Segurança em Cloud Computing

Débora Cole Bernardi[1,2], Bruno Batista Boniati[1]

[1]Colégio Agrícola de Frederico Westphalen – Universidade Federal de Santa Maria
Caixa Postal 54 – 98.400-000 – Frederico Westphalen – RS – Brasil

[2]Programa de Pós-graduação em Gestão de Tecnologia da Informação

debora_432@hotmail.com, bruno@cafw.ufsm.br

Abstract. *The main attractions of cloud computing are to reduce information technology costs through more efficient use of resources. However, safety issues and risk management with the use of technology cannot be minimized compared to the advantages offered by it. This article presents some efficient methods of control applicable safety in a Cloud Computing environment.*

Resumo. *Os principais atrativos de Cloud Computing são a redução dos custos com tecnologia da informação por meio de uma utilização mais eficiente dos recursos. Entretanto, questões de segurança e gestão de riscos com o uso da tecnologia não podem ser minimizados face às vantagens oferecidas pela mesma. Este artigo apresenta alguns métodos eficientes de controle de segurança aplicáveis em um ambiente de Cloud Computing.*

1. Introdução

Cloud computing (ou computação em nuvem) é uma tecnologia emergente que promete mudar radicalmente a maneira como os aplicativos e serviços de tecnologia da infomação são construídos, entregues e gerenciados. Grandes *datacenters* permitem o compartilhamento de recursos entre aplicações hospedadas e levam a economia de escala, tanto de *hardware* como de *software*.

Segundo uma recente pesquisa realizada [Rosado et al, 2012] a maioria dos contratantes esperam três pilotos principais da computação em nuvem: mais flexibilidade, redução de custos e melhor escalabilidade da TI. Por outro lado, o mesmo material observa que tais contratantes consideram as questões de segurança a sua principal preocupação em relação ao uso da computação em nuvem, constituindo-se como o maior fator de bloqueio das migrações para a nuvem.

Considerando essa problemática este artigo pretende apresentar alguns conceitos ligados à computação em nuvem e abordar melhores práticas para garantir maior segurança em tais ambientes. A seção dois fará definições sobre a tecnologia, a seção três abordará problemáticas ligadas a segurança em ambientes de *cloud computing*. Na seção quatro serão apresentadas práticas indicadas na literatura para aumentar o nível de segurança e por fim serão feitas as considerações finais e indicações de trabalhos futuros.

2. Cloud Computing

O termo *cloud computing* representa um novo ponto de inflexão para o valor da computação em rede, pois permite alta eficiência, escalabilidade massiva, mais rapidez e facilidade no desenvolvimento de *softwares*. Isso tudo vem resultando em novos modelos de programação, infraestrutura de TI e o estabelecimento de novos modelos de negócios [Sun Microsystem, 2009]

De acordo com [Lauro, 2011] a *cloud computing* apresenta-se em diferentes formas:

1. ***Software as a Service* (SaaS)**: Entrega de *software* no qual tanto o *software* como seus dados associados são hospedados na internet (nuvem) e são acessados pelos usuários de rede usando um navegador *web*.
2. ***Platform as a Service* (PaaS)**: Entrega de um ambiente de computação em camadas de soluções como serviço. É análogo ao SaaS, exceto que, ao invés de *software* entregue pela web, o que se entrega é uma plataforma (um ambiente) para a criação, hospedagem e controle de *software*.
3. ***Infrastructure as a Service*** (**IaaS**): Entrega de infraestrutura de servidores, sistemas de rede, armazenamento e todo o ambiente necessário para o funcionamento que passa a ser contratado como serviços. Ao invés de comprar servidores, *software*, espaço em *data centers*, os clientes usam estes recursos como um serviço totalmente terceirizado e sob demanda.

Somente no caso de IaaS, pode-se caracterizar a forma de contratação de três formas: nuvem públicas, nuvens privadas e nuvens híbridas [Sun Microsystem, 2009]. As nuvens públicas são gerenciadas por terceiros e podem trabalhar com diferentes clientes, sistemas de armazenamento e outras infraestruturas nos mesmos servidores. Os usuários finais não sabem que operações de outros clientes podem estar sendo executadas no mesmo servidor juntamente com suas próprias operações [Sun Microsystem, 2009].

Nuvens privadas são boas opções para empresas que trabalham com a proteção de dados e questões de nível de serviço. A demanda de infraestrutura é de propriedade de um único cliente que controla quais aplicativos são executados e onde. No caso das nuvens híbridas tem-se a combinação dos dois modelos anteriores (públicas e privadas). Neste caso o usuário é proprietário de uma parte da nuvem ao mesmo tempo em que e também partilha outras partes de outros proprietários, embora de uma forma controlada. [Sun Microsystem 2009].

3. Problemas de Segurança na Adesão a Nuvem

Segundo [Rosado et al, 2012] a esmagadora maioria dos contratantes em potencial consideram as questões de segurança a sua principal preocupação (motivo da não adesão) em relação ao uso da computação em nuvem. Além disso, questões de privacidade, legais e de conformidade são consideradas áreas de riscos.

Um estudo realizado pela Trend Micro em Junho de 2011 mostrou que 43 % das empresas pesquisadas tiveram problemas de segurança com seus provedores de serviços em nuvem [Sweeny 2011]. As falhas de segurança ocorrem pela falta de importância ao quesito segurança, os provedores de serviço estão mais focados no desempenho e na disponibilidade dos serviços do que na segurança das informações.

Além dos desafios normais de desenvolvimento de sistemas seguros de TI, computação em nuvem apresenta um nível adicional de risco dado ao fato de que os serviços essenciais são terceirizados. O aspecto exteriorizado da terceirização torna mais difícil manter a integridade, a privacidade dos dados, o suporte, e a disponibilidade de serviço. Ainda, tem-se como variável a conformidade com a cultura e política das organizações prestadoras desses serviços.

Outros aspectos sobre computação em nuvem também exigem uma grande reavaliação da segurança e risco. Dentro da nuvem, é difícil localizar fisicamente onde os dados são armazenados. Processos de segurança que antes eram visíveis agora estão

escondidos atrás de camadas de abstração. Esta falta de visibilidade pode criar uma série de questões de segurança e conformidade. [Buecker et al. 2009]

4. Melhores Práticas para Aumentar a Segurança em *Cloud Computing*

Para a adesão à tecnologia de *cloud computing* se faz necessário um modelo de gestão de risco bem elaborado que visa garantir que a informação esteja ao mesmo tempo disponível, protegida e segura. Os processos de negócios e procedimentos precisam levar em conta a segurança, e os gerentes de segurança da informação precisam ajustar suas políticas e procedimentos de segurança para atender às necessidades do negócio. A seguir serão apresentados alguns itens que foram mapeados como boas práticas ou melhores práticas para prover maior segurança em *cloud computing*.

4.1. Assegurar a Confidencialidade dos Dados

Privacidade é de extrema importância quando os dados deixam as fronteiras da organização. Além dos segredos internos e dados pessoais da empresa, metadados e dados transacionais também podem vazar detalhes importantes sobre empresas ou indivíduos. Confidencialidade é apoiada por, entre outras coisas, ferramentas técnicas, como a criptografia e controle de acesso, bem como proteções legais. [Friedman 2010].

4.2. Implementar o Acesso e Gestão de Identidade Forte

Acesso e gerenciamento de identidade são fundamentais para segurança na nuvem. Eles limitam o acesso aos dados e aplicativos para usuários previamente autorizados. A utilização dos padrões de autenticação e segurança tradicionais podem ser estendidos para a nuvem a fim de automatizar a configuração de contas, cumprindo modelos de autorização.

4.3. Implementar um Programa de Gestão de Governança e Auditoria

A governança da segurança como camada estratégica para atendimento ao segmento do negócio "Computação em Nuvem", envolve a aplicação de políticas com foco no uso dos serviços e mecanismos de controles a partir da definição de um *framework* com padrões de gestão da qualidade, conformidade, auditoria e ciclos de melhoria.

4.4. Implementar um Programa de Gerenciamento de Vulnerabilidade e de Intrusão (Programa de segurança)

Em um ambiente de nuvem confiável, deve-se implementar um programa de gestão rigorosa de vulnerabilidade e mecanismos como os sistemas de detecção de intrusão para garantir que os recursos de TI (servidores, rede, componentes de infraestrutura e terminais) sejam constantemente monitorados em busca de vulnerabilidades e brechas. No caso de uma violação de segurança, o programa de segurança pode fornecer informações cruciais sobre a forma como a nuvem está protegida, as respostas às ameaças, e uma linha de prestação de contas para a gestão de eventos [Buecker et al. 2009].

4.5. Manter Testes de Ambiente e Validação

A fim de manter intacto um ambiente de nuvem de TI, é necessário utilizar mecanismos diferentes para teste e validação de segurança de ambiente. [Buecker et al. 2009]. Os fornecedores de *cloud computing* possuem seus próprios métodos e formas de implementação para garantir a segurança, porém nada impede que o cliente possa sugerir ou adotar medidas de segurança de acordo com o que compreender ser essencial.

5. Considerações Finais

Para se tornar o paradigma dominante de uso no segmento de TI a *Cloud computing* ainda precisa evoluir nas questões de segurança, riscos e interoperabilidade. O conceito

segurança é sua maior barreira de adesão. Entende-se que é necessário que os usuários de *cloud computing* ampliem as medidas de controle da empresa para a nuvem, através do uso de computação confiável e aplicação de técnicas de criptografia. Estas medidas devem aliviar o receio de hoje da computação em nuvem potencializando seu uso.

Adoção de um conjunto de boas práticas para aumentar a segurança de *Cloud Computing* podem minimizar os riscos e ampliar as oportunidades de *cloud computing* de forma segura. Como trabalhos futuros pretende-se analisar as soluções de migração para nuvem, disponibilizadas por diferentes fornecedores.

Referências

Buecker, A., et al. (2009) "Cloud Security Guidance IBM Recommendations for the Implementation of Cloud Security". In: *IBM Redpaper*, páginas 1-17. International Technical Support Organization.

Friedman A. A. and West D.M (2010) "Privacy and Security in Cloud Computing". In: *Issues in Technology Innovation*, páginas 2 – 3. The Center for Technology Innovation, Washington, DC.

Lauro, L. (2011) "Entendendo as camadas do cloud computing: IaaS, PaaS e SaaS", In: *Dualtec Cloud Solutions White Paper*, páginas 5-10. São Paulo, SP.

Rosado, D. G., et al. (2012) "Security Analysis in the Migration to Cloud Environments", In: *Future Internet*, vol. 4, páginas 469-487.

Sun Microsystem (2009) "Sun Cloud Computing. Take your business to a Higher Level", páginas 4-14. Disponível em <http://www.oracle.com/us/dm/44034-cloud-computing-primer-332070.pdf>, acesso em setembro/2012.

Sweeny, M. (2011) "Cloud Insecurities: 43 Percent of Enterprises Surveyed Have had Security Issues With Their Cloud Service Providers", Disponível em <http://newsroom.trendmicro.com/index.php?s=43&year=0&type=current&news_item=886>, Acesso em maio/2012.