SEGURANÇA EM CLOUD COMPUTING

GABRIEL ALVES GABRIEL[1]

ALEX SANDER DE OLIVEIRA TOLEDO[2]

Resumo: Este trabalho aborda questões de segurança relativas aos processos e procedimentos realizados em sistemas em nuvens. Descreve também conceitos, objetivos, vantagens e desvantagens, além de expor as principais técnicas de segurança que são aplicadas nestes sistemas.

Palavras-chave: Compartilhamento, Computação, Nuvem, Sistema, Segurança.

1 INTRODUÇÃO

Diante aos avanços tecnológicos, a informação tornou-se o item mais valioso das empresas e a segurança dessa informação, um fator primordial. A tecnologia avançou rapidamente em pouco tempo e as empresas que utilizam destes avanços tecnológicos os aplicam na melhoria das operações organizacionais e otimizações de processos interno e externo.

Uma das vantagens de um sistema baseado em cloud computing é a virtualização de serviços e produtos computacionais, que reflete na redução dos custos com a tecnologia local, além disso, as empresas ganham em praticidade e mobilidade da informação. No entanto aumenta-se a preocupação com segurança dessa informação.

O uso da computação em nuvem por usuários domésticos se torna cada vez mais comum, diante da quantidade de serviços online disponíveis, dentre eles os serviços de e-mails, disco virtuais, programas de escritórios, editores de vídeos entre outros.

[1]Graduando do curso de Sistemas de Informação no Centro Universitário Newton Paiva (gabriel_alves_gabriel@yahoo.com.br).
[2]Professor do Centro Universitário Newton Paiva (alex.toledo.prof@newtonpaiva.br).

> *A segurança é o desafio mais visível a ser enfrentado, pois a informação que antes era armazenada localmente irá localizar-se na nuvem em local físico que não se tem precisão onde é e nem que tipos de dados estão sendo armazenados junto a ela. A privacidade e integridade das informações são então itens de suma importância, pois especialmente em nuvens públicas existe uma grande exposição a ataques. Dentre as capacidades requeridas para evitar a violação das informações está: a criptografia dos dados, o controle de acesso rigoroso e sistema eficaz de gerenciamento de cópias de segurança.* (KAUFMAN, L. M. Data Security in the World of Cloud Computing.)

Não é tarefa fácil impedir ameaças que podem fragilizar a segurança do sistema em nuvens, e para isso as organizações têm adotado diversas técnicas e mecanismos cada vez mais sofisticados para evitar o roubo de dados e acessos indesejados. Este artigo tem por fim apresentar os conceitos, modelos e métodos relacionados com o conceito de Computação nas Nuvens, bem como, relacionar os principais desafios para uso desta tecnologia.

2 SEGURANÇA DE SISTEMA

A segurança da informação pode ser entendida como medidas e condutas aplicadas aos sistemas de informação, com a finalidade de garantir a confiabilidade dos mesmos.

Estruturada sob a política de segurança da organização, as medidas de segurança têm como objetivo principal a proteção das informações das empresas, clientes e também dos usuários.

> *A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e da segurança da organização sejam atendidos. Convém que isto seja feito em conjunto com outros processos de gestão do negócio. (*ABNT NBR ISO/IEC 27002:2005)

Os sistemas em nuvem necessitam de uma segurança mais eficaz do que os sistemas locais, pois o seu meio de comunicação é realizado através de uma rede pública ou privado. Portanto, a segurança se torna um fator preocupante, diante da quantidade de pessoas que tem acesso a essa rede.

No entanto, para que os processos mantenham uma segurança aceitável, toda a infraestrutura de segurança deve garantir a proteção do sistema, sob os três princípios básicos da segurança da informação: confidencialidade, integridade e disponibilidade.

> Confiabilidade – Toda informação deve ser protegida de acordo com o grau de sigilo de seu conteúdo, visando à limitação de seu acesso e uso apenas às pessoas para quem elas são destinadas.
>
> Integridade – Toda a Informação deve ser mantida na mesma condição em que foi disponibilizada pelo seu proprietário, visando protegê-las contra alterações indevidas, intencionais ou acidentais.
>
> Disponibilidade – Toda a informação gerada ou adquirida por um individuo ou instituição deve estar disponível aos seus usuários no momento em que os mesmos delas necessitem para qualquer finalidade. (SÊMOLA, 2003, p.45).

Além dos três princípios básicos, existem outros princípios que devem ser seguidos conforme a figura 1.

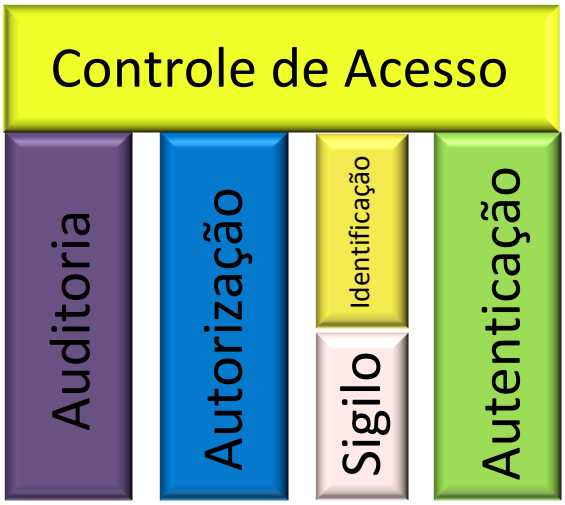

Figura 1 – Adaptação dos Princípios da Segurança da Informação - (ABNT NBR ISO/IEC 27002:2005).

Fonte: NORMA BRASILEIRA ABNT NBRISO/IEC 17799 de 2005 - Tecnologia da informação — Técnicas de segurança.

2.1 Principais Ameaças

De acordo com Cunha (2005), podemos definir ameaças como sendo agentes ou condições que causam incidentes que comprometem as informações e seus ativos por meio da exploração de vulnerabilidades.

As ameaças, quanto a sua intencionalidade, podem ser divididas nos seguintes grupos:

— **Naturais:** são decorrentes de fenômenos da natureza, como incêndios, enchentes, terremotos, tempestades eletromagnéticas, maremotos, aquecimento e poluição.

— **Involuntárias:** são ameaças inconscientes, quase sempre causadas pelo desconhecimento, elas podem ser causadas por acidentes, erros, faltas de energia e etc.

— **Voluntárias:** são propositais, causadas por agentes humanos como hackers, invasores, espiões, ladrões e etc.

2.2 Prejuízos causados com a ausência da Segurança da Informação

Uma parada repentina nos sistemas informatizados de uma empresa pode comprometer seus negócios ocasionando prejuízos financeiros, como também, afetando a credibilidade perante seus clientes e o mercado, principalmente se essa parada for ocasionada por algum tipo de ataque bem sucedido, que teve por objetivo a captura das informações da empresa. Ferreira (2003) afirma que alguns dos maiores riscos que uma empresa está vulnerável é pela falta de um nível adequado de segurança de informações aos quais destaca:

— Perdas por fraudes e erros;
— Imagem e credibilidade podendo ser afetadas;
— Vazamento de informações;
— Indisponibilidade da informação.

3 COMPUTAÇÃO EM NUVEM

A Computação nas Nuvens ou Cloud Computing se refere à ideia de utilizarmos, em qualquer lugar e independentemente da plataforma eletrônica utilizada, as mais variadas aplicações através da Internet.

Seu conceito ainda é recente, mas conforme Santos e Meneses (2009) pode-se definir como a virtualização de produtos e serviços computacionais, ou seja, é uma maneira de armazenar todas as informações em servidores virtuais chamados de “nuvem”, onde há uma tendência

mundial para este modelo, não necessitando de máquinas velozes com um grande potencial de hardware e sim de um simples computador conectado à internet para rodar todos os aplicativos.

> *A denominação cloud computing chegou ao conhecimento de muita gente em 2008, mas tudo indica que ouviremos este termo ainda por um bom tempo. Também conhecido no Brasil como computação nas nuvens ou computação em nuvem, cloud computing se refere, essencialmente, à ideia de utilizarmos, em qualquer lugar e independente de plataforma, as mais variadas aplicações por meio da internet com a mesma facilidade de tê-las instaladas em nossos próprios computadores. (ALECRIM. Emerson.* Escrito em 23_12_2008 - Atualizado em 10_01_2013).

A ideia de Computação nas Nuvens certamente não é uma novidade, mas a forma de implementá-la é um tanto inovadora. Grandes empresas estão investindo nessa nova tecnologia, onde atualmente destacam-se: Google, IBM, Dell, HP e Microsoft.

Alecrim (2008) destaca as principais características da Computação nas Nuvens:

— Acesso às aplicações independente do sistema operacional ou hardware;

— O usuário não precisará se preocupar com a estrutura para execução da aplicação: hardware, backup, controle de segurança, manutenção, entre outros, ficam a cargo do fornecedor de serviço;

— O compartilhamento de dados e o trabalho colaborativo se tornam mais fáceis, uma vez que todos os usuários acessam as aplicações e os dados estão guardados no mesmo lugar;

— Dependendo do fornecedor, o usuário pode contar com alta disponibilidade, já que, se, por exemplo, um servidor parar de funcionar, os demais que fazem parte da estrutura continua a oferecer o serviço.

4 CONDUTAS DE SEGURANÇA, NA ROTINA DOS USUÁRIOS.

A base de dados de um sistema baseado em Cloud Computing é muito bem programada e consolidada, pois são preparadas para fornecerem serviços de qualidade via internet.

Sendo assim, o ataque dos crackers a estes sistemas requer muita habilidade e tempo para investidas, e ainda há o risco de serem rastreados e identificados.

Como os servidores não são alvos fáceis, os alvos de investidas dos crackers tornaram-se os usuários, que geralmente desconhecem as boas práticas de segurança e nem possuem softwares de segurança tão eficazes.

Segundo Silva, "O problema da segurança da informação tem sempre duas faces, que são representadas pelas características inerentes de dois mundos diferentes e por vezes conflitantes: o mundo da tecnologia e o mundo dos seres humanos".

Serão descritas logo abaixo as principais falhas comportamentais realizadas em uma organização.

4.1 Descarte seguro de mídias

Grande parte dos vazamentos das informações ocorre devido ao descarte malfeito das mídias utilizadas. O lixo de uma empresa pode revelar documentos confidencias e estratégias que poderiam ter sido protegidas com a aplicação de cuidados especiais no momento de realizar o descarte. Os funcionários devem ser orientados a apagar todos os dados antes de se desfazerem de um CD, disquete, papel, etc. Caso contrário, qualquer pessoa que revire o lixo da empresa terá acesso a dados valiosos, que não deveriam ter se tornado público.

4.2 Engenharia social

A engenharia social são práticas de persuasão utilizadas por pessoas mal intencionadas a fim de adquirir alguma informação de um indivíduo, de forma que a pessoa em posse da informação não note.

Normalmente, isso acontece devido ao despreparo que os funcionários têm diante da tão grande importância que a informação pessoal ou da empresa agrega. Por isso é de extrema importância que seja feito um treinamento para os funcionários, que trabalham em setores de informação, por exemplo: dados dos clientes, vendas, informação de tomadas de decisão e etc. Para que as investidas dos engenheiros sociais não alcance o êxito.

4.3 Utilizações correta de e-mails

O e-mail é um dos principais meios de comunicação que uma empresa possui, tanto para comunicações internas e externas. No entanto, devem ser tomadas algumas medidas preventivas para que o e-mail não se torne, um fator de comprometimento do sistema e da imagem da empresa para com o seus clientes.

Os e-mails corporativos não devem ser utilizados como os e-mails pessoais, pois o mau uso pode gerar os “loops” de spam na rede de uma organização, que dependendo da estrutura do sistema de e-mail, pode enviar até mesmos falsos e-mails para os clientes, prejudicando a confiabilidade da instituição, além de poder resultar em divulgação dos dados do cliente.

Para evitar esses problemas, auditorias devem ser realizadas nos servidores de e-mail e em casos mais agravantes os funcionários que estiverem utilizando os e-mails de forma inadequada devem ser notificados.

4.4 Tarefas remotas (home-office)

Algumas vezes os usuários tem a necessidade de exercer suas atividades fora dos limites físicos da empresa, como em casa, lugares públicos que disponibilizam acesso com a internet – o chamado home office.

Importante dizer que toda vez que se utilize de dispositivos externos do local de trabalho para acesso de um sistema em nuvem os cuidados devem ser redobrados. Lembrar sempre de efetuar logoff no sistema, além de apagar cookies do navegador (arquivos que salvam informações dos usuários, normalmente senhas e dados de navegação).

O usuário deve conhecer os riscos e que não se torne hábito à utilização de meios públicos para acessar sistemas em nuvem, caso não tenha conhecimento dos meios de segurança, além disso, computadores públicos na maioria das vezes não possuem antivírus eficazes, alguns

vírus podem salvar suas senhas como os “Keylogs”, e permitir acesso não autorizado para os demais usuários que utilizarem aquele dispositivo.

4.5 Ferramentas de Segurança

As ferramentas de segurança contribuem para a confiabilidade de um sistema. Por isso devem ser instaladas e constantemente atualizadas como os softwares de proteção como antivírus, firewalls e anti-spam. Sua função é impedir a execução ou permissão de agentes não autorizados a infiltrar nos serviços oferecidos pelo sistema em nuvem, para uma maior eficácia deve ser orientado que o usuário não desative nenhuma dessas ferramentas, garantindo assim que o sistema esteja sempre protegido.

4.6 Níveis de acesso

Os níveis de acesso dos usuários são fatores relevantes para a segurança de qualquer sistema, pois um sistema em que todos têm total liberdade aos recursos disponíveis faz com que esse sistema se torne desorganizado e pouco confiável.

Devemos ressaltar que, as permissões dos usuários no sistema devem ser estritamente relacionadas à suas necessidades de acesso na realização do seu trabalho.

As permissões do sistema devem garantir que o usuário tenha acesso apenas e somente os recursos que são necessários para a realização das suas tarefas. Por exemplo, não tem razão em um sistema ERP o usuário do nível operacional, ter acesso aos dados do módulo SIE (Sistema de Informação Executivo), pois as informações que ali são apresentadas não competem aquele usuário.

4.7 Monitoramento

Os monitoramentos dos serviços corporativos devem ser feitos periodicamente com aviso prévios, para garantir que os dados do sistema estejam sempre íntegros, confiáveis e autênticos.

Varreduras de e-mail devem ser realizadas para que problemas comuns com spams e dados indesejados sejam removidos, e não ocasione problemas nos servidores de e-mail e nem nos sistemas compartilhados.

4.8 Campanhas de Segurança

As campanhas de segurança ou treinamentos devem ser realizadas com o objetivo de esclarecer e prevenir contra tentativas de invasões, principalmente por hackers. E também alertar sobre alguns comportamentos que podem comprometer a objetividade do sistema.

5 SEGURANÇA APLICADA EM SISTEMAS EM NUVEM

O maior desafio a ser enfrentado pela Computação nas Nuvens é a segurança. Para entender os potenciais riscos de segurança, as empresas devem fazer uma avaliação completa do serviço de nuvem – começando com a rede, checando as operações do fornecedor e desenvolvendo o aplicativo em nuvem.

Em um relatório do Gartner (2008, aput Brodkin, 2008), há um alerta para sete principais riscos de segurança na utilização de Computação nas Nuvens:

a) **Acesso privilegiado de usuários.** Dados sensíveis sendo processados fora da empresa trazem, obrigatoriamente, um nível inerente de risco. Os serviços terceirizados fogem de controles “físicos, lógicos e de pessoal” que as áreas de TI criam em casa.

b) **Compliance com regulamentação.** As empresas são as responsáveis pela segurança e integridade de seus próprios dados, mesmo quando essas informações são gerenciadas por um provedor de serviços.

c) **Localização dos dados.** Quando uma empresa está usando o cloud, ela provavelmente não sabe exatamente onde os dados estão armazenados. Na verdade, a empresa pode nem saber qual é o país em que as informações estão guardadas.

d) **Segregação dos dados.** Dados de uma empresa na nuvem dividem tipicamente um ambiente com dados de outros clientes. A criptografia é efetiva, mas não é a cura para tudo. "Descubra o que é feito para separar os dados," aconselha o Gartner.

e) **Recuperação dos dados.** Mesmo se a empresa não sabe onde os dados estão um fornecedor em cloud devem saber o que acontece com essas informações em caso de desastre.

f) **Apoio à investigação.** A investigação de atividades ilegais pode se tornar impossível em cloud computing, alerta o Gartner. "Serviços em cloud são especialmente difíceis de investigar, por que o acesso e os dados dos vários usuários podem estar localizados em vários lugares, espalhados em uma série de servidores que mudam o tempo todo. Se não for possível conseguir um compromisso contratual para dar apoio a formas específicas de investigação, junto com a evidência de que esse fornecedor já tenha feito isso com sucesso no passado.", alerta.

g) **Viabilidade em longo prazo.** No mundo ideal, o seu fornecedor de cloud computing jamais vai falir ou ser adquirido por uma empresa maior. Mas a empresa precisa garantir que os seus dados estarão disponíveis caso isso aconteça. "Pergunte como você vai conseguir seus dados de volta e se eles vão estar em um formato que você pode importá-lo em uma aplicação substituta," completa o Gartner.

A preocupação nesse aspecto fez com que a entidade Cloud Security Alliance (CSA) lançasse a segunda versão de um documento com orientações para segurança nas nuvens (www.cloudsecurityalliance.org)

6 DISPONIBILIDADE DOS SERVIÇOS

Para Almeida (2009), com todos os sistemas baseados na Internet, teremos grandes problemas, pelo menos aqui no Brasil, com questões como a conexão e com a estabilidade da Internet.

A internet foi desenvolvida com a finalidade de se dar o fim a centralização dos dados. Em uma possível guerra, o bombardeio às centrais de servidores poderiam deixar os Estados Unidos sem comunicação.

> *"O problema é a centralização mesmo. No caso de um ataque de hackers (ou terrorista de carne e osso) às centrais de servidores do Google, os 146 milhões de usuários do Gmail teriam uma grande dor de cabeça. Moral da história: a computação em nuvem é muito melhor e mais confortável que a de antes. Mas também é menos segura." (REVISTA SUPER INTERESSANTE, edição 273, 2009).*

Os datacenters por possuírem todos os dados das empresas centralizados, serão visados por pessoas mal intencionadas que se utilizando, ou não, de pestes virtuais, podem comprometer a qualidade da "nuvem".

7 NOVAS TECNOLOGIAS DE SEGURANÇA

A segurança da informação principalmente voltada para o ambiente em nuvem, como o caso de serviços bankline, sistemas remotos ERP (Sistema de Gestão Integrado) e outros sistema de igual grau. Por possuírem uma informação de caráter sigilosa, as empresas estão utilizando cada vez mais de diversas tecnologias, muitas dela são bem recentes, que tem como objetivo garantir a integridade dos dados e a confiabilidade dos mesmos como:

— **Dispositivos Tokens:** Os dispositivos Token, são aparelhos que geram chaves de segurança. Normalmente um conjunto de oito dígitos é gerado, de forma que a sequência seja gerada uma única vez por uso. Assim, além da autenticação padrão requerida pelo "usuário e senha", é necessário à digitação dessa chave gerada pelo dispositivo Token. A importância do dispositivo é garantir a autenticidade do usuário, principalmente em serviços que demandam uma maior segurança. Em caso de perda do dispositivo, não é preocupante, pois sem a informação do usuário e senha do cliente o dispositivo se torna inválido para efetuar qualquer operação.

— **Dispositivos Biométricos:** Os dispositivos biométricos são aparelhos que registram e leem digitais dos clientes e usuários. Esses aparelhos cada vez mais estão sendo utilizados devido a sua capacidade de garantir a autenticidade dos clientes. O seu uso está sendo aplicado em sistemas em nuvens que rodam nos terminais dos bancos, pois é fundamental em um sistema de banco, a garantia que um cliente tenha somente acesso a sua conta, a biometria aumenta de forma eficaz esse quesito.

8 CONCLUSÃO

As vantagens da computação em nuvem são inúmeras e a computação local esteja chegando ao seu fim. O futuro da tecnologia, talvez realmente seja a centralização dos dados nas nuvens, onde todos os dispositivos tenham acesso a todos os dados, softwares e sistemas.

Em consequência disso, à capacidade de armazenamento dos computadores locais serão bem menores do que a capacidade média dos dispositivos de armazenamento dos computadores dos dias de hoje e o acesso à internet será tão disponível como a “iluminação pública” que temos hoje. Porém a preocupação de todos é universal: a segurança.

As instituições envolvidas na prestação de serviços da Computação nas Nuvens têm alguns desafios, como a segurança e a confiabilidade. Pois, por ser um conceito novo ainda existem preocupações dos usuários em “entregar” seus sistemas e arquivos para a “nuvem”, as empresas precisam garantir que os usuários terão tais sistemas e arquivos, protegidos e disponíveis.

Normalmente as empresas que prestam os serviços de Computação em Nuvem, espalham seus servidores em diversos locais, longe do conhecimento do próprio usuário ou cliente, o que traz um problema de menor teor para os usuários comuns, mas uma preocupação agravante para as grandes instituições. Dados salvos em outros países estão sujeitos a outras normatizações, o que pode ocasionar vazamento de informação.

Outro fator importante e também agravante é a realização de backups pelas empresas que prestam os serviços de hospedagem em nuvem. O que exige cuidado e a certeza que além de ser feito o backup do prestador inclua a cópia dos dados em mais de um local.

Contudo, apesar de ser vantajoso o conceito de computação em nuvem e a vida prática e móvel que essa tecnologia permite, ainda parece ser seguro manter aplicativos e informações sigilosas no disco rígido do computador ou nos servidores das próprias empresas.

REFERÊNCIAS

ALECRIM, Emerson. **O que é Cloud Computing (Computação nas Nuvens)?**. Disponível em: <http://www.infowester.com/cloudcomputing. php>. Acessado em: 21/03/2013.

ALMEIDA, Juliana. **Todos sob as nuvens: uma nova visão sobre a informática**. Disponível em: <http://comunicacao2.0.vixtime.com.br/?tag=computacao-nas-nuvens>. Acessado em: 25/03/2013.

AMRHEIN, Dustin; QUINT, Scott. **Computação em Nuvem para a Empresa: Parte 1:Capturando a Nuvem**. Disponível em: <http://www.ibm.com/developerworks/br/websphere/techjournal/0904_amrhein/0904_amrhein.html>. Acessado em: 01/05/2013.

Associação Brasileira de Normas e Técnicas. **ABNT NBR ISO/IEC27002:** tecnologia da informação - técnicas de segurança - código de prática para a gestão da segurança da informação, 2005<Disponível em <http://www.vazzi.com.br/moodle/pluginfile.php/205/mod_resource/content/1/Abnt-Nbr-Isoiec-17799-Codigo-de-Pratica-para-a-Gestao-da-Seguranca-da-Informacao.pdf>. Acesso em: 13/05/2013

BRODKIN, Jon**. Conheça sete dos riscos de segurança em Cloud Computing.** Disponível em: <http://cio.uol.com.br/gestao/2008/07/11/conheca-sete-dos-riscos-de-seguranca-em-cloudcomputing>. Acessado em: 18/04/2013.

CAMPOS, **A. Sistema de segurança da informação: controlando os riscos**. 2. ed. Florianópolis: Visual Books, 2007.

Computação em Nuvem. Disponível em: <http://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2009_2/seabra/index.html>. Acessado em: 29/03/2013.

CUNHA, Meire Jane Marcelo (2005**). Proposta de documentação para subsidiar as atividades de implantação da Segurança da Informação**. Disponível em: <http://www.acso.uneb.br/marcosimoes/ TrabalhosOrientados/CUNHA2005.pdf>. Acessado em: 13/05/2013. CHIRIGATI, Fernando Seabra.

FERREIRA, Fernando Nicolau Freitas. **Segurança da informação.** 2003 – Rio de Janeiro – Editora Ciência Moderna.

NOGUEIRA, Matheus Cadori; PEZZI, Daniel da Cunha. **A computação agora é nas nuvens**. Disponível em: <http://under-linux.org/blogs/mcadori/attachments/64d1257953490-artigo-sobre-cloud.html Acessado em: 21/03/2013.

SÊMOLA, Marcos. **Gestão da Segurança da Informação: uma visão executiva** – Disponível em http://www.semola.com.br/Artigos.html>. Acesso em 22/04/2013