Segurança em Cloud Computing

Bruno Gonçalves Zanutto
Universidade Federal de São Carlos
Sorocaba, São Paulo
brunozanutto@gmail.com

***Resumo*—Este artigo aborta tópicos de segurança na cloud definidos pela CSA com alguns exemplos de problemas nos mesmos. Primeiro é feita uma breve introdução sobre o que é cloud computing e por que se discutir segurança na mesma. Depois os tópicos são explanados com mais detalhes, seguidos de um guia da CSA sobre migração para a nuvem, para empresas e usuários que estejam pensando em migrar para o serviço. Por fim, exemplos de serviços e empresas que tiveram problemas de segurança na cloud e como isso afeta as empresas do serviço no geral.**

***Palavras chave*— Segurança, Cloud, Nuvem.**

I. Introdução

CLOUD Computing: basicamente, é a utilização de memória, dispositivos de armazenamento e capacidade de cálculo (processamento) de computadores e servidores interligados por meio da internet de forma que isso seja o mais transparente possível para o usuário.

Com a Cloud Computing, um usuário pode ter acesso a recursos que se fossem executados na máquina do mesmo, exigiriam provavelmente maior capacidade de hardware por parte do equipamento do usuário, instalação de softwares que geralmente tem licenças caras, além maior gasto de energia, aumentando custos.

A Cloud Computing oferece então alguns modelos de serviço, explicados resumidamente:

Software as a Service (SaaS): o mais conhecido. Compreende aplicações que são executadas na nuvem, como por exemplo um cliente web de e-mail, o Google Docs, que permite criação e edição de documentos, planilhas e apresentações de slides via browser.

Platform as a Service (PaaS): este modelo permite ao usuário submeter aplicações desenvolvidas em linguagem de programação ou ferramentas de acordo com o a plataforma e executá-la dentro de um sistema operacional virtual. O usuário não tem controle sobre nada além de suas aplicações, como sistema operacional, rede e armazenamento.

Infrastructure as a Service (IaaS): neste modelo o usuário tem domínio sobre sistema operacional, rede (de forma limitada), armazenamento além do controle sobre suas aplicações submetidas. O usuário apenas não tem controle sobre a camada infraestrutural mais interior da nuvem.

Esclarecidos estes conceitos, fica claro que a cloud computing oferece diversas soluções e serviços para empresas e usuários finais. Mas apenas saber o que pode ser feito é suficiente para uma empresa grande adotar a cloud computing ?

Adotar a Cloud Computing significa colocar dados particulares em servidores espalhados até mesmo ao redor do mundo, de forma que estes dados viajarão pela internet.

Este artigo tratará durante o seu decorrer sobre quais os problemas relacionados à segurança em cloud computing e como eles podem ser divididos em categorias.

Além disso, o presente artigo contém uma seção com considerações sobre o que, quando, e como mover-se de uma estrutura tradicional para a nuvem, um guia para empresas ou mesmo usuários finais interessados em adotar o sistema de cloud computing.

Por fim, serão dados exemplos de serviços providos por cloud computing que apresentaram falhas de segurança, e como isso afetou (e ainda afeta) milhões de usuários em todo o mundo.

II. Os Sete pecados mortais de segurança em cloud computing

Jim Reavis, diretor executivo da CSA (Cloud Security Alliance), uma entidade não governamental dedicada à segurança em cloud computing divulgou uma lista com "os sete pecados mortais de segurança em Cloud Computing", uma lista de 7 itens de segurança na cloud computing que devem ser observados com mais atenção. A lista foi elaborada por ele e 29 consultorias e fornecedores do serviço.

Esta lista levanta questões de forma superficial, sem entrar em maiores detalhes, mas é uma ótima introdução para o tema que ainda será mais aprofundado posteriormente.
Segue a lista:

1) Pecado 1: Perda de dados ou vazamento

Segundo Reavis, não existe um nível aceitável de controle de segurança na nuvem. Segundo ele, aplicativos podem deixar dados vazarem, resultado de um mal controle de APIs, má geração de chaves, problemas de armazenamento ou gestão fraca. Além disso, políticas de destruição de dados podem simplesmente não existir, tanto não dando esta opção para o cliente ou mesmo indicando falsamente que o dado foi

removido, sendo que esta foi apenas retirado do índice de dados, e não propriamente deletados.

2) Pecado 2: Vulnerabilidade de tecnologias compartilhadas

Na nuvem, uma única configuração errada pode ser duplicada em um ambiente no qual vários servidores e máquinas virtuais compartilham essa informação. Devem existir acordos de nível de serviço (SLAs) para garantir gerenciamento de atualizações e melhores práticas possíveis para manutenção da rede e configuração dos servidores.

3) Pecado 3: Internos Maliciosos

É preciso confiar na equipe da empresa provedoras do serviço. Cada empresa provedora tem seus próprios níveis de segurança sobre o acesso aos datacenters, o que gera diferentes níveis de controle sobre a equipe entre as diferentes empresas. Segundo Reavis, Muitos dos provedores fazem um bom trabalho nesse sentido, mas é algo desigual.

De acordo com Archie Reed, tecnólogo selecionado pela HP e também membro da CSA, as empresas contratantes dos serviços de cloud computing tem interesse em colher os frutos do custo, disponibilidade e flexibilidade, benefícios oferecidos pela nuvem, mas se esquecem de considerar o risco de criar brechas para perdas de dados e queda de finanças e produtividade.

4) Pecado 4: Desvio de tráfego, contas e serviços

Muitos dados, aplicativos e recursos estão presentes na nuvem. A autenticação feita de forma insegura pode colocar o acesso a todos esses itens se obtiver acesso à máquina virtual de um cliente em dois casos básicos:

a) Acesso à conta do cliente: neste caso, um cliente tem todo conteúdo de sua máquina virtual exposto ao invasor;

b) Acesso ao administrador da nuvem: neste cenário, o invasor tem poder sobre todas as máquinas virtuais de todos os clientes, uma ameaça bem maior.

5) Pecado 5: Interfaces de programação de aplicativos (APIs) inseguras

APIs inseguras permitem que usuários mal intencionados utilizem-se de seus serviços para invadirem contas.

Segundo Reed, APIs inseguras são o "Oeste Selvagem" para ameaças de segurança. Existem milhares de apps de Web 2.0 hoje desenvolvidas pro programadores com pressa em divulgar seu trabalho funcionando. Alguns exemplos são os ataques à apps da Adobe e Microsoft, colocando bad loads ou cross scripting. Esses bad loads são colocados em uma máquina via e-mail, e comprometem o ambiente. Segundo Reed, esse ataque não é especificamente um problema para a Cloud Computing, mas para qualquer sistema. Todavia, a nuvem corre este risco.

Outro exemplo foi como o Google foi atingido pelo governo chinês. Segundo Reed, não se sabe se o ataque partiu do governo chinês ou de alguém mal intencionado dentro do mesmo, mas o que o ataque, batizado de Operação Aurora, mostra, é que esse tipo de ataque pode acontecer com qualquer banco, companhia de energia ou banco.

6) Pecado 6: Abuso e uso nefasto da cloud computing

É quando os serviços hospedados na nuvem sofrem acesso por pessoas não autorizadas com fins mal intencionados, como quebra de senhas ou outras ameaças para negócios.

Reed disse que coisas como o uso nefasto da cloud computing deixam os usuários com medo de possíveis ataques botnet no Amazon Web Service, por exemplo. O Serviço recentemente foi derrubado e a partir disso passou a ser usado como exemplo da nuvem sendo comprometida. "Todos podem se cadastrar, criar uma conta e começar a usar o serviço para fazer coisas ruins". O impacto disso não está apenas na ação direta destes, mas em IPs bloqueados para aqueles que dividem a nuvem com o transgressor. O transgressor está tirando recursos de quem precisaria, causando um mal indireto.

7) Perfil de risco desconhecido

Se por um lado a transparência facilita algumas coisas para o desenvolvedor que se utiliza da cloud computing, por outro lado essa transparência faz o contratante ver apenas uma interface, sem saber exatamente as plataformas sobre as quais seu serviço está rodando, ou mesmo os níveis de segurança empregados.

III. PRINCIPAIS TÓPICOS DE SEGURANÇA NA CLOUD

Nesta seção serão explicados com maiores detalhes os tópicos que mais impactam na segurança na cloud computing.

Originalmente, a CSA (Cloud Security Alliance) dividiu a segurança na cloud em 15 itens. Para melhor entendimento, eles foram categorizados em três tópicos. São eles:

- Segurança tradicional
- Disponibilidade
- Controle de dados por terceiros

Segurança Tradicional

São as invasões ou ataques que se tornam possíveis, ou pelo menos mais fáceis de acontecer, quando um sistema é migrado pra a nuvem.

Os provedores de serviços na nuvem respondem dizendo que seus sistemas de segurança estão mais maduros do que de outras companhias. Outro argumento usado é que é mais eficiente garantir a segurança se controlada por um terceiro do que internamente, se o que preocupa as companhias são as ameaças internas. Além disso, é melhor garantir a segurança com contratos com provedores do serviço do que com formas tradicionais de segurança.

As preocupações que concernem este tópico são:

1. Ataque no nível de Máquina Virtual (VM-Level attacks. Potenciais vulnerabilidades no hypervisor ou tecnologia de virtualização de máquinas (VM) empregada pelos provedores de cloud com arquiteturas para múltiplos usuários. Vulnerabilidades aparecem no VMWare, XEN e Microsoft Virtual PC e Virtual Server. Os provedores usualmente garantem a segurança através do uso de firewalls e

do monitoramento contante.

2. Vulnerabilidades do provedor da Cloud. São problemas a nível de plataforma, como SQL Injections ou scripts cross-site no salesforce.com. Mesmo o Google Docs, da Google, foi vítima desse tipo de ataque. Segundo a Google, não existe nada de novo no que diz respeito a esses ataques, apenas o contexto. Este tipo de ataque tem se tornado extremamente comuns ultimamente, alguns exemplos serão citados numa seção posterior. A IBM oferece sua ferramenta Rational AppScan, que procura por vulnerabilidades em web services como um serviço de segurança na nuvem.

3. Phishing de provedores de Cloud. Phising nada mais é do que se passar por alguém confiável (um site, por exemplo) para obter informações confidenciais como login e senha. Phishers e engenheiros sociais têm atacado através de phishing de provedores de Cloud, como os acontecidos com o Salesforce.com.

4. Superfície de Ataque a Rede Expandida. Diz respeito em como o usuário deve proteger a infraestrutura de comunicação com a nuvem, uma vez que esta geralmente estará do outro lado de um firewall.

5. Autenticação e Autorização. O framework de autenticação e autorização empresarial não se estende à cloud naturalmente. Como as companhias mesclam seus frameworks existentes para incluir os recursos da cloud?Além disso, como as empresas mesclam seus sistemas e métricas de segurança com os sistemas e métricas dos provedores de segurança da cloud (se houverem)?

6. Forense na Cloud. Em uma investigação forense tradicional, os investigadores levam em consideração o equipamento usado para recuperar os dados desejados. Em um sistema tradicional, a proporção de dados escritos, apagados e reescrito tem baixo impacto. Todavia, quando pensamos na cloud, temos uma escala muito maior, com os provedores de cloud rodando suas próprias infraestruturas multi-server.

Disponibilidade

Diz respeito a disponibilidade de serviços e dados críticos. Exemplos de incidentes neste quesito são a queda do Gmail em 2008 e do Amazon S3 também em 2008. Mais incidentes nesta categoria serão citados posteriormente.

1. Uptime. Assim como com os tópicos de segurança tradicional, os provedores de Cloud afirmam estar seguros neste quesito, mais até do que um sistema de datacenters controlado pela própria empresa cliente. Além do risco de ter o serviço fora do ar, ainda existe o risco da nuvem não conseguir ser escalável para aplicações. O CEO da SAP, Leo Apotheker diz que certas coisas não devem ser colocadas na nuvem, pois esta pode entrar em colapso, como empresas que oferecem um serviço para 50 milhões de clientes.

2. Único Ponto de Falha. Os provedores de nuvem são geralmente vistos como tendo uma disponibilidade muito maior do que a de um sistema interno, mas isso pode não ser verdade, uma vez que existem mais de um ponto isolado de falha para ataques. Imaginemos a nuvem da Amazon. Um atacante que tente derrubar um dos serviços nela hospedado pode derrubar todo o servidor, logo derrubando também serviços “inocentes”, que não eram originalmente alvos para o ataque.

3. Garantia de Integridade Computacional. Basicamente se trata de ter certeza que uma aplicação está em execução na nuvem e gerando resultados válidos. Como exemplo, o Folding@Home de Stanford realiza a mesma tarefa em múltiplos clientes e analisa o resultado que, espera-se, esteja em um consenso.

Controle de Dados por Terceiros

As implicações legais de dados e aplicações sendo mantidos por terceiros não são bem compreendidas e por vezes se torna algo complexo. Um risco quando dados são manipulados por terceiros é a falta de controle e a transparência. Uma das tendências da nuvem é permitir implementações de forma independente, mas isso vai contra conformidades regulamentares da cloud, que requerem transparência. Basicamente isso quer dizer que a mesma transparência que facilita algumas coisas para os desenvolvedores, também os impede de ter um maior controle sobre seus dados.

Com esses alertas, alguns provedores de Cloud estão começando a criar mais nuvens privadas a fim de evitar esses problemas e continuar usufruindo alguns dos benefícios da cloud.

Como exemplo, Benjamin Linder, CEO da Scalent Systems, diz que na sua posição de CEO o que ele mais vê no mercado são empresas tendo dificuldades em confiar em nuvens externas com sistemas proprietários e de alta disponibilidade. Dessa forma, elas estão criando nuvens internas que atendam suas necessidades de forma mais controlada.

1. Por Diligência. Uma empresa contratante de serviço de nuvem é autuada judicialmente ou sofre outra ação legal. Ela pode contar com uma resposta do provedor da nuvem em tempo hábil? Uma questão relacionada é no que diz respeito à exclusão de arquivos da Cloud segundo políticas da empresa contratante. Ela tem garantias que o seu dado foi realmente excluído?

2. Auditabilidade. Problemas de auditabilidade são outro problema causado pela falta de controle da nuvem. Imaginemos uma empresa com seus dados e serviços na cloud. Existe transparência suficiente nas operações do provedor de cloud para que estes dados e serviços sejam usados a fim de auditoria? A revista Information Security Magazine coloca em questão como é possível fazer a auditoria de um sistema de uma organização quando este se encontra na nuvem, um ambiente distribuído e dinâmico com vários usuários, além da empresa auditada, e que pode estar distribuído por todo o globo? Isso torna difícil para os auditores comprovarem que os dados estão seguros e não podem ser acessados indevidamente.

Uma preocupação relacionada diz respeito à administração de atividades na nuvem. É extremamente simples se tornar usuário da nuvem, às vezes mais do que deveria.
Uma das principais diretrizes de auditoria é a SAS 70, que define diretrizes para auditores avaliarem controles internos, para controle de instâncias de processos de informações sensíveis.
Algumas dessas diretrizes de auditorias exigem que os dados sejam processados em uma determinada localidade geográfica. As empresas provedoras de cloud estão respondendo a isto com ofertas de produtos "geolocalizados", que garantem este requisito.

3. Obrigações Contratuais. Quando se usa a infraestrutura de uma outra empresa, é fato que estas não têm interesses comuns. Mas algumas exigências contratuais no uso da cloud são até mesmo impressionantes. Como exemplo, este trecho retirado das condições de uso da Amazon EC2, usado também por outros provedores como o OpSource Cloud: " Não-afirmação. Durante e após o termo do acordo, com respeito a qualquer um dos serviços que você optar por usar, você não vai se valer de, autorizar, assistir, nem encorajará qualquer terceiro a afirmar contra nós ou contra qualquer um de nossos clientes, usuários finais, fornecedores, parceiros de negócios (incluindo vendedores de terceiros em websites operados por, ou em nosso nome) licenciados, sub-licenciados ou cessionários, qualquer violação de patentes ou outros alegando violação de propriedade intelectual com respeito a tais serviços".

Isso quer dizer que ao usar a EC2 da Amazon ou o OpSource, você não tem o direito de reinvidicar a patente de algo lá hospedado, se este vazar, acusando a Amazon ou qualquer um dos outros clientes da mesma. Até o momento, não se sabe da validade legal desse termo, mas o simples fato do mesmo existir não é um bom sinal para qualquer contratante que correria então o risco de ter uma patente violada.

4. Espionagem do Provedor da Cloud. Diz respeito à preocupação com roubo de dados proprietários da companhia por parte da empresa que provedora da nuvem. Exemplos disso são o Google Docs e o Google Apps. Ambos são serviços prestados por uma infraestrutura de nuvem fechada. Os usuários têm medo de confiar seus dados privados em nuvens assim, ainda que se trate de uma empresa gigante como a Google, como disse Shoukry Tiab, vice-presidente de TI da Jenny Craig, usuário do Postini e do Google Maps.

Pelo menos neste caso, os usuários da nuvem chegaram ao consenso que o risco era bem menor do que os benefícios de se confiar dados privados na nuvem. Logo esta não é a maior preocupação hoje no que diz respeito à Cloud Computing.

5. Bloqueio de Dados (Data Lock-in). Como um usuário da nuvem evite que seus dados fiquem bloqueados em um provedor da nuvem? Um provedor pode armazenar seus dados em formatos proprietários diferentes dos outros, e quando o usuário pretende uma migração de provedor, encontra muita dificuldade. Imagine então o cenário de um provedor deixando de prestar seu serviço. Foi o que aconteceu na Coghead. A empresa anunciou que deixaria de prestar seus serviços e deu um intervalo de tempo realmente curto (em torno de dois meses) para desenvolvedores migrarem de seus sistemas. Uma saída simples para o bloqueio de dados, é a padronização, com uso de GoGrid API, por exemplo.

6. Natureza Transitiva. Uma outra preocupação de usuários da nuvem é a transitividade da mesma. É possível que um provedor do serviço terceirize algumas funções para outras empresas, deixando ainda menos controle para usuários. Como exemplo, imaginemos uma empresa que ofereça o serviço de cloud computing, mas esta empresa cuida apenas do processamento e da rede para os usuários, deixando o armazenamento pesado de dados para uma outra empresa. Um exemplo claro de problemas nessa área é um provedor chamado The Linkup. O The Linkup armazenada dados no Nirvanix. O The Linkup então fechou as portas após a perda de alguns dados, dados estes que estavam confiados ao Nirvanix. Outro exemplo de problema que se pode fazer disso é o uso de equipamento de outras empresas. Um provedor de cloud pode alugar equipamento de outra empresa. Foi o caso da Carbonite, que processou seu fornecedor de hardware após a perda de dados de usuários.

IV. POR QUE, QUANDO E COMO MIGRAR PARA A NUVEM

A CSA (Cloud Security Alliance) tem um pequeno guia de análise de riscos sobre migração para a nuvem. Esta seção conterá um breve resumo do mesmo, já que dentre os tópicos abordados nas seções anteriores nem todos tem o mesmo peso.

Segundo o guia, a nuvem tem duas aplicações básicas, a saber:

1. Dados
2. Aplicações/Funções/Processos

Na cloud, podemos tanto mover os dados, quando aplicações, funções e processos para a nuvem, ou mesmo os dois ao mesmo tempo.

Uma das possibilidades da nuvem é essa divisão, que permite deixar os dados em um local, e o processamento em outro. Além disso, é possível deixar apenas parte de um processo na nuvem, através de um PaaS (Platform as a Service).
Basicamente o primeiro passo para migrar é decidir o que migrar para a nuvem. Avaliando os riscos e benefícios quando se trata de dados e processos.

Avaliação de Ativos

O próximo passo da avaliação de riscos é avaliar a importância do ativo (dado ou processo). a ser migrado.
Devem-se fazer as seguintes perguntas para cada ativo:

1. O quanto seríamos prejudicados se o ativo fosse largamente divulgado e se tornasse amplamente público?
2. O quanto seríamos prejudicados se um funcionário do provedor da nuvem tivesse acesso ao ativo?

3. O quanto seríamos prejudicados se alguém de fora executasse nossa função ou processo?
4. O quanto seríamos prejudicados se nossa função ou processo falhar em prover o resultado esperado?
5. O quanto seríamos prejudicados se informação ou dados forem alterados inesperadamente?
6. O quanto seríamos prejudicados se o ativo ficar fora do ar por um período de tempo?

Com isso estamos avaliando cada ativo para confidencialidade, integridade e disponibilidade no caso de todo ele ou parte dele ir para a nuvem.

Mapear o Ativo para os Possíveis Modelos de Implantação na Nuvem

Agora que o valor do ativo já é de nosso conhecimento, devemos escolher um modelo para implantá-lo na nuvem. Antes de escolher o provedor da nuvem em si, é preciso escolher dentre um dos seguintes modelos para determinar se está mais confortável em um deles do que no outro. As opções são:

1. Pública;
2. Privada, interna /em termos;
3. Privada, externa (incluindo infraestrutura compartilhada ou dedicada);
4. Comunitária (considerando posição geográfica do host, conhecimento dos outros membros da comunidade e potencial provedor do serviço);
5. Hibrida. Para efetivamente avaliar uma nuvem hibrida, é preciso conhecer um pouco onde a arquitetura, componentes e dados vão se localizar.

Avaliar Provedores de Nuvem

Nesse quesito tudo se baseia no nível de controle que se deseja ter sobre o sistema no que diz respeito, individualmente aos SPI (Software, Platform e Infrasctructure as a Service), dependendo da necessidade.

Se você já tem requisitos específicos de como manipular os ativos, leve-os em consideração na avaliação do provedor.

Faça o Rascunho do Potencial Fluxo de Dados

É importante saber o fluxo de dados, com o maior número de detalhes possível, da informação saindo da empresa (cliente), chegando na nuvem, e da nuvem até seu destino, seja este o cliente original ou outra nuvem ou um terceiro.

É extremamente importante saber como os dados se movem pela nuvem.

Esta seção trouxe alguns dos tópicos que devem ser levados em consideração ao migrar para a cloud. Um leitor deste artigo pode identificar diretamente o conteúdo abordado nas seções prévias nas perguntas e tópicos a serem avaliados.

V. EXEMPLOS REAIS DE PROBLEMAS DE SEGURANÇA NA CLOUD

PSN

A PSN (PlayStation Network) é o sistema da Sony para possibilitar jogos online multi-jogadores além de todo um sistema de compra de jogos e material especial através do console da Sony, o PlayStation 3 e do PSP, neste de forma mais limitada.

O que aconteceu:

Dia 21 de Março a PlayStation Network encontrou-se indisponível. A Sony, alguns dias depois, ainda sob a queda do serviço, afirmou que mais de 100 milhões de usuários foram afetados, e que dados confidenciais como dados de cartões de créditos foram obtidos por hackers.

Este exemplo permite-nos identificar falha em disponibilidade e em segurança tradicional, uma vez que a PSN foi hackeada e teve perda de dados. As estruturas de armazenamento de informações de cartões de créditos e o sistema que mantinha a rede funcionando eram primitivos e desatualizados, não fornecendo segurança aos usuários.

Além de afetar a Sony e 100 milhões de usuários da PSN, este caso teve um forte impacto na cloud.

Até o fim de 2010, as ações de empresas provedoras de cloud computing subiam vertiginosamente. Com este incidente, as empresas colocaram os pés nos freios na decisão de migrar para a nuvem.

Segundo Eric Johnson, professor na Universidade de Dartmouth, que auxilia grandes empresas sobre estratégias de tecnologia de computação: “Ninguém está seguro. A Sony foi só uma ponta desta coisa”.

Poucos dias depois da PSN sair do ar e a Sony admitir publicamente a situação, as ações da Salesforce.com caíram 3%. A VMWare, que vende softwares para provedores de cloud, teve queda de 2% de suas ações.

Por outro lado, especialistas dizem que a queda da PSN não reflete a situação dos provedores de cloud.

Em primeiro lugar, a Sony não é um provedor de cloud computing. Eles possuem uma nuvem interna, de uso exclusivo da Sony. Não é porque a Sony não protege seus dados e segue medidas de segurança de forma correta que os provedores de cloud computing o fazem. Eles estão bem mais focados em oferecer segurança ao usuário de seus serviços.

Amazon Elastic Cloud

O serviço de nuvem da Amazon. Seu grande diferencial é o fator elástico, onde o usuário tem espaço ilimitado da banda, armazenamento e processamento, e o usuário paga apenas pelo utilizado.

O que aconteceu:

Em Abril, a Amazon caiu por mais de um dia. Alguns serviços como Reddit e Foursquare foram afetados.

A Amazon justificou o ocorrido como um erro humano que ganhou proporções grandes graças a forma como a cloud estava projetada.

Apesar de a Amazon ter oferecido garantias que o mesmo não se repetirá, o efeito da queda da Amazon abalou fortemente a confiabilidade na cloud computing.

VI. Conclusão

Sem dúvidas o processo de migração para a nuvem oferece muitos potenciais riscos, contudo é preciso avaliar para cada ativo que se deseja colocar na nuvem uma relação de riscos e benefícios desta migração.

Os provedores do serviço tem se mostrados cada vez mais empenhados em oferecer soluções que agradem os usuários e que mitiguem todas suas preocupações em relação a nuvem, e que sigam diretivas de auditoria.

O exemplo da queda da Amazon EC2 mostra que não existe 100% de uptime. Mas dificilmente um datacenter de uma empresa comum tem um uptime parecido com o de uma empresa que tem como principal produto a cloud.

Assim como o uptime, a segurança tradicional é algo possivelmente mais forte na cloud do que em um ambiente normal, pois temos uma empresa especializada apenas em gerenciar este serviço.

É uma questão de tempo até cada vez mais a nuvem ser usada como formato para um maior número de aplicações, uma vez que sua flexibilidade e seus vários modos de operação a tornam abrangente, oferecendo segurança em diversos níveis.

Referencias

[1] CSA, “Security Guidance for Critical Areas of Focus in Cloud Computing v. 2.1”.

[2] PARC, Fujitsu Laboratories of America, “Controlling Data In the Cloud: Outsourcing Computation Without Outsourcing Control”

[3] CSA, Paolo del Nibletto. ”The Seven Deadly Sins In Cloud Computing” http://www.itbusiness.ca/it/client/en/home/News.asp?id=56870

[4] CSA, João Nóbrega. “Sete Pecados Mortais da Segurança na Cloud” http://www.computerworld.com.pt/2010/04/05/sete-pecados-mortais-da-seguranca-na-cloud/

[5] Reuters. “Sony Hacking May Hit Cloud Computing Hard” http://ibnlive.in.com/news/sony-hacking-may-hit-cloud-computing-hard/151512-11.html

[6] David Linthicum (Info World). “Why Sony’s PSN Problem Won’t Take Down Cloud Computing” http://www.infoworld.com/d/cloud-computing/why-sonys-psn-problem-wont-take-down-cloud-computing-391

[7] Ted Samson (Info World) . “Popular web-sites Crippled Down by Hours-long Amazon Cloud Service Outage” http://www.infoworld.com/t/managed-services/popular-websites-crippled-hours-long-amazon-cloud-service-outage-657

[8] Amazon EC2 Terms and Conditions. http://aws-portal.amazon.com/gp/aws/developer/terms-and-conditions.html

[9] OpSource Terms and Conditions. http://www.opsource.net/OpSource-Cloud-Terms

[10] Oliver Marks “Cloud Bursts as Coghead Calls It Quits”. http://www.zdnet.com/blog/collaboration/cloud-bursts-as-coghead-calls-it-quits/349