TIC em trilhas

Módulo 1 – Fundamentos de Segurança Cibernética

Segurança Cibernética:
Do Ataque à Defesa

TIC em trilhas

Sumário

TIC em trilhas

Aula 1:

Conhecendo a Área de Segurança Cibernética

1.1 Casos Famosos em Segurança Cibernética

Você provavelmente já deve ter ouvido falar de algum caso famoso em Segurança Cibernética, não é mesmo? Em um mundo cada vez mais interconectado, a Segurança Cibernética tornou-se um pilar fundamental para a proteção de informações pessoais, corporativas e governamentais. Ao longo dos anos, diversos incidentes famosos nos mostraram a importância deste tema e evidenciaram as fragilidades dos sistemas e dispositivos no mundo digital. Vamos conhecer alguns destes casos?

- **Stuxnet (AVAST, 2024)**

O ***Stuxnet***, descoberto em 2010, foi um *malware* (software malicioso) revolucionário projetado para sabotar os sistemas de controles industriais do programa nuclear iraniano. O *malware* alterou o funcionamento das centrífugas, causando danos físicos e a interrupção da operação das centrífugas. A invasão provavelmente iniciou-se a partir de um dispositivo infectado conectado à rede. Foi a primeira vez que um ataque cibernético teve consequências materiais significativas (estima-se que 1000 centrífugas foram danificadas), redefinindo as ameaças cibernéticas e a segurança global. Você viu como a proteção de sistemas críticos pode ser um fator preponderante para a defesa de um país?

- **Carolina Dieckmann (ARAUJO, 2023)**

Este incidente é um marco na legislação de Segurança Cibernética no Brasil. Em 2012, após a atriz Carolina Dieckmann ter seu computador invadido por hackers e ter fotos íntimas roubadas (inclusive sofrendo tentativas de extorsão para não ter suas fotos publicadas na internet), foi criada a Lei 12.737/2012, conhecida como ***Lei Carolina Dieckmann***. Esta foi a primeira lei no Brasil que tipifica crimes cibernéticos e pune a invasão de dispositivos digitais. Este episódio demonstra a importância da proteção dos nossos aparelhos e dados pessoais, pois estes podem causar tanto danos financeiros, quanto danos relacionados a nossa reputação e imagem.

- **WannaCry (KASPERSKY, 2024)**

O ataque *WannaCry* foi um grande incidente de Segurança Cibernética que ocorreu em 2017. Esse ataque afetou mais de 200 mil computadores em mais de 150 países. O *WannaCry* é um tipo de *ransomware*, um software malicioso que criptografa arquivos e dados, bloqueando o acesso dos usuários até que um resgate seja pago. Esse software malicioso explorou uma vulnerabilidade (chamada "*EternalBlue*") em sistemas operacionais Windows não atualizados. A propósito, sistemas atualizados e *backups* confiáveis poderiam ter

amenizado os danos deste e outros incidentes. Você verá mais detalhes sobre este tipo de software malicioso mais adiante na trilha.

- **Guerra entre Rússia e Ucrânia (SUZUKI, 2022)**

A guerra entre Rússia e Ucrânia iniciada em 2022, transcendeu o confronto físico, estendendo-se ao ciberespaço. Antes mesmo dos conflitos armados, a Ucrânia sofreu ataques cibernéticos significativos, visando desestabilizar infraestruturas críticas do país, como estações de energia. Essa guerra cibernética contínua, parte de uma estratégia de guerra híbrida, demonstra como o ciberespaço é um campo de batalha crucial na era moderna. Você consegue perceber como a Segurança Cibernética tem se tornado algo cada vez mais estratégico na garantia da soberania de uma nação?

- **Deepfake em Hong Kong (CHEN; MAGRAMO, 2024)**

Em um caso sem precedentes, em Hong Kong (2024), criminosos utilizaram a tecnologia *deepfake* para enganar um funcionário de uma multinacional, resultando na transferência de aproximadamente US$ 25 milhões. A fraude foi realizada por meio de uma videoconferência falsificada, onde a imagem e voz do diretor financeiro da empresa foram replicadas com precisão pelos criminosos, induzindo um dos funcionários da empresa a realizar a transferência fraudulenta. Este caso ocorrido em Hong Kong é um exemplo de golpe de Engenharia Social.

Você sabe quais mecanismos ou boas práticas poderiam ter sido utilizados para evitar esse problema? Nesta trilha, vamos apresentar como se proteger deste e de outros ataques.

1.2 Mercado de Trabalho

Os casos famosos na área de Segurança Cibernética podem ter lhe chamado atenção, então algumas das perguntas que você pode ter feito é: quais os valores envolvidos neste mercado e quais as carreiras que se pode seguir nesta área?

1.2.1 Mercado

O mercado de Segurança Cibernética está crescendo rapidamente. Em 2024, o tamanho do mercado mundial é estimado em US$ 203,78 bilhões e espera-se que atinja US$ 350,23 bilhões até 2029 um valor bastante significativo (MORDOR INTELLIGENCE, 2024). Em relação ao gasto das empresas com violações, em 2023, o custo médio global foi de US$ 4,45 milhões, um aumento de 15% ao longo de 3 anos. Em outras palavras, este é o valor que cada organização gasta em média para lidar com as implicações de um incidente cibernético (IBM, 2024). Já no Brasil, o custo médio de uma violação de dados aumentou quase 10% em 2022, chegando a R$ 6,45 milhões (IBM, 2022).

1.2.2 Carreiras

Vimos que o mercado apresenta volumes financeiros consideráveis, então quais são as possíveis carreiras que você poderá almejar neste mercado?

A seguir, algumas das principais carreiras na área de Segurança Cibernética:

- **Especialistas em segurança de software**

Combinam habilidades em desenvolvimento e arquitetura de software com conhecimentos nos requisitos e boas práticas de segurança, empregando práticas como *security-by-design* (segurança desde a concepção) e desenvolvimento seguro.

- **Hackers éticos**

São profissionais especializados em encontrar brechas de segurança em sistemas, atuando no papel de um adversário. Eles identificam, reportam e recomendam correções para as vulnerabilidades encontradas. Também são conhecidos como *pentesters* ou red teamers.

- **Pesquisadores em Segurança Cibernética**

Conduzem projetos de pesquisa na área da segurança avaliando as técnicas atuais e propondo novos mecanismos, algoritmos e técnicas para a proteção dos usuários. Este trabalho pode resultar na produção de artigos científicos, patentes e atividades de capacitação.

- **Analistas de segurança de redes e infraestrutura de TI**

Monitoram sistemas para identificar e responder prontamente a ameaças, protegendo bases de dados, redes e dispositivos contra-ataques cibernéticos.

- **Engenheiros, arquitetos e consultores de Segurança Cibernética**

São profissionais experientes em projetar, implementar e gerenciar sistemas de segurança. Eles dominam habilidades técnicas em desenvolvimento de software, segurança de rede, criptografia e outras áreas. Lideram equipes e estabelecem processos em uma empresa.

- **Gerentes de Segurança Cibernética**

Lideram e gerenciam equipes e programas de Segurança Cibernética, através da tomada de decisões e estabelecimento de processos em uma empresa. O principal executivo da área de Segurança Cibernética é chamado de CISO *(Chief* Information Security Officer).

- **Especialista em proteção de dados**

Garante a conformidade com leis e normas de proteção de dados, implementando, monitorando e auditando a conformidade de uma empresa, produto ou solução.

- **Perito em análise forense digital**

Investiga crimes cibernéticos, coletando evidências digitais para auxiliar na resolução de casos, contribuindo na elaboração de relatórios e teses para processos judiciais.

1.3 Tríade CID

Agora que você já tem um panorama da área de Segurança Cibernética, um dos principais conceitos que todo profissional da área deve conhecer é a **Tríade CID** (ou *CIA Triad*, em inglês). Este conceito apresenta os três princípios fundamentais da segurança: **C**onfidencialidade**, I**ntegridade e **D**isponibilidade (FORTINET, 2024).

Esses princípios são a base tanto para o desenvolvimento de sistemas de segurança como para a proteção das informações de usuários e organizações. Por essa razão, é importante entendermos do que se tratam e como são aplicados. Vamos a eles!

1. Confidencialidade (ou Sigilo)

Permite que uma informação seja acessível apenas por pessoas autorizadas, mantendo seu segredo e prevenindo o compartilhamento não autorizado. Por exemplo, quando uma instituição bancária utiliza criptografia e autenticação para proteger as informações financeiras de seus clientes, ela permite que apenas usuários autorizados tenham acesso aos dados confidenciais, como dados da conta e transações.

2. Integridade

Assegura que uma informação não seja alterada de forma não autorizada. Por exemplo, imagine que você está enviando um contrato importante por e-mail. Para detectar se o contrato foi alterado durante o trânsito, você pode utilizar a técnica de assinatura digital (explicada mais a frente nesta trilha) e que pode ser validada pelo destinatário, assim assegurando que a informação recebida não tenha sido modificada no percurso.

3. Disponibilidade

Estabelece que uma informação ou serviço esteja disponível e acessível para usuários quando necessário. Por exemplo, um caso clássico de disponibilidade é a Redundância de Servidores. Esse método é utilizado em caso de falha de algum servidor. Caso o servidor principal falhe, um servidor secundário deverá substituí-lo automaticamente, possibilitando que os serviços e dados continuem acessíveis sem interrupção.

Agora você já conhece os três princípios fundamentais de segurança que ajudam usuários e empresas a protegerem suas informações contra ameaças e vulnerabilidades do mundo cibernético.

1.4 Hackers e as Equipes de Segurança Cibernética

Você provavelmente já deve ter se deparado com alguma história sobre *hackers* em algum portal de notícias, filme ou até mesmo em algum caso que aconteceu no seu trabalho. Mas, você sabe o que é um *hacker*? Sabe por exemplo que existem diferentes tipos de *hackers* e com motivações diversas?

1.4.1 A Evolução do Termo Hacker

A origem do termo *hacker* surgiu nos anos de 1960, no MIT *(Massachusetts Institute of Technology)*, onde era usado para descrever estudantes com habilidades excepcionais em programação e solução de problemas em sistemas de computadores (BRASIL ESCOLA, 2024). Com o tempo, o termo evoluiu para representar indivíduos que exploram sistemas de computadores, seja por curiosidade, benefício próprio ou para destacar vulnerabilidades. Um *hacker* também pode ser chamado de **atacante**, **adversário**, **intruso**, entre outros termos, e durante esta trilha estes termos serão usados em diversos momentos. Também são conhecidos como *crackers* os *hackers* que exploram vulnerabilidades em benefício próprio.

1.4.2 Classificação dos Hackers

Os *hackers* podem ser classificados com relação a sua intenção ao realizar uma invasão e atuação. Alguns *hackers* procuram invadir sistemas para causar danos, ganhar reputação ou obter algum retorno financeiro, enquanto outros buscam oferecer seus conhecimentos para avaliar a segurança de um alvo. Adicionalmente, *hackers* podem (ou não) estar agindo de forma legal e com consentimento do alvo. Baseado nestas premissas, podemos definir alguns tipos de *hacker* (AVG, 2024):

- ***White Hat* (Chapéu Branco):** São os *hackers* éticos, trabalham para proteger sistemas e redes. Eles realizam testes e avaliações de segurança para possibilitar que as vulnerabilidades sejam descobertas e corrigidas antes que possam ser exploradas maliciosamente. Estes profissionais, antes de realizar qualquer teste, obtém a permissão explicita do alvo, incluindo até a combinação do que pode ou não ser realizado.

- ***Black Hat* (Chapéu Preto):** Estes são os mal-intencionados, que violam a segurança dos sistemas para roubo de dados, danos ou ganho financeiro. Dentro deste grupo, encontram-se os *crackers* e os praticantes de *hacktivismo*, que invadem sistemas por razões políticas ou sociais, muitas vezes para passar uma mensagem ou protesto.

- ***Gray Hat* (Chapéu Cinza):** Operam numa zona cinzenta, muitas vezes cruzando a linha entre o legal e o ilegal para descobrir falhas de segurança, geralmente sem a intenção maliciosa, reportando as descobertas para organizações afetadas (muitas vezes sem a

1.4.3 Equipes de Segurança Cibernética

Após explorar a evolução do termo hacker e entender as diversas classificações desses indivíduos habilidosos, é importante reconhecer que o conhecimento deles é como uma moeda e seus dois lados. Enquanto alguns optam por caminhos que ameaçam a segurança digital, outros escolhem defender o ciberespaço. É neste contexto que surgem as **Equipes de Segurança Cibernética**, grupos dedicados a proteger informações, sistemas e infraestruturas críticas.

As Equipes de Segurança Cibernética são a força oposta aos *hackers* mal-intencionados e compartilham uma compreensão profunda das mesmas técnicas e vulnerabilidades exploradas por eles. Em uma mesma organização é comum existirem equipes de segurança trabalhando em atividades diferentes, muitas vezes um testando a capacidade do outro. Essas equipes trabalham em conjunto para fortalecer a segurança através de simulações de ataque e defesa. Os dois tipos de times mais comuns são:

- ***Red Team* (Time Vermelho):** Esta é a equipe ofensiva, que simula ataques cibernéticos para testar a eficácia das medidas de segurança adotadas em uma organização. Os membros desta equipe usam as mesmas técnicas que um *hacker* mal-intencionado usaria, com o objetivo de encontrar e explorar pontos fracos, porém de maneira ética.
- ***Blue Team* (Time Azul):** Em contrapartida, essa equipe é a defensiva, focada em defender um sistema contra-ataques cibernéticos. Estes monitoram as redes, implementam defesas robustas e respondem a incidentes para proteger a organização contra as ameaças identificadas e exploradas pelo *Red Team.*

TIC em trilhas

Aula 2:

Criptografia

2.1 O que é Criptografia?

Você já ouvir falar sobre criptografia? Você sabe quando e porque a criptografia foi criada?

A criptografia é uma prática que vem da época da antiguidade, sendo crucial para a segurança da informação e para comunicações secretas. Uma das técnicas mais antigas e emblemáticas é a **Cifra de César**, que leva o nome do antigo imperador romano Júlio César, que a utilizava para proteger mensagens militares.

Esta cifra é um tipo de criptografia de **substituição** onde cada letra do texto original (referido como **texto em claro**) é substituída por outra que se encontra um número fixo de posições à frente no alfabeto. Após substituirmos todas as letras da mensagem original, obtemos o **texto cifrado**, que poderá ser compartilhado. Note que o deslocamento neste caso é considerado o **segredo (chave)** que possibilitará alguém reverter o processo. Por exemplo, com um deslocamento (chave) de três posições, ‘A’ seria substituído por ‘D’, ‘B’ por ‘E’, e assim sucessivamente (SIDHPURWALA, 2023), como ilustrado na Figura 1.

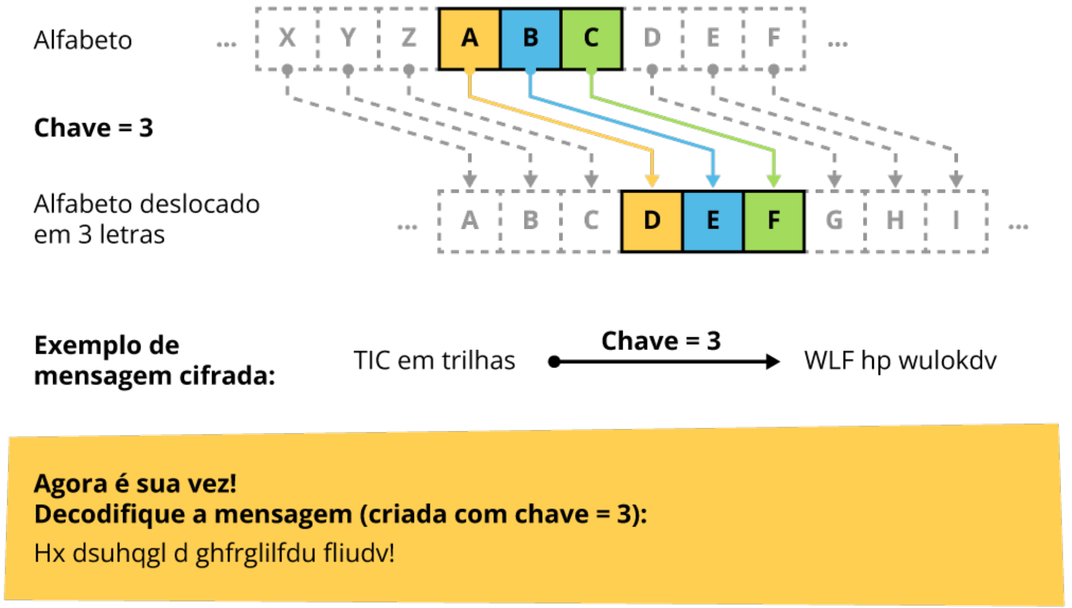

Figura 1: Exemplo de uma Cifra de César.

Fonte: feito pelo autor.

Embora seja facilmente decifrável com a utilização de técnicas estatísticas, a Cifra de César foi fundamental para o desenvolvimento da criptografia. Ela representa um dos primeiros usos documentados de criptografia para segurança de correspondências e teve um papel crucial na evolução das técnicas criptográficas. Atualmente, a Cifra de César é usada principalmente como ferramenta educacional para introduzir conceitos de criptografia e inspirou várias outras.

Agora, fica mais fácil de explicar em detalhes um dos principais, mas não único, uso da criptografia: **prover sigilo a uma informação**. Isso é possível através de algoritmos (funções muitas vezes contendo propriedades matemáticas) que utilizam de um segredo (conhecido como chave criptográfica), que é utilizado para cifrar (ou seja, embaralhar) o texto original de modo que ele se torne incompreensível. Apenas o destinatário, quem conhecerá o segredo, poderá utilizar um algoritmo com uma função de decifrar (ou seja, desembaralhar) o texto cifrado para recuperar a mensagem original.

A criptografia é, sem dúvida, umas das principais técnicas da área de Segurança Cibernética. Com ela, podemos prover os principais serviços de segurança que serão discutidos nesta trilha, como: **autenticação, sigilo, integridade** e **não-repúdio**.

Com o avanço da computação e da internet, desenvolveram-se algoritmos complexos que podem levar séculos para serem quebrados, mesmo com os computadores mais potentes. Esses avanços permitem a segurança de transações financeiras, comunicações confidenciais e dados pessoais.

Existem diferentes tipos de criptografia, como a simétrica e assimétrica, além das funções *hash* e outras tecnologias que empregam estas técnicas (ou seus conceitos) para fornecer outros serviços de segurança, como as assinaturas e certificados. A seguir, estes temas serão abordados em detalhes.

2.2 Criptografia Simétrica

Agora que entendemos os princípios da criptografia, vamos aprofundar em um dos principais tipos de criptografia, a **simétrica**. Talvez você nunca tenha ouvido falar, mas a utiliza diariamente.

A criptografia simétrica é um método eficiente de proteção de dados e atualmente é essencial para a segurança no mundo digital. Ela consiste no uso de uma **única chave criptográfica**, compartilhada de uma forma segura entre as partes que desejam se comunicar, e é utilizada para cifrar e decifrar informações.

Um exemplo prático da aplicação da criptografia simétrica pode ser observado quando estamos criando um arquivo ZIP comprimido e desejamos adicionar uma camada de proteção por senha, ou seja, apenas quem conhecer esta senha (segredo) poderá acessar o conteúdo do arquivo. Isso garante que, mesmo se o arquivo ZIP for capturado por alguém que não deveria, sem a chave correta (senha), os dados permanecem inacessíveis e seguros. Esse método é amplamente utilizado devido a sua simplicidade e eficácia na proteção de dados.

Veja a Figura 2 que exemplifica sua aplicação.

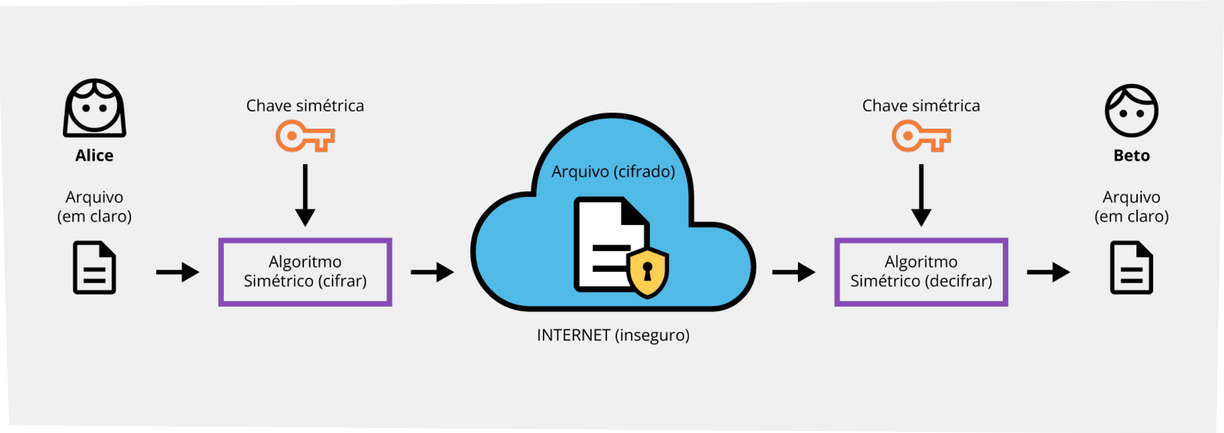

Figura 2: Utilização da Criptografia Simétrica para prover sigilo.
Fonte: feito pelo autor.

Entre os maiores desafios da Criptografia simétrica podemos citar o processo de troca de chaves (hoje realizado com o apoio de outro método, a **criptografia assimétrica)** e o gerenciamento das chaves criptográficas, que inclui o processo de geração, uso, armazenamento e destruição das chaves de forma segura e sem permitir o vazamento.

A **segurança da criptografia simétrica** depende do **tamanho da chave** secreta, com chaves menores sendo mais vulneráveis a ataques de força bruta. Já chaves maiores exigem mais recursos computacionais, o que pode ser um problema em ambientes com restrições, como em IoT. Além disso, a segurança também depende do **gerenciamento das chaves**, que devem ser mantidas em segredo para evitar comprometimento. Podemos pensar que as **chaves criptográficas simétricas** são como os **segredos de um cofre,** quanto maior é o segredo, mais difícil é para outros adivinharem.

É importante destacar que na criptografia simétrica, deve-se evitar a reutilização de chaves para dificultar ataques, que utilizem do acúmulo de material criptográfico que permita descobrir a chave secreta em algum momento, ou que, devido ao comprometimento de uma chave, os danos sejam minimizados quando se troca a chave. Desta forma, criar chaves aleatórias, armazená-las de forma segura e destruí-las após o uso para que nunca sejam recuperadas é um grande desafio.

Existem no mercado algumas soluções que facilitam o gerenciamento de chaves criptográficas:

- Serviços de terceiros, oferecidos por grandes empresas, como a *AWS*;
- Hardware específico, geralmente utilizado por empresas que exigem um alto nível de segurança, chamado de *HSM (Hardware Secure Module)*;
- Soluções em *software,* como o *Android KeyStore* ou *iOS Keychain*, utilizados por aplicações para lidar com a parte de segurança das chaves.

Apesar de suas limitações, a criptografia simétrica é rápida e adequada para lidar com grandes volumes de dados.

2.3 Criptografia Assimétrica

Após vermos quais as aplicações e o conceito da criptografia simétrica, o próximo passo é conhecermos a **criptografia assimétrica**. Assim como a criptografia simétrica, você a utiliza diariamente e pode ser que nem saiba. Você usa algum comunicador como *WhatsApp* ou um navegador de internet? Caso sim, então você está usando criptografia assimétrica.

Diferentemente da criptografia simétrica, que é basicamente baseada em substituições e mudanças realizadas no texto a ser cifrado com base na chave utilizada, a criptografia assimétrica é baseada em **funções matemáticas** para atingir suas propriedades que fornecem diferentes formas de segurança, dependendo de como é utilizada.

Outra diferença entre estes dois tipos de criptografias é na quantidade de chaves utilizada. Enquanto a simétrica utiliza a mesma chave para cifrar e decifrar uma mensagem, a assimétrica utiliza duas chaves diferentes, uma pública e outra privada, que trabalham juntas para se obter diferentes propriedades criptográficas.

A criptografia assimétrica oferece várias vantagens em seu uso, podendo ser utilizada para prover sigilo, autenticação e a realização de assinatura digital. Ela endereça um dos maiores problemas da criptografia simétrica: a **troca de chaves**.

A **chave pública**, como o próprio nome diz, é de **conhecimento de todos** e pode ser compartilhada abertamente, enquanto a **chave privada deve ser mantida em segredo**, só de conhecimento do usuário. Desta forma, sempre que utilizamos uma chave no processo de cifragem, devemos utilizar a sua correspondente no processo de decifragem. A ordem que utilizamos determina qual propriedade de segurança estamos interessados, como sigilo ou assinatura, conforme explicado a seguir.

Se você deseja sigilo, basta utilizar a chave pública do destinatário para cifrar um texto. Desta forma, somente o destinatário que detêm da posse da chave privada correspondente poderá decifrar a mensagem. Veja na figura 3 um exemplo de aplicação desta técnica.

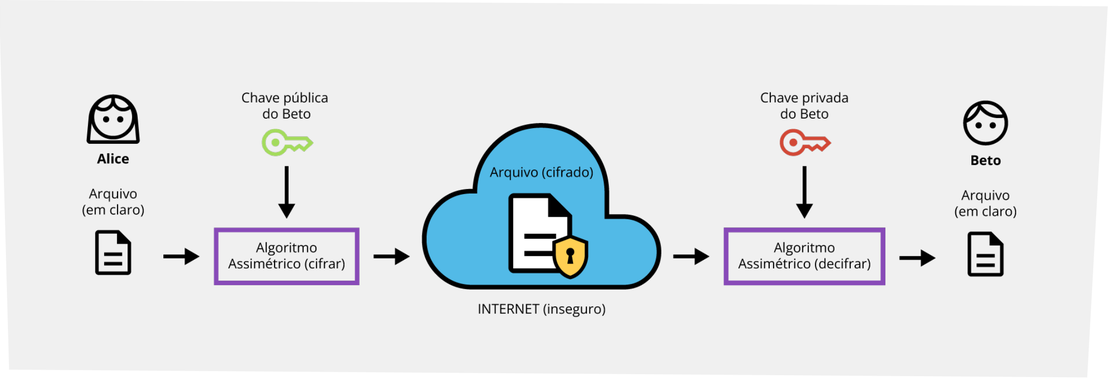

Figura 3: Provendo sigilo com o uso da criptografia Assimétrica.

Fonte: feito pelo autor.

Já no caso de uma assinatura digital, quem assinará a mensagem deverá utilizar sua chave privada para cifrar o texto (isso gerará a assinatura, que deve ser anexada ao documento). Como a chave privada deve permanecer em segredo e somente de posse do usuário, convenciona-se que foi ele quem assinou o documento digital. Qualquer pessoa poderá verificar a assinatura utilizando a chave pública deste usuário, decifrando a assinatura anexada ao documento e comparando com a versão original. Veja na figura 4 um exemplo resumido de aplicação desta técnica.

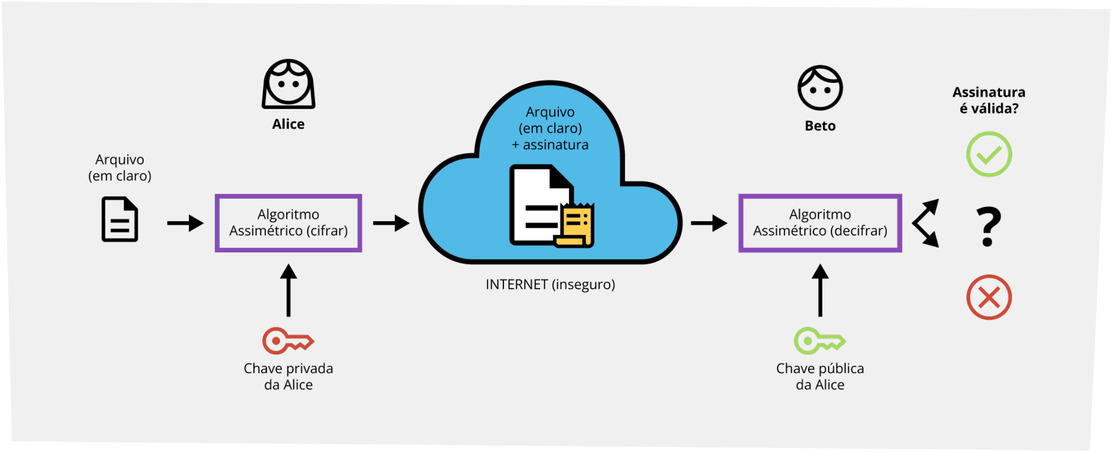

Figura 4: Assinatura digital através do uso da Criptografia Assimétrica.

Fonte: feito pelo autor.

Sigilo e assinatura são apenas dois casos da aplicação da criptografia assimétrica essencial para muitas aplicações modernas, como: o envio de e-mails seguros, a realização de transações financeiras online e a autenticação de usuários. Com o aumento constante das ameaças cibernéticas, a criptografia assimétrica continua a ser uma ferramenta crucial para proteger informações sensíveis e manter a privacidade online.

Contudo, uma de suas desvantagens é o **elevado custo computacional** para sua utilização, maiores que a criptografia simétrica. Por esta razão, em cenários práticos, ambas são utilizadas em conjunto, uma cifrando grandes quantidades de dados (simétrica) e a outra como forma de permitir a troca segura das chaves criptográficas (assimétrica).

Outra desvantagem é garantir que uma chave pública pertence de fato a um determinado usuário. Para mitigar este problema, foram criados os **certificados digitais**, mas estes ainda são limitados devido aos altos custos financeiros para se manter um processo sendo executado de forma confiável.

2.3.1 Certificado digital

O certificado digital é essencial para a assinatura digital, pois ele é emitido por uma Autoridade Certificadora (AC) confiável, responsável por atestar que uma determinada chave pública pertença a uma pessoa ou empresa. Ele contém informações como nome do titular, chave pública, número de série, datas de validade, assinatura digital da AC e o algoritmo de assinatura.

A AC verifica a identidade do solicitante antes de emitir um certificado, gerencia certificados revogados e oferece serviços de renovação e atualização, garantindo conformidade com normas e regulamentos. A Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) viabiliza a emissão de certificados digitais. O Instituto Nacional de Tecnologia da Informação (ITI) atua como Autoridade Certificadora Raiz, credenciando e supervisionando os demais participantes da cadeia de confiança. Exemplos de ACs no Brasil incluem *SERPRO*, *Serasa Experian* e *Certisign.*

Existem dois tipos principais de certificados: tipo A (para assinatura) e tipo S (para sigilo).

2.3.2 Certificado TLS

Quando você acessa um site e vê um cadeado ao lado do endereço URL, isso indica que o site está protegido por um **certificado SSL/TLS**. Esses certificados são utilizados para estabelecer uma conexão segura (criptografada) entre o servidor de um site e o navegador do usuário, possibilitando que todos os dados transmitidos sejam seguros e privados.

Certificados SSL/TLS desempenham um papel crucial na prevenção de ataques do tipo *Man-In-The-Middle (MITM)*, onde um invasor intercepta a comunicação entre um usuário e um site. Durante um ataque MITM, o invasor pode tentar se passar pelo site ou pelo usuário para alterar ou roubar dados confidenciais transmitidos durante a comunicação. No entanto, com um certificado SSL/TLS válido, é possível estabelecer uma comunicação entre o navegador do usuário e o servidor seguro (criptografada e autenticada). Isso significa que mesmo que os dados sejam interceptados, eles permanecerão incompreensíveis para o invasor devido ao uso da criptografia. Além disso, a verificação da autenticidade do certificado confirma a identidade do servidor, impedindo conexão fraudulenta.

Como você já pode estar concluindo, a combinação destes mecanismos aqui descritos nesta seção, possibilitam a confiança e a segurança nas comunicações digitais, permitindo que as mensagens sejam autênticas e que as identidades dos participantes sejam verificáveis.

2.4 Função Hash

Você sabe o que é exatamente uma função *hash*?

É uma técnica criptográfica que permite transformar uma entrada de qualquer tamanho, seja um texto simples ou até mesmo um grande arquivo, como uma enciclopédia completa, em uma sequência única de caracteres de **tamanho fixo**, conhecida como valor *hash* (DONOHUE, 2014). Por exemplo, se aplicarmos a função *hash* SHA-256 a uma simples frase:
“Olá, mundo!”

O resultado seria um valor *hash* como este:
ff99b66abad87baefe7203fd886a2ed85ac5a1250fa3f6945b645241d5b4cfca

Esse processo é **unidirecional** e projetado para ser **computacionalmente inviável de reverter**, o que significa que, a partir do valor *hash*, não é possível recuperar a frase original **“Olá, mundo!”**.

Outra característica destas funções é o **efeito avalanche**, na qual se você mudar um caractere na entrada, a saída irá mudar completamente. Considerando o exemplo acima, se mudarmos a frase inicial para:
“Ola, mundo!”

Note que trocamos o caractere “á” por “a”, removendo o acento apenas, o novo valor *hash* será completamente diferente:
c10c191fd7285e36ab961700b7fb8dbf727e4a76d08a46ba2fc1ffb00a8ad1d5

Você pode encarar uma função *hash* como um método capaz de criar uma espécie de ***“impressão digital”*** de uma entrada qualquer, seja uma mensagem ou arquivo, sendo o resultado único e compacto, permitindo o seu armazenamento e comparação com outros *hashes* de forma muito eficiente.

No cotidiano, as funções *hash* são aplicadas de várias maneiras para possibilitar a **integridade dos dados**, inclusive em assinaturas digitais. Ao baixar um arquivo da internet, por exemplo, um software pode usar um valor de *hash* para verificar se o arquivo foi corrompido ou alterado durante o download. Em sistemas de gerenciamento de senhas, os valores *hash* das senhas dos usuários são armazenados em vez das próprias senhas. Isso aumenta a segurança em caso de violação de dados, pois mesmo que os valores *hash* sejam acessados, eles não revelam as senhas originais.

2.5 Além da Criptografia: Esteganografia

Você já conhecia o termo esteganografia?

Imagine que a criptografia é como um cofre que guarda joias valiosas, e a esteganografia é o quadro na parede que esconde a entrada para o cofre.

Vamos entender melhor!

Suponha que você queira enviar uma mensagem secreta para um amigo. Em vez de simplesmente criptografar a mensagem, você decide usar esteganografia. Você tira uma foto de um objeto e, usando um software especial, altera ligeiramente os valores de alguns *pixels* da imagem de forma que representem a sua mensagem. Para qualquer pessoa, a imagem parece apenas uma foto comum, mas para o seu amigo que sabe onde procurar e como decodificar o conteúdo oculto, a mensagem está claramente lá. Veja o exemplo na Figura 5.

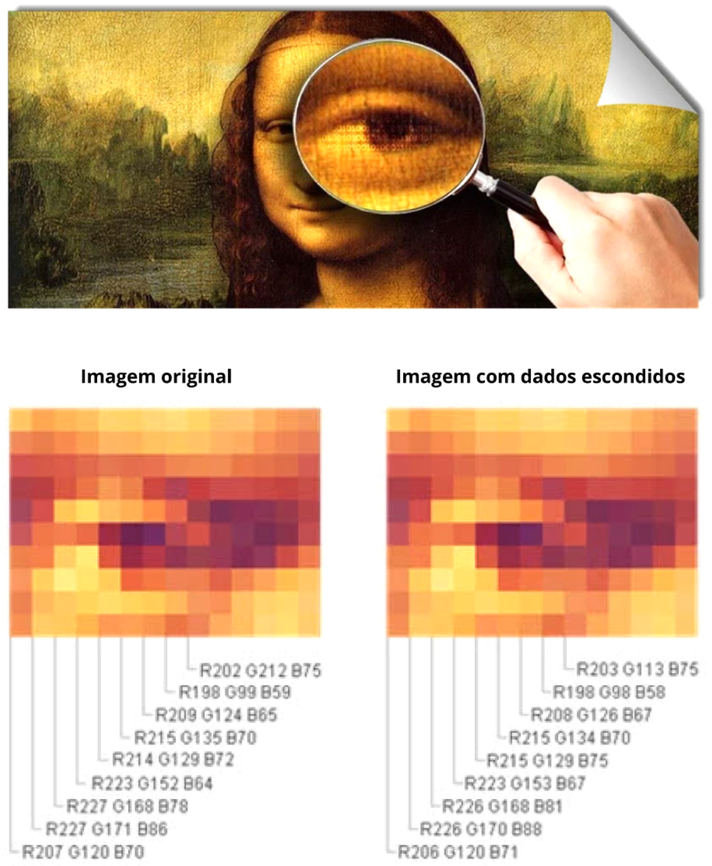

Figura 5: Uso de esteganografia para ocultar uma mensagem.

Fonte: Proteger mi PC, 2018. Disponível em: <https://protegermipc.net/2018/06/26/introduccion-a-la-esteganografia/>

O principal objetivo desta técnica (com nome difícil de pronunciar) é a realização de uma comunicação secreta. Ela trabalha lado a lado com a criptografia, mas com um objetivo distinto. Enquanto a criptografia transforma a mensagem original em algo ilegível para esconder seu conteúdo, a esteganografia esconde a própria existência da mensagem.

Na prática, a esteganografia pode ser aplicada de diversas maneiras, incluindo, mas não se limitando, a imagens digitais, onde mensagens podem ser escondidas alterando-se sutilmente os valores dos *pixels* da imagem. A técnica também pode ser utilizada em arquivos de áudio e vídeo, onde as informações são inseridas em frequências inaudíveis ou em *frames* imperceptíveis durante a reprodução.

Um caso de aplicação interessante desta técnica é na verificação de direitos autorias, onde marcas especiais (chamadas marca d'água) são inseridas no conteúdo a ser protegido e, em caso de distribuição ilegal, o autor poderá verificar se sua marca está oculta no arquivo sob investigação.

Contudo, a mensagem oculta pela esteganografia não está protegida da mesma forma como quando aplicamos um algoritmo criptográfico. Existem métodos capazes de identificar padrões em dados para indicar a presença ou não de uma mensagem oculta. O sucesso destes métodos pode variar, por isso, além de aplicar esteganografia, se sigilo é um requisito necessário, também podemos cifrar a mensagem antes de ocultá-la.

E você, consegue imaginar mais algum tipo de mídia ou objeto em que a esteganografia poderia ser aplicada?

TIC em trilhas

Aula 3:

Segurança Cibernética na prática

3.1 Como estudar segurança cibernética

Após todos esses conceitos apresentados nesta trilha você pode estar se perguntando: "OK, mas como isso pode ser aplicado na prática?". A resposta pode estar em uma combinação de métodos tradicionais e práticas interativas. Enquanto livros didáticos e cursos fornecem uma base sólida, competições de *Capture the Flag*, exploração de Aplicações Vulneráveis e a utilização de Máquinas Virtuais podem oferecer experiências imersivas que trazem a teoria à vida.

3.1.1 Capture the Flag

Capture the Flag (CTF) são competições de segurança da informação que desafiam os participantes a resolver uma variedade de tarefas que podem variar desde um quebra-cabeça simples a problemas complexos sobre *hacking* e *pentest* (teste de intrusão). Geralmente, essas tarefas estão categorizadas em áreas como criptografia, esteganografia, engenharia reversa, ataque *web*, forense digital, entre outras. Ao resolver cada desafio, os participantes obtêm uma “bandeira” (*flag* em inglês), que é um código ou um texto específico que prova que eles conseguiram superar o desafio proposto, e que deverá ser fornecido a plataforma do desafio.

Essas competições são excelentes para aprender novas habilidades, testar conhecimentos e melhorar técnicas de forma prática, divertida, ética e legal. Destacam-se as plataformas: *picoCTF*, *TryHackMe* e *Hack the Box*.

3.1.2 Aplicações Vulneráveis

Outra alternativa interessante são as aplicações vulneráveis, que são ferramentas educacionais projetadas para ensinar Segurança Cibernética através da prática em ambientes controlados. Essas aplicações são intencionalmente inseguras para que os estudantes possam aprender a identificar e explorar vulnerabilidades comuns em aplicações.

Algumas sugestões são: OWASP Juice Shop, DVWA (*Damn Vulnerable Web Application*), DIVA (*Damn Insecure and Vulnerable App*) e DVIA-v2 (*Damn Vulnerable iOS App*), sendo as duas primeiras voltadas para a plataforma *Web*, a terceira para o Android e a quarta para o iOS.

3.1.3 Bug Bounty

Você já se considera uma pessoa mais experiente no campo da Segurança Cibernética? Quando esta resposta for sim, então você também já pode se arriscar nos programas de recompensa por falhas (*Bug Bounty*), pois estes oferecem a oportunidade de testar habilidades

em ambientes reais e contribuir para a segurança de empresas e produtos, incentivando a descoberta e a correção de vulnerabilidades antes que possam ser exploradas maliciosamente. Além disso, permitem que profissionais e interessados em segurança se destaquem no mercado, ganhem reconhecimento e, em muitos casos, recebam recompensas financeiras significativas por suas contribuições.

HackerOne é uma plataforma agregadora de *Bug Bounty*, conectando organizações a *hackers* éticos para identificar e corrigir vulnerabilidades, fortalecendo a segurança digital através de testes colaborativos e recompensas por bugs encontrados.

3.1.4 Máquina Virtual

Caso sua pergunta agora seja: "E se eu quiser estudar na minha própria infraestrutura?". Provavelmente a resposta curta será: “Máquinas Virtuais”.

Máquina Virtual (VM) é como ter um computador dentro de outro computador. Máquinas Virtuais (VMs) são criadas e gerenciadas por um software chamado *hipervisor*, que permite que cada VM tenha seu próprio sistema operacional e aplicativos, independentemente do sistema principal do computador. VMs são ferramentas essenciais no estudo da Segurança Cibernética, pois permitem experimentar e entender conceitos teóricos em um ambiente controlado e seguro.

No contexto de Segurança Cibernética, o *Linux* é um sistema operacional muito utilizado devido à sua estabilidade, versatilidade e segurança, tornando-o também interessante para ambientes de aprendizado. Ele serve como uma base sólida para uma variedade de distribuições, como por exemplo *Ubuntu*, *Arch* e *Kali*, cada uma com suas próprias características, propósito e conjunto de ferramentas.

Entre as distribuições de *Linux*, a *Kali Linux* é amplamente utilizada para uma variedade de tarefas relacionadas à segurança. Ela é projetada para testes de intrusão e análise forense, contendo uma coleção de ferramentas poderosas que ajudam os profissionais e estudantes a identificar vulnerabilidades e melhorar a segurança.

Uma ferramenta muito utilizada no mundo *Linux* é o terminal, também conhecido como "linha de comando". O terminal é uma ferramenta que permite que usuários possam interagir diretamente com o sistema operacional através de uma interface textual onde pode-se executar comandos, *scripts* e acessar funções avançadas do sistema que muitas vezes não estão disponíveis em interfaces gráficas. Curiosamente, muitas vezes, o terminal também é popularmente chamado de "tela preta", pois frequentemente é apresentado nesta cor, conforme ilustrado na Figura 6.

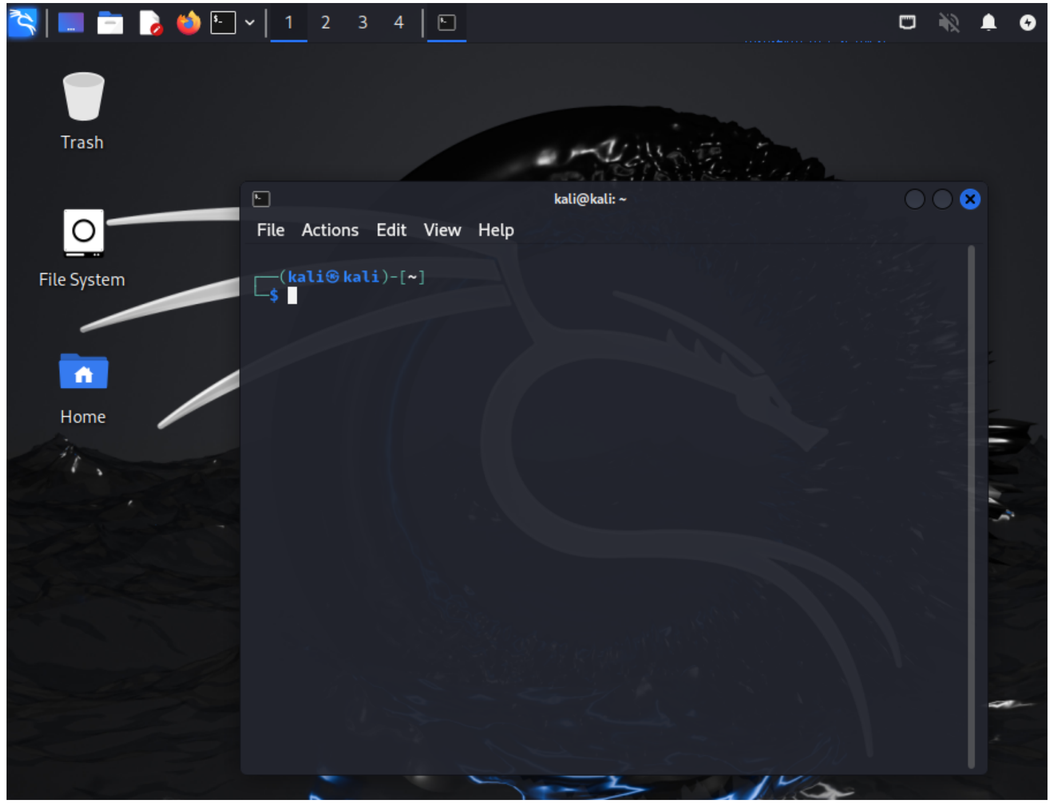

Figura 6. Captura de tela exibindo um terminal no *Kali Linux* (versão 2024.1).

Atenção!

Em muitos países é crime tentar invadir aplicações, sistemas ou infraestruturas sem o consentimento e a devida permissão do detentor do alvo a ser explorado. Antes de iniciar qualquer tentativa de invasão, é necessário buscar um alinhamento com a organização responsável pelo alvo a ser testado, definindo o que poderá ser realizado, por quanto tempo, em quais horários, quais ambientes, dentre outros pontos pertinentes, para não causar danos ao detentor e correr risco de um processo judicial.

Após o alinhamento, é boa prática a criação de um documento contendo tudo o que foi acordado, que será assinado por ambas as partes. Note que, mesmo que um site ou aplicativo, por mais que este esteja acessível a qualquer um, não se deve testar nenhuma técnica de invasão sem as devidas permissões neste alvo, pois intencionalmente ou não, se o alvo ficar indisponível ou seu banco de dados for corrompido devido aos testes realizados, por exemplo, o detentor do alvo poderá processar e exigir reparação do dano a quem o causou, além de penas criminais, dependendo da legislação.

Explore mais!

O ***podcast TecSec*** explora o mercado e tendências de cibersegurança através da visão de especialistas da área.

O ***website da CISO Advisor*** é uma maneira de se manter informado sobre as últimas notícias de Segurança Cibernética.

O ***website SecurityWeek*** oferece notícias, *insights* e análises sobre cibersegurança. Cobrindo tópicos como ataques cibernéticos, vulnerabilidades, eventos de segurança e tendências da indústria, é uma fonte confiável para profissionais da área. Conteúdo em inglês.

Criptografia Simétrica: AES. Entenda como funciona o algoritmo de criptografia simétrica mais utilizado e recomendado para uso nos dias de hoje.

Criptografia Assimétrica: RSA. Entenda como funciona um dos algoritmos assimétricos mais utilizados atualmente.

Função Hash: SHA-2. Entenda como funciona uma das funções *hash* recomendadas por especialistas.

Livro sobre Criptografia. Quer aprender em detalhes sobre criptografia, algoritmos simétricos, assimétricos, funções de *hash* e conhecer a matemática por trás desta técnica? Veja o livro “***Criptografia e Segurança de Redes: Princípios e Práticas”***, de William Stallings, da editora Pearson.

Vídeo ensinando os comandos básicos do Terminal do Linux.

Referências bibliográficas

Stuxnet: o que é e como funciona? AVAST. Disponível em: https://www.avast.com/pt-br/c-stuxnet. Acesso em: 02 maio 2024.

ARAUJO, J. **Dez anos de vigência da Lei Carolina Dieckmann: a primeira a punir crimes cibernéticos.** Disponível em: https://www12.senado.leg.br/radio/1/noticia/2023/03/29/dez-anos-de-vigencia-da-lei-carolina-dieckmann-a-primeira-a-punir-crimes-ciberneticos. Acesso em: 02 maio 2024.

O que é o *ransomware WannaCry*? Kaspersky. Disponível em: https://www.kaspersky.com.br/resource-center/threats/ransomware-wannacry. Acesso em: 02 maio 2024.

SUZUKI, S. **A guerra cibernética paralela entre Rússia e Ucrânia.** Disponível em: https://www.bbc.com/portuguese/internacional-60551648. Acesso em: 02 maio 2024.

CHEN, H; MAGRAMO. K. **Golpistas usam deepfake de diretor financeiro e roubam US$ 25 milhões.** Disponível em: https://www.cnnbrasil.com.br/economia/negocios/golpistas-usam-deepfake-de-diretor-financeiro-e-roubam-us-25-milhoes/. Acesso em: 02 maio 2024.

Relatório de custo de uma violação de dados 2023. IBM. Disponível em: https://www.ibm.com/br-pt/reports/data-breach. Acesso em: 02 maio 2024.

Estudo IBM: consumidores pagam o preço por violações de dados. IBM. Disponível em: https://www.ibm.com/blogs/ibm-comunica/estudo-ibm/. Acesso em: 02 maio 2024.

Tamanho do mercado de segurança cibernética e análise de participação – Tendências e previsões de crescimento. Mordor Intelligence. Disponível em: https://www.mordorintelligence.com/pt/industry-reports/cyber-security-market. Acesso em: 02 maio 2024.

Tríade CID: Confiabilidade integridade e disponibilidade. Fortinet. Disponível em: https://www.fortinet.com/br/resources/cyberglossary/cia-triad. Acesso em: 02 maio 2024.

O que é *hacker*? Brasil Escola. Disponível em: https://brasilescola.uol.com.br/informatica/o-que-e-hacker.htm. Acesso em: 02 maio 2024.

Diferentes tipos de cibercriminosos: *White hat, black hat, gray hat* e muito mais. AVG. Disponível em: https://www.avg.com/pt/signal/types-of-hackers. Acesso em: 02 maio 2024.

SIDHPURWALA, H. **Uma breve história da criptografia.** Disponível em: https://www.redhat.com/pt-br/blog/brief-history-cryptography. Acesso em: 02 maio 2024.

O que é criptografia de dados? Definição e explicação. Kaspersky. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/encryption. Acesso em: 02 maio 2024.

O que é criptografia? Kaspersky. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/what-is-cryptography. Acesso em: 02 maio 2024.

MARTINS, M. **Uma breve noção de criptografia.** Disponível em: https://stakey.club/pt/uma-breve-nocao-de-criptografia/. Acesso em: 02 maio 2024.

DONOHUE, B. ***Hash:* o que são e como funcionam.** Disponível em: https://www.kaspersky.com.br/blog/hash-o-que-sao-e-como-funcionam. Acesso em: 02 maio 2024.

Chaves Públicas e Privadas no Certificado Digital: como funcionam? Certisign. Disponível em: https://blog.certisign.com.br/chaves-publicas-e-privadas-no-certificado-digital-como-funcionam/. Acesso em: 02 maio 2024.

ICP-Brasil. Instituto Nacional de Tecnologia da Informação. Disponível em: https://www.gov.br/iti/pt-br/assuntos/icp-brasil. Acesso em: 02 maio 2024.

O que é esteganografia? Definição e explicação. Kaspersky. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/what-is-steganography. Acesso em: 02 maio 2024.

Introducción a la Esteganografía. Proteger mi PC. Disponível em: https://protegermipc.net/2018/06/26/introduccion-a-la-esteganografia/. Acesso em: 02 maio 2024.