Uni Edition

Segurança Cibernética

DataWizards

Conteúdo

Introduction/Prologue

> *"A única maneira de lidar com ameaças cibernéticas é considerar que a segurança não é um estado, mas uma prática contínua."*
>
> *–Bruce Schneier, especialista em segurança cibernética e criptografia*

Esta seção é dedicada à introdução ou prólogo[1], destacando a importância da segurança cibernética em um mundo cada vez mais conectado.[1]

[1] *Notas de rodapé são uma ótima maneira de fornecer informações.*

Parte I

Cybersecurity

Capítulo 1

Introdução à Cibersegurança

A segurança cibernética é o conjunto de práticas, tecnologias e estratégias destinadas a proteger sistemas, redes, dispositivos e informações contra ameaças digitais. Ela é fundamental em um mundo altamente conectado, onde grande parte das atividades humanas, como comunicação, transações financeiras e armazenamento de informações, depende de sistemas

digitais. Seu objetivo principal é garantir que os dados e os sistemas estejam protegidos contra acessos não autorizados, manipulações maliciosas, interrupções ou destruição.

No núcleo do conceito de segurança cibernética estão três princípios fundamentais: **confidencialidade, integridade e disponibilidade**. A confidencialidade visa assegurar que somente pessoas ou sistemas autorizados tenham acesso às informações, utilizando mecanismos como criptografia e controle de acesso. A integridade busca proteger os dados contra alterações indevidas, garantindo que as informações permaneçam completas e precisas. Já a disponibilidade foca em manter sistemas e serviços acessíveis e funcionando sempre que necessário, mesmo diante de possíveis ataques ou falhas.

As ameaças cibernéticas são diversos tipos de ataques ou softwares maliciosos que visam comprometer sistemas, roubar informações ou causar danos.

Diversas empresas no Brasil sofreram com ataques cibernéticos com o passar do anos como: * **RecordTV(2022):** Sofreu ataque de Ransomware, crip-

tografando os conteúdos e matérias. * **Copel(2021):** Que também sofreu Ransomware, porém conseguiram agir rápido. E diversas outras também, Grupo Fleury, Renner, Metalfrio, Banco BRB, PicPay. Só em 2022, o país sofreu 103 bilhões de ataques cibernéticos.

Por isso há uma importância quando se trata sobre a segurança cibernética, com tantos tipos de ameaças cibernéticas possíveis, ela se torna necessária para o bem de dados tanto empresariais, tanto pessoais, seja conformidades normativas que as empresas adotam em setores, como requisitos para proteger dados confidenciais, até as verificações em duas etapas que você cadastra seu email, então sua conta como também vai passar por uma permissão enviada para o email.

Capítulo 2

Princípios Básicos de Segurança Digital

Objetivo

Este capítulo apresenta os fundamentos essenciais de segurança digital, proporcionando uma base para que qualquer usuário possa proteger seus dados e dispositivos de ameaças cibernéticas.

A Tríade CIA:

Confidencialidade, Integridade e Disponibilidade A tríade CIA é um dos pilares da segurança da informação, composta pelos seguintes conceitos:

Confidencialidade: A confidencialidade assegura que a informação esteja acessível apenas para as pessoas autorizadas. Exemplo: O uso de criptografia para proteger dados sensíveis como senhas ou informações financeiras.

Integridade: A integridade garante que os dados não sejam alterados ou corrompidos durante o armazenamento ou transmissão. Exemplo: Verificação de hash em arquivos baixados da internet para assegurar que não foram modificados.

Disponibilidade: A disponibilidade assegura que os sistemas, serviços e informações estejam acessíveis sempre que necessário. Exemplo: Serviços de backup em nuvem que garantem o acesso a informações críticas mesmo em caso de falha local.

Autenticação e Criptografia Básica: Autenticação é o processo de verificar a identidade de um

usuário antes de conceder acesso a um sistema, os principais tipos de autenticação são:

Autenticação por Senha: Utiliza uma senha ou PIN.

Autenticação Biométrica: Reconhecimento de impressão digital, facial ou íris.

Autenticação Multifator (MFA): Combina dois ou mais métodos, como senha e código SMS.

Criptografia

A criptografia é uma técnica que converte informações legíveis em um formato inacessível a usuários não autorizados, existem dois tipos principais:

Criptografia Simétrica: Utiliza a mesma chave para criptografar e descriptografar os dados. Exemplo: Algoritmo AES (Advanced Encryption Standard).

Criptografia Assimétrica: Utiliza um par de chaves, uma pública e outra privada. Exemplo: Certificados digitais usados em conexões HTTPS.

A Importância de Senhas Fortes e Autenticação Multifator

Senhas Fortes:

Uma senha forte é a primeira linha de defesa contra invasões. Para criar uma senha segura, siga estas diretrizes:

Utilize pelo menos 12 caracteres que combinem letras maiúsculas, minúsculas, números e símbolos. Evite senhas óbvias como datas de nascimento ou sequências (ex.: "123456"ou "senha"). Utilize um gerenciador de senhas para criar e armazenar combinações complexas. Autenticação Multifator (MFA) O MFA adiciona uma camada extra de segurança ao exigir mais de uma forma de autenticação. Mesmo que uma senha seja comprometida, o segundo fator protege a conta.

Entender e aplicar os princípios básicos de segurança digital é essencial para proteger suas informações pessoais e profissionais. A combinação de boas práticas, como o uso de senhas fortes, autenticação multifator e criptografia, reduz os riscos de ataques.

Capítulo 3

Ameaças Cibernéticas Comuns

Objetivo

Este capítulo explora as principais ameaças cibernéticas que afetam tanto usuários quanto empresas. Compreender essas ameaças é o primeiro passo para preveni-las e proteger seus dados e sistemas.

Malware

1. Malware: Vírus, Ransomware e Spyware Malware (do inglês malicious software) é um software malicioso projetado para danificar, explorar ou controlar sistemas sem o consentimento do usuário. As principais categorias incluem:

Vírus

1.1. Vírus Um vírus é um programa que se anexa a arquivos legítimos e se espalha quando esses arquivos são executados. Como afeta: Pode corromper arquivos, causar perda de dados ou até mesmo deixar o sistema inutilizável. Exemplo prático: Um documento de texto infectado que, ao ser aberto, compromete todo o sistema.

Ransomware

1.2. Ransomware Ransomware é um tipo de malware que sequestra os dados da vítima, criptografando-os e exigindo um resgate para liberar o acesso. Como afeta: Empresas podem perder acesso a informações críticas, resultando em interrupções nas operações

e prejuízos financeiros. Exemplo prático: O ataque de ransomware WannaCry em 2017 afetou sistemas de hospitais, empresas e órgãos públicos ao redor do mundo.

Spyware

1.3. Spyware Spyware é um software que coleta informações sobre o usuário sem o seu conhecimento, como senhas, histórico de navegação e dados financeiros. Como afeta: Pode levar ao roubo de identidade, acesso não autorizado a contas bancárias e monitoramento não consentido. Exemplo prático: Um spyware instalado em um dispositivo móvel pode capturar senhas de redes sociais e aplicativos bancários.

Phishing e Engenharia Social

2. Phishing Phishing é uma técnica de engenharia social que visa enganar as vítimas para que revelem informações sensíveis, como senhas e números de cartão de crédito. Isso é geralmente feito por meio de e-mails, mensagens ou sites falsos.

Como afeta: Pode resultar em roubo de identidade, acesso não autorizado a contas bancárias ou comprometimento de sistemas empresariais. Exemplo prático: Um e-mail falso de um "banco"solicitando que o usuário clique em um link para atualizar sua senha.

Engenharia Social

2.1. Engenharia Social Engenharia social é a manipulação psicológica de pessoas para levá-las a divulgar informações confidenciais ou realizar ações prejudiciais.

Como afeta: Pode comprometer a segurança de sistemas, mesmo quando as proteções técnicas estão em vigor. Exemplo prático: Um atacante se passa por funcionário de TI para convencer um colaborador a revelar sua senha.

Ataques DDoS

3. Ataques DDoS (Negação Distribuída de Serviço) DDoS (Distributed Denial of Service) é um ataque que tenta tornar um serviço ou site indisponível

sobrecarregando-o com um grande volume de tráfego de diferentes fontes.

Como afeta: Pode derrubar sites, interromper serviços online e causar perda de receita para empresas que dependem da disponibilidade de seus sistemas. Exemplo prático: Ataques DDoS coordenados por redes de bots (botnets) podem derrubar plataformas de e-commerce durante datas importantes como Black Friday.

Exemplos Práticos de Impacto em usuários e empresas:

João recebe um e-mail aparentemente legítimo do seu banco pedindo para atualizar suas informações pessoais, ele clica no link e insere seus dados em uma página falsa, resultando no roubo de sua conta bancária.

Empresa: Uma pequena empresa é vítima de um ataque de ransomware. Todos os arquivos críticos da empresa são criptografados, e os sistemas ficam paralisados. A empresa não possui backup atualizado e decide pagar o resgate, resultando em perdas financeiras significativas.

Infraestrutura Crítica: Um hospital sofre um ataque DDoS em seus sistemas de atendimento online. Pacientes não conseguem agendar consultas ou acessar resultados de exames, afetando a prestação de serviços de saúde.

Capítulo 4

Boas Práticas para Proteção Digital

Objetivo

Este capítulo oferece práticas de segurança digital que podem ser aplicadas no dia a dia, ajudando usuários a se protegerem contra ameaças cibernéticas.

Cuidados Básicos na Navegação e Verificação de Links e E-mails

A navegação na internet e o uso de e-mails são rotinas cotidianas, mas também são portas de entrada para diversas ameaças. Algumas práticas recomendadas incluem:

Verificação de Links Sempre passe o cursor sobre um link antes de clicar para verificar o destino real. Desconfie de links encurtados ou de URLs que contenham caracteres suspeitos.

Verificação de E-mails Desconfie de e-mails não solicitados, especialmente os que pedem informações pessoais ou financeiras.Verifique o endereço do remetente domínios genéricos ou variações de domínios legítimos podem indicar fraudes, nunca abra anexos de remetentes desconhecidos.

Atualizações e Uso de Antivírus

Manter sistemas e aplicativos atualizados é fundamental para corrigir vulnerabilidades conhecidas que podem ser exploradas por atacantes. Ative as atua-

lizações automáticas sempre que possível, priorize a atualização de sistemas operacionais, navegadores e aplicativos críticos. O uso de um bom antivírus pode detectar e bloquear ameaças conhecidas, como malwares e spyware. Mantenha o antivírus atualizado, realize verificações regulares no sistema.

Exemplo Prático: Um sistema desatualizado pode ser vulnerável a exploits conhecidos, como os utilizados no ataque EternalBlue, explorado pelo ransomware WannaCry.

Importância de Backups Regulares

Fazer backups regulares é uma das medidas mais eficazes para proteger seus dados contra perda ou comprometimento, seja por ataques de ransomware ou falhas de hardware.

Boas Práticas de Backup: periodicidade Realize backups regularmente (diários ou semanais, dependendo da criticidade dos dados).

Localização: Mantenha backups em locais diferentes, como um disco rígido externo e um serviço de nuvem confiável.

Testes: Periodicamente, teste a restauração dos dados para garantir que os backups estão funcionais.

Gerenciadores de Senhas

Senhas fortes são essenciais, mas podem ser difíceis de lembrar, especialmente quando usadas para várias contas. Gerenciadores de senhas oferecem uma solução prática e segura.

Utilize gerenciadores de senhas confiáveis, como LastPass, Bitwarden ou 1Password. Ative a autenticação multifator no gerenciador para maior segurança.

Capítulo 5

Conclusão e Recomendações Finais

A segurança digital está cada vez mais presente no nosso dia a dia, desde proteger nossos dados pessoais até garantir a integridade de sistemas em grandes empresas, ela exige atenção constante e esforço para nos mantermos atualizados. Praticar Faz Toda a Diferença colocar em prática o que aprendemos é essencial. Pequenas mudanças, como usar senhas fortes,

habilitar autenticação multifator e ficar atento aos links suspeitos, já fazem uma grande diferença.

5.1 Recomendações

Aqui estão algumas sugestões para quem quer começar ou se aprofundar em segurança digital:

Livros: Cybersecurity Essentials - Charles J. Brooks The Art of Invisibility - Kevin Mitnick

Cursos e Recursos Online: CS50's Introduction to Cybersecurity (edX) Introduction to Cyber Security (OpenLearn) Blogs e Sites: Krebs on Security Dark Reading

5.2 Glossário

DDoS (Distributed Denial of Service) O que é? Um ataque que sobrecarrega um site ou sistema para que ele fique fora do ar.

Backup O que é? Uma cópia dos seus dados para evitar perdas caso algo dê errado.

Patch de Segurança O que é? Uma atualização que corrige falhas no software e ajuda a evitar ata-

ques.