VULNERABILIDADES DE NUVENS COMPUTACIONAIS

Data de aceite: 01/09/2023

Jhoyce Kelly Bonfort Santos
Universidade de Vassouras
Vassouras-RJ

David Caravana de Castro Moraes Ricci
http://lattes.cnpq.br/5353303642350569

RESUMO: A segurança na nuvem é uma disciplina de segurança cibernética dedicada a proteger sistemas de computação em nuvem. Isso inclui manter os dados privados e seguros em toda a infraestrutura, aplicativos e plataformas online. Proteger esses sistemas envolve os esforços dos provedores de nuvem e dos clientes que os utilizam. Os provedores de serviços em nuvem hospedam os serviços em seus servidores por meio de conexões de Internet sempre ativas. Como sua empresa depende da confiança do cliente, os métodos de segurança na nuvem são usados para manter os dados do cliente privados e armazenados com segurança. No entanto, a segurança na nuvem também está parcialmente nas mãos do cliente. Compreender ambas as facetas são fundamentais para uma solução de segurança em nuvem saudável. Sendo assim, o objetivo do presente trabalho é apresentar a vulnerabilidade de nuvens computacionais. A metodologia é de referencial bibliográfico.

PALAVRA-CHAVE: Computação em nuvem. Segurança cibernética. Provedor de nuvem.

COMPUTING CLOUD VULNERABILITIES

ABSTRACT: Cloud security is a cybersecurity discipline dedicated to protecting cloud computing systems. This includes keeping data private and secure across infrastructure, applications and online platforms. Securing these systems involves the efforts of cloud providers and the customers who use them. Cloud service providers host the services on their servers over always-on internet connections. As your business depends on customer trust, cloud security methods are used to keep customer data private and securely stored. However, cloud security is also partly in the hands of the customer. Understanding both facets are critical to a healthy cloud security solution. Therefore, the objective of this work is to present the vulnerability of computational clouds. The methodology is based on a bibliographic reference.

KEYWORDS: Cloud computing. Cyber security. Cloud provider

1 | INTRODUÇÃO

A segurança na nuvem é o conjunto de estratégias e práticas para proteger dados e aplicativos hospedados na nuvem. Assim como a segurança cibernética, a segurança na nuvem é uma área muito ampla e é impossível evitar todos os tipos de ataques. No entanto, uma estratégia de segurança em nuvem bem projetada reduz muito o risco de ataques cibernéticos.

A computação em nuvem normalmente, diante de tanto risco ainda é considerada mais segura quando comparada a computação local, visto que, os provedores de nuvem possui mais recursos de segurança e é capaz de manter os dados mais seguros, o que de fato obriga os provedores de nuvem a manter uma infraestrutura mais atualizada, com constante correção de possíveis vulnerabilidade de maneira mais rápida.

A segurança na nuvem é toda a tecnologia, protocolos e práticas recomendadas que protegem os ambientes de computação em nuvem, os aplicativos executados na nuvem e os dados armazenados na nuvem. A segurança na nuvem começa com a compreensão exata do que está sendo protegido, bem como quais aspectos do sistema precisam ser gerenciados.

O desenvolvimento do suporte contra vulnerabilidades de segurança está, em grande parte, nas mãos dos provedores de serviços em nuvem. Além de escolher um provedor preocupado com a segurança, os clientes precisam se concentrar acima de tudo na configuração adequada do serviço e nos hábitos de uso seguro, devem garantir que o hardware e as redes do usuário final estejam devidamente protegidos.

Uma segurança de nuvem fraca pode expor usuários e provedores a todos os tipos de ameaças de segurança cibernética. Algumas ameaças comuns à segurança na nuvem incluem: riscos de infraestrutura baseados em nuvem, incluindo plataformas de computação herdadas incompatíveis e interrupções em serviços de armazenamento de dados de terceiros; ameaças internas devido a erro humano, como configuração incorreta dos controles de acesso do usuário; e ameaças externas causadas quase exclusivamente por agentes mal-intencionados, como malware, phishing e ataques DDoS.

Diante disso surge a seguinte questão: Quais são os problemas de segurança na nuvem? Para responder à questão o objetivo do presente trabalho é apresentar a vulnerabilidade de nuvens computacionais. A metodologia é referencial bibliográfico.

2 | DESENVOLVIMENTO

As principais tecnologias voltadas para a segurança na nuvem, possui estratégias tecnológicas como a criptografia, cujo sistema embaralha todos os dados para que somente as partes autorizadas podem entender as informações que estão guardadas. Sendo assim, se invasor tentar invadir a nuvem de um cliente ou empresa e não encontrar a criptografia,

terá a oportunidade de fazer qualquer tipo de ação maliciosa com esses dados, como vende-los, vaza-los, ou usar os mesmos para um ataque, entre outras coisas. (MELO, 2022).

Contudo, se esses dados estiverem criptografados o invasor somente encontrará os dados protegidos, ou seja, criptografados e não poderá fazer nada, exceto se de alguma maneira encontrar a chave da criptografia, o que praticamente é impossível. Por isso a criptografia ajuda a prevenir ataques de invasores evitando divulgação ou vazamento dos dados, mesmo diante de falhas de outras medidas de segurança. (SILVA, 2019).

A criptografia dos dados pode ocorrer de duas formas, ou seja, em trânsito – que seria no mesmo tempo que estiver sendo enviado a outro lugar e em repouso, que seria o momento que está sendo armazenado. É importante que a criptografia seja realizada dessas duas maneiras, pois isso evitará que possíveis invasores possam intercepta-los e ainda realizar a leitura. (PETER; CHRISTIAN, 2019).

A modalidade da criptografia em trânsito precisa abordar os dados que trafegam entre um usuário e em nuvem. Esses dados que trafegam de uma nuvem para outra é como uma nuvem híbrida ou ambiente *multicloud.* Sendo assim, os dados tem que ser criptografados quando estão sendo armazenados dentro de um banco de dados ou ainda a partir de serviços de armazenamento de nuvem. (MELO, 2022).

Vale mencionar que, se as nuvens multicloud ou híbrida estiverem conectadas diretamente na camada de rede, a criptografia pode acorrer em trafego por VPN. E se a conexão for por camada de aplicativo, essa criptografia ocorre em SSL/TLS, pois o mesmo precisa criptografas o tráfego entre nuvem e usuário. (SILVA, 2019).

De acordo com Peter e Christian (2019), no Gerenciamento de Identidade e Acesso (GIA) o rastreamento é na identificação do usuário e o que o mesmo pode fazer, como também ocorre a autorização e negação do acesso para aqueles que não são autorizados. O GIA é de grande importância na computação da nuvem devido a identificação do usuário e o privilégio de acesso aos dados, e não permite que a localização e ou dispositivo do usuário.

Sendo assim, o GIA reduz a ameaça de usuários que não estão autorizados em acessar ativos internos ou ainda de não fazer uso de forma excessiva aos privilégios. Para Peter e Christian (2019), o GIA de certa forma ajuda a mitigar diversas modalidades de ataques, como ataques internos e principalmente invasões de contas, podendo incluir diversos serviços de diferentes modalidades ou ainda pode ser um único serviço, mas que combina como seguintes recursos:

- Os serviços de logon único (SSO), o qual autentica identidades dos usuários para diferentes aplicativos, de forma que os usuários somente precisam fazer seu login e acessar os serviços em nuvem;

- Provedor de identidade (IdPs) o qual somente realiza a identidade do usuário;

- O serviço de Firewall, o qual controla o acesso, restringindo ou permitindo o acesso

do usuário firewall, já que o mesmo fornece na nuvem uma camada de proteção em volta dos ativos, bloqueando diretamente o tráfego de qualquer web malicioso e;

- O serviço de autenticação multifator, o qual fortalece diretamente a autenticação do usuário.

No entendimento de Silva (2019), os firewalls tradicionais são hospedados de forma local e apenas defendem o perímetro da rede, mas o firewall em nuvem se hospeda na própria nuvem e com isso forma uma forte barreira de segurança em toda a infraestrutura da nuvem.

Lembrando que a maioria do firewall relacionado a aplicativo também se encaixa nesta categoria. Os firewall de nuvem é capaz de bloquear os ataques do DDoS, cuja atividade de bot é maliciosa e possui alto grau de exploração de vulnerabilidade, e isso proporciona uma redução nos ataques cibernéticos que prejudica diretamente a infraestrutura da nuvem de qualquer organização. (SILVA, 2019).

As mais importante práticas para manter em segurança todos os dados de uma nuvem, além de todas as mencionada acima ou quaisquer produto que for adicionado na segurança, ainda não é suficiente para proteger de forma completa a nuvem, pois as melhores práticas voltadas para a segurança cibernética ainda precisa alguns requisitos. (SOUZA; MIERS, 2019).

Um desses requisitos seria a correta configuração da segurança do próprio servidor da nuvem, isto é, a partir do momento que uma organização não é capaz de configurar corretamente a segurança, poderá acontecer um vazamento dos dados, por isso, servidores em nuvem que não foi corretamente configurado tem a chance de ter seus dados públicos na internet. (THOMAZ *et al.,* 2022).

Contudo, para definir de forma correta as configurações de segurança na nuvem é necessário ter um especialista em segurança na nuvem, já que existe a possibilidade de uma colaboração próxima diretamente com o provedor da nuvem. Desta forma, Souza e Miers (2019) afirmam que políticas de segurança que sejam consistentes em nuvem e principalmente em data centers, são de fatos medidas de segurança que deve ser aplicada em qualquer e toda infraestrutura das empresas, em especial quando se tratar de nuvens públicas, local e privada. (SOUZA; MIERS, 2019).

Melo (2022) afirma que se qualquer aspecto da infraestrutura de nuvem de uma organização – com o serviço de nuvem de caráter público com o processamento de big data não for protegido com uma boa criptografia de autenticação do usuário, é bem provável que ocorra invasão atacando diretamente o elo mais fraco. (MELO, 2022).

Em planos de backup, conforme qualquer outro tipo de segurança, precisa existir um plano para ser usado quando as coisas derem errado e sair do controle e der tudo errado. É muito importante que todos os dados sejam copiados para evitar perde-los mediante uma adulteração ou mesmo por perde-los. Devendo sempre existir um plano *failover* vigorando para que jamais haja interrupção dos processos de negócios caso a segurança da nuvem

falhar. (THOMAZ *et al.,* 2022).

Conforme afirma Thomaz et al., (2022) as vantagens da nuvem híbridas ou multicloud é que diferentes nuvens podem permite fazer bachup de forma simultânea, ou seja, o armazenamento de dados na nuvem também pode ser realizado em um banco de dados local.

Por isso, é muito importante a capacitação de funcionários e usuários, pois a porcentagem mais de violação dos dados acontece devido um ataque de *phishing*, que acabou sendo instalado um malware sem saber, ou seja, a partir do uso de um dispositivo que esteja desatualizado e totalmente vulnerável. Após a capacitação, certamente existe uma redução do risco de sofrer um ataque de malware. (THOMAZ *et al.,* 2022).

O maior risco representado pela nuvem é que não há perímetro. A segurança cibernética tradicional se concentra na proteção do perímetro, mas os ambientes de nuvem são altamente conectados, o que significa interfaces de programação de aplicativos (APIs) inseguras e sequestros de contas podem representar problemas reais. (SOUZA; MIERS, 2019).

Diante dos riscos de segurança que afetam a computação em nuvem, os profissionais de segurança cibernética devem adotar uma abordagem mais centrada nos dados. A interconexão também apresenta problemas para as redes. Atores mal-intencionados geralmente acessam redes devido a credenciais comprometidas ou fracas. (MELO, 2022).

Depois que um hacker obtém acesso a uma rede, ele pode facilmente se espalhar e usar as interfaces mal protegidas da nuvem para localizar dados em diferentes bancos de dados. Pode até usar seus próprios servidores em nuvem como destino para exportar e armazenar os dados roubados. A segurança tem que estar na nuvem e não servir como elemento exclusivo de proteção contra o acesso aos dados ali armazenados. (THOMAZ *et al.,* 2022).

O armazenamento de dados por terceiros e o acesso via Internet também representam suas próprias ameaças. Se, por qualquer motivo, esses serviços forem interrompidos, o acesso aos dados poderá ser perdido. Por exemplo, uma interrupção na rede telefônica pode significar que a nuvem não pode ser acessada em um momento essencial. (SOUZA; MIERS, 2019).

Como alternativa, uma queda de energia pode afetar o data center onde os dados são armazenados, o que pode levar à perda permanente de dados. Tais interrupções podem ter repercussões de longo prazo. Uma queda de energia em uma instalação de dados em nuvem da Amazon resultou na perda de alguns dados do cliente devido a falhas de hardware do servidor. Este é um bom exemplo de por que deve ter backups locais de pelo menos alguns dados e aplicativos. (THOMAZ *et al.,* 2022).

O que torna a segurança na nuvem diferente é que a segurança tradicional do computador passou por uma imensa evolução devido à mudança para a computação baseada em nuvem. Embora os modelos de nuvem permitam maior conveniência, a

conectividade sempre ativa requer novas considerações para mantê-la segura. A segurança na nuvem, como uma solução de segurança cibernética modernizada, difere dos modelos de computação herdados de algumas maneiras. (MELO, 2022).

A *Data Warehousing* – A maior distinção é que os modelos de TI mais antigos dependiam fortemente do data *warehousing* local. As empresas há muito descobriram que criar todas as plataformas de computação internas para controles de segurança granulares e personalizados é caro e rígido. As plataformas baseadas em nuvem ajudaram a transferir os custos de desenvolvimento e manutenção de sistemas, mas também a remover algum controle dos usuários. (THOMAZ *et al.,* 2022).

A velocidade de dimensionamento, da mesma forma, a segurança na nuvem exige atenção exclusiva ao dimensionar os sistemas corporativos de TI. A infraestrutura e os aplicativos centrados na nuvem são altamente modulares e rapidamente mobilizados. Embora essa capacidade mantenha os sistemas consistentemente ajustados às mudanças nos negócios, ela também apresenta problemas quando a necessidade de melhorias e conveniência de uma empresa supera sua capacidade de acompanhar a segurança. (SOUZA; MIERS, 2019).

Em relação a interface do sistema do usuário final, para empresas e usuários individuais, os sistemas em nuvem também se conectam a muitos outros sistemas e serviços que precisam ser protegidos. As permissões de acesso devem ser mantidas desde o nível do dispositivo do usuário final até o nível do *software* e até mesmo o nível da rede. Além disso, fornecedores e usuários devem estar cientes das vulnerabilidades que podem causar por meio de acesso inseguro ao sistema e comportamentos de configuração. (MELO, 2022).

Quanto a proximidade com outros dados e sistemas em rede, como os sistemas em nuvem são uma conexão persistente entre os provedores de nuvem e todos os seus usuários, essa importante rede pode comprometer até o próprio provedor. Em ambientes de rede, um único dispositivo ou componente fraco pode ser explorado para infectar o restante. (THOMAZ *et al.,* 2022).

Os provedores de nuvem se expõem a ameaças dos muitos usuários finais com os quais interagem, estejam eles fornecendo armazenamento de dados ou outros serviços. Responsabilidades adicionais pela segurança da rede recaem sobre os fornecedores cujos produtos entregues, de outra forma, dependeriam apenas dos sistemas dos usuários finais e não dos seus próprios. (MELO, 2022).

3 I CONCLUSÃO

Resolver a maioria dos problemas de segurança na nuvem significa que tanto os usuários quanto os provedores de nuvem, tanto em ambientes pessoais quanto empresariais, devem ser proativos em relação às suas próprias funções de segurança

cibernética.

Essa abordagem em duas frentes significa que usuários e provedores precisam abordar o seguinte: configuração e manutenção segura do sistema; educação em segurança do usuário, tanto no nível comportamental quanto no nível técnico. Sendo assim, conclui que os provedores e usuários de nuvem devem ter transparência e responsabilidade para garantir que ambas as partes estejam seguras.

REFERÊNCIAS

MELO, V. R. **Computing cloud:** vulnerabilidade de nuvens computacionais com ênfase na infraestrutura da Google. São Luís: Centro Universitário UNDB, 2022.

MELO, A O. **As *fake news* e seu potencial risco para a segurança de ativos informacionais pessoais:** um estudo acerca das vulnerabilidades dos estudantes do Centro de Ciências Sociais Aplicadas da UFRN. 2022. 129f. Monografia (Graduação em Biblioteconomia) - Centro de Ciências Sociais Aplicadas, Universidade Federal do Rio Grande do Norte, Natal, 2022.

PETER, L. N; CHRISTIAN, M. C. **Caracterização do tráfego de rede de nuvens computacionais OpenStack com ênfase na segurança de contêineres.** In: ESCOLA REGIONAL DE ALTO DESEMPENHO DA REGIÃO SUL (ERAD-RS), 19., 2019, Três de Maio. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2019. ISSN 2595-4164.

SILVA, M. P. H. **Uma metodologia para melhorar a segurança em ambientes de computação em nuvem:** estudo de caso 2019. 41 f. TCC (Graduação em Redes de Computadores) - Universidade Federal do Ceará, Campus de Quixadá, Quixadá, 2019.

SOUZA V. O. K; MIERS, C. **Uma análise de segurança no uso de contêineres do tipo Docker em nuvens IaaS OpenStack**. In: ESCOLA REGIONAL DE ALTO DESEMPENHO DA REGIÃO SUL (ERAD-RS), 19., 2019, Três de Maio. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2019. ISSN 2595-4164.

THOMAZ, G. A.; *et al.,* **CACIC:** Controle de Acesso Confiável Usando Enclaves a Dados em Nuvem da Internet das Coisas. In: SIMPÓSIO BRASILEIRO DE REDES DE COMPUTADORES E SISTEMAS DISTRIBUÍDOS (SBRC), 40., 2022, Fortaleza. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2022. p. 573-586. ISSN 2177-9384. DOI: https://doi.org/10.5753 /sbrc.20 22.222377.