Proteção Cibernética

Entenda sobre a CiberSegurança e sua importância na realidade comtemporânea

Karoline Santos Barros

Novembro, 2024

Conteúdo

Capítulo 1

Introdução à Cibersegurança

1.1 Objetivo

O que hoje chamamos de CiberSegurança, tem por objetivo proteger os sistemas de computadores, dispositivos, dados e pessoas contra os roubos de informações e outras várias ameaças cibernéticas.

A proteção cibernética é indispensável na realidade hodierna, uma vez que auxilia na proteção de dados sensíveis, preservando a privacidade de cada individuo, bem como a defesa contra ataques criminosos que cresce cada dia mais com a vulnerabilidade de informações pessoais, prevenindo, detectando e diminuindo esse ataques de forma considerável.

1.2 Definição de Cibersegurança

Se trata de um conjunto de práticas, tecnologias e processos projetados para proteger sistemas, redes, dados e dispositivos contra ataques, acessos não autorizados e danos. A cibersegurança abrange uma ampla gama de práticas, incluindo a proteção de infraestruturas, dados pessoais, e a defesa contra ameaças digitais.

1.3 Principais Ameaças

Atualmente, o exemplos de ameaças mais comuns a serem citadas, são: O Malware que se trata de um vírus projetado para prejudicar e explorar qualquer dispositivo através do que chamam de "software malicioso", temos ainda o Ransomware que se trata de um bloqueio com a finalidade de criptografar conteúdos para fins financeiros por exemplo, bem como o conhecido "phishing"que se trata de golpes onde pode ser formalizados emails ou até mesmo ligações falsas que fazem com que a vitima acredite ser um órgão oficial solicitando suas informações de forma a persuadir a mesma a entregar esses dados com facilidade, entre outros vários golpes presentes no no nosso cotidiano.

1.4 Relevância para Usuários e Profissionais de TI

É de suma importância o papel da CiberSegurança aos profissionais de TI, pois garante a segurança de informações e proteção contra ameaças cibernéticas, esses profissionais precisam garantir a segurança de dados dos usuários de forma com que não tenha espaço para falhas, principalmente com as ameaças estando em constante evolução, isso pode ser feito aplicando regulamentação, tal como a lei LGPD, além da educação e conscientização dos usuários.

Capítulo 2

Princípios Básicos de Segurança Digital

Os princípios básicos da segurança digital são orientações que tem por objetivo proteger informações e sistemas contra ameaças acessíveis a qualquer usuário

2.1 Conceitos de Confidencialidade, Integridade e Disponibilidade (CIA Triad)

Esse modelo é a base da segurança da informação, de forma a garantir a confidencialidade de dados que por sua vez só são acessados por pessoas e sistemas autorizados, como por exemplo o uso de senhas e criptografias, assegurando a integridade dos dados e certificando que as informações estejam acessíveis sempre que necessário.

2.2 Autenticação e Criptografia Básica

A autenticação se da pelo processo de verificação de identidade de um usuário ou sistema, seja ela por senhas, biometria ou até mesmo tokens. Já a Criptografia é o processo de transformação de informações para um formato ilegível que garante a proteção dos dados, como por exemplo a comunicação segura via HTTPS nos casos web e criptografia de e-mails para informações sensíveis.

2.3 Senhas Fortes e Autenticação Multifator

O uso de senhas fortes eleva o grau de proteção dos dados do usuário, enquanto a autenticação MFA adiciona uma camada extra de segurança através da solicitação de dois ou mais métodos de autenticação, afim de proteger contra o acesso indevido mesmo que a senha seja comprometida

Capítulo 3

Ameaças Cibernéticas Comuns

3.1 Malware

Conhecido como "software malicioso", se trata de um vírus projetado para causas danos, roubo de informações e comprometimento de sistemas, podendo se manifestar como um vírus que infecta arquivos e sistemas.

3.1.1 Ransomware

Há também o chamado Ransomware que criptografa dados, geralmente exigindo pagamento para desbloqueá-los, ou ainda o chamado Spyware, que se trata de monitoria de atividades de um usuário afim de coletar informações sigilosas.

3.2 Phishing e Engenharia Social

Já o Phishing e Engenharia Social, se trata de técnicas utilizadas para obter informações sensíveis como senhas e dados bancários através de golpes. O Phishing normalmente é realizado por formulações de e-mails, SMS ou até mesmo sites falsos fraudados que se passam por órgãos legítimos, enquanto que a Engenharia Social é feita por manipulações psicológicas que induzem a vitima a fornecer dados ou realizar ações prejudiciais.

3.3 Ataques DDoS

Esse método, tem como objetivo sobrecarregar um servidor, site ou serviço, elevando o volume do tráfego de forma que torna o mesmo inacessível ao usuário, eles são geralmente realizados através dos "botnets"que enviam grandes quantidade de requisições ao mesmo tempo.

Capítulo 4

Boas Práticas para Proteção Digital

Este capítulo apresenta práticas recomendadas para proteger a segurança digital no cotidiano.

4.1 Cuidados Básicos na Navegação

Para uma navegação segura, o usuário pode evitar as armadilhas cibernéticas com a verificação de links antes de clicar no mesmo, evitando links suspeitos e encurtados, desconfiando de mensagens que induzem o mesmo a digitar informações pessoais, erros gramaticais, entre outros.

4.2 Atualizações e Antivírus

É sempre importante também, que o usuário mantenha seus sistemas atualizados e faça o uso de ferramentas de proteção essenciais para bloquear e tornar menos vulnerável a exploração de hackers. O uso de um bom antivírus é indispensável, pois o mesmo tem o poder de detectar e remover os malwares, bem como oferecer a proteção durante downloads e navegações.

4.3 Backups Regulares

Já os backups, garantem aos usuários a proteção contra perdas de dados e informações, basta que o mesmo realize seus backups com frequência e para maior segurança armazene seus dados em locais distintos, além da verificação periódica dos backups a serem restaurados,

4.4 Gerenciadores de Senhas

O uso de um gerenciador de senhas também auxilia na proteção de informações de forma a evitar acessos indevidos, deve-se fazer também um bom uso da senha, gerando senhas fortes que dificultem outros acessos, podendo ser combinado também com o uso de autenticação multifator e sincronização de dados entre dispositivos.

Capítulo 5

Noções Básicas de Segurança para Profissionais de TI

5.1 Segurança de Redes e Firewalls

Segurança de redes, trata-se basicamente da proteção e comunicações digitais contra acessos não autorizados e ataques, garantindo a confidencialidade e integridade de dados, podendo ser implementado com a segmentação de redes que limita o alcance de ataques, uso de VPNs e monitoramento constante. Do mesmo modo, o firewall se trata de uma barreira confiáveis e não confiáveis de redes com base em regras definidas, como por exemplo em Hardware que protege redes inteiras e Software que operam de forma individual por dispositivos, bloqueando acessos maliciosos e filtrando conteúdos indesejados.

5.2 Gestão de Vulnerabilidades

Pode-se dizer, que é o processo de identificação, avaliação e mitigação de falhas de segurança em sistemas, aplicativos e redes, utilizando de ferramentas de varredura, priorização com base na gravidade, aplicação de patches e configurações seguras, bem como a reavaliação de novas vulnerabilidades.

5.3 Práticas Seguras no Desenvolvimento de Software

Se tratam de práticas que auxiliam na segurança de dados, identificando riscos durante fases de design, inspeção manual ou com ferramentas automáticas para detectar falhas, testes de segurança, como por exemplo o SAST E DAST, monitoramento de bibliotecas externas e limitação de acessos a funcionalidades críticas no sistema.

Capítulo 6

Conclusão e Recomendações Finais

Percebe-se, portanto, que a segurança digital é uma área dinâmica e em constante evolução, que se torna de suma importância na realidade hodierna. Sendo assim, a prática e aprendizado contínuos, são recomendados e essenciais, afim de garantir a proteção do ambiente digital. Com isso, entende-se que os ataques cibernéticos estão cada vez mais sofisticados, exigindo que as soluções também estejam em constante evolução, tornando indispensável o acompanhamento de atualizações, notícias, publicações e até mesmo participações em eventos

Glossário de Termos Essenciais em Cibersegurança

- **Malware**: Software malicioso projetado para danificar ou obter acesso não autorizado a sistemas.
- **Ransomware**: Tipo de malware que exige pagamento para restaurar o acesso a dados.
- **Phishing**: Tentativa de obter informações confidenciais por meio de engano.