**Segurança Na Nuvem**

**Alexander Souza – G00317835**

**Resumo -** Devido ao grande potencial da nuvem para os diversos serviços informáticos, cresce também o questionamento em relação a segurança, sendo assim serão apresentados neste artigo as diversas situações em que mais preocupam os utilizadores, abordando também alguns dos problemas mais comuns. Após analisar os diversos tipos de problemas, poderemos também apresentar possíveis soluções. Para entender melhor esses problemas, serão mostradas algumas superfícies de ataques, e alertar para alguns problemas clássicos.

**Introdução**

Computação na nuvem é um assunto recente que irá modificar o conceito de computação e a forma como as pessoas utilizam os computadores, utilizara grande parte das funções locais dos computadores locais, para servidores interligados em nuvem. Esta nuvem, disponibiliza recursos computacionais, tais como processamento e armazenamento, agregando vantagens para utilizadores e empresas, reduzindo os riscos, utilizando uma melhor infraestrutura e a não necessidade de mão de obra especializada, deixando esta função para as empresas de prestação de serviços na nuvem. Esta atribuição de responsabilidades levanta questões ao nível da estabilidade e segurança.

Iremos explorar os problemas de segurança e privacidade, identificando as principais situações que podem afetar os serviços na nuvem e as soluções, mostrando inconvenientes com o alojamento de múltiplos utilizadores na mesma máquina física e a partilha dos recursos computacionais entre eles, vamos abordar soluções de escolhas que um cliente poderá optar para se proteger. Para melhor entender iremos definir os diferentes modelos. Vamos identificar os principais intervenientes na infraestrutura da nuvem, definições e conceitos, problemas e implicações na segurança e as suas respetivas soluções com exemplos.

2 DEFINIÇÃO E ARQUITETURAS

As definições da Nuvem que são mais utilizadas palas as empresas da área, foi criada pela a organização NIST (National Institute of Standarts and Technology) [1] em 2011. De acordo com esta organização nuvem tem de ter algumas características como: serviço auto consumível, acessível pela rede, centralização de recursos, rápida elasticidade e um serviço medido. A agencia ainda definiu mais três modelos de infraestruturas na nuvem:

Afim de proteger alguns dados sensíveis, para que os utilizados não possam aceder a determinados recursos, foram introduzidos quatro tipos de implementação.

Private Cloud: É feito apenas para um utilizador (uma empresa ou organização por exemplo). A infraestrutura física utilizada pertence à organização ou a um provedor que a gere, existindo um controlo total por parte da organização, em relação às aplicações que são implementadas e executadas na nuvem. Este tipo de nuvem oferece uma maior segurança e transparência, mas requer um investimento mais avultado.

Public Cloud: A infraestrutura, neste tipo de nuvem, pertence ao provedor e os serviços estão disponíveis através de uma rede pública a múltiplos utilizadores.

Tem um baixo custo e é muito escalável.

Community Cloud: A infraestrutura da nuvem pertence e é partilhada por diversas organizações sendo destinada a uma comunidade especifica que partilham as mesmas preocupações, características ou interesses.

Hybrid Cloud: É a composição dos modelos públicos e privados. Neste tipo de nuvem é permitido que

uma nuvem privada veja os seus recursos aumentados usando para isso os recursos de uma nuvem pública.

Considerando a administração da nuvem não ser física os dados dos utilizadores estarão totalmente do lado do provedor levando a problemas de segurança:

Provedor da Cloud: é a entidade que fornece e distribui as infraestruturas da nuvem;

Provedor do Serviço: é a entidade que utiliza as infraestruturas da nuvem para fornecer aplicações e serviços aos consumidores finais;

Consumidor do Serviço: é a entidade que utiliza os serviços hospedados na infraestrutura da nuvem;

Cada um destes intervenientes tem um papel importante nas funções que desempenham na nuvem, principalmente quanto aos aspectos da segurança e da privacidade dos

dados. Para combater este tipo de problema é introduzida alguma segurança através do SLA (Service Level Agreement), sendo este um acordo legal que tem de ser discutido, negociado e aceite por todos os intervenientes da nuvem, antes da compra/utilização do serviço. O conteúdo deste documento deve abordar e identificar todos os aspetos do sistema, tais como: as necessidades do cliente, definir os serviços necessários, simplificar questões complexas, reduzir áreas de conflito, equilibrar as expectativas do cliente, garantias e segurança do sistema. Visto que cada serviço disponível pela nuvem poderá ter diferentes tipos de infraestruturas a realização de um acordo não segue nenhum padrão standard, o que leva a que cada provedor faça o seu SLA consoante os clientes ou os serviços que dispõe.

Uma vez que o utilizador não possui controle físico sobre a nuvem, necessita de uma interface para conseguir aceder à mesma, através da Internet. Nesta interface é fulcral que existem mecanismos robustos de segurança, sendo que tipicamente o utilizador acede à nuvem ou utilizando um serviço web baseado em SOAP (Simple Object Acess Protocol) ou através de uma aplicação web REST [\*\*\*\*]. Para os serviços web baseados em SOAP, a segurança é assegurada devido à utilização de certificados X.509 e assinaturas XML. Para serviços baseados em aplicações web REST a segurança é

obtida através de autenticação usando password. Quer nos serviços que utilizam SOAP, quer nos serviços que usam REST é fulcral que a conexão se realize sobre HTTPS. A virtualização é essencial para que existam nuvens. Através da virtualização um sistema é altamente escalável, o que não acontecia antes do surgimento da mesma - eram utilizados servidores físicos ligados através de VLANs [\*\*\*\*\*].

A identificação e análise das diferentes superfícies de ataque de um sistema é um exercício bastante importante, que deve ser realizado tanto por utilizadores, assim como pelo provedor do serviço, desta forma será mais fácil selecionar e identificar problemas no sistema/infraestrutura da nuvem. Como já vimos anteriormente, a nuvem é definida particularmente por três classes diferentes: utilizadores, serviços e provedor do serviço. Cada uma destas classes cria pares de interação. Através deste esquema montado à custa das três classes identificadas é mais fácil expor as diferentes superfícies de ataque que um sistema de computação na nuvem tem.

A maior desvantagem conhecida no uso da computação na nuvem e aquela que inibe mais a expansão e adoção da computação na cloud, pelas empresas, é sem duvida a possibilidade de sofrerem ataques e de serem quebradas a privacidade e segurança das mesmas. De forma a enriquecer o conceito de computação na cloud e a apaziguar os distúrbios na segurança, vários grupos de investigadores e organizações assim como agências governamentais, têm levado acabo, vários estudos com objetivo de identificar brechas e problemas de segurança, de maneira a desenvolver novas capacidades e técnicas para cada um desses problemas. Nos últimos anos, noticiou-se vários ataques e vários vazamentos de informação, e em vários deles foi observado um pensamento comum que passava pela culpabilização inicial dos sistemas da cloud. Cada um destes ataques realizado foi estudado, de forma a determinar se de facto este ataque foi sucedido devido a uma quebra de segurança na cloud ou se simplesmente é um ataque realizado à custa de estratégias tradicionais, como por exemplo problemas das aplicações web, ataques Bruteforce.

**Problemas Tradicionais de Segurança**

Por vezes, certos problemas de segurança, tais como vazamento de dados de clientes da cloud são atribuídos inicialmente a defeitos dos sistemas da cloud mas mais tarde vem se a constatar que esses problemas não passam de problemas tradicionais/clássicos de segurança dos dados em sistemas digitais de comunicação, como por exemplo Phishing [8]. Existem vários exemplos destes, em 2014 várias fotos intimas de celebridades que estavam na sua conta backup na iCloud da Apple foram publicadas na Web [9]. Inicialmente o problema foi atribuído a uma brecha de segurança na Cloud, mais tarde, devido a investigações realizadas pela Apple, determinou-se que o problema não foi devido à alguma fraqueza da sua nuvem, mas sim a um ataque tradicional da web de exploração baseado em Bruteforce no username e passwords dessas celebridades, no sistema "Find My Phone" da Apple e desta maneira o hacker obteve as credencias de acesso ao sistema que armazenava as fotos das vitimas. [10] Outro exemplo de um problema que não foi relacionado com uma quebra nos servidores da nuvem foi o caso que envolve o vazamento de fotos da aplicação móvel SnapChat, serviço este, que diz não guardar os conteúdos partilhados pelos clientes nos seus servidores. O provedor do serviço, negou ter culpas neste ataque e atribui as culpas a uma terceira parte (SnapSaved) que guardava as fotos e conteúdo dos seus clientes através de uma API, e que mais tarde viria a ser pirateada, colocando os conteúdos a público. [11] Este processo de identificação do verdadeiro problema e do verdadeiro culpado é bastante importante pois ajuda em futuras investigações e taxonomias nos problemas da cloud, fazendo com que os sistemas da nuvem se tornem cada vez mais robustos e resistentes contra ataques e desta forma beneficiar tanto os utilizadores assim como os provedores de serviço.