Cibersegurança para Iniciantes: Proteja-se Contra Ameaças Online

Bianca, Daniel, Eduardo, Jeferson, Kauã, Letícia, Maria Eduarda, Mariana, Patrick, Polyana, Stephany.

Conteúdo

Seção 1

Introdução à Cibersegurança

A cibersegurança se tornou um tema essencial em nossa sociedade digital. Com o aumento do uso de dispositivos conectados à internet, como smartphones e computadores, a proteção de dados e sistemas contra ameaças cibernéticas é mais importante do que nunca. Ataques como vírus, phishing e ransomware visam roubar informações pessoais e danificar redes, tornando vital o entendimento sobre como nos proteger.

A cibersegurança é crucial em nosso cotidiano por diversas razões. Primeiro, ela protege nossos dados pessoais. Quando fazemos compras online ou compartilhamos informações nas redes sociais, precisamos garantir que nossos dados estejam seguros contra roubos. Além disso, a segurança financeira é uma preocupação crescente, com transações digitais em alta, proteger contas bancárias e cartões de crédito é imprescindível.

Outro ponto importante é a confiança nas tecnologias. Quando as pessoas se sentem seguras ao usar serviços online, estão mais dispostas a adotar novas tecnologias. Por outro lado, ataques

cibernéticos podem gerar desconfiança e prejudicar a economia. As empresas também são alvos frequentes de ataques, e investir em cibersegurança é fundamental para proteger informações sensíveis e garantir a continuidade dos negócios.

Em suma, a cibersegurança é vital na era digital. Proteger nossos dados e promover um ambiente online seguro deve ser uma prioridade para todos nós. Boas práticas de segurança, como senhas fortes e educação sobre riscos online, são passos importantes na luta contra as ameaças cibernéticas.

1.1 Definição de Cibersegurança

Cibersegurança refere-se ao conjunto de práticas, tecnologias, processos e políticas adotadas para proteger sistemas de informação, redes, dispositivos e dados contra ataques, danos ou acessos não autorizados. Dessa forma, é possível garantir que dados valiosos não vazem ou sejam violados em ataques cibernéticos.

Esses ataques podem ter a intenção de acessar servidores, roubar senhas, sequestrar dados ou até mesmo fraudar transações financeiras. A cibersegurança envolve diversas áreas, como criptografia, controle de acesso, monitoramento de redes, resposta a incidentes e defesa contra ameaças emergentes.

1.2 Como funciona a cibersegurança?

A segurança de computadores vai muito além dos softwares antivírus e antimalware convencionais. No contexto das empresas, é preciso fazer bem mais para garantir a integridade de redes, sistemas e máquinas.

A cibersegurança funciona como um escudo para blindar toda a parte de TI, seus dispositivos, e suas operações.

Para isso, realiza-se procedimentos como:

- Testes de intrusão automáticos com análise de vulnerabilidades
- Implementação de plataformas de segurança centralizadas para controle, monitorização e neutralização de ameaças na rede, endpoints e distração de eventuais atacantes
- Proteção para dispositivos Bluetooth e Wi-Fi
- Blindagem de dados confidenciais.
- Criptografia, firewalls e atualizações
- Sistemas de detecção de intrusos (IDS).

Seção 2

Princípios Básicos de Segurança Digital

A segurança digital é um tema fundamental em nossa era conectada. Com a crescente dependência de tecnologias digitais, é essencial entender os princípios básicos de segurança digital para proteger nossa informação e evitar ameaças.

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

O CIA Triad representa os pilares da segurança da informação:

- Confidencialidade: Garante que apenas pessoas autorizadas possam acessar informações sensíveis. Isso é al-

cançado por meio de métodos como controle de acesso e criptografia, reduzindo o risco de vazamentos de dados.

- Integridade: Refere-se à proteção dos dados contra alterações não autorizadas ou acidentais. Mecanismos como funções de hash e registros de auditoria são empregados para monitorar e verificar mudanças, assegurando a confiabilidade da informação.
- Disponibilidade: Assegura que sistemas e dados estejam acessíveis sempre que necessário, mesmo diante de falhas técnicas ou ataques. Estratégias incluem redundância de sistemas, backups e planejamento para recuperação de desastres. Esses conceitos são fundamentais para entender a segurança digital e proteger nossa informação.
- Autenticação e Criptografia Básica: A autenticação e criptografia são fundamentais para garantir a segurança e confiabilidade em sistemas e aplicações.

2.2 *O que é Autenticação?*

A autenticação é um processo fundamental para garantir a segurança e confiabilidade em sistemas e aplicações. É o processo de verificar a identidade de um usuário ou sistema antes de conceder acesso a recursos protegidos. São tipos de autenticação, eles:

- Autenticação por Senha: Verifica identidade com uma sequência de caracteres secreta.
- Autenticação por Biometria: Utiliza características físicas únicas, como impressão digital ou rosto.
- Autenticação por Certificado Digital: Utiliza certificados digitais emitidos por autoridades confiáveis.
- Autenticação por Token: Utiliza um dispositivo portátil que gera um código de acesso único.

A autenticação garante que apenas usuários autorizados tenham acesso a recursos protegidos, protegendo contra acessos não autorizados e ataques de segurança.

A autenticação multifator (AMF) é um processo que requer mais de um método de autenticação para acessar uma conta ou sistema. As vantagens da Autenticação Multifator, são:

- Reduz o risco de acessos não autorizados
- Protege contra ataques de phishing e malware
- Melhora a segurança de dados sensíveis
- É obrigatória em muitas indústrias regulamentadas

2.3 Criptografia

A criptografia é a técnica de proteger informações por meio de códigos e algoritmos. Os Principais tipos de Criptografia, são:

- Criptografia Simétrica (AES): Utiliza a mesma chave para cifrar e decifrar dados. É rápida e eficiente, mas requer compartilhamento da chave.
- Criptografia Assimétrica (RSA): Utiliza pares de chaves: pública para cifrar e privada para decifrar. É mais segura, mas lenta.

A combinação de autenticação e criptografia oferece várias vantagens, incluindo segurança, confiança, controle e privacidade. No entanto, também existem desafios, como vulnerabilidade, complexidade e escalabilidade.

Duas das principais medidas para proteger nossos dados e contas são senhas fortes e autenticação multifator.

Uma senha forte é aquela que é difícil de adivinhar ou descobrir por meio de ataques de força bruta. As principais características de senhas fortes incluem:

- Tamanho: mínimo de 12 caracteres
- Complexidade: combinação de letras maiusculas e minúsculas, números e símbolos
- Originalidade: evite utilizar senhas
- Mudança regular: altere senhas a cada 60-90 dias.

Seção 3

Ameaças Cibernéticas Comuns

Nesse tópico abordaremos alguns tópicos fundamentais relacionados à segurança digital, como Malware, Phishing, ataques de DDos e alguns exemplos práticos relacionados a isso.

3.1 Walmare

Desde os primeiros dias da internet, os Malwares são um tipo de preocupação decorrente e discutidos nas empresas ou entre seus usuários. Eles são programas de caráter malicioso que evoluíram ao longo dos anos, tornando-se cada vez mais perigosos, e capazes de comprometer os dados sensíveis de cada um, tornando-os alvos de ataques devastadores que podem trazer sérios prejuízos financeiros a empresas e em seus dados, como e-mails, registros pessoais e senhas.

Segundo Mcafee, empresa de seguranças de computadores, diz em seu site que um Malware abrange todos os tipos de softwares

maliciosos por razões como:

- Enganar a vítima para roubo de informações;
- Roubo de cartões de crédito ou dados financeiros;
- Infectar computadores, a fim de aplicar as minas de bitcoin e outras moedas virtuais.

Esses são só alguns exemplos de objetivos de um cibercriminoso em roubo de informações, mas você sabe onde ele está presente ou onde ele se espalha? Ele está presente em e-mails, anúncios em alguns tipos de sites populares, unidades USB infectadas e até mesmo em mensagens de texto. Dentro dele existem várias modalidades sendo eles:

- **Vírus**: um tipo de ataque que pode vir por aplicativos e até mesmo em e-mail, onde aparecem sugestões e que propagam a você informações falsas, onde ao clicar em um link por exemplo, o seu dispositivo se torna infectado.
- **Ransomware**: É uma modalidade onde são roubados os seus dados e são cobrados um resgate virtual do que foi vazado anteriormente.
- **Worms**: Ela tem como objetivo copiar dados de uma máquina para outra, sem a presença de um usuário, geralmente ocorrendo por uma falha de segurança.
- **Cavalos de troia**: Tendo o nome inspirado no conto da mitologia Grega, o Cavalo de Troia tem por finalidade se

disfarçar de aplicativos inofensivos e enganar as pessoas, com a ideia de baixar aplicativos em seu sistema, proporcionando um tipo de vírus, que rouba os seus dados e trava a sua máquina.

- **Spyware**: É um tipo de programa que se instala em um computador sem o seu monitoramento e monitora e rouba informações pessoais de forma autônoma em um dispositivo alvo, sendo usado por órgãos governamentais e policiais do mundo inteiro.

3.2 *Phishing*

Agora que você já está por dentro do que é um Malware, que tal conhecer um pouco sobre Phishing?

Sabia que Phishing é um ataque cibernético que tenta roubar o seu dinheiro, ou a sua identidade fazendo o usuário revelar informações como números de cartões e até mesmo informações bancárias? Ela ocorre de forma sútil, ou seja, criminosos se passam por outras pessoas ou empresas e até mesmo amigos e parentes, que podem te induzir a clicar em links de acesso a sites, PDFs e arquivos que contenham anexos, gerando um tipo de ataque.

Segundo Carlos Prokisch, autor do livro “Cibersegurança”, uma forma de se proteger é se atentar para o endereço de e-mail do remetente, caso o indivíduo tenha recebido um anexo de e-mail suspeito de uma instituição financeira, é possível notar que se inicia como “infoemail” seguido de um número que gera um

tipo de spam. Isso não é uma prática comum em nenhum Banco e se isso acontecer é porque provavelmente ele foi criado por softwares que criam qualquer tipo de extensão de caráter falso.

3.3 Engenharia Social

Embora a segurança digital dependa de sistemas de altíssimo nível, o maior defeito muitas vezes se encontra nas pessoas, pois são elas próprias que divulgam as suas informações de forma leiga e a Engenharia Social explora exatamente isso.

Ela é um exemplo de como a segurança de alguém pode ser comprometida em relação aos roubos de dados, acontecendo de forma pacífica sem nenhum tipo de violência. Quando alguém, ou um amigo de trabalho pede informações como senhas de sistemas, de bancos ou números de cartões está cometendo uma Engenharia Social.

Podendo se dar em um contexto pessoal ou profissional, sendo uma técnica comum e pode ser utilizada por qualquer pessoa sem nenhum tipo de aplicativo ou sistemas avançados, basta somente uma ligação ou uma simples conversa entre duas pessoas.

O motivo dela funcionar tão bem, é porque ela explora a fragilidade da mente humana, fazendo com que os indivíduos tomem decisões de forma rápida através da persuasão, ou seja, se algo acontece de forma comum no nosso dia dificilmente iremos parar para analisar a situação de forma clara.

3.4 Ataques DDoS

Um ataque de “Distribuição de Serviço Negado” ou DDos ocorre quando um cibercriminoso aproveita dos limites de tráficos da rede e envia múltiplas solicitações com o único objetivo de exceder a capacidade com que o site tem de funcionar, gerando uma sobrecarga no site, servidor ou serviço.

Ela funciona da seguinte forma, um site utiliza de recursos da rede como largura da banda e servidor da internet para se manter conectado, possuindo uma capacidade finita de recursos. Sempre que excede o número de acessos, ela gera um mau funcionamento, gerando uma resposta lenta e tornando algumas solicitações totalmente ignoradas de seus usuários.

Isso acontece porque a pessoa por trás, controla as redes de computadores infectados por vírus, controlando ações de cada computador em uma escala para sobrecarregar os sites das vítimas.

Em resumo, ataques de DDos apresentam um risco à segurança de usuários da rede e uma forma de combater é usar de firewall e monitoramentos para se proteger desse risco.

Seção 4

Boas Práticas para Proteção Digital

A crescente digitalização das atividades cotidianas trouxe benefícios inegáveis, mas também ampliou o risco de ciberataques e ameaças digitais. Em um cenário onde a dependência de sistemas online e de dados digitais se torna cada vez maior, adotar boas práticas de segurança digital não é apenas recomendável, mas essencial.

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

O primeiro passo para manter a segurança digital é ter cautela ao navegar na internet e interagir com e-mails. Muitos ataques cibernéticos, como o phishing, são baseados na engenharia social,

onde golpistas tentam enganar os usuários para que revelem informações confidenciais, como senhas ou dados bancários. A seguir, algumas boas práticas para evitar cair em armadilhas online:

- Verifique URLs e e-mails antes de clicar: Ao acessar um site ou clicar em links recebidos por e-mail, sempre verifique se o endereço começa com "https"(indicando uma conexão segura). Além disso, desconfie de pequenos erros de digitação, como "goggle.com"em vez de "google.com". Estes são sinais de tentativas de phishing, onde golpistas tentam imitar sites legítimos para coletar informações. Ferramentas como Gmail, Outlook, e outros provedores de e-mail, geralmente possuem filtros automáticos para identificar e-mails suspeitos.
- Cuidado com e-mails não solicitados: Evite abrir e-mails que pedem informações pessoais ou financeiras, principalmente se você não os solicitou. Empresas legítimas raramente pedem dados sensíveis dessa forma. Caso receba um e-mail suspeito de uma instituição financeira, por exemplo, entre em contato diretamente com a empresa para verificar sua autenticidade.
- Evite redes Wi-Fi públicas: As redes Wi-Fi abertas e não protegidas são um convite para ataques cibernéticos. Elas são vulneráveis à interceptação de dados por hackers. Caso precise usar uma rede pública, utilize uma VPN (Rede Privada Virtual), que criptografa sua conexão e torna mais difícil para terceiros acessarem suas informações.

4.2 Tecnologias e Soluções de Cibersegurança

A adoção de soluções de cibersegurança também é essencial para fortalecer a proteção contra ciberataques. Algumas tecnologias recomendadas incluem:

- Firewalls avançados: Esses sistemas monitoram e controlam o tráfego de rede, impedindo que invasores acessem sistemas internos.
- Monitoramento contínuo: Softwares que detectam e respondem a ameaças em tempo real são fundamentais para mitigar os riscos de ataques.
- Soluções antivírus e antimalware: Softwares atualizados que protegem contra as ameaças mais recentes, incluindo trojans, vírus e worms.

Figura 4.1: *Legenda da imagem pequena.*

Seção 5

Noções Básicas de Segurança para Profissionais de TI

Para proteger os três princípios de segurança e garantir seu equilíbrio é necessário usar controles de autenticação. Podem ser digitais ou físicas. Consistem no uso de identificação, senhas e autenticação de dois fatores (ou autenticação multifator), que é uma verificação adicional em forma de código ou aplicativo.

Ainda, outra maneira de proteger a confidencialidade do sistema é com o uso de controles de acesso, limitando o acesso dos dados. Dentre os tipos de controle de acesso, os principais são:

- Classificação de conteúdo: determina quem pode visualizar ou modificar as informações.
- Links com tempo limitado: limita o tempo que um indivíduo tem acesso àquele conteúdo.

- Listas de acesso atualizadas: são importantes para que as pessoas que não fazem mais parte da empresa não tenham mais acesso aos dados da mesma.

Um firewall é um software, ou hardware, comumente usado para a proteção de redes. É uma ferramenta para restringir o fluxo de tráfego entres as redes, reduzindo o risco de ataques cibernéticos e impedindo o acesso a recursos não autorizados ao mesmo tempo.

Os firewalls de rede analisam os dados dentro das quatro camadas de comunicação TCP/IP (Transmission Control Protocol/Internet Protocol) da mais alta para a mais baixa: aplicativo, transporte, IP e link de dados de ambos os lados do tráfego, então permitindo ou bloqueando a conclusão do tráfego com base na política nele estabelecida. Quanto mais avançada a tecnologia de segurança do firewall, mais ordens podem ser examinadas por ele, o tornando mais preciso e detalhado.

O Gerenciamento de Vulnerabilidades é um processo contínuo, muitas vezes automatizado, que protege os sistemas, redes e aplicativos de uma empresa contra ataques cibernéticos e violações de dados. Ele identifica, avalia e corrige falhas de segurança, ajudando a prevenir ataques e minimizar danos, caso ocorram. Seu objetivo é reduzir a exposição da empresa a riscos, mitigando vulnerabilidades, por mais que seja uma tarefa difícil devido à quantidade de possíveis falhas e recursos limitados para correção. O processo deve necessariamente ser contínuo para acompanhar ameaças emergentes e os ambientes, que estão sempre em constante mudança.

Um programa de Gerenciamento de Vulnerabilidades deve possuir funcionalidades de descoberta de ativos no inventário, verificação de vulnerabilidades, gerenciamento de patch, gerenciamento de configuração, SIEM (gerenciamento de eventos e incidentes de segurança), teste de penetração, inteligência contra ameaças e vulnerabilidades de correção para ser eficaz. As etapas para gerenciar vulnerabilidades são:

- Identificar vulnerabilidades;
- Avaliar as vulnerabilidades;
- Abordar as vulnerabilidades;
- Relatar vulnerabilidades.

Entre os benefícios da implementação de um gerenciamento de vulnerabilidades em uma empresa, estão:

- melhoria na segurança e controle;
- relatórios atualizados;
- visibilidade e eficiência operacionais.

Seção 6

Conclusão e Recomendações Finais

A crescente interconexão digital trouxe inúmeras oportunidades, mas também amplificou os desafios relacionados à segurança cibernética. O tema abordado ao longo deste ebook reforça a relevância da cibersegurança para indivíduos, organizações e governos, evidenciando que investir em conhecimento e práticas preventivas é essencial para mitigar riscos.

6.1 Recomendações para Usuários e Organizações

Para maximizar a proteção, recomenda-se:

- Adotar uma cultura de segurança: Promova treinamentos regulares e campanhas de conscientização em organizações.

- Implementar tecnologias de ponta: Ferramentas como firewalls de última geração e autenticação multifator devem ser padrão em qualquer ambiente corporativo.
- Realizar auditorias regulares: Revisões periódicas ajudam a identificar vulnerabilidades e a garantir conformidade com normas, como a LGPD.
- Praticar a segurança preventiva: Manter sistemas atualizados, realizar backups e evitar comportamentos de risco, como clicar em links suspeitos, são práticas simples, mas altamente eficazes.

6.2 Considerações

A cibersegurança não é um esforço pontual, mas uma responsabilidade contínua. Com a aplicação de boas práticas e o compromisso com a educação continuada, é possível criar um ambiente digital mais seguro, fortalecendo a confiança e promovendo o uso responsável das tecnologias. O desafio é grande, mas, com preparação e resiliência, é possível reduzir significativamente os riscos e danos associados às ameaças cibernéticas.