. Disponível em: <http://cio.uol.com.br>. Acesso em 16 out. 2009.