JACKELINE CARVALHO

# Segurança em cloud: uma eterna incerteza

Especialistas ensinam como proteger informações críticas hospedadas na nuvem e são unânimes ao dizer que não há ferramenta que garanta um ambiente 100% seguro, principalmente em se falando de cloud computing

"Vai demorar algum tempo até que consigamos convergir segurança e sensação de segurança na computação em nuvem. Estamos vivendo um processo semelhante ao que ocorreu com os bancos, à época de lançamento dos internet banking"
**SILVIO MAEMURA, DA HP**

A computação em nuvem está entre as práticas mais requisitadas ou estudadas pelos gestores de TI. Porém, estatísticas dão conta de que a segurança ainda emperra a decisão de migrar informações críticas para este ambiente, principalmente quando estão em pauta dados de grandes corporações. Especialistas em segurança indicam alternativas para ter um sono tranqüilo com os dados em cloud.

Muitas organizações no mundo estão falando em migrar para a nuvem, sendo que 75% a 81 % (77% a 82% na América Latina), pelo menos, estão discutindo todas as formas de nuvem, segundo levantamento divulgado pela Symantec no final de 2011.

No entanto, poucos migraram totalmente para a nuvem. Menos de 20% no mundo, e 25% na América Latina, relataram ter concluído a implementação de ao menos uma das áreas de foco da nuvem abrangidas pela pesquisa. Cerca de uma em cada quatro organizações no mundo e na região está atualmente em fase de implementação. Entre 40% e 43% dos entrevistados globais, e metade na América Latina, ainda estão em fase de discussões iniciais, testes, e entre 18% e 23% não consideram a migração para a nuvem de forma alguma.

FOTOS: DIVULGAÇÃO

Esse último grupo pode-se interpretar predominantemente composto por grandes corporações, montante mais resistente à computação em nuvem por questões de segurança e de compliance, principalmente. O levantamento sobre a Situação de Cloud Computing também revelou que as corporações têm visões variadas em relação a segurança na computação em nuvem, sendo este quesito a maior

preocupação dos entrevistados.

A pesquisa reúne 5.300 respostas de 38 países, traz resultados de 500 empresas da América Latina, sendo 150 brasileiras, e aborda as várias formas de computação em nuvem, incluindo software como serviço público e privado, infraestrutura ou plataforma como serviço híbrido, bem como infraestrutura ou plataforma como serviço público e privado.

Segundo a pesquisa, as organizações estão em conflito em relação à segurança - classificando o assunto como principal objetivo, assim como uma grande preocupação. Oitenta e sete por cento dos entrevistados no mundo estão confiantes de que a mudança não causará impacto e melhorará a segurança. No entanto, ter segurança em ambientes de cloud computing é uma grande preocupação para essas empresas, que citaram potenciais riscos, incluindo malware, roubos por hackers ou perda de dados confidenciais.

Quando se falava em segurança da informação há cerca 10 ou 15 anos atrás, estava-se pensando em perímetro, ou seja, a empresa tinha que ser isolada de forma segura. Isso era funcional principalmente em ambiente de mainframe. No entanto, hoje praticamente todos os dispositivos têm uma capacidade de armazenamento, e isso significa que, se antes a empresa tinha que se preocupar com um único disco, hoje as mesmas informações e até mais valiosas estão navegando em dispositivos menores que estão muito mais sujeitos a furtos, roubos ou perdas propriamente ditas.

O diretor técnico operacional da Silverlilnk, Stefan Victor Wieczorek, lembra que quando se transfere esta informação para um ambiente de cloud, se maximiza a questão ao copiar as informações para uma área sobre a qual não se tem o menor controle. E esta é a grande preocupação das empresas ao pensar em cloud computing.

Segundo ele, para ter controle no ambiente de cloud computing, é preciso proteger não o perímetro, mas sim utilizar uma proteção intrínseca aos dados, independente de onde esteja a informação, se trafegando na rede, no disco de backup, ou outra mídia. "A forma mais segura para isso é a criptografia, porque o arquivo criptografado só permite a leitura do começo do cabeçalho, que é importante

para que tanto o sistema operacional quanto o usuário que tenta acessar a informação entendam que se trata de um arquivo protegido e não de um arquivo corrompido", diz Wieczorek. "E o acesso a este arquivo é feito via certificado digital, única forma de garantir que o usuário é realmente quem ele diz ser", completa.

**Despreparo**

O resultado da pesquisa feita pela Symantec mostrou que as áreas de TI podem não estar preparadas adequadamente para a migração, com quase metade dos entrevistados afirmando que suas equipes de TI não estão prontas neste momento. Em nível global e na América Latina, os principais modelos de gerenciamento em cloud computing que as empresas contratam estão relacionados a gerenciamento ou segurança de e-mail, segurança de mensagens e web e gerenciamento de segurança.

Mas o que fazer para reverter este cenário de insegurança em relação ao cloud computing? Como garantir que os dados em nuvem estarão protegidos? Especialistas ouvidos pela TI Inside são unânimes em afirmar que é praticamente impossível garantir segurança 100% em ambientes virtuais. Mas, em contrapartida, confirmam que é possível, sim, desenvolver ambientes cada vez mais herméticos e, consequentemente, menos vulneráveis, se forem seguidos os passos da política de segurança, avaliação de riscos e vantagens da migração, aquisição e implantação corretas de ferramentas adequadas a cada necessidade.

De acordo com analistas do Gartner, embora os princípios fundamentais da segurança da informação sejam os mesmos em centros de dados físicos, virtualizados ou em nuvens privadas, a maneira pela qual as companhias prestam serviços de segurança deve mudar.

Para apoiar a computação em nuvem privada, pública, ou em ambas, a segurança deve ser adaptável e suportar um modelo onde as cargas de trabalho estão dissociadas do hardware físico e dinamicamente alocadas para uma estrutura de recursos de computação, segundo o Gartner.

"No lado das empresas, é preciso determinar o apetite para o risco, e contratar um conjunto de tecnologias

> "Deve-se ter uma infraestrutura parruda e também fazer marketing, o que garante a percepção dos stakeholders de que a empresa está tomando uma decisão consciente e planejada de ir para nuvem"
>
> **ALBERTO FÁVERO, DA ERNST & YOUNG**

## DESPREPARO DAS PMES

*Quando o assunto é segurança da informação, a preocupação das empresas de pequeno e médio porte não deve se limitar somente ao investimento em antivírus e firewall. "No Brasil ainda são gastos bilhões com essas ferramentas e poucos milhões para proteger as aplicações", explica Rafael Sampaio, especialista em segurança da informação e CEO da Future Security, empresa brasileira de gestão de segurança da informação.*

*Com budget reduzido, profissionais pouco qualificados e deficiências tecnológicas, as PMEs têm como alternativa a parceria com fornecedores que reúnem equipe técnica atualizada, tecnologia de ponta e infraestrutura para uma atuação 24 horas, sete dias por semana.*

*Atualmente, o segmento de PME representa 20% do faturamento global da Future Security e o foco é ampliar essa participação para 35% ao ano oferecendo serviços de gerenciamento de segurança compatíveis com as necessidades dessas empresas. Entre as iniciativas para atender de forma diferenciada este perfil de cliente está a manutenção de uma área dedicada exclusivamente às PMEs, em nível nacional e adequação de tecnologias para oferecer às PMEs alto nível em segurança da informação com excepcional relação custo-benefício.*

que possam transmitir a segurança", prescreve Carlos Alberto Costa, líder de segurança da informação da Accenture.

**Novos tempos**

Costa avalia que "estamos vivendo um momento de grande mudança tecnológica em que se precisa definir uma série de arquiteturas e padrões e fazer com que isso seja cumprido. Trata-se de um momento intrigante, talvez comparado apenas a internet, com todas as tecnologias interferindo no dia a dia". E a insegurança não se trata de falhas sistêmicas, mas da sensação que cada corporação transmite aos seus gestores, funcionários, clientes e acionistas, sobre o grau de inviolabilidade de seus sistemas.

"Vai demorar algum tempo até que consigamos convergir segurança e sensação de segurança na computação em nuvem. Estamos vivendo um processo semelhante ao que ocorreu com os bancos, à época de lançamento dos internet banking. Essa é uma sensação que precisa ser trabalhada", indica Silvio Maemura, diretor da unidade de software da HP.

Ele conta que a HP oferece ferramentas de software que mapeiam todos os recursos portados para cloud e geram alertas de suspeitas para que a empresa possa se antecipar a ataques e agir para que nada aconteça.

"Não há diferença alguma se cloud pública ou privada, o importante é monitorar os ativos. Se é um ativo que não tem informação relevante, pode até alertar, mas classifica como ativo não relevante. Mas se for uma conta bancária ou uma informação confidencial da Justiça, classificamos como ativo de risco e alertamos a cada tentativa de violação", descreve.

**Questão de marketing**

Alberto Fávero, sócio de consultoria da Ernst & Young, indica que em muitas situações a implantação de ferramentas de segurança e o marketing feito sobre a baixa vulnerabilidade do ambiente são temas que devem caminhar juntos. "Deve-se ter uma infraestrutura parruda e também fazer marketing, o que garante a percepção dos stakeholders de que a empresa está tomando uma decisão consciente e planejada de ir para nuvem."

Para ele, a estratégia de adoção de um serviço em nuvem deve privilegiar a infraestrutura da ponta, ou seja, aquela que leva até a nuvem. Em seguida ou em conjunto com a construção da funcionalidade, a base de segurança - com criptografia, tunelamento, VPN (virtual private network) etc - e em paralelo construir a percepção, ou seja, apresentar os mecanismos, como funcionam, o uso correto etc. "Aí todos os usuários do sistema passam a ver e a interagir sem grandes desconfianças", alega.

"Estamos vivendo um momento de grande mudança tecnológica em que se precisa definir uma série de arquitetura e padrões e fazer com que isso seja cumprido. Trata-se de um momento intrigante, talvez comparado apenas a internet, com todas as tecnologias interferindo no dia a dia"
**CARLOS ALBERTO COSTA, DA ACCENTURE**

FOTO: DIVULGAÇÃO

Seja um pequeno negócio dependente dos aplicativos oferecidos pelo Google Does para compartilhamento de documentos ou uma empresa que esteja movendo seu sistema de ERP global para a nuvem, ambos devem exigir exigir que alguns requisitos comuns de segurança e de conformidade sejam cumpridos pelos fornecedores que entregam aplicativos e serviços através da web.

Estes requisitos envolvem desde quem pode acessar aplicativos e dados, bem como os sistemas de hospedagem, onde os dados estarão armazenados, e se os dados estão hospedados em servidor dedicado em vez de hardware compartilhado. Essas exigências garantem registros detalhados de quem acessou dados e aplicativos, de modo a cumprir as normas societárias e regulatórias, e verificar se a informação está devidamente criptografadas - um fator que é mais crítico fora do firewall corporativo.

**PARA APOIAR A COMPUTAÇÃO EM NUVEM PRIVADA, PÚBLICA, OU AMBAS, A SEGURANÇA DEVE SER ADAPTÁVEL E SUPORTAR UM MODELO ONDE AS CARGAS DE TRABALHO ESTÃO DISSOCIADAS DO HARDWARE FÍSICO E DINAMICAMENTE ALOCADAS PARA UMA ESTRUTURA DE RECURSOS DE COMPUTAÇÃO, SEGUNDO O GARTNER**

## RECOMENDAÇÕES SYMANTEC

- Assuma a liderança na adoção da computação em nuvem. A TI precisa assumir um papel proativo na adoção de Cloud Computing. Muitas áreas de TI estão tendo uma abordagem lenta, metódica e conservadora em relação à transição para a nuvem. Como líder de TI, você deve manter o controle sobre aspectos importantes, como segurança, disponibilidade e custo. Isso é difícil de fazer sem que sua equipe tenha treinamento e preparo adequados
- Defina camadas de informações e aplicações. Nem todas as informações e aplicações foram criadas da mesma forma. Faça uma análise e distribua as informações e aplicações em camadas para determinar o que você acha que deve ser migrado para a nuvem
- Avalie os riscos e defina políticas adequadas. Garanta que as informações confidenciais estejam acessíveis apenas para usuários autorizados e que essas informações não saiam da empresa. Você também deve certificar-se de que os prestadores de serviços na nuvem sejam capazes de cumprir os requisitos de conformidade. Por fim, avalie potenciais fornecedores de acordo com questões operacionais, como alta disponibilidade e capacidade de recuperação de desastres
- Comece agora. Você não tem que ter uma abordagem "tudo ou nada" para a computação em nuvem. Explorar os serviços é um primeiro passo fácil para começar a migração. Ainda que se preparar para migrar aplicações críticas para os negócios possa levar tempo, você pode começar agora com serviços e aplicações mais simples

**Fonte: TI Inside, São Paulo, ano 8, n. 76, p. 20-22, jan/fev. 2012.**