Desafios na Segurança da Informação usando Virtualização na Computação em Nuvem

Challenges in Information Security using Virtualization in Cloud Computing

Gabriel De Oliveira Rosa, Aluno de Segurança da informação da Fatec Americana, gabriel.rosa12@fatec.sp.gov.br

Henrique Santos Canteiro, Aluno de Segurança da informação da Fatec Americana, henrique.canteiro@fatec.sp.gov.br

Cleberson Eugenio Forte, Professor de Segurança da informação da Fatec Americana, cleberson.forte@fatec.sp.gov.br

Resumo

Como uma das maiores vantagens, a computação em nuvem torna possível o acesso a uma grande variedade de aplicações e serviços de forma prática e ágil, sem a necessidade de grandes investimentos em hardware e software. Além disso, a nuvem oferece a possibilidade de escalar os recursos de acordo com as necessidades da empresa, sendo possível liberar ou reduzir a quantidade de memória, processamento e armazenamento utilizados a qualquer momento. Outra grande vantagem é a mobilidade, já que a nuvem permite o acesso aos dados e às aplicações a partir de qualquer lugar, bastando apenas ter acesso à internet. Por fim, é importante destacar que a computação em nuvem oferece maior flexibilidade nas soluções implementadas. Neste artigo apresentamos uma visão geral sobre os desafios da segurança da informação na computação em nuvem usando virtualização. Primeiramente, vamos fazer uma breve introdução sobre o início do desenvolvimento da *cloud computing* e logo em seguida iremos explicar de uma forma breve sobre o conceito da virtualização e o impacto sobre a nuvem e depois iremos nos basear nos tópicos da Cloud *Security Alliance* (CSA) para poder abordar alguns pontos cruciais de segurança na nuvem.

Palavras-chave: computação em nuvem, cloud computing, segurança na nuvem, desafios na segurança na nuvem.

Abstract

As one of the biggest advantages, cloud computing makes it possible to access a wide variety of applications and services in a practical and agile way, without the need for large investments in hardware and software. In addition, the cloud offers the possibility to scale resources according to the needs of the company, being possible to free up or reduce the amount of memory, processing and storage used at any time. Another great advantage is mobility, as the cloud allows access to data and applications from anywhere, just having access to the internet. Finally, it is important to highlight that cloud computing offers greater flexibility in the implemented solutions. In this article we present an overview of information security challenges in cloud computing using virtualization. First, we will make a brief introduction about the beginning of the development of cloud computing and then we will briefly explain the concept of virtualization and the impact on the cloud and then we will base ourselves on the Cloud Security Alliance (CSA) topics to be able to address some cloud security essentials.

Keywords: cloud computing, cloud security, cloud security challenges.

1. Introdução

Em 1957, John McCarthy, criador da linguagem LISP, apresentou um conceito de cloud computing, essa ideia seria de “Time Sharing”, ou seja, o computador poderia ser compartilhado entre vários usuários dividindo assim o processamento entre elas (PEREIRA BORGES, 2022).

Na década de 70, a IBM lançou a primeira máquina virtual que permitia a comparação da computação simultânea. Essa foi a primeira forma comercial do conceito de McCarthy de time sharing e, nas décadas seguintes, a internet estava sendo desenvolvida e a fusão das duas ideias fora cada vez mais se tornando uma realidade.

O termo Computação em Nuvem (*Cloud Computing)* foi usado pela primeira vez em 1997 pelo professor Ramnath Chellappa. e todo o conceito como conhecemos atualmente da nuvem estava presente, como estrutura de servidores conectados a internet que ofereciam poder de processamento e armazenamento para seus usuários (PEREIRA BORGES, 2022).

A segurança da informação na nuvem pública é um tema relevante e, consequentemente, muito debatido. Uma das principais razões para isso é que as organizações estão cada vez mais migrando seus serviços e dados para a nuvem, deixando de lado o modelo tradicional de TI.

Assim, a segurança da informação na nuvem pública é um tema relevante e, consequentemente, muito debatido. Uma das principais razões para isso é que as organizações estão cada vez mais migrando seus serviços e dados para a nuvem, deixando de lado o modelo tradicional de TI.

Diante deste cenário, surge a necessidade de se discutir sobre os principais riscos à segurança da informação na nuvem. O conceito moderno de *Cloud* mostra que um usuário tem acesso a recursos que se fossem executados localmente, como poder de processamento de hardware, armazenamento e instalação de softwares com licenças extremamente caras, esses mesmos recursos são oferecidos na nuvem (ALECRIM, 2008)
.

Alguns modelos de serviços são oferecidos na *Cloud,* e será apresentado de uma forma bem resumida a seguir e pode ser visto na figura 1:

Infrastructure as a Service (IaaS) é um modelo no qual disponibiliza para os clientes recursos físicos computacionais, tais como armazenamento, memória, servidores, banco de dados, acesso a internet ou por uma rede privada. Ele é a base para a virtualização

Software as a Service (SaaS) é um modelo de uso de software baseado na nuvem, o sistema fica alojado em servidores e pode ser acessado pela internet. A desenvolvedora da aplicação disponibiliza mediante pagamento mensal, trimestral, semestral etc. Resumidamente é apresentado como um serviço e não como um produto como era feito antigamente. Na maior parte das vezes não é necessário instalar em computadores locais, pois pode ser acessado online.

Plataform as Service (PaaS) fornece uma plataforma completa de cloud com uma boa relação custo-benefício para desenvolvimento, execução e gerenciamento de aplicativos. Esse modelo proporciona aos usuários um conjunto completo de hardware, software e infraestrutura para desenvolvimento, execução e gerenciamento de aplicativos sem o custo, falta de inflexibilidade e a complexidade que acompanha a implementação e manutenção localmente (PEREIRA BORGES, 2022).

Sabendo dos modelos que existem, podemos nos concentrar nos problemas na parte relacionada a segurança e como podem ser mitigados. Além disso, iremos discutir sobre as vantagens e desvantagens em ter serviços na nuvem ou ter na forma tradicional. Iremos também apresentar exemplos de alguns serviços que apresentam falhas na nuvem.

1.1 Objetivos

Introduzir em âmbito de pesquisa a tecnologia de *Cloud Computing* e demonstrar a gestão de segurança, riscos e benefícios ao se utilizar desta plataforma por empresas e organizações. Promover o conhecimento sobre *Cloud Computing*, enfatizando a sua segurança tanto para o fornecedor da tecnologia quanto para as organizações e instituições que usufruem do serviço, de forma a relacionar os riscos que geram discussões e sustentar as ideias com modelos de gestão de segurança que tragam

confiança e favoreçam o avanço desta tecnologia.

Cloud Computing é uma tecnologia que permite às empresas e organizações acessar um conjunto de aplicações e serviços através da Internet. A *Cloud Computing* pode ser usada para armazenar e processar dados, fornecer aplicações e serviços e gerenciar redes e dispositivos. A segurança é um dos principais desafios enfrentados pelas empresas e organizações que usam a *Cloud Computing*. Os riscos à segurança da *Cloud Computing* podem ser divididos em três categorias: riscos técnicos, riscos de negócios e riscos jurídicos. Os riscos técnicos são os riscos associados às vulnerabilidades dos sistemas e à má configuração dos serviços. Esses riscos podem levar à violação da segurança dos dados, à interrupção de serviços e problemas mais graves nos dados das empresas.

2. Referencial Teórico

Neste artigo foi baseado em estudos e recomendações feito através de vários especialistas na área que são citados ao longo de todo o artigo e sendo referenciados ao final do artigo para que se possa ter mais detalhes do material que foi usado para compor as referências argumentativas ao longo do artigo.

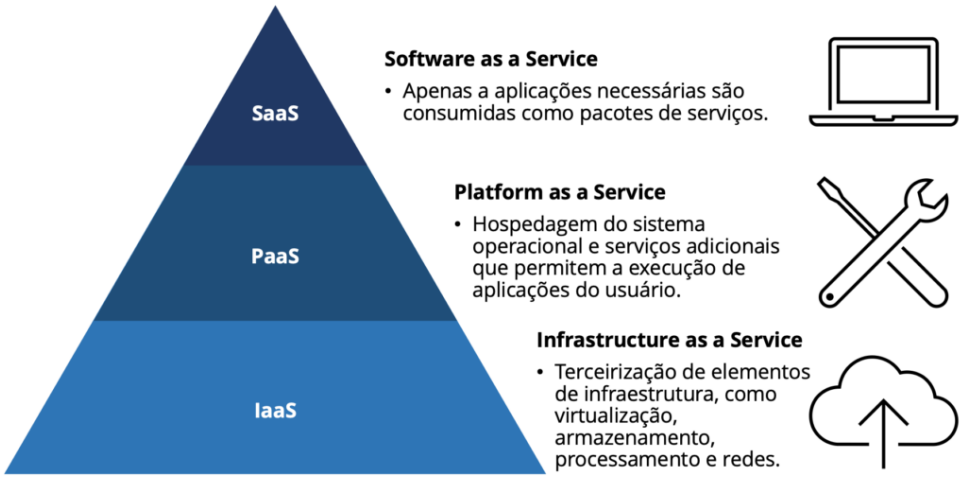
3. Metodologia

A metodologia que foi usada nesse artigo é da forma de uma pesquisa documental baseando-se em artigos de especialistas na área de segurança e acadêmicos, sendo que as conclusões são qualitativas com os dados coletados ao das referências usadas para compor esse trabalho.

4. Virtualização

Segundo Odun-Ayo, Ajayi e Okereke em seu artigo, afirmam que a maioria das atividades na nuvem está baseada na ideia de virtualização, os pesquisadores Kumar e Rathore confirmam que toda a base da infraestrutura da nuvem é o conceito de virtualização. Podemos ver na imagem a seguir os modelos de serviços na nuvem que são baseados em virtualizações (TAURON, 2009).

Figura 1 – Definição dos modelos de serviços na Cloud



Fonte: https://www.doutoriot.com.br/cloud-computing/o-que-e-nuvem/

O conceito básico da virtualização é a utilização de recursos computacionais que imitam outros recursos ou um computador inteiro. Existem várias vantagens em usar virtualizações, como por exemplo a possibilidades de execuções de múltiplos sistemas, economia de recursos, economia do uso de energia, balanceamento de processamento, manutenção, isolamento e maior disponibilidade dos sistemas (SINGH, 2018).

No ponto de vista da segurança, a combinação do isolamento com o fato que se cria uma camada de abstração entre a máquina que hospeda a máquina virtual e a máquina virtual ajuda aumentar a segurança tanto na máquina virtual como na máquina que hospeda a máquina virtual.

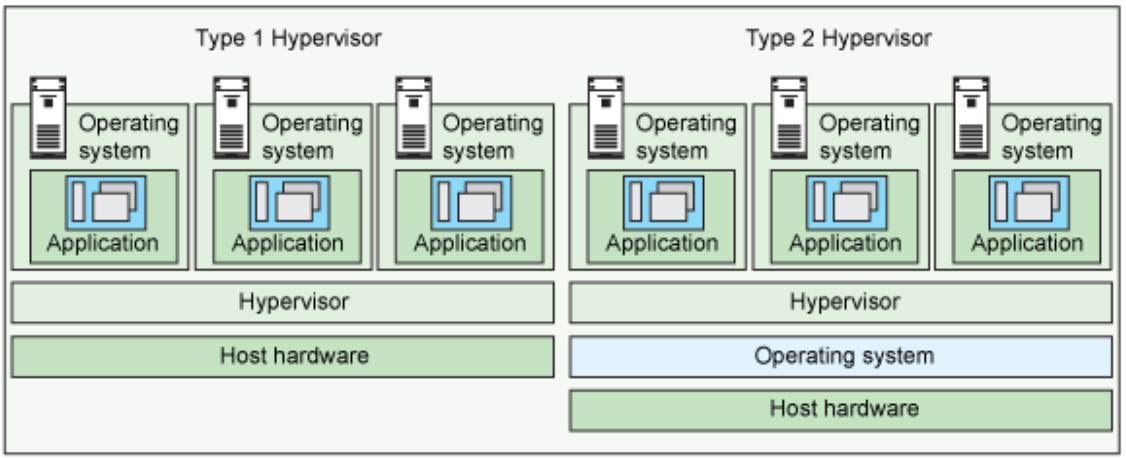
Apesar da tecnologia surgir na década de 1960, ela só teve uma ampla aceitação no início dos anos 2000. Na década de 1990, a maioria das empresas tinha servidores físicos e a tecnologia presa apenas a um servidor. Com isso não permitia a execução de aplicativos de diferentes fornecedores. À medida que as empresas atualizavam os ambientes de TI com servidores comuns, sistemas operacionais e softwares mais econômicos por diferentes fornecedores, ficavam limitadas pela subutilização de hardwares físicos (OUSMANE, IBRAHIMA, DOUDOU, 2018).

Uma solução criativa, foi a virtualização, que resolvia dois problemas principais: as empresas podiam particionar seus servidores e executar softwares legados em vários

tipos e versões de sistema operacional. Com essa adoção de tecnologia aumentou a eficiência dos servidores resultando em uma redução de custos pela aquisição , configuração, refrigeração e manutenção do ambiente TI.

Os hipervisores são programas que separam os recursos físicos dos ambientes virtuais que precisam utilizar esses recursos. Podem ser usados em máquinas comuns como em servidores, e esse é o tipo mais comumente usado na maioria das empresas. Os hipervisores divem os recursos físicos para a utilização de diferentes ambientes virtuais. Existem dois tipos de hypervisors, o do tipo 1 chamado de “bare metal” roda diretamente no sistema da máquina, e o tipo 2 roda em um sistema de hóspede que tem gerenciamento de memória, suporte a máquina e outros recursos de virtualização. na figura 2 pode-se ter uma ideia dos dois tipos de hypervisors (OUSMANE, IBRAHIMA, DOUDOU, 2018).

Figura 2 – Estrutura básica de funcionamento de um Hipervisor



Fonte: https://vapour-apps.com/what-is-hypervisor/

Os recursos são divididos conforme a necessidade entre os ambientes virtuais. Os usuários executam suas atividades nos ambientes virtuais, que recebem o nome de máquina virtual. A máquina virtual funciona como um único arquivo de dados e pode ser transferida de um computador para outro e ser executada em qualquer um.

Podemos perceber que a virtualização pode estar presente em praticamente todos os recursos computacionais. Um outro conceito muito importante entender é o chamado

Full Virtualization, que consiste em uma completa simulação de todo o hardware, inclusive instruções privilegiadas, acesso de memórias e assim por diante.

5. Os Problemas dos ambientes virtuais

Apesar de ter muitas vantagens em ter um ambiente virtual, como foi descrito anteriormente, existem pontos que precisam ser discutidos com atenção. Pesquisadores como Kumar e Rathore dizem que apesar de muito conveniente e eficiente, a computação em nuvem não está sendo adotada em grande parte devido a uma preocupação com segurança. No relatório de Ousamne, Ibrahima e Doudon é exposto as vulnerabilidades associadas à Nuvem em seu relatório (OUSMANE, IBRAHIMA, DOUDOU, 2018).

Fica evidente que existe uma quantidade enorme de vulnerabilidades possíveis em ambiente de nuvem. Isso tem vários motivos, mas o principal é o vasto ecossistema computacional que é necessário para viabilizar o oferecimento de serviços na nuvem. Realmente, existem muitos pontos de ataques que estão disponíveis nessa situação, pois existe uma grande quantidade de códigos que estão sendo executados, infraestruturas sendo utilizadas e todo um compartilhamento isolado que são desafiados a toda hora. Para dar um exemplo, uma linha de código insegura já é o suficiente para que agentes maliciosos possam comprometer o sistema inteiro (COMPASTIÉ, M., BADONNEL, R., FESTOR, 2020).

Na figura 3, 4 e 5 que seguem são apresentados exemplos distintos quanto à classificação dos desafios de segurança em nuvem em relação a tecnologia de virtualização.

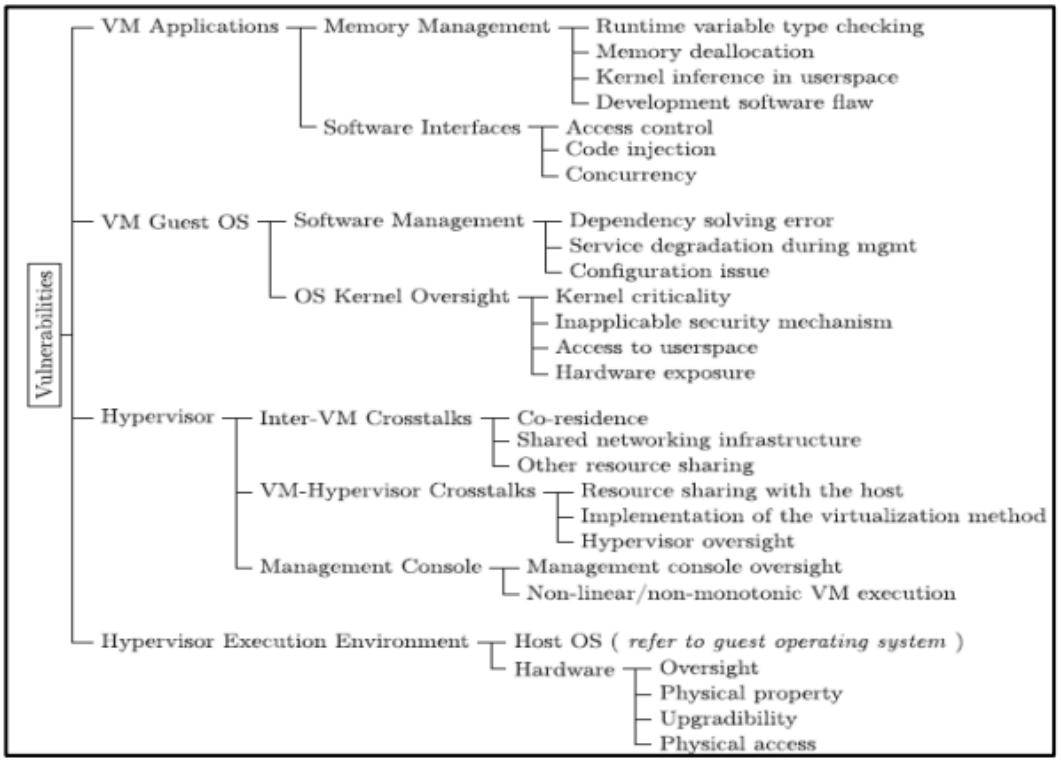
Figura 3 – Vulnerabilidades relacionadas à
virtualização na nuvem apresentado por Ousmane,

Ibrahima e Doudou.

Vulnerabilities	Techniques	Type of attacks
Shared cache	Prime+Probe	Access-driven
Page sharing	Prime+Probe	Access-driven
Huge page	Prime+Probe	Access-driven
Page sharing, inclusive cache	Flush+Reload	Access-driven
Page sharing, inclusive cache	Flush+Reload	Access-driven
Page sharing	Flush+Reload	Access-driven
Xen scheduler	timing attack	Scheduler
Linux 2.6 scheduler	timing attack	Scheduler
4.4BSD	timing attack	Scheduler
History	Brute force attack	Migration and rollback
Hypervisor	-	VM escape
Hypervisor on OpenStack	-	VM escape
Compute node	-	VM escape

Fonte: https://www.ic.unicamp.br/~reltech/PFG/2021/PFG-21-52.pdf

Figura 4 – Vulnerabilidades relacionadas a
virtualização na nuvem apresentado por Compastié,
Badonnel, Festor e He

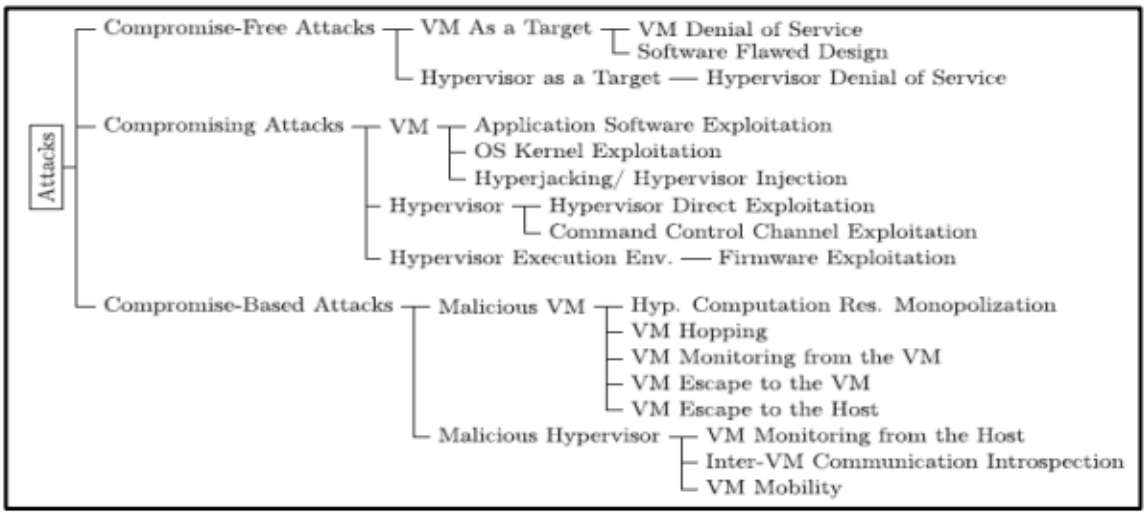


Fonte: https://www.ic.unicamp.br/~reltech/PFG/2021/PFG-21-52.pdf

Figura 5 – Ataques relacionados a virtualização na

nuvem apresentados por Compastié, Badonnel, Gestor e He.

.



Fonte: https://www.ic.unicamp.br/~reltech/PFG/2021/PFG-21-52.pdf

6. Desafios de Segurança em Nuvem

Segundo a CSA (*Cloud Security Alliance*) que é uma entidade não governamental que é dedicada em segurança em cloud computing divulgou uma lista com alguns pontos sensíveis na segurança da nuvem. o diretor da CSA, Jim Reavis juntamente com 29 consultorias levantou esses pontos depois de um longo estudo (CSA, 2022).

6.1 Vazamento ou perda de dados

Não existe um nível aceitável na nuvem. Segundo a CSA, aplicativos podem vazar dados, isso sendo um resultado de mau gerenciamento de API´s, má geração de chaves criptografadas ou não, problemas de armazenamento. Um outro grande problema seria uma falta de política de destruição de dados, podendo até mesmo não existir uma. Um exemplo seria mostrar de uma forma errônea para o usuário que o dado foi destruído, onde apenas foi retirado do índice da tabela de armazenamento e não ter sido realmente deletado.

6.2 Vulnerabilidades de tecnologias compartilhadas

Como a nuvem compartilha recursos para ter uma melhor performance, há uma grande chance de configurações erradas serem compartilhadas, fazendo com que se potencialize o

risco de brechas de acesso. Uma forma de mitigar esse risco seria padronização de processos de atualizações de serviços ou configurações através da rede.

6.3 Ataques internos maliciosos

Segundo Archie Reed, tecnólogo membro da CSA, empresas provedoras de serviço tem seu próprio nível de segurança de acesso aos servidores, mas mesmo com isso pode ter brechas com pessoas com más intenções e que tenham acesso suficiente para contaminar o processo nos servidores.

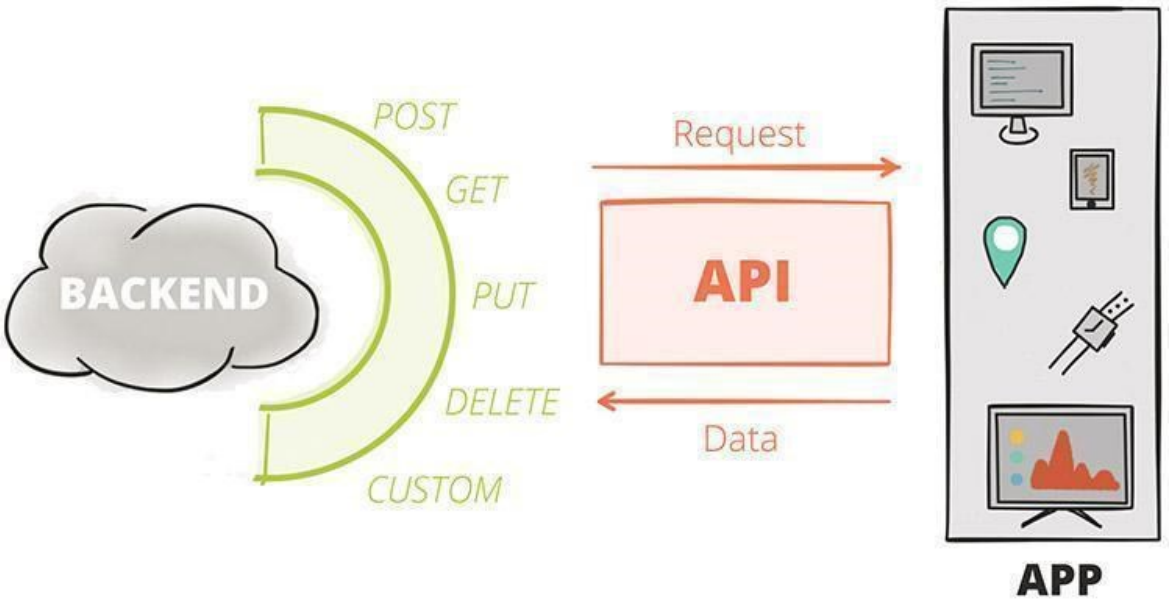
6.4 Desvio de tráfego, contas e serviços

Como boa parte dos aplicativos estão hospedados na cloud. Um outro problema é uma autenticação feita de uma forma insegura pode colocar em risco dados da máquina virtual como por exemplo acesso a conta do cliente ou em alguns casos o acesso de administrador, que nesse caso o invasor teria um acesso a todas as contas e teria um impacto muito maior do que apenas o acesso a conta do cliente.

6.5 API inseguras

Muitas aplicações modernas usam o conceito de consumo de dados usando API´s como é apresentado na figura 6. Mas quando não se tem um cuidado especial para proteger os endpoints do consumo das API´s cria-se um problema com isso. Segundo Archie Reed, APIs inseguras são o “Oeste Selvagem” para ameaças de segurança. Um exemplo bem conhecido aconteceu a aplicativos da Adobe e Microsoft que colocou bad loads e cross scripting. Foi inserido scripts maliciosos em e-mails e acabou comprometendo o ambiente, mesmo que indiretamente isso não seja um problema para a cloud de uma forma geral, isso pode comprometer qualquer sistema, e a cloud também pode correr esse risco quando tem ataques específicos.

Figura 6 – Estrutura básica de funcionamento de uma API



Fonte: https://lvivity.com/what-is-an-api-and-how-does-it-work

6.6 Abuso da computação em nuvem

Isso acontece quando os serviços hospedados sofrem acesso por pessoas não autorizadas com finalidades mal-intencionadas, como por exemplo quebra de senhas e outras ameaças para negócios.

"Todos podem se cadastrar, criar uma conta e começar a usar o serviço para fazer coisas ruins", conforme afirma Reed. O impacto dessa ação não está apenas na ação direta, mas no bloqueio de IPs para clientes que dividem a nuvem com o transgressor. O transgressor acaba tirando recursos dos clientes que precisaria e acaba prejudicando indiretamente.

7. Tópicos principais de segurança na Nuvem

O estudo original da CSA apresentou 15 itens de segurança que estão divididos em segurança tradicional, disponibilidade e controle de dados por terceiros. A seguir vamos expandir cada item com mais detalhes (CSA, 2022).

7.1 Segurança Tradicional

Quando um sistema é migrado para a nuvem, podem ocorrer invasões ou ataques

nesse processo. Os provedores de serviços de nuvem afirmam que seus ambientes estão mais seguros do que sistemas locais. Mas existe uma grande preocupação de segurança como por exemplo: Ataque ao nível das máquinas virtuais, vulnerabilidade no hypervisor ou na tecnologia que de virtualização das máquinas virtuais que os provedores usam, os provedores rebatem dizendo que seus firewalls são sempre atualizados e monitoradas 24/7. Um outro ponto seria vulnerabilidades a nível de plataforma no provedor, podemos ressaltar como exemplo injeção de SQL ou script cross -site no salesforce.com. Esse tipo de ataque é muito comum, mesmo serviços como google doc tem sofrido com esses tipos de ataques. Provedores como a IBM Cloud usam uma ferramenta Rational AppScan que procura por vulnerabilidades na nuvem (ALI, M., KHAN, S. U., VASILAKOS, 2015).

O *phishing attack* é um ataque que se baseia em engenharia social onde o invasor tenta se passar por alguém confiável como por exemplo um site.

Um outro exemplo de vulnerabilidade é quando o usuário tem que proteger a conexão de seu ambiente local com o ambiente da nuvem, geralmente ambientes híbridos tem pontos sensíveis de segurança.

7.2 Disponibilidade

Nesse tópico iremos analisar a disponibilidade de dados críticos. Os provedores afirmam que sua gestão é mais eficiente e mais segura do que a própria empresa em seus datacenters. O CEO da SAP, Leo Apotheker, afirma que certos serviços não podem ser colocados na nuvem, pois essa pode entrar em colapso.

Os provedores são considerados como tendo uma disponibilidade muito maior do que sistemas locais, mas isso não é verdade por completo. Se imaginarmos um ataque que tenta derrubar um serviço hospedado, pode também derrubar outros serviços que não eram alvos do ataque inicial.

7.3 Controle de dados por terceiros

Quando pensamos como é mantido dados armazenados, acabamos por não entender a implicação direta de como os dados podem ser manipulados e armazenados. Um exemplo disso é o risco quando os dados são manipulados por terceiros é a falta de controle e a transparência. Uma das vantagens da cloud é a permissão de implementações de forma independente, mas isso é contra as regulamentações da cloud que exigem transparência. Resumidamente, a mesma transparência que facilita alguns serviços impede de ter um maior

controle sobre os seus dados.

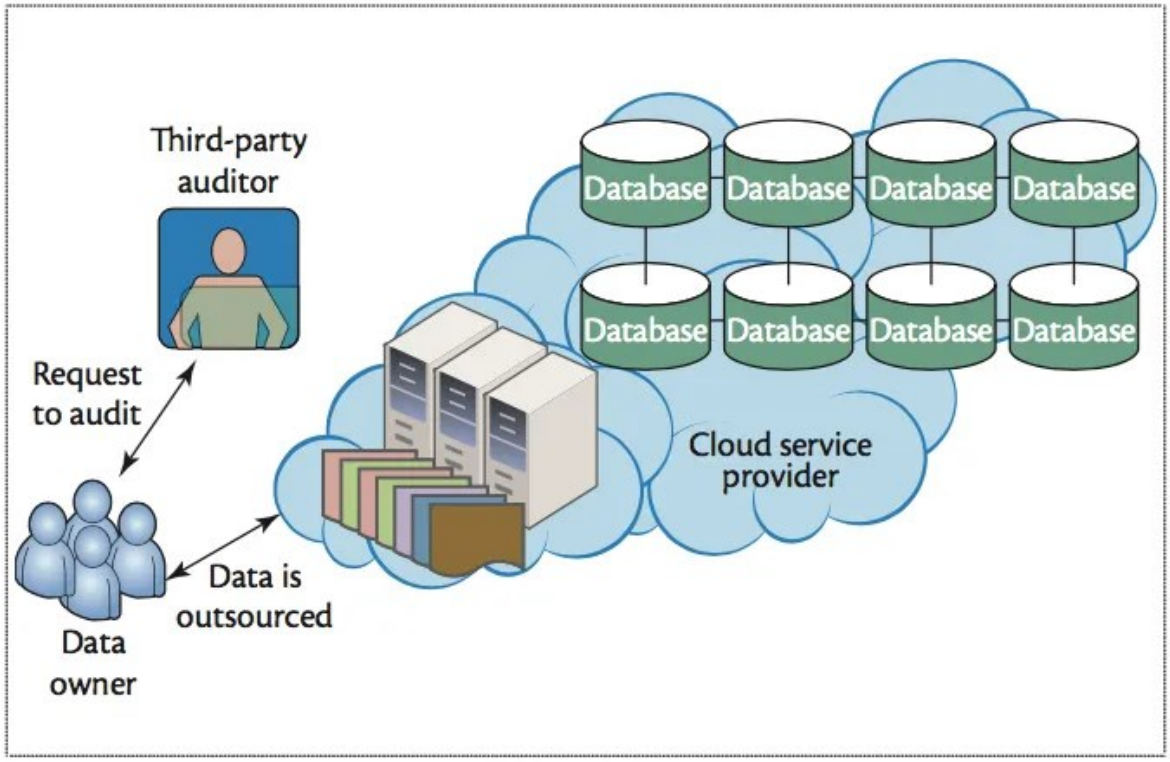
Uma forma de amenizar esse problema seria a criação de nuvens privadas e mesmo assim continuar a usar os benefícios da nuvem.

Um exemplo que vale ressaltar é o do CEO da *Scalent Systems*, Benjamin Linder que afirma que existem muitas empresas que têm dificuldades em confiar por completo em nuvens externas com sistemas proprietários e de alta disponibilidade. Para resolver isso, estão criando nuvens internas que atendem suas necessidades e têm um controle maior.

Um ponto muito relevante, seria no caso quando uma empresa contratante da nuvem, tem que excluir dados por motivos judiciais, existem garantias que tais dados foram realmente excluídos na nuvem? ou que o provedor tenha uma resposta em tempo hábil quando a empresa contratante precisa responder alguma ação judicial.

O problema da audibilidade é um ponto muito questionado também. A revista Information Security Magazine questiona como é possível fazer auditoria de um sistema de uma empresa quando está totalmente na nuvem, no qual está distribuído por todo o globo, na figura a seguir pode-se ter uma ideia. Isso acaba se tornando muito difícil para auditores comprovarem que dados estão seguros e não podem ser acessados de uma forma indevida.

Figura 7 – Esquema de auditoria de dados em nuvem.



Fonte: https://www.infoq.com/articles/cloud-data-auditing/

Uma preocupação relacionada diz respeito à administração de atividades em nuvem. Algumas diretrizes de auditoria exigem que dados sejam processados em uma determinada localidade geográfica. As provedoras de nuvem estão respondendo a isso com ofertas de produtos geolocalizados, que garantem esse requisito.

8. Resultados e Discussões

Em virtude da importância atribuída ao tema, este trabalho tem como objetivo realizar uma revisão da literatura sobre a Governança de Segurança da Informação em ambientes de Computação em Nuvem. Para tanto, a pesquisa bibliográfica foi realizada utilizando os principais mecanismos de busca disponíveis na web (Google, Google Acadêmico, Scopus e IEEE Xplore).

Os resultados obtidos permitem concluir que a Governança de Segurança da Informação em Computação em Nuvem é um tema relevante e de extrema importância para as organizações que desejam adotar a Computação em Nuvem como solução de TI.

Para minimizar os riscos de ataques à nuvem, recomenda-se que sejam utilizados

mecanismos de segurança, tais como criptografia, controle de acesso, detecção e resposta a incidentes. Além disso, é importante manter o ambiente sempre atualizado, utilizando as últimas ferramentas de segurança disponíveis e monitorando constantemente as atividades da nuvem.

9. Considerações Finais

Apesar de existirem algumas falhas pontuais de segurança na nuvem, boa parte dos provedores de nuvem estão trabalhando para cada vez mais oferecer serviços que possam suprir as necessidades dos usuários e garantir segurança por todos os serviços do provedor, contudo é preciso avaliar quais partes da empresa é viável a migração para a nuvem levando em relação ao risco e benefícios desta migração.

É uma questão de tempo até que as empresas possam mudar seus processos internos e usem mais e mais serviços da nuvem uma vez que existem uma flexibilidade em seus vários modos de operação.

Referências

ALECRIM, Emerson. O que é Cloud Computing? InfoWester, São Paulo, dez. 2008. Disponível em:<http://www.infowester.com/cloudcomputing.php>. Acesso em: 28 out. 2022

ALI, M., KHAN, S. U., VASILAKOS, A.V. Security in Cloud Computing: Opportunities and Challenges. Artigo Científico. North Dakota State University, Kuwait University e COMSATS Institute of Information Technology. (2015)

COMPASTIÉ, M., BADONNEL, R., FESTOR, O. e HE, R. From virtualization security issues to cloud protection opportunities: An in-depth analysis of system virtualization models. Artigo Cientìfico. University of Lorraine e Orange Labs. (2020).

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

CSA, Paolo del Nibletto. ”The Seven Deadly Sins In Cloud Computing” http://www.itbusiness.ca/it/client/en/home/News.asp?id=56870, Accesso em: 28 out. 2022

KUMAR, V. e RATHORE, R. S. Security Issues with Virtualization in Cloud Computing. Artigo Científico. Galgotias College of Engineering and Technology. (2018)

ODUN-AYO, I., AJAYI, O. e OKEREKE, C. Virtualization in Cloud Computing: Development and Trends. Artigo Científico. Covenant University e University of Lagos Nigeria. (2017)

OUSMANE, S. B., IBRAHIMA, N. e DOUDOU, F. A Review of Virtualization, Hypervisor and VM allocation Security: Threats, Vulnerabilities, and Countermeasures. 24 Artigo Científico. Cheikh Anta Diop University e Nara Institute of Science and Technology. (2018)

PEREIRA BORGES, H. et al. COMPUTAÇÃO EM NUVEM. [s.l: s.n.]. Disponível em: <https://livroaberto.ibict.br/bitstream/1/861/1/COMPUTA%c3%87%c3%83O%20EM%20NUVEM.pdf>.

TAURION, Cezar. Cloud Computing: computação em nuvem. Rio de Janeiro, ed. Brasport, 2009.

SINGH, M. Virtualization in Cloud Computing - A Study. Artigo Científico. Government of NCT of Delhi. (2018)

Agradecimentos

Gostaria de deixar meu agradecimento ao professor Cleberson por suas valiosas considerações em revisões e discussões que puderam nos guiar no estudo um pouco mais aprofundado na área de segurança na Cloud.