Como proteger o e-mail corporativo na nuvem?
Patricia Peck

Definir uma estratégia de migração para o correio eletrônico exige cuidados. O modelo de cloud usado deve estar em conformidade legal com as regras do país de origem do conteúdo.

Um assunto que deve ser bastante discutido em um futuro próximo é a questão do uso do correio eletrônico em nuvem, a famosa cloud computing. Por ser este um tema ainda muito novo, não há um posicionamento específico do judiciário brasileiro quanto aos contratos de cloud computing, bem como sobre os aspectos de discussão de territorialidade.

O uso da "nuvem" significa a aplicação de um modelo de disponibilização de softwares e de infraestruturas de processamento e armazenamento de dados através de uma rede (internet). O princípio da nuvem é de virtualização total e de máxima disponibilidade dos dados, onde é irrelevante o local de acesso e o dispositivo utilizado. Ou seja, um princípio que desafia o modelo jurídico atual, ainda baseado em fronteiras físicas.

Considerando que a nuvem pressupõe um mundo sem barreiras, mas que apesar de plano e globalizado ainda é extremamente local - no sentido da legislação de cada país e da própria soberania dos Estados -, há elevada preocupação no tocante a segurança da informação e a eventual indisponibilidade do serviço que impeça acesso aos dados, bem como infração a leis específicas de proteção de dados sensíveis ou sigilosos, dependendo do tipo de informação e dos países envolvidos (país do prestador de serviço, país do contratante detentor das informações, país da origem dos dados das pessoas ou empresas).

Já há uma oferta de quatro modelos de "nuvem". A nuvem privada é de propriedade exclusiva de uma empresa, para uso próprio, que detém seu controle e suporta seus custos de infra-estrutura. Já a nuvem pública é a mais conhecida pelo custo baixíssimo e grande parte dos serviços e aplicações da web estão baseados nela, de caixa postal, de e-mail gratuito a redes sociais. A nuvem comunitária envolve um conjunto de empresas que se conhecem e se reúnem para compartilhar os custos de infra-estrutura, tem sido bem comum em alguns mercados ou mesmo em grupo de empresas. E o último formato, que é a da nuvem híbrida, faz uso de um ou mais modelos, diferenciando o tipo de nuvem conforme o grau de segurança necessário a aplicar aos dados e às exigências legais relacionadas aos mesmos.

O mercado

A computação em nuvem é tida como a solução de TI para o século 21. De acordo com o estudo do Carbon Disclosure Project, as companhias americanas planejam acelerar a adoção de computação em nuvem de 10% para 69% de seus gastos com TI até 2020, visando reduzir seu consumo de energia, diminuir suas emissões de carbono e seus investimentos em recursos de TI, além de aumentar a eficiência operacional.

Entre todos os países da América Latina, o Brasil é o líder no uso de Cloud Computing, de acordo com o estudo realizado pela consultoria IDC. Cerca de 18% das médias e grandes empresas já utilizam alguma forma de cloud e a expectativa é que em 2013 o número salte de 30% para 35%. Além disso, há pesquisa recente realizada pela revista COMPUTERWORLD, que aponta que o principal modelo de nuvem adotado pelas empresas tem sido o de nuvem privada 60,6%.

Porém, como todas as demais ferramentas tecnológicas, a computação em nuvem além de benefícios, também apresenta riscos e sua aplicação deve ser analisada no caso a caso, principalmente em relação à proteção das informações e dados que irão transitar e ser armazenados em uma infraestrutura totalmente externa. Esta análise de riscos deve envolver o aspecto jurídico do uso do serviço de cloud computing, visto que há que se observar leis vigentes do país de origem dos dados (não apenas da empresa que os detém, mas dos clientes também) e dos países em que os mesmos serão armazenados ou disponibilizados.

O e-mail na nuvem

Uma das principais razões para se pensar em e-mail na nuvem é a significativa economia de escala obtida com esse modelo computacional. A maioria das corporações não tem mais que centenas ou milhares de usuários, enquanto um provedor de nuvem pode fornecer esses serviços para dezenas de milhões de usuários, a custos bem menores – podendo chegar, no limite, a zero. Além disso, devido a restrições orçamentárias, o e-mail interno às organizações não disponibiliza grande capacidade de armazenamento. É comum um e-mail interno ser restrito a 500 MB por usuário, enquanto um e-mail na nuvem oferta 30 GB. O custo por GB na nuvem é bem menor pela economia de escala ofertada e, logo, o provedor pode oferecer, com custo mínimo, maior capacidade de armazenamento.

Entretanto, definir uma estratégia de migração para e-mail na nuvem exige cuidados. No aspecto legal, o modelo de nuvem a ser utilizado precisa estar em conformidade legal com as regras do país de origem do conteúdo (empresa contratante). Há empresas que preferem que os dados estejam mais facilmente acessíveis no local onde podem precisar atender a solicitações de autoridade, fiscalização e/ou auditoria. Há outras que por uma questão de gestão de risco do próprio negócio preferem o oposto, ou seja, deixar os dados em um país distinto do país sob o qual recaem suas obrigações legais para evitar que ações de busca e apreensão ou outras medidas até mesmo políticas possam acessar facilmente as informações da empresa.

Logo, a análise da questão territorial é relativa, depende muito de como está o modelo de governança da empresa. Pode tanto ser positivo como negativo ter os dados em outro país, dependendo da estratégia de gestão adotada pela empresa. No entanto, um ponto é inquestionável (a proteção dos dados perante o acesso de terceiros não autorizados). Ou seja, o uso de nuvem para finalidade corporativa não pode trazer a prerrogativa ou o direito para o fornecedor também ver e utilizar a informação que está colocada em sua nuvem.

No Brasil, a Constituição Federal e os demais diplomas legais são genéricos ao tratar de privacidade e intimidade dos dados dos cidadãos e pessoas jurídicas, cabendo ao entendimento doutrinário, jurisprudencial ou alguma lei específica cuidar da abrangência de proteção aos dados que são considerados privados.

Portanto, deve-se ficar muito atento aos termos de uso e contratos antes de aderir a uma solução de correio eletrônico na nuvem, principalmente, para não expor indevidamente informações classificadas, que venham a transitar, desprotegidas, no e-mail em nuvem.

O contratante precisa ter certeza de que o provedor de e-mail em nuvem suporta suas necessidades e fornece garantias e mecanismos de controle de segurança, de acordo com a dinâmica exigida pelo ambiente em nuvem. Logo, antes de se adotar o correio eletrônico na nuvem, é preciso levar em conta os custos ocultos, as questões legais, as contratuais e seguir diversas recomendações, inclusive as de segurança.

Cuidados

Para que isso ocorra, os seguintes aspectos e melhores práticas devem ser observadas:

- Definir o tipo de nuvem a ser utilizado que melhor atenda aos aspectos de segurança da informação (em geral as empresas têm adotado modelo privado ou híbrido);

- Definir a limitação territorial da nuvem e quais países há maior colaboração do ponto de vista legal (tem sido restrito o uso de nuvem global, em geral tem sido exigida a nuvem no Brasil, visto que mesmo a nuvem nos EUA pode trazer um acesso mais fácil a informação por parte de autoridade estrangeira, e tem se evitado o uso de nuvem em países como China e Irã);

- Escolher bem o fornecedor da solução que já atenda outros clientes com o mesmo tipo de requisitos e exigências (em geral os serviços gratuitos não atendem os requisitos de segurança da informação necessários);

- Elaborar um contrato blindado (evitar mera tradução de minutas em idioma estrangeiro, deve estar aderente com as leis do país de origem do conteúdo, no caso, o Brasil), com SLA detalhado e Plano de Contingência e Continuidade (considerando cenário de apagão digital);

- Fazer uso de autenticação forte e criptografia de dados;

- Criar uma campanha de conscientização das equipes antes da implementação da solução para orientação sobre uso de criptografia e outros cuidados essenciais para uso de nuvem segura;

- Fazer a monitoração permanente da nuvem e da internet em geral para identificação rápida de incidentes.

Fonte: CIO online, 27 de mar. 2012: [Portal]. Disponível em: < http://cio.uol.com.br >. Acesso em 28 de mar. 2012.