Um Panorama das Técnicas de Segurança em Cloud Computing

Pedro Paulo Vezzá Campos

3 de novembro de 2010

Resumo

A Computação em Nuvem, ou cloud computing vem avançando tanto no mercado empresarial quanto para usuários finais como uma forma de reduzir custos e facilitar a manutenção ao delegá-la a empresas especializadas. Porém, ao mesmo tempo surgem diversos questionamentos quanto à segurança dos dados confiados a empresas terceiras. Neste artigo em formato de *survey* será abordado o estado da arte nas técnicas de proteção produzidas para cloud computing.

1 Motivação

cloud computing é um novo nicho de mercado que tornou-se mais atrativo com o barateamento de insumos necessários à computação como energia, poder de processamento, armazenamento e transmissão de dados, permitindo uma economia de escala [**?**]. Através da Computação em nuvem, surgiu a noção de computação como um serviço, elástico, virtualmente ilimitado e pago apenas pela porção realmente utilizada, muito similar ao sistema de distribuição elétrica.

Diante desse cenário, *players* como Amazon, Google, Microsoft, HP, IBM dentre outros, adentraram essa área oferecendo diversas modalidades de cloud computing, desde a mais abstrata, SaaS ou Software como Serviço, na qual é fornecido um software pronto para ser utilizado utilizando recursos da nuvem, até a mais básica, IaaS ou Infraestrutura como Serviço, que permitem uma personalização da computação desde o nível de *kernel* até camadas superiores.

Por outro lado, críticas e dúvidas são levantadas por opositores dessa tecnologia. Um exemplo é Richard Stallman, evangelista do software livre, que afirma em uma tradução livre:

> "É estupidez. É pior que estupidez: É uma campanha de marketing. Alguém está dizendo que isso é inevitável — e sempre que você ouvir alguém falando isso, é muito provável que seja um conjunto de empresas realizando campanha para torná-lo verdade." [**?**]

Paralelamente às oportunidades possibliltadas através do uso de cloud computing há um aumento das preocupações com a segurança dos dados armazenados na núvem. Frente a isso diversas pesquisas abordaram técnicas tradicionais e inovadoras parta solucionar esse problema. Neste trabalho serão apresentadas as mais importantes dessas propostas apresentadas.

2 Objetivos

Neste trabalho serão apresentados inicialmente os conceitos fundamentais da área de cloud computing como forma de fundamentação para as próximas seções. Posteriormente, serão apresentados os mais importantes tópicos de preocupação de usuários e administradores de sistemas a respeito da Computação nas Nuvens. Por fim, serão apresentados os últimos avanços na área de segurança, apresentados por diversos pesquisadores da área.

3 Trabalhos Correlatos

Em [**?**] são apresentados diversas preocupações com cloud computing, categorizadas segundo a três macro áreas, como apresentado abaixo. Ao longo desse trabalho serão apresentados e discutidos os itens contidos em cada uma dessas categorias.

- Segurança tradicional
- Disponibilidade
- Controle de dados por terceiros

Em [**?**], Chen et. al. fazem um paralelo entre os desafios tradicionais enfrentados pelos provedores de cloud computing e novas possibilidades ataques. O trabalho é permeado por exemplos de técnicas de proteção em sistemas históricos, como o Multics, comprometimento de sistemas e suas consequências, dentre outros.

4 Conceitos básicos

O significado de cloud computing ainda é motivo de discussão na indústria e academia, uma vez que seu significado é amplo. Uma das tentativas de sistematizar a definição desse termo pode ser encontrada em [**?**]. Ainda, segundo o *National Institute of Standards and Technology*, algumas das características essenciais do cloud computing incluem:

- Serviço sob demanda
- Acesso em banda larga
- *Pooling* de recursos
- Elasticidade rápida
- Consumo medido, similar ao do sistema de distribuição elétrica, por exemplo.

4.1 Modelos de serviços

Atualmente há três modelos de serviços reconhecidos como cloud computing, cada um variando no nível de configurabilidade e abstração, como é possível ver abaixo:

SaaS - Software-as-a-Service SaaS, ou Software como um Serviço, é a modalidade de cloud computing mais abstrata de todas. O usuário possui apenas a capacidade de configurar a aplicação utilizada. Nesta faixa encontram-se serviços tais como o Gmail, Google Apps, Evernote, etc.

PaaS - Platform-as-a-Service PaaS, ou Plataforma como um Serviço, é a versão intermediária de computação em núvem. Nesta, o usuário possui o poder configurar certas varáveis do ambiente de hospedagem. Aqui encontram-se serviços tais como o Google App Engine.

IaaS - Infrastructure-as-a-Service IaaS, ou Infraestrutura como um Serviço, é a versão mais básica de computação em núvem. Neste ponto o usuário tem total controle do ambiente desde o kernel até camadas mais superires. Um exemplo de IaaS é o Amazon EC2.

Ainda, há variadas maneiras de implementar uma núvem, variando no compartilhamento de recursos entre diferentes clientes:

Cloud Pública Nesse modelo qualquer pessoa ou empresa pode contratar o serviço de cloud computing.

Cloud Comunitáira Aqui o serviço é fornecido a apenas algumas organizações.

Cloud Privada A núvem passa a ser exclusiva de uma organização.

Cloud Híbrida Uma mistura dos modelos anteriores.

5 Principais preocupações em Cloud Computing

A natureza da cloud, uma estrutura normalmente externa ao firewall da organização e possívelmente gerenciada por terceiros, gera a necessidade de estudos detalhados de análise de riscos antes de adotar uma solução de cloud computing. Algumas das preocupações estão descritas abaixo:

Ataque à virtualização Os hipervisores de virtualização são pontos sensíveis a um ataque direcionado, uma vez que eles são responsáveis por garantir o isolamento entre máquinas virtuais. Vulnerabilidades importantes já foram encontradas em diversas ferramentas, como apresenta [**?**].

Vulnerabilidades do provedor de cloud Outra possibilidade é a invasão ser dirigida ao provedor de cloud computing. Um ataque pode comprometer a infraestrutura de autenticação do sistema e assim permitir o invasor o acesso irrestrito a dados sensíveis do usuário.

Maior superfície de ataque Com a cloud encontrando-se possivelmente fora do firewall da empresa há a necessidade de haver uma proteção da infraestrutura que os conectam.

6 Técnicas tradicionais de segurança

Na área de técnicas tradicionais, pode-se incluir a criptografia como forma de controlar o acesso a informações privilegiadas armazenadas na núvem. Ainda, o fator humano continua sendo crucial, ataques de engenharia social continuam sendo bastante efetivos em conseguir comprometer um sistema.

Por outro lado, as organizações devem estar preparadas para a recuperação de disastres, dessa forma, backups são essenciais. A ausência de um cuidado simples pode levar a sérias consequências como é possível encontrar na bibliografia.

7 As novas possibilidades de ataques e defesas

No contexto de cloud computing, uma possibilidade pouco explorada anteriormente é a de captura do tráfego gerado e a transmissão ativa de dados por um agente malicioso. Isso é possível graças ao compartilhamento de recursos realizado pela núvem. Outra possiblidade é a de um invasor conseguir recuperar informações sobrescritas ou apagadas por um cliente.

Por outro lado, uma vantagem da computação em núvem é a concentração de expertise em segurança. Um único provedor de cloud computing pode diluir os custos para manter políticas de segurança e uma equipe de segurança responsável por controlar possíveis falhas e repará-las.

Isso leva a uma modalidade de serviços conhecida como *Security-as-a-Service* na qual um provedor fornece soluções prontas de segurança tais como frameworks, criptografia, antivírus, etc.

Uma prova da importância da área de segurança em cloud computing é a criação de eventos importantes na área tais como: ACM Cloud Computing Security Workshop e a ACM Conference on Computer and Communications Security.

8 Conclusão

Como foi possível perceber ao longo do artigo a área de segurança em cloud computing alia tanto conceitos tradicionais de segurança de redes, quanto novas técnicas de proteção. A área ainda permanece em constante evolução à medida que novas técnicas de ataques surgem e novas soluções a essas invasões são implementadas. A culminação disso, foi o surgimento, por exemplo, do *Security-as-a-Service* que abrange diversas soluções prontas para serem aplicadas ao ambiente

de computação em núvem.