Fundamentos de Cibersegurança

Uniara

November 28, 2025

Contents

Chapter 1

Introdução à Cibersegurança

A cibersegurança representa o conjunto de práticas, estratégias, ferramentas e tecnologias utilizadas para proteger sistemas, dispositivos e dados contra ataques maliciosos. Com o crescimento acelerado da transformação digital, cresce também o número e a complexidade das ameaças cibernéticas.

Este eBook tem como objetivo servir como um

guia completo e aprofundado, explanando conceitos essenciais, técnicas modernas, metodologias de segurança, ameaças reais e práticas de defesa aplicadas na indústria.

1.1 O crescimento das ameaças digitais

A transformação digital global tem ampliado a superfície de ataque, criando oportunidades para cibercriminosos explorarem vulnerabilidades em:

- sistemas corporativos;
- dispositivos móveis;
- redes sociais;
- infraestrutura crítica;
- dispositivos IoT;
- ambientes em nuvem.

Com isso, a cibersegurança deixou de ser uma opção e tornou–se uma necessidade estratégica para qualquer organização.

1.2 CIA Triad: Confidencialidade, Integridade e Disponibilidade

O modelo CIA, amplamente adotado, é o alicerce da segurança da informação:

Confidencialidade: garante que informações sejam acessadas apenas por pessoas autorizadas.

Integridade: assegura que dados permaneçam precisos e não sejam alterados indevidamente.

Disponibilidade: garante que informações e sistemas estejam disponíveis sempre que necessários.

Chapter 2

Ameaças Cibernéticas

Atacantes utilizam diversos vetores para comprometer sistemas e usuários. A seguir estão as principais categorias de ameaças digitais.

2.1 Malware

O termo *malware* refere–se a qualquer software criado para causar dano. Os tipos mais comuns incluem:

- vírus;

- worms;
- trojans;
- ransomware;
- spyware;
- adware.

Ransomware

Ransomware é uma das ameaças mais destrutivas da atualidade. Ele criptografa dados e impede o acesso aos sistemas até que um resgate seja pago.

Grandes incidentes como WannaCry e NotPetya mostraram o impacto global desse tipo de ataque.

2.2 Phishing e Engenharia Social

Engenharia social explora a vulnerabilidade humana. Os atacantes manipulam usuários para obter acesso, credenciais ou dados. Phishing é o exemplo mais comum, normalmente realizado via:

- e–mail;

- mensagens instantâneas;
- sites falsos;
- chamadas telefônicas (vishing).

2.3 Ataques de Rede

Incluem práticas como:

- ARP spoofing;
- DNS poisoning;
- man–in–the–middle (MITM);
- ataque de força bruta;
- DDoS.

Chapter 3

Criptografia

A criptografia é um pilar da cibersegurança, responsável por proteger dados durante a comunicação ou armazenamento. Ela se divide em:

3.1 Criptografia Simétrica

Utiliza uma única chave para cifrar e decifrar. É rápida, porém exige compartilhamento seguro da chave. Exemplos incluem:

- AES;

- DES (obsoleto);
- 3DES.

3.2 Criptografia Assimétrica

Usa par de chaves: pública e privada. Permite troca segura de informações e protocolo TLS/SSL. Exemplos:

- RSA;
- ECC;
- Diffie-Hellman.

3.3 Hashing

Garantia de integridade sem necessidade de chave. Exemplos:

- SHA–256;
- SHA–3;
- BLAKE2.

Chapter 4

Segurança em Redes

A proteção das redes envolve técnicas e ferramentas para garantir comunicação segura entre dispositivos.

4.1 Firewalls

Firewalls filtram e monitoram tráfego. Podem ser:

- *packet–filtering*;
- *stateful*;
- *next–generation firewall*.

4.2 IDS e IPS

Ferramentas de detecção (IDS) e prevenção (IPS) de intrusões analisam tráfego baseado em assinaturas ou comportamento.

Exemplos reais

- Snort (IDS);
- Suricata (IDS/IPS);
- Wazuh (SIEM/monitoramento).

Chapter 5

Segurança na Computação em Nuvem

Ambientes em nuvem trazem novos desafios e exigem modelos modernos de segurança.

5.1 Responsabilidade Compartilhada

Cada provedor define limites de responsabilidades entre provedor e cliente. Exemplos:

- AWS Shared Responsibility Model;
- Azure Security Framework;
- Google Cloud Security Model.

5.2 Ameaças comuns

- Má configuração;
- vazamento de credenciais;
- APIs inseguras;
- exposição de buckets;
- pobre segmentação.

Chapter 6

Pentest e Segurança Ofensiva

Testes de invasão verificam vulnerabilidades antes que atacantes reais as explorem.

6.1 Etapas de um Pentest

1. Coleta de Informações;
2. Enumeração;

3. Exploração;
4. Pós-exploração;
5. Relatório.

6.2 Ferramentas de Pentest

- Metasploit Framework;
- Nmap;
- Burp Suite;
- Hydra;
- Wireshark.

Sobre os Autores

Este eBook foi desenvolvido por estudantes da Uniara com base em pesqisas sobre Cibersegrança

- **Alison Henrique da Silva**
- **Lucas Dario Claro**
- **Matheus Fernandes Ribeiro**
- **Miguel Silva Gobbi**
- **Murilo Martiniano**

Cada autor contribuiu com pesquisas, revisão técnica e organização do conteúdo, com o propósito de auxiliar estudantes e profissionais na construção de uma base sólida em segurança da informação.