Pesquisa Experimental sobre Ataques Cibernéticos em Infraestruturas de Nuvens Públicas Baseadas em Microsoft Azure

Mateus Da Silva Dos Santos[1], **Daniel Stefani Marcon**[2]

[1]Universidade do vale do rio dos sinos - Unisinos
Av. Unisinos - 93022-750 - São Leopoldo - RS - Brasil

mateussantos@edu.unisinos.br, danielstefani@unisinos.br

Abstract. *The cloud infrastructure has become an essential model for meeting business needs as well as IT needs. Similar to other disruptive technologies, the cloud infrastructure is expected to meet a certain level of information security. In this scenario, this paper performs experiments regarding security solutions available in Microsoft Azure public infrastructure and evaluates the efficiency and effectiveness of available controls through cyber attacks. The obtained results show low effectiveness of security mechanisms offered by Microsoft Azure and demonstrate resource consumption overhead due to Azure Security Center activation.*

Resumo. *A infraestrutura em nuvem se tornou um modelo primordial para atender às necessidades do negócio e da TI das organizações. Assim como outras tecnologias disruptivas, a infraestrutura em nuvem também aborda de forma robusta a segurança da informação. Neste cenário, este artigo realiza uma pesquisa experimental das soluções de segurança disponíveis no ambiente de infraestrutura como serviço da Microsoft Azure e apresenta uma avaliação da eficiência e da efetividade dos controles disponíveis através de ataques cibernéticos. Os resultados obtidos mostram a baixa efetividade dos mecanismos de segurança oferecidos pela Microsoft Azure e demonstram os acréscimos relacionados ao desempenho da solução de segurança empregada pelo provedor.*

1. Introdução

Uma das tecnologias que surgiram para apoiar a transformação dos negócios e também da própria infraestrutura de TI é a infraestrutura baseada em nuvem. A computação em nuvem emergiu como um dos novos paradigmas da computação e atraiu o interesse dos provedores de tecnologia e dos usuários que a utilizam [Zimba and Chama 2018]. Em contrapartida, a computação em nuvem herda os desafios das tecnologias subjacentes. Uma das preocupações mais debatidas a esse respeito é a segurança da informação. Como a computação em nuvem é desenvolvida utilizando várias tecnologias que possuem seus próprios desafios, as preocupações com segurança são equitativamente proporcionais, pois devem proteger o entrelaçado de tecnologias que compõem uma infraestrutura de nuvem [Zimba and Chama 2018].

O presente artigo apresenta uma pesquisa experimental com base na solução de segurança *Azure Security Center* disponibilizada pela Microsoft, a qual possui o objetivo de oferecer uma proteção avançada contra ataques cibernéticos em infraestrutura de nuvem como serviço. O resultado do experimento apresenta a efetividade e os acréscimos relacionados ao desempenho da solução.

As principais contribuições deste trabalho são: (i) avaliar a efetividade e desempenho dos controles de segurança disponibilizados pelo provedor Microsoft; (ii) apresentar os resultados e métodos para execução de ataques cibernéticos em uma infraestrutura de nuvem como serviço (IaaS); e (iii) a análise dos dos resultados, os quais demonstram uma baixa efetividade da solução *Azure Security Center* para detecção de ataques cibernéticos e uma sobrecarga de utilização dos recursos computacionais após ativação da solução de segurança.

O restante do artigo está estruturado da seguinte maneira. A Seção 2 discute os trabalhos relacionados. A Seção 3 descreve a metodologia utilizada e a Seção 4 apresenta os experimentos e os resultados obtidos. Por fim, a Seção 5 descreve as conclusões e perspectivas de trabalhos futuros.

2. Trabalhos Relacionados

Esta seção tem o objetivo de apresentar os principais trabalhos relacionados sobre segurança cibernética em nuvem. [Golnoosh Tajadod, Lynn Batten, K.Govinda 2012] realizaram uma avaliação e comparação das soluções de segurança disponibilizadas pelos provedores Amazon e Microsoft. O artigo apresenta detalhes sobre as comparações realizadas com foco específico em confidencialidade, integridade e disponibilidade dos dados. A análise ocorreu através de avaliações das características e informações disponibilizadas por cada provedor de nuvem. Por meio da pesquisa, os autores concluíram que ambos os provedores de serviços incluíram definições significativas para lidar com problemas de segurança. No entanto, a solução de segurança oferecida pela Microsoft consegue oferecer controles avançados de integridade e confidencialidade de dados e, portanto,do ponto de vista de segurança, a Microsoft oferece um nível de segurança mais adequado em comparação com o provedor Amazon.

Já [Roveda et al. 2016] se baseiam no trabalho de taxonomia de infraestruturas de nuvem desenvolvido por [Dukaric and Juric 2013] e realizam uma análise das peculiaridades de segurança oriundas de ferramentas de nuvem *open source*, como, por exemplo, as soluções *OpenStack*, *Open Nebula* e *CloudStack*. Tais trabalhos, no entanto, apresentam um comparativo qualitativo das soluções de segurança, sem comprovar a eficácia e usabilidade dos controles de segurança.

O estudo de [Hugo and Moia 2015] propõe uma abordagem prática para a utilização de criptografia de arquivos, com objetivo de garantir a confidencialidade e integridade das informações armazenadas em nuvem. Todavia, a pesquisa apresenta lacunas de segurança relacionadas ao ambiente que hospeda os servidores e, consequentemente, riscos relacionados ao armazenamento das chaves criptográficas utilizadas no processo de criptografia. O trabalho de [Medeiros 2014] foca em ataques de negação de serviço em nuvem. A metodologia utilizada pelo autor possui semelhança com este trabalho. Porém, o autor direciona seus controles em soluções de IDS (*intrusion detection system*) próprias (geralmente sem escalabilidade), utilizando métodos defasados de assinatura de anomalias (ou seja, insuficientes atualmente).

[Naseer Amara, Huang Zhiqui, Awais Ali 2017] apontam os principais problemas de segurança relacionados a soluções em nuvem, realçando que a segurança é a principal barreira à sua adoção. O estudo destaca os princípios arquiteturais da computação em nuvem, ameaças à segurança em nuvem e técnicas para mitigação. Destaca-se que o trabalho apresenta uma grande diversidade de ataques para todos os modelos de nuvem. Entretanto, não apresenta de forma experimental os ataques citados. Os autores concluem

que muitas pesquisas estão sendo conduzidas sobre a segurança em nuvem, mas devido à rápida evolução da tecnologia, os pesquisadores e engenheiros de segurança têm sido incapazes de fornecer soluções competitivas de acordo com os crescentes problemas encontrados nessa área. Como trabalhos futuros destacam-se a implementação de técnicas para avaliar a eficácia dos métodos de mitigação apresentados e a possibilidade de ocorrências das ameaças.

3. Metodologia

A pesquisa é definida como um procedimento racional e sistemático que possui o objetivo de proporcionar respostas aos problemas que são propostos [Antônio Carlos Gil 2002]. Ela é requerida quando não se dispõe de informações suficientes para responder a determinado problema, ou então quando a informação disponível se encontra em tal estado de desordem que não pode ser adequadamente relacionada ao problema. O tema desenvolvido neste artigo é importante pelo fato de não existirem informações imparciais referente à eficiência e desempenho das soluções de segurança disponibilizadas pelo provedor Microsoft *Azure* frente a ataques cibernéticos.

A análise experimental consiste em determinar um cenário de estudo, selecionar as variáveis capazes de influenciá-lo e definir os modelos de controle e observação dos efeitos que as variáveis aplicadas produzem no objeto. Portanto, trata-se de um estudo em que o pesquisador é um agente ativo durante a análise, e não um observador passivo [Antônio Carlos Gil 2002].

Nesse contexto, o termo experimento possui duas acepções, uma geral e outra específica [Hernandez Sampieiri 2013]. Este trabalho emprega a metodologia definida como pesquisa experimental e utiliza a acepção específica, a qual refere-se a definir os estímulos e após analisar as consequências e resultados obtidos através dos estímulos executados.

Com o objetivo de manter o experimento neutro (sem influência de fornecedores ou soluções de segurança), todos os estímulos definidos para o experimento seguiram como base a documentação sobre testes de invasão em nuvem [Cloud Security Alliance 2019], elaborada pela *Cloud Security Alliance* em conjunto com a comunidade técnica.

4. Experimentos

Para o presente experimento, definiu-se a implementação de todos os recursos computacionais na localidade leste dos Estados Unidos. Essa definição seguiu a premissa de otimização de custos durante a execução dos experimentos. Mesmo assim, a definição de localidade não interfere nos resultados obtidos pelo experimento.

4.1. Soluções de Segurança

A avaliação tem como base a principal solução de segurança da Microsoft, denominada central de segurança do Azure (*Azure Security Center*). A arquitetura disponibilizada pela Microsoft provê três níveis de segurança:

- **Modelo Sem Azure Security Center:** Este modelo possui menor cobertura de segurança, visto que apenas é implementada a solução de antivírus, denominada *Windows Defender Security Center* e também o recurso de monitoramento utilizado para capturar as informações de desempenho do servidor, denominado como

Microsoft Monitor Agent. Destaca-se que esses recursos são implementados automaticamente em todas máquinas virtuais no modelo de infraestrutura como serviço.

- **Azure Security Center Básico:** Este modelo contempla todos os requisitos do seu antecessor, como também acrescenta o recurso denominado *Azure Security Center* (Central de segurança do Azure), o qual fornece gerenciamento de segurança unificado e proteção contra ameaças para a infraestrutura hospedada em nuvem. A versão implementada nesse modelo é classificada como gratuita. Portanto, possui algumas limitações referente ao uso e recursos de segurança e detecção de ameaças.
- **Azure Security Center Standard:** Adicionalmente aos modelos anteriores, é possível ampliar a solução do *Azure Security Center* para a versão padrão, a qual implementa todos os recursos de segurança disponibilizados pelo provedor de serviços e também permite a extensão do *Azure Security Center* para a infraestrutura interna. Entretanto, esse modelo de implementação requer o custo adicional para a ativação e sustentação da infraestrutura.

.

A execução das simulações dos ataques cibernéticos transcorreu através de uma máquina virtual Kali Linux no computador do autor, ou seja, a máquina atacante estava fora da infraestrutura da nuvem Microsoft Azure.

4.2. Execução dos Ataques

Os cenários avaliados neste experimento abrangem as seguintes variáveis: sem recurso de segurança, com o *Azure Security Center* básico e com *Azure Security Center standard*. A mensuração dos resultados transcorreu de forma equivalente para todos os cenários.

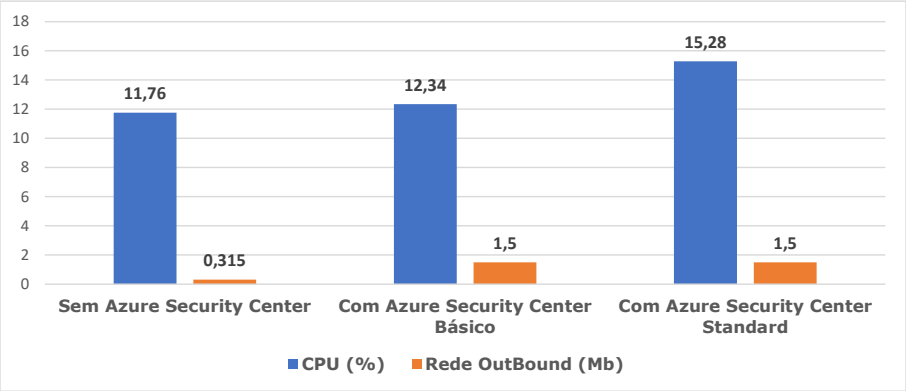
Em relação aos aspectos legais, destaca-se que os ataques cibernéticos executados cumpriram de forma integral todas as diretrizes estipuladas pelo provedor [Microsoft 2019]. Nas próximas seções, são apresentados os ataques cibernéticos e os seus respectivos resultados, os quais foram obtidos através do recurso Azure monitor.

4.2.1. Elevação de Privilégios

Para o ambiente do experimento foram utilizados os seguintes protocolos: *Secure Shell (SSH)* com propósito de conexão remota ao ambiente Linux e protocolo *File Transfer Protocol (FTP)* para publicação e transferência de informação para o ambiente Windows. Para o ataque, foi utilizada a ferramenta `ncrack` com listas de usuários e senhas geradas através das principais bases de dados publicadas na Internet. No total foram testadas 1.685 combinações de credenciais (5 usuários e 337 senhas).

A Figura 1 demonstra a utilização de recursos computacionais durante o ataque, o qual obteve sucesso e nenhum módulo de segurança do provedor conseguiu detectar o ataque realizado no protocolo *SSH*. Todavia, houve uma sobrecarga dos recursos computacionais utilizados, destacando-se o grande incremento relacionado ao tráfego de rede.

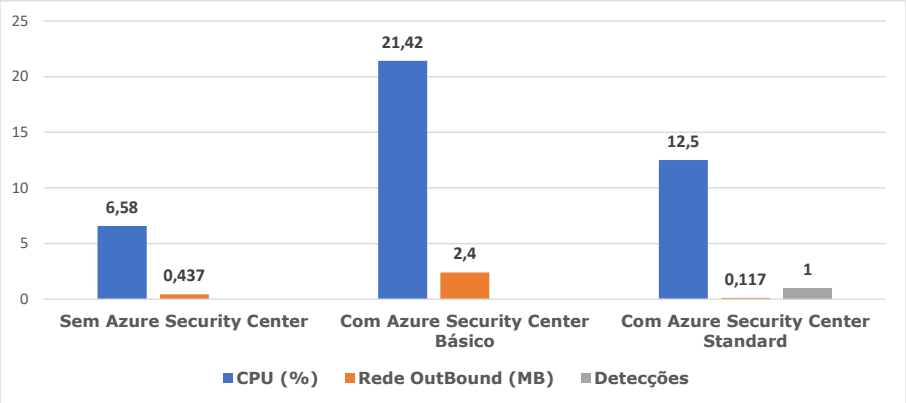
Figura 1. Recursos computacionais – SSH.



Fonte: Desenvolvido pelo autor (2019)

O experimento direcionado ao protocolo *FTP* também foi realizado com a ferramenta `ncrack`. A Figura 2 demonstra a utilização de recursos computacionais durante o ataque. Todos os ataques com o protocolo *FTP* obtiveram sucesso. Entretanto, o *Azure Security Center standard* teve êxito na detecção e alerta do ataque. Também houve um acréscimo dos recursos computacionais utilizados após a implementação dos recursos de segurança.

Figura 2. Recursos computacionais – FTP.



Fonte: Desenvolvido pelo autor (2019)

Através dos experimentos realizados, pode-se constatar que o recurso de segurança *Azure Security Center* demonstrou melhor eficácia na detecção dos ataques direcionados para o cenário desenvolvido através da tecnologia Microsoft Windows.

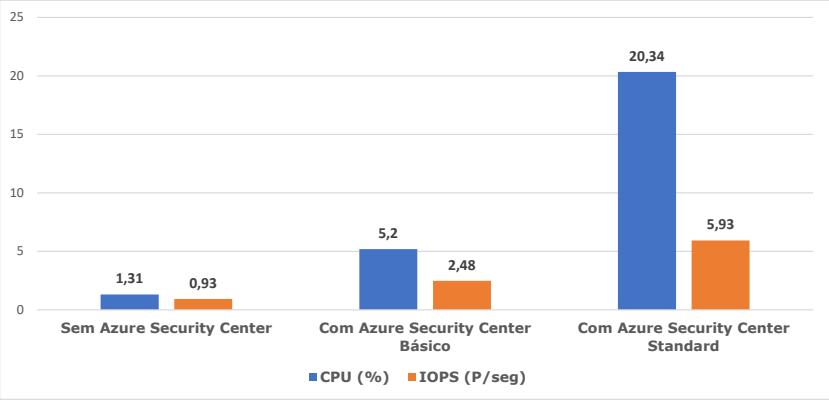
4.2.2. Adulteração e Repúdio

Os ataques realizados buscam comprometer os logs processados pelas máquinas virtuais do ambiente. O escopo dos ataques contempla um servidor Linux e um servidor Windows. Para a execução do experimento, foram gerados 3 MB de arquivos de logs para o ambiente Windows, contemplando todas as categorias disponíveis através do coletor de eventos da Microsoft. Para o ambiente Linux, foram gerados 3.7 MB de logs armazenados na

categoria de autenticação do sistema. Os ataques ocorreram através da execução de dois *scripts* desenvolvidos pelo autor (um em *powershell* para o Windows e outro em *bash* para o Linux).

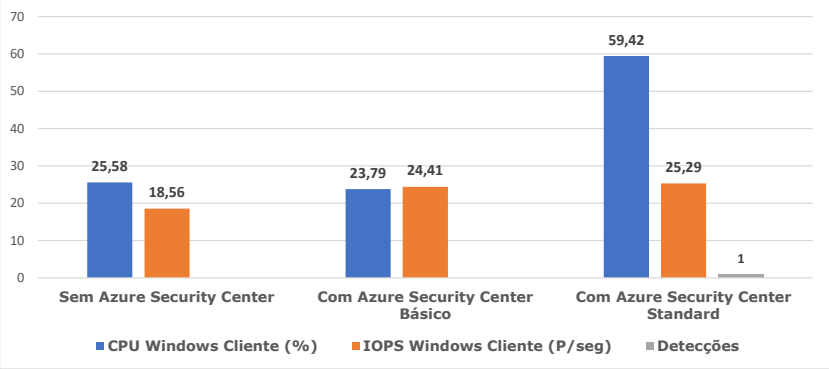
Os experimentos realizados no servidor Linux (Figura 3) obtiveram sucesso e foram efetivos para a exclusão dos dados. Entretanto, o recurso de segurança do Azure não obteve sucesso na detecção do ataque. Além disso, a ativação dos recursos de segurança aumentou a utilização dos recursos computacionais do ambiente.

Figura 3. Recursos computacionais - Servidor Linux.



Fonte: Desenvolvido pelo autor (2019)

Figura 4. Recursos computacionais - Servidor Windows.



Fonte: Desenvolvido pelo autor (2019)

Os experimentos realizados no servidor Windows (Figura 4) obtiveram sucesso, mas o *Azure Security Center standard* foi capaz de detectar o ataque. Além disso, note que há um acréscimo do consumo dos recursos computacionais utilizados após a implementação dos recursos de segurança.

4.2.3. Vazamento de Informações

Este experimento transcorreu no servidor 02 (Linux), onde foram desenvolvidos dois *datasets* contendo dados sensíveis gerados através de simuladores públicos. O primeiro *dataset* desenvolvido em extensão `.xlsx` compõe-se das seguintes colunas: *ID, NameSet,*

Title, GivenName, StreetAddress, City, ZipCode, EmailAddress, Username, Password, Birthday, Age, CCNumber, CVV2, CCExpires, NationalID e CCType. Este *dataset* possui 4000 mil registros totalizando 661 KB de dados. O segundo dataset foi gerado através da extensão `.txt` contendo apenas o número do cartão de crédito, CVV e data de validade, possuindo 1000 registros que totalizaram 30kb de dados. Para o experimento foram gerados 5000 registros com dados sensíveis armazenados em dois arquivos com diferentes extensões.

A rede e o *firewall* foram configurados de forma padrão, conforme recomendação do provedor, permitindo apenas a comunicação através das portas 80 e 443, o que restringe a execução do experimento.

Para a realização dos ataques, definiu-se a utilização da ferramenta *Open Source* denominada *Data Exfiltration ToolKit (DET)*, disponível em `github.com/sensepost/DET`. Conforme definido pelos autores, a ferramenta é caracterizada como uma prova de conceito para execução de exfiltração de dados, utilizando diversos canais de comunicação ao mesmo tempo. O objetivo fundamental da ferramenta é executar uma prova de conceito para identificar possíveis imperfeições em ferramentas de *Data Loss Prevention (DLP)* ou soluções de monitoramento de rede.

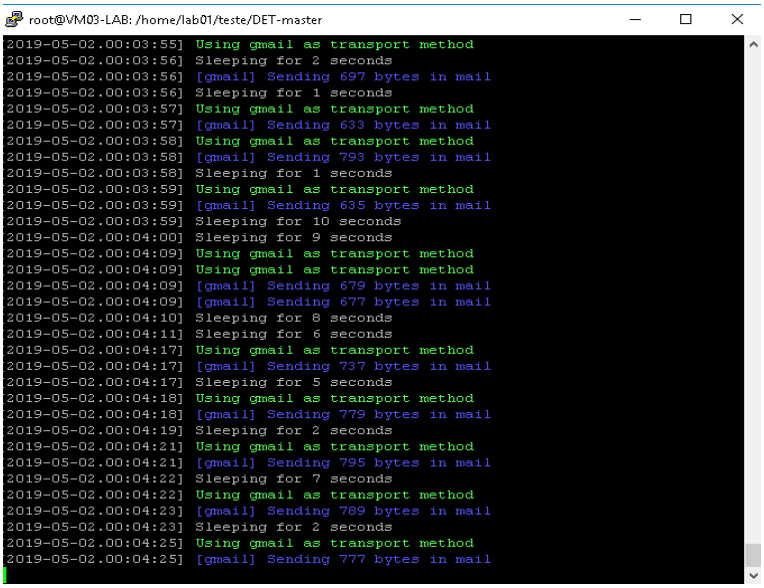
Diante do cenário proposto, utilizou-se o módulo de exfiltração através da integração com a *Application Programming Interface (API)* do Gmail. Para o pleno funcionamento do módulo selecionado, foi necessário realizar a configuração do arquivo `config-sample.json` localizado no servidor que possui os arquivos e também no servidor responsável pela execução do ataque. As configurações realizadas definiram a conta de e-mail utilizada para exiltração, a chave de criptografia utilizada e intervalo de tempo para a transferência das informações. Destaca-se que todas as configurações do arquivo `config-sample.json` precisam estar idênticas, caso contrário o ataque não será efetivo.

O tráfego externo das informações é realizado de forma segmentada e aplicada criptografia dos arquivos. Para isso, a ferramenta utiliza o protocolo *AES*, no qual o atacante possui a responsabilidade de definir a chave de criptografia. Portanto, a ferramenta realiza a criptografia, envia para a conta de e-mail e o atacante utiliza a mesma ferramenta para receber os e-mails e descriptografar as informações. A Figura 5 demonstra a execução da exfiltração dos dados do servidor-alvo, constatando as características apresentadas acima.

A ferramenta utilizada obteve sucesso para realizar a exfiltração de todos os arquivos que continham informações sensíveis. Durante a execução do ataque, não transcorreu nenhuma detecção através do mecanismo de segurança da Azure. Ademais, houve um acréscimo de utilização dos recursos computacionais após a implementação dos recursos de segurança, conforme pode ser observado na Figura 6.

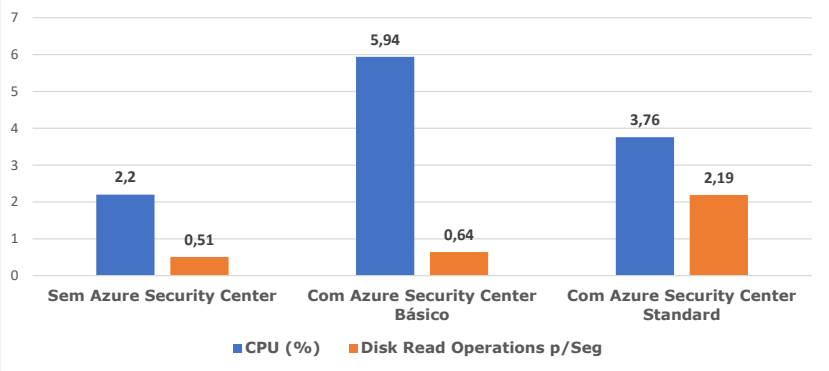
Diante do contexto apresentado, conclui-se que o controle de segurança *Azure Security Center* não apresentou efetividade na detecção referente ao ataque de exfiltração de dados. Entretanto, identificou-se um acréscimo dos recursos computacionais após a implementação dos módulos de segurança.

Figura 5. Execução da Exfiltração dos dados.



Fonte: Desenvolvido pelo autor (2019)

Figura 6. Recursos computacionais.



Fonte: Desenvolvido pelo autor (2019)

5. CONCLUSÃO

Este artigo apresenta uma avaliação do mecanismo de segurança da Azure por meio de experimentos em um ambiente IaaS. Ao total foram realizados quinze (15) simulações de ataques, sendo que o *Azure Security Center* obteve sucesso na detecção de apenas duas simulações (em torno de 13.3% de efetividade da solução). Além disso, houve um acréscimo significativo em certos casos na utilização de recursos computacionais por causa do mecanismo de segurança. Diante dos resultados apresentados, sugere-se a implementação de soluções de segurança complementares àquelas disponibilizadas pelo provedor.

Como trabalhos futuros, considera-se: (i) realizar o experimento novamente após a implementação do novo recurso de segurança da Microsoft (denominado *Azure Sentinel*); e (ii) realizar experimentos comparativos entre as soluções de segurança disponibilizadas pela Microsoft e por outros provedores de nuvem.

Referências

Antônio Carlos Gil (2002). *Como Elaborar Projetos de Pesquisa*. Atlas, São Paulo, 4ª edition.

Cloud Security Alliance (2019). Cloud penetration testing guidance.

Dukaric, R. and Juric, M. B. (2013). Towards a unified taxonomy and architecture of cloud frameworks. *Future Generation Computer Systems*, 29(5):1196–1210.

Golnoosh Tajadod, Lynn Batten, K.Govinda (2012). Microsoft and Amazon A comparison of approaches to cloud security. *IEEE 4th International Conference on Cloud Computing Technology and Science*, page 6.

Hernandez Sampieiri, R. C. F. e. M. d. P. B. (2013). Metodologia de pesquisa.

Hugo, V. and Moia, G. (2015). Uma forma de tratar o desafio de proteger a privacidade dos usuários de armazenamento de dados em nuvens.

Medeiros, G. D. O. (2014). Mitigando Ataques de Negação de Serviços em Infraestruturas de Computação em Nuvem.

Microsoft (2019). Penetration testing rules of engagement.

Naseer Amara, Huang Zhiqui, Awais Ali (2017). Cloud Computing Security Threats and Attacks with their Mitigation Techniques. *International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*, page 8.

Roveda, D., Vogel, A., Souza, S., and Griebler, D. (2016). Uma Avaliação Comparativa dos Mecanismos de Segurança nas Ferramentas OpenStack, OpenNebula e CloudStack. *Revista Eletrônica Argentina-Brasil de Tecnologias da Informação e da Comunicação*, 1(4).

Zimba, A. and Chama, V. (2018). Cyber Attacks in Cloud Computing: Modelling Multistage Attacks using Probability Density Curves. *International Journal of Computer Network and Information Security*, 10(3):25–36.