O que é Cibersegurança?

A **cibersegurança** é o conjunto de práticas, tecnologias e processos usados para proteger sistemas, redes, dispositivos e dados contra ataques cibernéticos, acessos não autorizados e danos. Seu objetivo é garantir a **confidencialidade, integridade e disponibilidade (CIA)** das informações.

Principais Ameaças

1. Spyware

Projetado para rastrear e espionar o usuário, o spyware monitora a atividade online e pode registrar todas as teclas pressionadas, capturando dados sensíveis, como informações bancárias. Ele se instala frequentemente junto com softwares legítimos ou cavalos de tróia.

2. Adware

Software que exibe anúncios automaticamente no navegador, muitas vezes instalados sem o consentimento do usuário. É comum que o adware venha acompanhado de spyware.

3. Backdoor

Permite que hackers obtenham acesso remoto a um sistema sem autenticação adequada. Funciona em segundo plano e é de difícil detecção.

4. Ransomware

Malware que criptografa arquivos e exige pagamento para liberá-los. Propaga-se frequentemente por e-mails de phishing ou exploração de vulnerabilidades do sistema.

5. Scareware

Utiliza táticas de medo para enganar usuários e levá-los a instalar programas maliciosos

6. Rootkit

Modifica o sistema operacional para criar backdoors, tornando-se praticamente indetectável. Muitas vezes, a solução é reinstalar o sistema operacional.

7. Vírus

Programas maliciosos que se replicam e infectam outros arquivos. Requerem ativação do usuário e podem causar desde pequenas alterações até danos significativos.

8. Cavalo de Troia (Trojan)

Disfarçado como software legítimo, explora os privilégios do usuário para acessar e comprometer o sistema.

9. Worms

Se replicam automaticamente e se espalham pela rede sem necessitar de interação do usuário. Podem causar grandes prejuízos ao consumir recursos da rede.

Sintomas de Infecção por Malware

- Alto uso da CPU e lentidão no sistema.
- Computador travando ou reiniciando inesperadamente.
- Navegação na internet mais lenta.
- Arquivos modificados ou desaparecidos.
- Presença de programas desconhecidos.
- Envio de e-mails sem autorização do usuário.

Engenharia Social

Métodos utilizados para manipular pessoas e obter informações sigilosas.

Principais tipos de ataques

- **Pretexting:** O invasor finge ser uma entidade confiável para obter dados pessoais.
- **Tailgating:** Um atacante segue um funcionário autorizado para acessar uma área restrita.
- **Quid pro quo:** O invasor oferece algo em troca de informações confidenciais.

Ataques de Negativação de Serviço (DoS e DDoS)

- **DoS:** Envia um volume excessivo de solicitações a um sistema, sobrecarregando-o.
- **DDoS:** Usa uma rede de computadores zumbis (botnet) para realizar o ataque.

Ataques de Senha

- **Ataque de força bruta:** Testa todas as combinações possíveis.
- **Ataque de dicionário:** Usa palavras comuns como senhas prováveis.

- **Ataque de pulverização:** Testa poucas senhas populares em muitas contas.
- **Tabelas arco-íris:** Utiliza hashes pré-calculados para decifrar senhas.

Principais Dispositivos de Proteção

- **Firewalls:** Bloqueiam tráfego não autorizado.
- **Sistemas de Prevenção de Invasão (IPS):** Detectam e bloqueiam ataques.
- **VPNs:** Criam conexões seguras entre redes.
- **Antivírus e Antimalware:** Identificam e removem códigos maliciosos.

Ferramentas de Detecção e Resposta a Incidentes

- **SIEM:** Coleta e analisa eventos de segurança.
- **DLP:** Evita vazamento de dados confidenciais.
- **Honeypots:** Atraem invasores para monitoramento.

Carreiras na Cibersegurança

🔹 Carreiras Técnicas

Analista de Segurança da Informação

Monitora e protege redes, sistemas e dados de empresas contra ameaças.

Pentester (Testador de Penetração)

Realiza testes de invasão para identificar vulnerabilidades em redes e aplicações.

Analista de Resposta a Incidentes (Analista SOC)

Atua no monitoramento de eventos de segurança e resposta a incidentes (níveis L1, L2 e L3).

Engenheiro de Segurança

Implementa e gerencia soluções de segurança, como firewalls, SIEM e IDS/IPS.

Especialista em Forense Digital

Investiga ataques cibernéticos e coleta evidências para análise criminal e auditorias.

🔹 Carreiras Estratégicas e de Gestão

Consultor de Segurança da Informação

Avalia riscos, implementa medidas de proteção e orienta empresas sobre segurança.

Gerente de Segurança da Informação (CISO)

Responsável pela estratégia de segurança da organização.

Auditor de Segurança da Informação

Realiza auditorias e avaliações de conformidade (ISO 27001, LGPD, GDPR).

🔹 Carreiras Especializadas

Engenheiro de DevSecOps

Íntegra segurança no ciclo de vida do desenvolvimento de software.

Especialista em Segurança na Nuvem

Protege infraestruturas de computação em nuvem (AWS, Azure, Google Cloud).

Criptógrafo

Desenvolve e implementa sistemas de criptografía para proteger dados.