COLÉGIO JOÃO PAULO I - UNIDADE SUL
INTRODUÇÃO À METODOLOGIA CIENTÍFICA 2022
TURMA: 9ºB

SEGURANÇA CIBERNÉTICA

Aluno: Rafael Monteiro Ravazzolo
Orientador: Lucas Floriano

Porto Alegre/RS
2022

SUMÁRIO

1. INTRODUÇÃO

A segurança cibernética é usada para proteger sistemas de invasões e ameaças cibernéticas. O crime cibernético é uma ameaça séria e está em constante evolução. No passado, os cibercriminosos se contentavam em roubar dados para fins monetários. Contudo, agora, eles estão procurando roubar propriedade intelectual e segredos comerciais. O setor de segurança cibernética vem evoluindo rapidamente nos últimos anos para acompanhar essas mudanças. Há muitas maneiras pelas quais as empresas podem se proteger do cibercrime, mas nem todas são eficazes. Por exemplo, uma empresa pode investir em tecnologia de ponta para proteger seus dados, mas isso pode não ser suficiente se seus funcionários forem descuidados com suas senhas ou não atualizarem seus softwares regularmente. (SCHULTZ F, 2020).

A segurança cibernética é uma grande preocupação para muitas empresas. É importante ter um forte plano de segurança cibernética para proteger seu negócio contra hackers e outras ameaças cibernéticas. Existem tipos diferentes de planos de segurança cibernética que se podem implementar nas empresas. Um dos tipos mais populares de planos de segurança cibernética é a estratégia de "defesa em profundidade". Ela envolve a execução de várias camadas de proteção para tornar mais difícil para os hackers romperem suas defesas e acessarem informações confidenciais. (BENJAMIN M, 2021)

O antivírus é um programa que protege os computadores contra a invasão de ataques hackers. Um computador protegido por software antivírus é muito mais seguro do que um sem ele. Além disso, alguns programas populares não precisam ser instalados para fornecer proteção eficaz. Em vez disso, eles funcionam como navegadores da web. (CANALTECH, 2014)

Os principais componentes de um programa antivírus são atualizações de código e banco de dados. O código é a parte que ajuda a detectar e remover ameaças. As atualizações do banco de dados possuem informações sobre arquivos e códigos maliciosos para que o software consiga funcionar de forma adequada. Os antivírus são feitos para serem fáceis de usar e podem ser administrados por usuários com níveis variados de conhecimento. Tudo o que é necessário para

executar um programa antivírus eficaz é saber onde encontrar os arquivos corretos. (ESET, 2021)

Os hackers estão sempre procurando novas maneiras de invadir um sistema. Eles buscam novas vulnerabilidades e as exploram assim que as encontram. Existem muitas maneiras de evitar ataques de hackers, mas o mais importante é estar ciente dos riscos e tomar precauções. (BENJAMIN M, 2021).

A segurança cibernética é um campo de trabalho em crescimento que precisa de mais pessoas para atuar nessa área. O número de ataques cibernéticos aumentou exponencialmente nos últimos anos e essa tendência continuará. O papel de quem trabalha com segurança cibernética é identificar as vulnerabilidades existentes nos sistemas, os riscos envolvidos e proteger os dados da empresa de serem hackeados, roubados ou vazados para concorrentes e outras companhias. (INDEED, 2021)

O mercado de trabalho para a segurança é muito competitivo. Existem vários fatores que podem afetar suas chances de conseguir um emprego nessa área da tecnologia. Um dos aspectos importantes é o currículo; porém, quando se trata de segurança cibernética, o conhecimento adquirido através da experiência com situações adversas acaba se tornando essencial. Um currículo bem escrito pode ajudar a conseguir uma entrevista, mas não é suficiente para conseguir o emprego, é preciso entender o assunto e estar preparado para as invasões. Normalmente a pessoa que trabalha com segurança cibernética ganha entre R$2.000,00 e R$19.000,00, o salário pode variar bastante conforme o trabalho que a pessoa exerce, o valor médio é de R$13.000,00. (EQUIPE EDITORIAL INDEED, 2021)

O maior ataque de hackers da história foi a violação da Equifax. Foi um ataque de dados que ocorreu em 2017 e comprometeu as informações pessoais de 143 milhões de americanos. Os hackers conseguiram acessar nomes, números de segurança social, datas de nascimento, endereços e números de carteira de motorista e muitas informações pessoais. (INDEED, 2021)

JUSTIFICATIVA

Este tema foi escolhido porque a segurança cibernética é um assunto muito importante e vem sendo muito discutido na atualidade. Acontecem vários ataques

hackers diariamente em grandes empresas, na maioria das vezes com a intenção de obter algum ganho monetário. Não só empresas, mas pessoas em suas casas, com seus computadores e celulares, devem tomar todos os cuidados possíveis, pois podem ter seus dados vazados e seus dispositivos invadidos a qualquer momento.

Este tema será um dos mais discutidos no futuro, como está sendo no atual momento com a guerra da Ucrânia e da Rússia, que também gerou uma guerra cibernética entre grupos de *hackers*, alguns defendendo o lado russo, e outros, o lado ucraniano. O grupo Anonymous, que possui afiliados no mundo inteiro, conseguiu invadir sites da Rússia colocando mensagens contra as invasões na Ucrânia.

De uma forma geral, as pessoas não têm um conhecimento mais detalhado sobre os riscos existentes no mundo da tecnologia da informação, tornando-se, assim, alvos fáceis de hackers e de crimes cibernéticos.

OBJETIVOS

Objetivo geral: entender a importância da segurança cibernética e conhecer os problemas que podem ser causados caso não sejam tomados os cuidados necessários.

Objetivos específicos:
1. identificar a importância da segurança cibernética;
2. identificar as consequências das invasões *hackers;*
3. analisar o prejuízo dos maiores ataques já acontecidos.

2. METODOLOGIA

Para o desenvolvimento do trabalho, foram usadas informações de sites e de artigos encontrados no Google, com o foco em como a segurança cibernética funciona e nos cuidados necessários em relação aos ataques *hackers*, estando todos disponíveis na internet. Como palavras-chave, foram usadas: Segurança Cibernética, Ataque Cibernético, Ataque Hacker, Hackers etc. A partir desses dados, foi possível analisar todas as informações contidas no trabalho.

3. RESULTADOS

A partir dessa pesquisa, espera-se contribuir para que as pessoas consigam ter os cuidados necessários para combater os ataques cibernéticos, tendo o foco na instalação de antivírus e de medidas preventivas, como não entrar em links desconhecidos que facilitam a entrada de vírus que podem danificar seus dispositivos eletrônicos. Com essas medidas, a navegação na internet pode se tornar mais segura. É possível perceber que o principal problema na atualidade é a falta de conhecimento e alguns cuidados, sendo que as pessoas de mais idade normalmente têm mais dificuldade com tecnologia, e, dessa forma, acabam acessando links e abrindo e-mails que não são seguros, caindo em golpes básicos.

4. CONCLUSÃO

A partir dos resultados encontrados nesta pesquisa, concluímos que a segurança cibernética é algo essencial em qualquer eletrônico que tenha contato com a internet. Isso se dá pela falta de proteção nos computadores que acabam sendo muito vulneráveis com ataques hackers. Por isso, existem os antivírus, que ajudam a proteger o sistema de invasões cibernéticas.

Atualmente, é básico ter um antivírus; no entanto, precisa-se ter o cuidado mínimo da pessoa que o está utilizando. Por esses motivos, é possível perceber que é necessário usar essas proteções e tomar as atitudes necessárias para que não aconteça o pior.

5. REFERÊNCIAS BIBLIOGRÁFICAS

BENJAMIN, M. **Ataques Hackers**. 2021. Disponível em: <https://www.tecmundo.com.br/seguranca/223487-3-dicas-prevenir-ataques-ciberneticos-pc.htm>. Acesso em: 01 de maio de 2022.

Canaltech. **O que é um antivírus**. 2014. Disponível em: <https://canaltech.com.br/antivirus/o-que-e-antivirus/>. Acesso em: 10 de agosto de 2022.

Claranet. **O que é a segurança cibernética**. 2021. Disponível em: <https://br.claranet.com/blog/o-que-e-seguranca-cibernetica>. Acesso em: 11 de agosto de 2022.

EQUIFAX. Maior Ataque Hacker, 2017. Disponível em: <https://g1.globo.com/tecnologia/noticia/equifax-empresa-de-credito-dos-eua-diz-que-ataque-hacker-foi-causado-por-vulnerabilidade-em-servidor.ghtml>. Acesso em: 01 de maio de 2022.

Eset. **Vantagens de um antivírus**. 2021. Disponível em: <https://www.eset.com/br/artigos/o-que-e-um-antivirus>. Acesso em: 10 de agosto de 2022.

FELIX, S. **Segurança Cibernética**, 2020. Disponível em: <https://blog.milvus.com.br/seguranca-cibernetica-o-que-e/>. Acesso em: 01 de maio de 2022.

Indeed. Segurança Cibernética, 2021. Disponível em: <https://br.indeed.com/conselho-de-carreira/pagamento-salario/quanto-ganha-ciberseguranca>. Acesso em: 01 de maio de 2022.

McAfee. **Dicas de prevenção de ataque**. 2020. Disponível em: <https://www.mcafee.com/blogs/pt-br/internet-security/>. Acesso em: 10 de agosto de 2022.

SENAI. **Cibersegurança**. 2020. Disponível em: <https://www.portaldaindustria.com.br/industria-de-a-z/ciberseguranca/>. Acesso em: 01 de maio de 2022.

STARTI. **Guia da segurança cibernética**. 2020. Disponível em: <https://br.claranet.com/blog/o-que-e-seguranca-cibernetica>. Acesso em: 11 de agosto de 2022.