ANDRÉ ARAÚJO MENDONÇA[1]

LUCAS HENRIQUE LOPES COSTA[1]

PEDRO GONÇALVES COSTA MELO[1]

GUSTAVO DE JESUS TEODORO[1]

DAVI AZIZ SANTOS SALAZAR[1]

GUSTAVO HENRIQUE MORAES FILHO[1]

[1] *UFLA - SISTEMAS DE INFORMAÇÃO*

O QUE É CIBERSEGURANÇA?:

UM RELATÓRIO SOBRE CONTEXTO DA CIBERSEGURANÇA, FUNDAMENTAÇÃO TEÓRICA, DEFINIÇÃO, EXEMPLOS DE APLICAÇÕES E SUAS TENDÊNCIAS

1^a edição

LAVRAS - MG

2023

ANDRÉ ARAÚJO MENDONÇA[1]
LUCAS HENRIQUE LOPES COSTA[1]
PEDRO GONÇALVES COSTA MELO[1]
GUSTAVO DE JESUS TEODORO[1]
DAVI AZIZ SANTOS SALAZAR[1]
GUSTAVO HENRIQUE MORAES FILHO[1]

[1] *UFLA - SISTEMAS DE INFORMAÇÃO*

O QUE É CIBERSEGURANÇA?:
UM RELATÓRIO SOBRE CONTEXTO DA CIBERSEGURANÇA, FUNDAMENTAÇÃO TEÓRICA, DEFINIÇÃO, EXEMPLOS DE APLICAÇÕES E SUAS TENDÊNCIAS

1^a edição

Relatório para projeto de seminário da matéria Introdução a Computação realizada na UFLA, ministrada pelo professor Maurício Ronny de Almeira Souza.

Maurício Ronny de Almeira Souza
Orientador

LAVRAS - MG
2023

Ficha catalográfica elaborada pela Coordenadoria de Processos Técnicos da Biblioteca Universitária da UFLA.

André Araújo Mendonça, Lucas Henrique Lopes Costa, Pedro Gonçalves Costa Melo, Gustavo de Jesus Teodoro, Gustavo Henrique Moraes Filho e Davi Aziz Santos Salazar.

O que é cibersegurança? : Um relatório sobre contexto da cibersegurança, fundamentação teórica, definição, exemplos de aplicações e suas tendências / . 1^a ed. l. – Lavras : UFLA, 2023.

24 p. : il.

Relatório–Universidade Federal de Lavras, 2023.
Orientador: Maurício Ronny de Almeira Souza.
Bibliografia.

1. Relatório. 2. Cibersegurança. 3. Computação.

CDD-808.066

Nós só podemos ver um pouco do futuro, mas o suficiente para perceber que há muito a fazer. (Alan Turing)

RESUMO

A cibersegurança vem sendo um tema de extrema importância na era digital, onde a tecnologia está em praticamente todos os aspectos da vida moderna. Este relatório busca apresentar uma análise abrangente sobre o contexto da cibersegurança, fornecendo uma fundamentação teórica sólida e exemplos relevantes de suas aplicações. Com a crescente interconectividade e a proliferação de dados pessoais e empresariais na esfera virtual, a proteção contra ameaças cibernéticas tornou-se imprescindível, deixando de ser considerada um luxo restrito a grandes empresas ou usuários tecnicamente experientes. O objetivo principal deste trabalho é destacar a relevância crescente da cibersegurança e suas tendências para garantir um ambiente digital mais seguro e confiável.

Vamos, nesse relatório, abordar os diversos aspectos da cibersegurança, fornecendo uma visão abrangente desde sua fundamentação teórica até a identificação de tendências emergentes. Através da análise de exemplos de aplicações e do estudo de soluções inovadoras, busca-se compreender como a cibersegurança evoluiu de um tópico restrito a especialistas para se tornar uma necessidade universal. Com esse conhecimento, poderemos fortalecer nossas defesas contra as crescentes ameaças cibernéticas e garantir a segurança do mundo digital em constante transformação.

Palavras-chave: Relatório, Cibersegurança, Computação.

ABSTRACT

Cybersecurity has been a topic of extreme importance in the digital age, where technology is practically every aspect of modern life. This report seeks to present a comprehensive analysis of the context of cybersecurity, providing a solid theoretical foundation and relevant examples of its applications. With increasing interconnectivity and the prospect of personal and business data in the virtual realm, protection against cyberthreats has become a presence, no longer considered a luxury restricted to large companies or technically savvy users. The main objective of this work is to highlight the growing protection of cybersecurity and its trends to ensure a safer and more reliable digital environment.

In this report, we will address the various aspects of cybersecurity, providing a comprehensive view from its theoretical foundation to the identification of emerging trends. Through the analysis of application examples and the study of innovative solutions, we seek to understand how cybersecurity evolved from a topic restricted to specialists to become a universal necessity. With this knowledge, we can strengthen our defenses against rising cyber threats and secure the ever-changing digital world.

Keywords: Reporting, Cybersecurity, Computing.

SUMÁRIO

1 INTRODUÇÃO

1.1 Contexto

1.1.1 A Origem da Internet

O mundo como conhecemos hoje não seria nada sem a Internet. Absolutamente tudo o que fazemos está conectado a ela, seja direta ou indiretamente. Essa rede surge décadas atrás, como é dito por Santana Filho (Santana Filho, 2005) em suas anotações:

> "A origem da internet se deu nos anos de 1960 com o projeto do governo americano chamado Arpanet [...] no final desta década a internet era utilizada basicamente para troca de mensagens, informações e arquivos entre pesquisadores, e ainda não era permitida a sua utilização comercial. No início dos anos 90, o que realmente impulsionou o crescimento da internet foi o surgimento da teia de alcance mundial, a world wide web (www), que é uma forma mais fácil de acessar as informações através de uma interface gráfica, utilizando um aplicativo chamado navegador."

Com a internet, é possível realizar ações como: acessar sites em busca de respostas para suas perguntas, assistir conteúdos que estão sendo transmitidos ao vivo, se conectar com pessoas do outro lado do mundo e muitas outras.

1.1.2 Armazenamento de Dados

Independentemente da ação executada, uma coisa é fato: Informações serão movimentadas. Isso significa que, toda e qualquer ação feita dentro da internet requer dados que já estavam armazenados previamente. Esse armazenamento dos dados pode ser feito de várias formas, mas todas elas tem em comum um aspecto: a segurança deles. É de suma importância que todos os dados fornecidos a um site ou a uma empresa sejam muito bem guardados, para evitar o mal uso dos mesmos. Esse é o papel da Cibersegurança, tema sobre o qual este relatório é escrito.

1.2 Objetivo do Relatório

Este texto, que tem como objetivo dissertar sobre a Cibersegurança e todo o ambiente que a envolve, está organizado da seguinte forma: O capítulo 2 aborda temas de relevância para o entendimento do documento. O capítulo 3 Fala sobre a Cibersegurança em si. E o capítulo 4 conclui o texto, fazendo as considerações finais.

2 FUNDAMENTAÇÃO TEÓRICA DA CIBERSEGURANÇA

2.1 Conhecimentos Necessários

2.1.1 Proteção de Rede

Segundo Howana, Prunes (Howana, Mario Jorge, 2000) "O modelo de segurança de rede permite que se concentrem atenções no controle dos acessos à rede, no lugar de se tentar garantir a segurança "host a host". Este tipo de abordagem inclui a construção de firewall para a proteção do sistema de internet e redes e o uso da criptografia para proteger os dados em trânsito na rede."

2.1.1.1 Firewall

O firewall é uma solução de segurança baseada em software (parte não física de uma máquina) e hardware. A "Parede de fogo", bloqueia qualquer tipo de tráfego de dados indesejados em sua máquina, evitando ataques e também restringe entradas e saídas de um único ponto, controladamente. (Alecrim, Emerson, 2013)

2.1.2 Malware

Malware é um termo mais amplo para algum tipo de software que é projetado para prejudicar e explorar o seu dispositivo, os "atacantes"cibernéticos usam para extrair informações de suas vítimas para ganhos financeiros ou pessoais. (McAfee, 2023)

2.1.2.1 O que são Spywares

O spyware, é um software que é uma especialidade de Malware se passando por um espião, ele costuma ser instalado no computador ou celular sem o próprio usuário saber. Uma vez que ele está em seu computador ele tem acesso a sua atividade online, dados pessoais, entre outros. (Araújo, Giulia, 2019)

2.1.3 Definição de Banco de dados

O banco de dados é a organização e armazenagem de informações sobre um domínio específico. De forma mais simples, é o agrupamento de dados que tratam do mesmo assunto, e que precisam ser armazenados de forma criptografada para segurança dos dados. É comum que empresas, segundo Ivam Souza (Souza, Ivan, 2020), tenham diversas informações que precisam ser organizadas e disponibilizadas dentro do negócio para que sejam consultadas posteriormente pela equipe e pela gerência. Por isso, é interessante ter um sistema de gerenciamento de banco de dados, SGBD (Sistema de Gerenciamento de Banco de Dados), para conseguir manipular as informações e tornar a rotina da empresa muito mais simples.

2.1.4 Vírus

O vírus operacional, é um programa malicioso, que podem ser passados por hardwares. Eles precisam de alguns "gatilhos"para funcionarem, pois, não conseguem entrar em ação sozinhos. Hoje em dia é pouco comum ataques por vírus computacionais, porque já existem softwares maliciosos ou malware que são mais eficientes e que não precisam do gatilho para serem ativados.(Gogoni, Ronaldo, 2023)

2.1.5 Hackers

Segundo Augustènè, Agnèm (Agnė Augustėnė, 2022)"[...] Hacker é alguém com profunda capacidade de analisar, entender, explorar e modificar (e até desenvolver) programas, sistemas, funcionalidades, redes e até mesmo recursos de hardware."

Existem bons hackers, mas também os que não são. Esses que não são utilizam dos vírus, malwares e seus conhecimentos de sistemas, para atacar corporações, empresas, pessoas entre outros, para benefício próprio (dinheiro, diversão, vingança). Já os que são, trabalham justamente para impedir esses outros,

acabando com esses ataques cibernéticos, e são popularmente conhecidos como hackers éticos.(Kovacs, Leandro, 2023)

3 O QUE É?

3.1 Definição de Cibersegurança

De acordo com as informações disponíveis no site (kaspersky, 2021), a Cibersegurança abrange várias práticas para proteger computadores, servidores, dispositivos, e sistemas eletrônicos contra ataques maliciosos, como malwares, spywares, virus, e hackers no geral. É uma abordagem que engloba diversos cenários, desde ambientes corporativos até a computação móvel, e pode ser dividida em várias categorias comuns, com o objetivo de garantir a proteção e a integridade das informações.

3.1.1 Segurança de Rede

Foca na proteção de uma rede de computadores contra invasões e malwares, independentemente de serem ataques direcionados ou oportunísticos. Garantir a Segurança de Rede é essencial para manter a integridade e a confidencialidade dos dados que trafegam pelas redes, evitando que informações sensíveis caiam em mãos erradas e protegendo a infraestrutura de comunicação em um mundo digital altamente conectado e sujeito a diversas ameaças cibernéticas.

3.1.2 Segurança de Aplicativos

O foco principal da Segurança de Aplicativos é assegurar que o software e os dispositivos permaneçam protegidos contra possíveis ameaças, evitando que aplicativos comprometidos possam fornecer acesso não autorizado a dados sensíveis. A segurança nessa área começa na fase de projeto do programa ou dispositivo.

3.1.3 Segurança de Informações

Visa proteger a integridade e a privacidade dos dados, tanto em repouso (armazenamento) quanto em trânsito, a segurança de informações utiliza criptografia e controles de acesso rigorosos para garantir a proteção adequada.

3.1.4 Segurança Operacional

Envolve processos e decisões para tratar e proteger arquivos e dados. Isso inclui definir permissões de acesso dos usuários à rede e estabelecer procedimentos para armazenamento e compartilhamento de dados.

3.1.5 Recuperação de Desastres e continuidade dos negócios

São estratégias para responder a incidentes de cibersegurança ou outros eventos que possam resultar na perda de operações ou dados. Políticas de recuperação de desastres determinam como restaurar as operações e informações para recuperar a capacidade operacional após um incidente. A continuidade dos negócios é o plano para operar sem determinados recursos em situações adversas.

3.1.6 Educação do Usuário Final

Foca no fator humano e imprevisível da cibersegurança. Através da educação dos usuários finais, ensina-se as melhores práticas de segurança, como evitar abrir anexos suspeitos em e-mails e não conectar unidades USB desconhecidas, entre outras lições importantes, visando garantir a segurança das organizações.

3.2 Exemplos de aplicações da Cibersegurança

Existe uma variedade de ataques virtuais que podem ser feitos em softwares, hardwares e redes, e, apesar dos ataques serem bem variados, existem casos

que ocorrem com maior frequência no mundo digital. E o papel da cibersegurança é se defender desses ataques.(FIA, 2022)

3.2.1 Phishing

Um dos exemplos mais comuns é o “phishing”. Nas palavras de Leandro Kovacs (Leandro Kovacs, 2023): “Resumidamente, phishing é um tipo de fraude na Internet que visa obter as credenciais de um usuário enganando-o. Inclui roubo de senhas, números de cartão de crédito, detalhes de contas bancárias e outras informações confidenciais.” Ou seja, quase sempre são golpistas que fingem ser empresas ou um órgão governamental, com o objetivo de roubar informações importantes. O melhor jeito de se proteger desse ataques é com a “Educação do Usuário Final”. Isto é, ensinar procedimentos básicos como: Verificar com cuidado os remetentes dos e-mails. Prestando atenção em erros ortográficos ou endereços de e-mail suspeitos. Nunca clicar em links suspeitos, etc.

3.2.2 Malwares

Outro ataque comum aos sistemas digitais é o “malware”. Como no “phishing”, o estelionatário finge ser alguém que não é. Mas, diferentemente do “phishing”, a vítima não passa os dados, ela clica em um anexo que, muitas vezes, levam aplicações do tipo .exe (executável), onde, após aberto, o vírus se instala no computador do alvo. A melhor forma de se prevenir é, não só, com a educação digital, mas também com a “segurança de rede”.

3.2.3 Man-in-the-Middle(MitM)

Um último ataque que vale ser mencionado é o “Man-in-the-Middle”, onde um invasor intercepta a comunicação de duas partes legítimas, e com isso rouba suas informações e dados confidenciais. Uma das técnicas mais utilizadas pelos golpistas é a de utilizar uma rede Wi-Fi pública, onde o invasor pode moni-

torar o tráfego de rede e realizar ataques de interceptação. A melhor forma de se prevenir é com a “segurança de informações”.

4 CONCLUSÃO

Desse modo, é possível concluir que a Cibersegurança deixou de ser apenas um luxo às grandes empresas, ou até mesmo aos usuários com maior experiência técnica no assunto, e tornou-se algo imprescindível para todos. De modo que diversos tópicos discutidos anteriormente, como o tópico de segurança em aplicativos, demonstram a grande importância de dar a devida atenção a questões de autoproteção.

Ademais, com os rápidos avanços tecnológicos ocorridos ao longo do tempo, torna a área de cibersegurança uma área com grandes necessidades de pesquisas e inovações a todo momento, pois a todo instante práticas de ataques cibernéticos, como o "Phishing", "Man-in-the-Middle"ou os "Malwares", ameaçam e tornam o ambiente virtual em um local inseguro. Partindo desse pressuposto, faz-se necessário um amplo desenvolvimento da Cibersegurança, a qual desempenha um papel fundamental na construção de uma defesa sólida contra as crescentes ameaças cibernéticas.

Portanto, é importante que inovações relacionadas a segurança virtual, como a chegada das IA's(inteligências artificiais) que se demonstram capazes de mentir para humanos com alguma finalidade secundária, sejam tratadas de forma precavida e segura. Contudo, torna-se evidente a importância das práticas apresentadas em questão, visto que o número de pessoas conectadas virtualmente e que armazenam parte importante de suas vidas, como fotos, documentos e informações pessoais, nos meios virtuais aumentam cada vez mais, visando tornar o ambiente virtual mais seguro e permitindo desde uma simples troca de mensagens entre amigos até grandes transferências bancárias entre empresas, prevenindo riscos iminentes e garantindo a segurança do mundo digital em que vivemos.

REFERÊNCIAS

Agnė Augustėnė. **O que é um hacker e como se proteger deles?** 2022. <https://nordvpn.com/pt-br/blog/o-que-e-hacker/>. [Online; acesso em 13 de julho de 2023].

Alecrim, Emerson. **O que é firewall? - Conceito, tipos e arquiteturas**. 2013. <https://www.infowester.com/firewall.php>. [Online; acesso em 13 de julho de 2023].

Araújo, Giulia. **O que é spyware? Entenda como age o 'app espião' e veja como se proteger**. 2019. <https://www.techtudo.com.br/noticias/2019/07/o-que-e-spyware-entenda-como-age-o-app-espiao-e-veja-como-se-proteger.ghtml>. [Online; acesso em 13 de julho de 2023].

FIA. **Cibersegurança: o que é, importância, tipos e carreira na área**. 2022. <CiberseguranÃğa:oqueÃl',importÃćncia,tiposecarreiranaÃąrea>. [Online; acesso em 22 de julho de 2023].

Gogoni, Ronaldo. **O que é vírus? [e a diferença para malware]**. 2023. <https://tecnoblog.net/responde/o-que-e-virus/>. [Online; acesso em 13 de julho de 2023].

Howana, Mario Jorge. **Segurançana/ntemet: Políticas e Firewall**. 2000. <http://monografias.uem.mz/bitstream/123456789/1600/1/2000%20-%20Honwana%2c%20M%c3%a1rio%20Jorge%20.pdf>. [Online; acesso em 13 de julho de 2023].

kaspersky. **O que é cibersegurança?** 2021. <https://www.kaspersky.com.br/resource-center/definitions/what-is-cyber-security>. [Online; acesso em 6 de julho de 2023].

Kovacs, Leandro. **O que é um hacker?** 2023. <https://tecnoblog.net/responde/o-que-e-um-hacker/>. [Online; acesso em 6 de julho de 2023].

Leandro Kovacs. **O que é phishing?** 2023. <https://tecnoblog.net/responde/o-que-e-phishing/>. [Online; acesso em 22 de julho de 2023].

McAfee. **O que é malware?** 2023. <https://www.mcafee.com/pt-br/antivirus/malware.html#:~:text=Malware%20%C3%A9%20um%20termo%20gen%C3%A9rico,v%C3%ADtimas%20para%20obter%20ganhos%20financeiros>. [Online; acesso em 13 de julho de 2023].

Santana Filho. **Modos de utilização da internet e suas implicações na vida**. 2005. <https://www.bu.ufmg.br/snbu2014/anais_anterior/xivsnbu/pdf/210.pdf>. [Online; acesso em 12 de julho de 2023].

Souza, Ivan. **Banco de dados: saiba o que é, os tipos e a importância para o site da sua empresa**. 2020. <https://rockcontent.com/br/blog/banco-de-dados/>. [Online; acesso em 13 de julho de 2023].