Alunos:

* Erick Giffoni - 170141161
* Nícolas Roberto - 200042360

## Introdução

Este trabalho será conduzido por alunos de Engenharia de Software da Universidade de Brasília, no semestre de 2022/1, sendo parte do projeto final da disciplina de Tópicos Especiais em Engenharia de Software.

O tema do trabalho é segurança cibernética para ambientes *cloud*. Assim, tem-se como proposta entender os seguintes pontos:

1. Quais são os principais problemas de segurança em ambientes na *cloud* ?
   1. Perda ou vazamento de dados
   2. Tecnologias compartilhadas
   3. Controle de acesso de usuários maliciosos
   4. Disponibilidade dos serviços
   5. Desvios de contas, serviços e tráfego

(WESTCON-COMSTOR, 2022?)

1. Quais são as principais ameaças de segurança em ambientes na *cloud* ?
   1. Violações de dados
   2. Roubo de conta
   3. Ameaças internas
   4. Interfaces e APIs inseguras
   5. Falhas na metaestrutura e na infraestrutura

(VIOLINO, 2020)

1. Quais são os principais ataques de segurança em ambientes na *cloud* ?
   1. Falhas de configuração ou conformidade
   2. Exploração de vulnerabilidades
   3. Exploração de API’s inseguras
   4. Ataques DoS
   5. Comprometimento de credenciais de contas

(SEGURANÇA..., 2019)

A partir do entendimento acima, o objetivo do trabalho é aprensentar as principais maneiras para proteger ativos nos ambientes na nuvem *(cloud*)*.*

## Ref Teórico

1. O que é cloud ? Qual a importância de ter segurança na cloud ?

De uma forma simples, cloud computing, ou computação na nuvem, é uma tecnologia que permite acesso remoto a softwares, armazenamento de arquivos e processamento de dados por meio da internet. Por isso, a segurança na cloud é fundamental, uma vez que há muitos dados pessoais e importantes de diversos tipos e de diferentes pessoas.

Nos últimos anos, a grande maioria das empresas decidiu por utilizar algum tipo de serviço em nuvem. Antes disso, as organizações eram dependentes de terem os próprios data centers on-premisses, por exemplo. Mas, com o avanço das tecnologias cloud isso passou a mudar, já que são várias as vantagens de adotar serviços na nuvem, como melhor custo-benefício, alta escalabilidade e desempenho melhorado (MANAGEENGINE, ZOHO CORPORATION, 2022b).

Nos últimos anos, a grande maioria das empresas decidiu por utilizar algum tipo de serviço em nuvem. Antes disso, as organizações eram dependentes de terem os próprios data centers on-premisses, por exemplo. Mas, com o avanço das tecnologias cloud isso passou a mudar, já que são várias as vantagens de adotar serviços na nuvem, como melhor custo-benefício, alta escalabilidade e desempenho melhorado (MANAGEENGINE, ZOHO CORPORATION, 2022b).

A típica configuração arquitetônica das redes de computadores roteia os endpoints através do data center da empresa. Enquanto o modelo de trabalho for o que todos os usuários estão conectados e localizados dentro do perímetro de rede da empresa, aquela arquitetura é aplicável. Porém, a realidade atual apresenta os usuários acessando os sistemas remotamente, de várias localidades diferentes, o que gera problemas e complexidades nos limites das redes, ou seja, nos endpoints dos usuários (MANAGEENGINE, ZOHO CORPORATION, 2022b).

Outro fator que tem colaborado para que as empresas adotem serviços em nuvem é a dependência dos usuários de aplicações SaaS (Software as a Service). Assim, os dados passam a ser movidos dos data centers tradicionais para os em cloud (MANAGEENGINE, ZOHO CORPORATION, 2022b). Isso gera requisitos de acesso diferentes e uma necessidade de arquitetura de redes mais robusta.

Conforme os usuários continuam trabalhando e acessando recursos de maneira remota, eles utilizam diferentes redes de computadores, múltiplos dispositivos de acesso (como celulares, notebooks, tablets) e afinam os limites entre vida profissional e a pessoal. Isso leva colaboradores a deixarem a guarda baixa e a práticas inseguras em relação à segurança cibernética. Sendo assim, existe uma necessidade urgente de uma abordagem unificada e robusta para a segurança da redes baseadas na cloud e que possa ser implementada independente da localização do usuário (MANAGEENGINE, ZOHO CORPORATION, 2022b).

1. Como aplicar a segurança nos ambiientes em cloud ?

Segundo ManageEngine, Zoho Corporation (2022b), conforme a complexidade das ameaças de segurança cibernética que ataca os ambientes em cloud cresce, torna-se impossível para uma única solução de segurança defender os ativos em nuvem. Como dito anteriormente, usuários acessam os serviços remotamente de diferentes localidades e dispositivos, o que aumenta a superfície de ataque.

Ao mesmo tempo em que as medidas de segurança evoluíram ao longo dos anos, também aconteceu isso com as ameaças. Ao passo que tecnologias de segurança cibernética atuam contra certos tipos de ataques, um único ataque pode ser formado por diferentes vetores, o que ocasiona uma cadeia de etapas para a exploração (cyber kill chain) (MANAGEENGINE, ZOHO CORPORATION, 2022b).

Logo, para que seja possível fornecer segurança cibernética na cloud, todas as medidas de segurança devem atuar coerentemente e em conjunto contra a cyber kill chain. Desse forma, caso uma dessas medidas falhe, haverá outra na sequência, ou seja, aplicar-se-á uma defesa em profundidade para não permitir que um ataque se espalhe. Isso evidencia que uma estratégia unificada de segurança cibernética composta por múltiplas soluções trabalhando juntas é a abordagem correta para garantir a segurança na cloud (MANAGEENGINE, ZOHO CORPORATION, 2022b).

1. Exemplo de problema de segurança em cloud (caso de uso)

Na cloud da Microsoft Azure foi detectado uma vulnerabilidade permite ataque do tipo "Elevação de Privilégio" por meio de falha no "Serviço de Fabric Container", o CTIR Gov solicitou às instituições da Administração Pública Federal (APF) e orienta as demais entidades/instituições, que identifiquem sistemas vulneráveis sob sua responsabilidade e apliquem com urgência as devidas correções (LOBO, 2022).

As ações do Alibaba tiveram a maior queda em um mês na sexta-feira, depois que o Wall Street Journal publicou que a divisão de computação em nuvem da gigante de tecnologia chinesa foi convocada pelas autoridades de Xangai em conexão com um roubo de dados policiais. Um hacker anônimo afirmou no início deste mês ter obtido informações pessoais de mais de 1 bilhão de chineses junto à polícia de Xangai. Um painel de gerenciamento do banco de dados ficou aberto na internet por mais de um ano sem proteção de senha, o que facilitou o acesso ao conteúdo, publicou o Wall Street Journal, citando pesquisadores de segurança eletrônica (HORWITZ, 2022).

## Abordagem

Para que o objetivo do trabalho proposto seja atingido, a abordagem adotada terá como ponto de partida a pesquisa e a documentação de métodos que solucionem ou mitiguem cada problema, ameaça e ataque de segurança em cloud que será apresentado. Mais ainda, pretende-se informar como tais métodos podem ser implementados no Security Development Lifecycle (SDL).

Essa abordagem acontecerá de maneira cíclica, seguindo os passos abaixo:

1. Pesquisa de livros, artigos ou notícias sobre o tema;
2. Escolha dos recursos relevantes;
3. Leitura dos recursos;
4. Escrita do trabalho, abordando o que for apresentado pelos recursos selecionados;
5. Relacionar o conteúdo visto, estudado e escrito com o SDL.

## Critérios de sucesso

Os seguintes critérios serão observados para que o objetivo seja tido como atingido:

* Explicar pelo menos 3 dos principais problemas de segurança *cloud*;
* Explicar pelo menos 3 das principais ameaças de segurança *cloud*
* Explicar pelo menos 3 dos principais ataques de segurança *cloud;*
* Apresentar pelo menos 3 maneiras de proteger os ativos em *cloud*;
* Para cada problema, elucidar ao menos 1 possível solução ou forma de mitigação;
* Para cada ameaça, elucidar uma maneira de evitá-la;
* Para cada ataque, elucidar uma forma de proteção e uma de mitigação (para o caso do ataque acontecer);

## Cronograma de atividades

O trabalho seguirá o seguinte cronograma:

|  |  |
| --- | --- |
| **Atividade** | **Período** |
| Pesquisa, escolha e leitura de materiais (livros, artigos) | 24/07 a 06/08/22 |
| Escrita do trabalho, abordando os recursos escolhidos e relacionando o conteúdo ao SDL | 07/08 a 27/08/22 |
| Ajustes e correções finais | 28/08 a 03/09/22 |
| Entrega do relatório | até 05/09/22 |

## Rerências

RANSOME, James; MISRA, Anmol. Core Software Security: Security at the Source. 1. ed. [S. l.]: Auerbach Publishers, Incorporated, 2013. 317 p. ISBN 9781466560963. E-book.

MANAGEENGINE, ZOHO CORPORATION. The National Security Agency‘s recommendations for cloud security. Cloud Security, [S. l.], p. 1-8, 20 jul. 2022a. E-book.

MANAGEENGINE, ZOHO CORPORATION. SASE: SECURING THE CLOUD NETWORK ARCHITECTURE. Cloud Security, [S. l.], p. 1-17, 20 jul. 2022b. E-book.

WESTCON-COMSTOR, SYNNEX. QUAIS OS PRINCIPAIS PROBLEMAS NA NUVEM E COMO RESOLVÊ-LOS?. [S. l.], 2022?. Disponível em: https://digital.br.synnex.com/quais-os-principais-problemas-na-nuvem-e-como-resolve-los. Acesso em: 23 jul. 2022.

VIOLINO, Bob. As 11 principais ameaças à segurança na nuvem. [S. l.], 21 out. 2020. Disponível em: https://itforum.com.br/noticias/as-11-principais-ameacas-a-seguranca-na-nuvem/. Acesso em: 23 jul. 2022.

CRYPTOID. Segurança na nuvem: confira os 6 tipos de ataques mais praticados e saiba como preveni-los. [S. l.], 16 jul. 2019. Disponível em: https://cryptoid.com.br/seguranca-em-cloud/seguranca-na-nuvem-confira-os-6-tipos-de-ataques-mais-praticados-e-saiba-como-preveni-los/. Acesso em: 23 jul. 2022.

LOBO, Ana Paula. Governo adverte para falha no Azure, da MS, e manda aplicar correção urgente. [S. l.], 1 jul. 2022. Disponível em: https://www.convergenciadigital.com.br/Cloud-Computing/Governo-adverte-para-falha-no-Azure%2C-da-MS%2C-e-manda-aplicar-correcao-urgente-60729.html?UserActiveTemplate=site. Acesso em: 23 jul. 2022.

HORWITZ, Josh. Ações do Alibaba têm maior queda em um mês após investigação sobre vazamento de dados. [S. l.], 15 jul. 2022. Disponível em: https://www.uol.com.br/tilt/noticias/reuters/2022/07/15/acoes-do-alibaba-tem-maior-queda-em-um-mes-apos-investigacao-sobre-vazamento-de-dados.htm. Acesso em: 23 jul. 2022.