Segurança Em Computação Em Nuvem: Garantindo A Confiabilidade Dos Dados E A Estabilidade Da Nuvem

Lucas Pereira Da Silva[1]

RESUMO

A chegada da Computação em Nuvem trouxe um série de inovações que podem ser de grande valia para corporações e organizações, garantindo que estas possam ter o gerenciamento dos seus recursos de TI de forma melhorada. Essas melhorias vão desde diminuições de custos do ponto de vista econômico, até a um menor desgaste dos responsáveis pela área de TI destas organizações, no sentido de ser necessário um menor controle dos recursos de informática. Porém, para que isso seja necessário as organizações precisam ter garantias de que a utilização de uma nuvem, seja ela pública ou privada não acarretará em problemas futuros. E esse acarretamento de problemas futuros está diretamente ligado com o fato de garantir a segurança e confiabilidade dos dados bem como a estabilidade dos serviços prestados por quem fornece a estrutura da nuvem.

INTRODUÇÃO

A Computação em Nuvem está em evolução e sua primeira etapa do seu desenvolvimento muito se falou sobre esse tema, porém, havia pouca coisa de concreto. Agora, a Computação em Nuvem pulou para um novo patamar onde conceitos mais concretos estão sendo desenvolvidos.

Em um primeiro momento as ofertas de Computação em Nuvem eram baseadas em fornecimento de aplicativos para uso comercial ou aplicativos corporativos que gerenciavam dados onde sua confidencialidade não era um aspecto chave. Além disso a necessidade de fornecer garantias de confidencialidade não era um objeto de forte estudo já que havia ainda aspectos mais fundamentais a serem desenvolvidos e discutidos sobre as nuvens.

Entretanto essa situação mudou e a confiabilidade e segurança dos dados em uma nuvem passam a receber um maior foco de estudo e para que a Computação em Nuvem possa evoluir mais é necessário atender as necessidades corporativas em relação a segurança dos dados de tal forma que se elevem os níveis de segurança a fim de garantir aplicativos corporativos mais confidenciais.

1 Aluno do curso de Ciências da Computação da UFSC

NUVENS PÚBLICAS

Nas nuvens publicas existem os provedores de serviços que são executados em nuvem e desta forma estes serviços podem ser acessados por um protocolo de internet de tal forma que o cliente não necessite saber muitas informações sobre a forma como este serviço está sendo oferecido, tão pouco a localização geográfica dos recursos de TI que executam estes serviços.

A segurança necessária em uma nuvem irá depender de que tipo de serviço está sendo oferecido. Podemos classificar esse serviços em três categorias:

- SaaS (Software como serviço): É quando um serviço é fornecido como um aplicativo para os clientes. Assim, o cliente acessa este aplicativo e realiza as operações desejadas. Nesse tipo de serviço o cliente possui funcionalidades disponíveis bem delimitadas. Como exemplo de SaaS podemos citar o Gmail e o Google Docs.
- PaaS (Plataforma como serviço): Provê além de serviços de software uma estrutura para desenvolvimento de aplicativos na forma de serviços Web que possam ser integrados e hospedados. Como exemplo posse-se citar o AppExchange.
- IaaS (Infraestrutura como serviço): Oferece todo uma estrutura no formato de recursos remotos de modo que o cliente possa realizar gerenciamentos de tarefas. Como exemplo podemos citar o Atmos e o Elastic Compute Cloud.

Para que a computação em nuvem possa atender as expectativas é necessário realizar melhorias e principalmente no que tange a segurança. Hoje, a maior parte dos aplicativos voltados para nuvem pública são aplicativos que se centram no consumidor e realizam a integração e armazenamento de dados juntamente com transações desses dados.

Um ponto importante a se observar nessa etapa de crescimento da computação em nuvem é que os dados que são processados são em sua maioria dados não confidenciais e grande parte dos serviços de computação em nuvem não oferecem grandes seguranças em relação a confidencialidade e integridade dos dados. E um ponto negativo disso é que essas ofertas de nuvem pública possuem em grande parte poucos padrões.

Conforme as informações aumentam o problema da segurança tanto para as organizações que utilizam nuvens publicas, quanto para os provedores da nuvem só aumentam. A maioria das informações confidenciais são criadas por indivíduos pertencentes a essas organizações, entretanto a responsabilidade pela segurança dessas informações é das próprias organizações.

A QUESTÃO DA SEGURANÇA

Entre os benefícios da Computação em Nuvem estão uma maior economia a médio prazo e mais estabilidade no gerenciamento dos recursos de TI de uma organização. A segurança de um nuvem é um fator que se for comprometido irá comprometer estes dois benefícios podendo trazer para a empresa ou organização grandes gastos e muitas dores de cabeça. É justamente por esses motivos que a segurança em uma nuvem é de suma importância para garantir que a utilização dessa nuvem seja um fator que traga vantagens.

Em um data center convencional a segurança se basei em estruturas firmes que garantem a proteção dos dados através da utilização de estruturas físicas, estruturas de hardware e estruturas de software. Nesse caso dos data centers convencionais a segurança tem forte pilar no controle de acesso dos usuários e mantenedores. Já na Computação em Nuvem, apesar de ainda existir um data center, o controle deste é feito de forma encapsulada de modo que isso garanta uma maior segurança. Essa maior segurança é garantida através de certos padrões.

A computação em nuvem é com certeza uma promessa de integração facilitada, entretanto nem sempre essas facilidades de integração acontecem, isso porque é necessário manter certos padrões de segurança e a integração entre diversos prestadores de serviço pode comprometer esses padrões de segurança. É necessário que ocorra uma portabilidade de identidades entre diversas nuvens para que assim se possa cumprir a promessa de integração e segurança, ao mesmo tempo. Conforme serviços mais complexos forem fornecidos por nuvens públicas então é necessário que se aumente a portabilidade e aumente as comunicações entre nuvens pública independentes.

Um dos maiores medos na computação em nuvem é que dados que são confidenciais deixem de ser confidenciais e por isso os departamentos de TI das empresas têm tantas dores de cabeça tentando garantir formas cada vez mais concretas preservar a integridade desses dados. É ai que as nuvens públicas enfrentam um outro problema: como garantir que os funcionários da empresa que fornece o serviço de nuvem são de total confiança e não vão quebrar o sigilo dos dados? E principalmente, como se proteger eficientemente das ameaças internas? Essa deve ser um responsabilidade do provedor de nuvem e é ele quem precisa mostrar como a estrutura organizacional do próprio provedor de nuvem provê essas garantias. A necessidade de controle das informações precisa estar de acordo com a necessidade do usuário em ter um controle de acesso que seja eficiente. Os usuários e as organizações possuem expectativas de que exista transparência no acesso.

Um aspecto essencial para as nuvens é a existência de informações de identificação pessoal e outros dados confidenciais ou regulamentados. Há um empasse sobre quem deve ser responsável por assegurar a conformidade dos dados: a organização que contrata um serviço de

nuvem publica ou o provedor de nuvem. A grande dificuldade é associar os níveis de segurança para as informações e dessa forma transferir esses níveis para a nuvem com um custo baixo, entretanto com uma grande segurança.

PROTEGENDO A NUVEM

A proteção de um nuvem pública está ligada com o fato de que a medida em que uma organização migra seu ambiente tradicional para um ambiente de computação em nuvem, é necessário que se abra mão de alguns níveis de controle e isso somente é possível se a organização puder confiar no provedor do serviço da nuvem.

A garantia da segurança na nuvem passa obrigatoriamente por aspectos como: controle do acesso dos usuários, segurança dos dados, gerenciamento de eventos e outros. Também é importante garantir a segurança da identidade, pois está preserva a integridade e a confidencialidade dos dados e dos aplicativos, deixando também níveis de acesso conforme cada tipo de usuário. Desse modo, a identidade irá sendo gerenciada de tal forma que isso gere segurança e estabilidade para o cliente.

Para garantir a segurança dos dados em um nuvem pública é necessário centralização das informações e os dados precisam de segurança própria que envolvem:

- Isolamento de dados: é necessário isolar os dados principalmente nas quando os mesmos são multi-alocados e precisam ser compartilhados. Para isso utiliza-se ferramentas com a virtualização, criptografia e controle de acesso que fornecem uma certa robustez para permitir níveis e realizar a separação entre corporações, comunidades e usuários.
- Segurança granular dos dados: conforme é aumentada a confidencialidade das informações, é necessário aumentar a granularidade da classificações dos dados. Nas nuvens públicas o nível de segurança dos dados poderá ser feita em nível de arquivo, de campo ou até mesmo de bloco e dessa forma poder atender as demandas existentes.
- Segurança consistente dos dados: existem uma necessidade de proteção do conteúdo baseado em políticas que atendem as necessidades da organização que está utilizando o serviço da computação em nuvem. É necessário que exista criptográfica tanto para dados em trânsito, quanto para dados que estão armazenados na nuvem.
- Classificação dos dados: na computação em nuvem existe uma alta troca de

recursos e é necessário de alto desempenho onde existem cada vez mais requisitos de segurança. Nesse cenários a classificação dos dados é fundamental e serve para as organizações saberem a importância de cada informação e onde estas estão localizadas, além de existir a necessidade de realizar a prevenção contra a perda de dados.

- Controle e conformidade: é importante que exista informações para gerenciamento e validação para que se possa monitorar e auditar o estado da segurança das informações. Nesse sentido é necessário que se verifique se os doados estão sendo administrados seguindo as regulamentações, se existem coleta de registros e a criação de relatórios.

A estrutura de um nuvem deve ser entre outras coisas segura e independente é para isso é necessário satisfazer alguns requisitos:

- Segurança inerente no nível do componente: é necessário projetar a nuvem para ser segura e ser construída com componentes que possuem interfaces sólidas para outroas componentes e seja sustentada de forma segura, através de procedimentos de avaliação de vulnerabilidades e garantias de nível de serviço que passem confiança.
- Segurança de interface mais granular: garantir políticas de controle e segurança granulares nos locais onde há transferências de dados de forma que estejam satisfeitas as condições de consistência e responsabilidade. Para isso deve existir um padrão que forneça políticas sólidas de segurança e que estas estejam implementadas de forma consistente.
- Gerenciamento do ciclo de vida de recursos: uma das grandes vantagens da computação em nuvem é que o fator da multi-alocação traz vantagens econômicas para os dois lados. Conforme as necessidades de uma organização mudam, os provedores da nuvem precisam realizar mudanças nas alocações e para isso largura de banda, servidores, armazenamento e a segurança precisam estar garantidos adequadamente nessas trocas de alocação.

CONCLUSÃO

A Computação em Nuvem traz uma promessa de mudar o paradigma de como se utilização os data centers convencionais e aparentemente essa mudança trará muitos benefícios. Entretanto, antes de realizar a transição para utilizar uma nuvem publica, por exemplo, é necessário

que hajam medidas cautelares que garantam aspectos como: autenticação sólida, autorização delegada, gerenciamento de chaves para dados criptografados, proteções contra a perda de dados e gerenciamento de relatórios para análise.

Assim, fica claro que a computação em nuvem precisa garantir mais segurança para que possa ser aceita com total tranquilidade por parte das organizações que necessitam de um serviço de nuvem pulica. Conforme a confiança por parte das organizações em relação os provedores for aumento o crescimento da computação em nuvem também aumentará. Para isso é necessário que haja uma reciprocidade entre as organizações e os provedores de nuvem, de forma que ambos trabalhem juntos para que se garantam a confidencialidade, integridade e disponibilidades dos dados no momento tanto quando esses estiverem sendo transmitidos ou processados quanto quando eles estiverem armazenados.

REFERÊNCIAS BIBLIOGRÁFICAS

DOKRAS, Satchit et al. **O papel da segurança na computação em nuvem confiável**, em: <http://www.rsa.com/solutions/business/wp/11022_CLOUD_WP_0209_PG.pdf>.

MARCON, Arlindo *el al*. **Aspectos de segurança e privacidade em ambientes de computação em nuvem**, em: <http://professor.ufabc.edu.br/~joao.kleinschmidt/aulas/seg2011/nuvem.pdf>.

CARNEIRO, José e RAMOS, Christian. **A segurança na preservação e uso das informações na computação nas nuvens**. Faculdade De Tecnologia De João Pessoa, em: <http://www.4learn.pro.br/guarino/sd/08-Cloud%20Computing.pdf>.

Cloud Security Alience. **Guia de segurança para áreas criticas focado em Computação em Nuvem**, em <https://cloudsecurityalliance.org/guidance/CSAGuidance-pt-BR.pdf>.

KORZENIOWSKI, Paul. **Computação em nuvens: como obter a desejada segurança**, em: <http://itweb.com.br/35702/computacao-em-nuvens-como-obter-a-desejada-seguranca/>.

FONTES, Edison. **Segurança na Computação em Nuvem**, em: <http://www.mbi.com.br/mbi/biblioteca/artigos/20091013fontes/>.

ASSI, Marcos. **Computação na nuvens, adesão ainda depende de proteção aos dados**, em: <http://marcosassi.com.br/computacao-na-nuvens-adesao-ainda-depende-de-protecao-aos-dados>.