Ebook sobre a Segurança Cibernética

Conteúdo

Parte I

Introdução à Segurança Cibernética

Capítulo 1

Definição de Segurança Cibernética

Segurança Cibernética, também conhecida como Cibersegurança ou Segurança Digital, envolve muito mais do que apenas ferramentas e sistemas tecnológicos. Ela abrange desde o comportamento do indivíduo na internet, passando por proteção de dados, legislações específicas, até o cumprimento de normativas legais, como a LGPD (Lei Geral de Proteção de

Dados Pessoais). A LGPD (Lei nº 13.709/2018) é a legislação brasileira que regula a coleta, armazenamento e tratamento de dados pessoais, promovendo transparência e proteção à privacidade. Inspirada no GDPR europeu, essa lei entrou em vigor em setembro de 2020.

Capítulo 2

Importância da Segurança Digital

Segurança Cibernética é o conjunto de práticas destinadas a proteger sistemas, redes e dados contra ataques e acessos não autorizados.

Compreender a importância da Segurança Digital é essencial para reduzir riscos e evitar prejuízos, financeiros ou de privacidade.

Capítulo 3

Dados e Estatísticas sobre Ataques no Brasil e no Mundo

- O Brasil é o segundo maior país em número de ataques. [1]
- O valor médio por violação de dados no Brasil é de US$1.36M. [2]

- O crescimento esperado de ataques na América do Sul entre 2023 e 2028 é de 17,7% ao ano. [3]
- Os danos causados pelos ataques cibernéticos chegarão a 10,5 trilhões de dólares anuais até 2025. [4]

Figura 3.1: *Ataques nos países*

Parte II

Principais Ameaças e Riscos

Capítulo 4

Descrição dos Principais Riscos Percebidos e Dados sobre Preocupações Contemporâneas

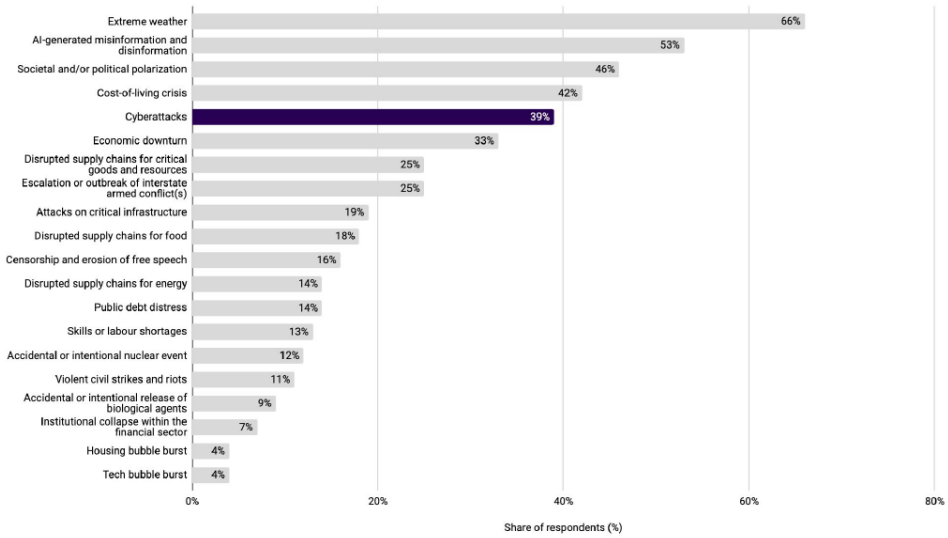

Figura 4.1: *Riscos e Ameaças percebidos e medidos pela porcentagem de respostas*

Cada barra representa um risco específico, e a porcentagem indica quantos entrevistados consideram esse risco uma preocupação.

Os principais riscos identificados no gráfico incluem:

- Eventos climáticos extremos (66%)
- Desinformação e informação errada gerada por IA (53%)

- Polarização social e/ou política (46%)
- Crise do custo de vida (42%)
- Ataques cibernéticos (39%)

Esses fatores são seguidos por outras preocupações como desaceleração econômica, interrupções na cadeia de suprimentos, conflitos armados, ataques à infraestrutura crítica, e vários outros.

Em geral, o gráfico destaca as preocupações contemporâneas relacionadas a questões climáticas, econômicas, tecnológicas e de segurança, refletindo os riscos percebidos pela população ou pelos participantes das pesquisas

Parte III

Princípios Básicos de Segurança Digital

Confidencialidade, Integridade e Disponibilidade são os 3 pilares que sustentam Segurança da Informação e juntos têm como objetivo garantir a Confiabilidade das informações.

Capítulo 5

Confidencialidade

Um dos pilares da segurança é a confidencialidade, que deve garantir a restrição de acesso a informações por pessoas não autorizadas.

Um bom exemplo sobre confidencialidade é a autorização em pastas e arquivos em uma rede interna.

Imagine que o funcionário Joaquim trabalhe no setor Comercial, ele deverá ter autorização de acesso às pastas e arquivos utilizados pelo seu setor, porém não poderá acessar, por exemplo, a pasta do setor Financeiro.

Confidencialidade também é muito associado a criptografia.

Capítulo 6

Integridade

A integridade deve garantir que a informação seja completa e exata, além de prevenir que usuários sem autorizações façam modificações nelas.

Um ótimo exemplo de integridade é uso do HASH, não entrarei em detalhes sobre o HASH, mas uma das suas funções é garantir que um arquivo não sofreu alterações.

Imagine como exemplo o download de um arquivo txt, chamado exemplo.txt com o conteúdo “Esse arquivo é um arquivo de teste”. O HASH desse arquivo

seria um código único, como pode ver na imagem a seguir.

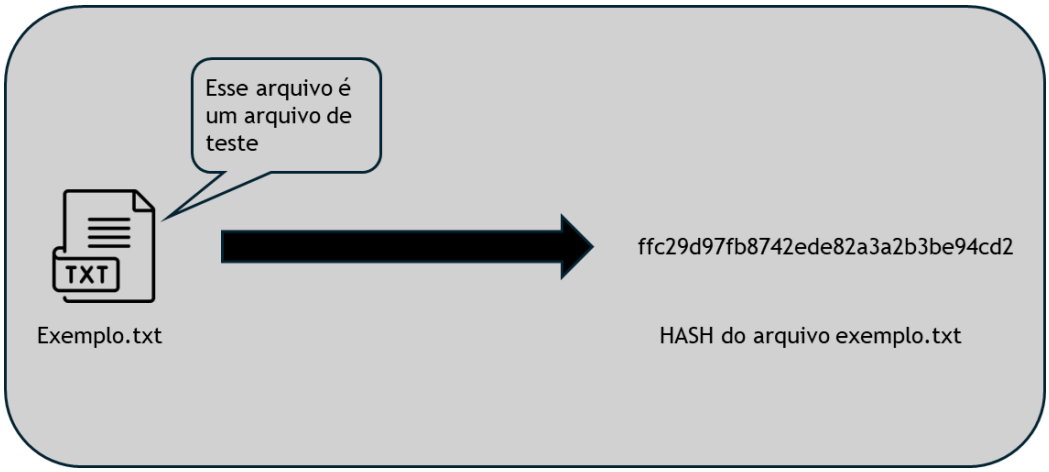

Figura 6.1: *Exemplo de HASH*

Qualquer alteração mínima resultará em um HASH completamente diferente. Como exemplo veja como o código HASH ficaria se trocássemos a letra “é” para a letra “e” sem assento.

Ou seja, com o uso do HASH pode ser validado se o arquivo que foi baixado realmente está integro e que não sofreu nenhum dano ou alteração no caminho.

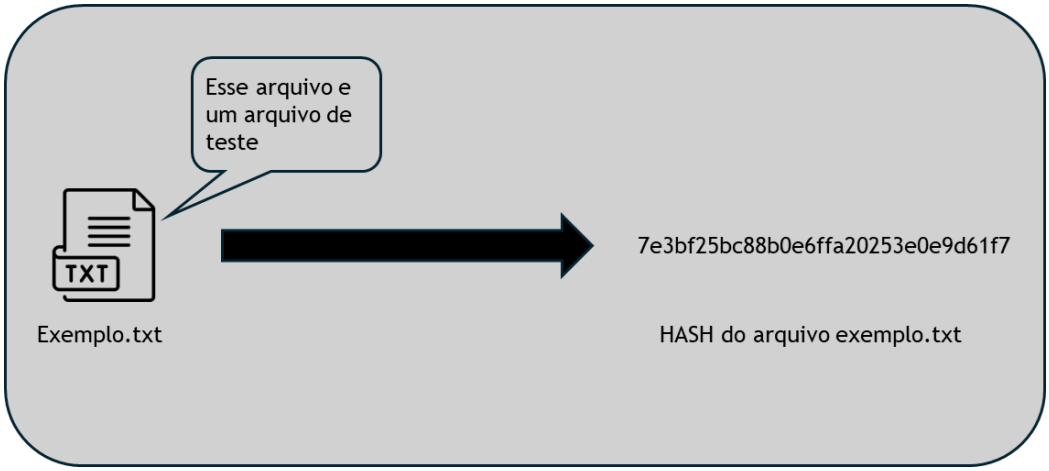

Figura 6.2: *Exemplo de HASH alterado*

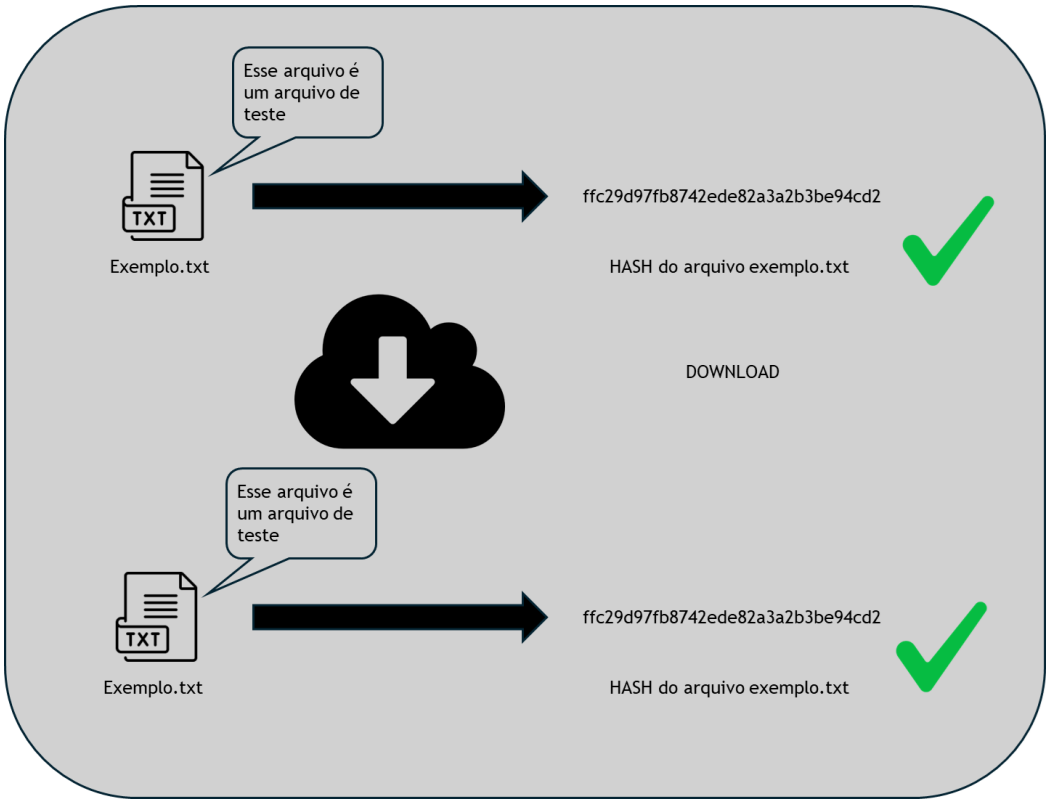

Figura 6.3: *Exemplo de HASH correto para download*

Capítulo 7

Disponibilidade

A disponibilidade deve garantir que a informação esteja acessível e utilizável sempre que necessário.

Mesmo que os dados sejam mantidos confidenciais e sua integridade seja preservada, muitas vezes são inúteis, a menos que estejam disponíveis para aqueles na organização e os clientes que atendem. Isso significa que os sistemas, redes e aplicativos devem estar funcionando como e quando deveriam. Além disso, as pessoas com acesso a informações específicas devem poder acessá-las quando necessário, e o

acesso aos dados não deve levar um tempo excessivo.

Se, por exemplo, houver uma queda de energia e não houver um sistema de recuperação de desastres em vigor para ajudar os usuários a recuperar o acesso a sistemas críticos, a disponibilidade será comprometida. Além disso, um desastre natural, como uma inundação ou até mesmo uma tempestade de neve grave, pode impedir que os usuários cheguem ao escritório, o que pode interromper a disponibilidade de suas estações de trabalho e outros dispositivos que fornecem informações ou aplicativos essenciais para os negócios. A disponibilidade também pode ser comprometida por meio de atos deliberados de sabotagem, como o uso de ataques de negação de serviço (DoS) ou ransomware.

Para garantir a disponibilidade, as organizações podem usar redes, servidores e aplicativos redundantes. Eles podem ser programados para ficarem disponíveis quando o sistema primário tiver sido interrompido ou quebrado. Você também pode aumentar a disponibilidade mantendo-se atento sobre atualizações de pacotes de software e sistemas de segurança. Dessa

forma, você torna menos provável que um aplicativo apresente mau funcionamento ou que uma ameaça relativamente nova se infiltre no seu sistema. Backups e planos completos de recuperação de desastres também ajudam uma empresa a recuperar a disponibilidade logo após um evento negativo.

Capítulo 8

Autenticação e Criptografia Básica

8.1 Definição e Importância

Criptografia é o processo de converter dados legíveis em um formato codificado para proteger informações de acessos não autorizados. É essencial na segurança de dados, sendo usada tanto por indivíduos quanto por grandes corporações.

8.2 Funcionamento

Dados são transformados em "texto cifrado"usando uma chave criptográfica, que pode ser descriptografada apenas por quem possui a chave correta. Quanto mais complexa a chave, mais segura a criptografia.

8.3 Técnicas Comuns

- Criptografia Simétrica: Usa a mesma chave para criptografar e descriptografar.
- Criptografia Assimétrica: Usa um par de chaves (uma pública e uma privada), oferecendo maior segurança.

8.4 Tipos de Criptografia

- Em Trânsito: Protege dados enquanto são transferidos entre dispositivos.
- Em Repouso: Protege dados armazenados em dispositivos de armazenamento, como discos rígidos.

- Criptografia de Ponta a Ponta: Garante que somente os usuários autorizados possam acessar os dados, protegendo mensagens e informações mesmo contra o provedor do serviço.

8.5 Benefícios

Protege a integridade e a privacidade dos dados.Ajuda organizações a cumprir regulamentações de segurança.Protege dados durante transferências e no armazenamento em nuvem.Contribui para a proteção de escritórios e propriedades intelectuais.Usos Comuns: Aparece em transações bancárias, e-mails, mensageiros (como WhatsApp), VPNs, e em segurança de dispositivos e sites (SSL).

Capítulo 9

A importância de Senhas Fortes e Autenticação Multifator

9.1 Definição e Importância

A MFA é uma camada extra de segurança nas contas online, exigindo mais de uma forma de autenticação além do nome de usuário e senha. Ela pode bloquear mais de 99,9% dos ataques, segundo a Microsoft.

9.2 Funcionamento

A MFA exige que o usuário forneça informações adicionais para acessar uma conta, como um código enviado por SMS ou e-mail, autenticação biométrica, ou uma chave de segurança física. A autenticação de dois fatores (2FA) é uma forma de MFA que requer um único fator adicional.

9.3 Benefícios

Camadas Extras de Segurança: Aumenta a proteção, dificultando o acesso de hackers que tenham apenas o nome de usuário e a senha.

Proteção em Caso de Violação de Dados: Mesmo que um cibercriminoso tenha as credenciais de login, a MFA impede o acesso sem a segunda autenticação.

Notificação de Tentativas Suspeitas: Alertas de tentativas de login suspeitas permitem que o usuário troque a senha rapidamente.

9.4 Opções de MFA

- Tokens por SMS ou E-mail: Códigos enviados após o login correto.
- Códigos TOTP: Códigos temporários gerados por aplicativos autenticadores.
- Chave de Segurança Física: Dispositivos físicos para autenticação.
- Autenticação Biométrica: Verificação via reconhecimento facial, digital ou íris.

Parte IV

A Realidade da Segurança Cibernética

Capítulo 10

Mito da Proteção Completa

Existe uma falsa percepção de que, ao investir em segurança, é possível ficar completamente protegido contra qualquer ameaça. No entanto, ninguém está 100% seguro em nenhum ambiente digital, nem mesmo grandes organizações, como a NASA ou gigantes como Microsoft, que enfrentam ataques constantes, mesmo investindo bilhões de dólares em se-

gurança.

Capítulo 11

Preparação e Reação a Incidentes

A segurança cibernética trabalha não para garantir que nenhum incidente aconteça, mas para reduzir riscos e mitigar impactos. O foco está em estar preparado e em saber reagir rapidamente quando problemas surgirem.

Parte V

Áreas da Segurança Cibernética

Segurança Cibernética pode ser analisada sob diferentes perspectivas, cada uma com seu foco e desafios.

Figura 11.1: *Diferentes áreas de segurança na área de tecnologia da informação*

Capítulo 12

Segurança de Aplicações (Application Security)

A segurança cibernética trabalha não para garantir que nenhum incidente aconteça, mas para reduzir riscos e mitigar impactos. O foco está em estar preparado e em saber reagir rapidamente quando problemas surgirem.

Capítulo 13

Segurança da Internet (Internet Security)

Medidas para proteger usuários e dados na internet contra ameaças online, como malwares e ataques de phishing. Envolve a proteção de redes e sistemas conectados, visando prevenir ataques que exploram falhas em serviços online, como websites e infraestrutura na nuvem.

Capítulo 14

Segurança de Computadores (Computer Security)

Focada na proteção de sistemas de computador e seus dados contra acessos não autorizados e danos.

Capítulo 15

Segurança da Informação (Information Security)

A segurança cibernética trabalha não para garantir que nenhum incidente aconteça, mas para reduzir riscos e mitigar impactos. O foco está em estar preparado e em saber reagir rapidamente quando problemas surgirem.

Capítulo 16

Segurança de Dados (Data Security)

Garante a proteção de dados armazenados e em trânsito, impedindo acesso não autorizado e perda de dados. Abrange políticas e práticas para proteger informações confidenciais e evitar vazamento de dados, além de garantir a conformidade com leis e regulamentos, como a LGPD no Brasil e o GDPR na Europa.

Capítulo 17

Segurança de Redes (Network Security)

Protege redes de computadores contra acessos não autorizados, ataques e vazamentos de dados. Essas áreas trabalham juntas para fornecer uma abordagem abrangente à segurança cibernética, cada uma focada em um aspecto específico da proteção de sistemas e dados.

Capítulo 18

Segurança em Inteligência Artificial (IA)

É uma área emergente e cada vez mais explorada é a segurança no contexto de Inteligência Artificial. Com o avanço rápido dessa tecnologia, surgem novos desafios, como:

- Exploração de modelos de IA: pessoas malicio-

sas podem tentar manipular ou explorar algoritmos de IA para obter vantagem, como ataques adversariais.

- Segurança de dados em IA: O uso de grandes volumes de dados para treinar modelos exige um cuidado especial com privacidade e conformidade com a legislação.

Essa é uma área que está crescendo e se tornando foco de estudo em várias disciplinas de tecnologia e cibersegurança.

Parte VI

Abordagem Integrada para a Segurança Cibernética

Quando pensamos em Segurança Cibernética, não basta focar em apenas uma área específica. É essencial adotar uma abordagem integrada e abrangente, pois diferentes tipos de segurança estão interligados.

Capítulo 19

Segurança de Rede

A configuração adequada de firewalls e sistemas de prevenção de intrusão é essencial para proteger a infraestrutura

Capítulo 20

Políticas de Usuários e Provisionamento

Garantir que cada colaborador tenha apenas os acessos estritamente necessários reduz o risco de vazamento de informações.

Capítulo 21

Segregação e Minimização de Dados

Limitar o acesso e manter apenas as informações essenciais armazenadas são práticas fundamentais para proteger dados sensíveis.

Parte VII

Gestão de Riscos em Segurança Cibernética

Capítulo 22

Importância da Avaliação de Impacto e Definição de Níveis de Proteção

Assim como em outros setores, Segurança Digital também lida com gestão de riscos. Empresas, independentemente do tamanho, precisam avaliar o

impacto de ataques e definir o nível de proteção necessário. Por exemplo:

Qual o impacto de uma empresa perder dados sigilosos?

Quais as consequências se um celular pessoal for hackeado?

Nenhuma organização, grande ou pequena, está isenta de sofrer ataques.

Empresas menores também podem ser responsabilizadas legalmente por vazamentos de dados, e é essencial que todas adotem boas práticas de segurança.

Capítulo 23

Segurança no Contexto Pessoal e Corporativo

No contexto Pessoal, a Segurança Cibernética protege a privacidade e os dados sensíveis, como informações bancárias e fotos.

Segurança Cibernética, já em ambientes Corporativos, ela é essencial para proteger sistemas críticos e garantir a continuidade dos negócios, evitando prejuízos financeiros e danos à reputação.

Capítulo 24

Exemplos de Incidentes em Grandes Empresas

Mesmo com investimentos significativos, algumas grandes empresas já foram vítimas de ataques que causaram sérios prejuízos:

24.1 Renner

Sofreu um ataque de ransomware e ficou inoperante por dias, impactando suas operações.

24.2 TOTVS

A maior desenvolvedora de software de gestão do Brasil também foi vítima de um ataque, afetando diversos clientes, como universidades e indústrias.

24.3 Companhias Aéreas

Uma falha de atualização global de software impactou a operação de várias companhias, gerando atrasos e prejuízos milionários.

Esses casos mostram que mesmo grandes empresas, com sofisticadas estratégias de segurança, não estão imunes a incidentes.

Parte VIII

Tipos Comuns de Ameaças Cibernéticas

As ameaças cibernéticas descrevem um conjunto de riscos que o ambiente digital oferece para usuários e organizações. Elas se referem a situações, mecanismos e ações maliciosas realizadas por hackers em busca de explorar vulnerabilidades de rede, sistemas e dispositivos. O objetivo é comprometer a segurança da informação, obter acesso não autorizado, interromper serviços, causar danos, normalmente, em busca de ganhos financeiros ilegais.

Para isso, os hackers buscam explorar as fraquezas nos sistemas das organizações e/ou a falta de conscientização dos usuários. Por isso, é importante contar com medidas preventivas para proteger sistemas e dados contra esses ataques. Entre as ameaças mais comuns em Segurança Cibernética, destacam-se:

Figura 24.1: *Principais ameaças cibernéticas*

Capítulo 25

Engenharia Social

Técnica de manipulação psicológica para enganar pessoas e obter informações confidenciais ou acesso a sistemas.

Exemplo: Um golpista se passa por suporte técnico e convence o usuário a fornecer sua senha.

Capítulo 26

Ransomware

Um tipo de malware que sequestra dados e exige um resgate (normalmente em criptomoedas) para liberá-los.

Exemplo: Empresas têm seus sistemas bloqueados e recebem exigências de pagamento para restaurar o acesso.

Capítulo 27

Malware

Software malicioso desenvolvido para causar danos ou acessar sistemas sem autorização. Pode incluir vírus, worms e spyware.

Exemplo: Vírus que apaga arquivos ou spyware que monitora atividades de um usuário sem o seu conhecimento.

Capítulo 28

Phishing

Tentativa fraudulenta de obter informações sensíveis, como senhas e dados bancários, por meio de e-mails, sites ou mensagens falsas.

Exemplo: E-mails que se passam por bancos pedindo para o usuário atualizar suas informações de conta.

Capítulo 29

Força Bruta

Um ataque de força bruta usa o método de tentativa e erro para adivinhar informações de login, chaves de criptografia ou encontrar uma página da Web oculta. Invasores trabalham com todas as combinações possíveis na esperança de acertar.

Usando combinações automáticas, esses ataques são feitos por "força bruta"; eles usam tentativas excessivamente fortes para tentar "forçar"a entrada em suas contas privadas.

Esse é um método de ataque antigo, mas ainda é

popular e eficiente entre os hackers.

De acordo com o comprimento e complexidade da senha, isso pode levar de alguns segundos até muitos anos.

Na verdade, a que alguns hackers visam os mesmos sistemas todos os dias por meses e até anos.

Esses ataques são usados para descobrir senhas que combinam palavras comuns com caracteres aleatórios.

Exemplo: Ataque desse tipo incluiria senhas como SãoPaulo1993 ou Thor1234.

Capítulo 30

Ataques Man-in-the-Middle (MitM)

Ataque em que um invasor intercepta e manipula a comunicação entre duas partes, sem que elas saibam.

Exemplo: Um atacante intercepta dados enviados entre um cliente e um servidor, como credenciais de login.

Capítulo 31

Aplicativos Maliciosos

Programas ou aplicativos aparentemente legítimos, mas que contêm código malicioso.

Exemplo: Aplicativos falsos em lojas online que roubam dados de usuários ou instalam spyware.

Capítulo 32

Ataques de Negação de Serviço (DoS)

Ataque que sobrecarrega um servidor ou serviço com um grande volume de tráfego, tornando-o indisponível.

Exemplo: Um site de e-commerce recebe milhões de solicitações simultâneas e sai do ar, perdendo vendas.

Capítulo 33

Exploração de Dia Zero (Zero Day)

Ataque que se aproveita de uma vulnerabilidade desconhecida em um software, antes que o desenvolvedor possa lançar uma correção.

Exemplo: Uma falha no sistema operacional é explorada antes de a atualização de segurança ser liberada.

Parte IX

A Importância das Atualizações de Segurança

Capítulo 34

Necessidade de Manter Sistemas Atualizados

Manter sistemas atualizados é essencial para evitar brechas de segurança. Muitas falhas exploradas por pessoas maliciosas ocorrem porque as empresas ou pessoas não aplicam atualizações de segurança a tempo.

Capítulo 35

Riscos de Atrasar Atualizações de Segurança

Mesmo que algumas atualizações automáticas possam ser incômodas, protelar essas atualizações aumenta a exposição a riscos. Empresas precisam adotar uma postura proativa e garantir que sistemas críticos estejam sempre protegidos e isso serve também para

usuários comuns como em seu computador pessoal.

Parte X

Ciclo de Segurança Cibernética

A segurança cibernética também envolve a gestão eficaz de incidentes. O ciclo de resposta a incidentes pode ser dividido em cinco etapas, baseadas nas práticas do NIST (National Institute of Standards and Technology):

Figura 35.1: *Ciclo de Segurança Cibernética*

Capítulo 36

Identificar (Identify)

Detectar a ocorrência de um incidente e avaliar seu impacto. Envolve a identificação de ativos, riscos e vulnerabilidades na infraestrutura de TI, compreendendo o que precisa ser protegido.

Capítulo 37

Proteger (Protect)

Implementar medidas para limitar o dano. Implementa medidas de segurança para proteger os ativos identificados, como controles de acesso e treinamentos de conscientização.

Capítulo 38

Detectar (Detect)

Monitorar continuamente os sistemas para identificar ameaças em tempo real. Monitoramento contínuo para identificar ameaças e atividades suspeitas, permitindo respostas rápidas a incidentes.

Capítulo 39

Responder (Respond)

Agir rapidamente para conter o incidente e minimizar o impacto. Procedimentos para responder a incidentes de segurança, minimizando danos e controlando a situação.

Capítulo 40

Recuperar (Recover)

Restaurar os sistemas e implementar melhorias para evitar incidentes futuros. Foca na recuperação das operações normais após um incidente, restaurando serviços e corrigindo vulnerabilidades para evitar futuros problemas.

Parte XI

Conclusões e Recomendações

Capítulo 41

Importância de Práticas Seguras para Indivíduos e Empresas

Essas etapas formam um ciclo contínuo, permitindo que as organizações aprimorem sua postura de segurança cibernética ao longo do tempo.

A falta de processos claros para responder a incidentes pode resultar em demora na reação e grandes

prejuízos financeiros.

A segurança cibernética é uma área cada vez mais crítica para empresas e indivíduos. Em um mundo conectado, o custo de não investir em segurança pode ser catastrófico.

Além disso, é importante lembrar que:

- Indivíduos devem manter senhas fortes, atualizadas e ativar a MFA sempre que possível, gerenciadores de senha podem ajudar a organizar senhas fortes e armazenar códigos de 2FA com segurança, facilitando o preenchimento automático em sites e aplicativos e ainda a autenticação multifator é uma medida essencial para proteger contas online, combinando segurança com praticidade ao bloquear a maioria das tentativas de invasão;

- Criptografia para a segurança digital, protegendo dados pessoais e informações sensíveis contra-ataques cibernéticos e garantindo a integridade e autenticidade de dados;

- Evitar baixar aplicativos suspeitos; e
- Ficar atentos a e-mails fraudulentos.

As Empresas precisam implementar políticas claras, realizar auditorias regulares e investir na capacitação de seus funcionários.

Segurança digital não é apenas uma questão técnica, mas também envolve comportamento e conscientização.

Capítulo 42

Necessidade de Investimentos Contínuos em Segurança

O investimento certo em segurança cibernética pode reduzir significativamente os riscos, garantindo a continuidade dos negócios e a proteção das informações

pessoais e corporativas.

Bibliografia

[1] Trend Micro. (2023). Relatório de Segurança Cibernética. Disponível em: https://www.trendmicro.com.

[2] IBM Security. (2022). Custo de uma Violação de Dados. Disponível em: https://www.ibm.com.

[3] Fortune Business Insights. (2023). Cybersecurity Market Analysis. Disponível em: https://www.fortunebusinessinsights.com.

[4] McKinsey & Company. (2023). Cybersecurity Insights 2023. Disponível em: https://www.mckinsey.com.

[5] Cardoso, Guilherme (Gui). *Palestra de Cibersegurança: Conceitos e práticas para ambientes domésticos e corporativos. Data: 18/10/2024. Local: Uniara.* CEO @ Vulneri Segurança Digital e Professor @ UNIFEB.

[6] https://www.contacta.com.br/blog/ameacas-cibernetica s-principais-tipos-e-como-se-prevenir

[7] https://www.kaspersky.com.br/resource-center/definitions/what-is-cyber-security

[8] https://deak.com.br/blog/ataque-cibernetico-o-que-e-e-como-proteger-os-dados-da-sua-empresa/

[9] https://4future.com.br/index.php/2021/08/16/triade-cia-os-3-pilares-da-seguranca-da-informacao/

[10] https://www.fortinet.com/br/resources/cyberglossary/cia-triad

[11] https://www.kaspersky.com.br/resource-center/definitions/encryption

[12] https://www.kaspersky.com.br/resource-center/definitions/brute-force-attack

[13] https://www.keepersecurity.com/blog/pt-br/2022/10/27/how-multi-factor-authentication-protects-against-cybersecurity-threats/