Introdução e Princípios Básicos

Criptografia é o estudo a aplicação de técnicas para comunicação e armazenamento seguro de dados em sistemas computacionais e outros como telefonia e televisão.

A palavra “criptografia” vem do grego “kyptós” e “graphein”, significando escrita oculta.

Para estudar criptografia, é importante conhecer os termos chave, veja alguns deles:

- **Texto Plano/Puro:** Dados não-encriptados (não precisa ser literalmente textos, mas tudo que possa ser visto.
- **Texto Cifrado:** Dados encriptados (mesmo caso acima, não precisa ser literalmente textos).
- **Chave (Key):** Dados utilizados para encriptar um texto plano, ou desencriptar um texto cifrado.
- **Algoritmo de Criptografia:** Método matemático empregado para encriptar ou desencriptar dados com o uso das chaves de criptografia.

Encriptação é a conversão de dados legíveis para um formato ilegível (texto cifrado) por pessoas não-autorizadas, usando uma chave e um algoritmo criptográfico. Seu objetivo é proteger a privacidade ao armazenarmos dados ou trocarmos informações de outras pessoas. O receptor da mensagem encriptada pode decriptá-la e ler seu conteúdo, no formato original.

Desencriptação é o processo inverso da encriptação, ou seja, a transformação de dados encriptados (ilegíveis) em dados legíveis, usando uma chave e um algoritmo criptográfico (cifra).

Criptoanálise é o processo de transformação de dados cifrados (encriptados) em dados legíveis (decriptados) sem que se conheça a chave de encriptação. Portanto, trata-se de “quebrar” a encriptação dos dados para obter acesso ao conteúdo das mensagens, porém, com o intuito de descobrir falhar nos algoritmos para torná-los mais seguros, validá-los ou descartá-los (por exemplo, criptografia wep). Criptologia é o estudo científico da criptografia (arte de criar mensagens cifradas) e da criptoanálise (arte de desvendar as mensagens cifradas).

Esses são os requerimentos de segurança em comunicações:

- Autenticação.
- Integridade.
- Confidencialidade.
- Não-Repúdio.

Autenticação é um princípio importante. Ela assegura que a mensagem foi realmente originada pelo remetente, e não por outra pessoa.

Integridade é outro conceito importante, que é o que diz respeito ao conteúdo das informações trocadas entre transmissor e receptor. Deve-se garantir que o conteúdo da mensagem chegue íntegro ao seu destino, ou seja, que não seja alterado de nenhuma forma no meio do caminho.

Confidencialidade significa que a informação não está disponível para pessoas e processos que não tenham autorização para acessá-la e utilizá-la.

Não-repúdio também é importante, já que deve-se também evitar que uma mensagem, após ter sido enviada, seja repudiada pelo transmissor (ele não poderá negar que a transmitiu). Para isso podemos utilizar, por exemplo, assinaturas digitais, que estudaremos mais pra frente.

Tipos – Simétrica, Assimétrica e Funções de Hash

Basicamente, há três tipos de técnicas de criptografia:

- Criptografia de chave privada ou simétrica.
- Criptografia de chave pública ou assimétrica.
- Funções de hash.

A criptografia de chave privada utiliza uma única chave. O emissor utiliza essa chave para encriptar a mensagem, e o receptor utiliza a mesma chave para decriptá-la (chave compartilhada – shared key). Por utilizar a mesma chave na encriptação e decriptação, trata-se de uma técnica de criptografia simétrica (que é usada no modo stream). Exemplos de algoritmos conhecidos são DES, 3DES, Blowfish, AES, OTP (One-Time-Pad).

Na criptografia de chave pública, usamos duas chaves distintas, de modo a obtermos comunicação segura através de canais de comunicação inseguros. Trata-se de uma técnica de criptografia assimétrica pelo fato de usar um par de chaves diferentes (onde um transmissor e receptor possuem chaves diferentes, com tamanhos que variam entre 512 e 20487 bits, usadas em modo de bloco. Exemplos de algoritmos são DSA, RSA e GPG.

Cada participante possui uma chave pública e uma privada. A chave privada é secreta, e só o proprietário a conhece, ao passo que a chave pública é compartilhada com todos que se comunicação conosco. Por exemplo: Fábio quer se comunicar com Ana de forma segura, então Fábio encripta a mensagem com a chave pública de Ana, de modo que a mensagem só pdoe ser aberta usando-se a chave privada de Ana (que só ela possui).

A técnica de hash não utiliza uma chave como as técnicas vistas anteriormente, utiliza um valor de hash de tamanho fixo, o qual é computado sobre o texto plano. São usadas para verificar a integridade dos dados para garantir que não tenham sido inadvertidamente alterados. Verificações de senha pode usar funções de hash também, assim como downloads de arquivos como ISO (alguns exemplosde funções de hash utilizadas atualmente incluem MD5, SHA1 e SHA256.

Basicamente, a definição é isso:

- A chave pública (assimétrica) é compartilhada a outros usuários para que possam ser verificadas as assinaturas e integridade de arquivos e mensagens, ou criptografar arquivos e mensagens para que possam ser abertos pela sua chave privada.
- Já a chave privada (simétrica) deve ser guardada com você, e é usada para criptografar e assinar arquivos e mensagens, além de descriptografar mensagens encriptadas com sua chave pública.
- E o hash é um valor de tamanho fixo, geralmente em hexadecimal, computado sobre uma frase ou arquivo, que sempre gerará o mesmo valor, desde que não seja alterada absolutamente nada nessas mesmas frases ou arquivos, por mínimo que seja.

Revisão e Operações Lógicas AND, OR, NOT e XOR

Uma operação lógica é uma operação em álgebra booleana (com valores binários – bits), que podem ser 0 ou 1.

As operações lógicas mais comuns são o AND, OR, NOT e XOR. No caso, o true e o false são tratadas como 1 e 0, respectivamente.

A operação XOR possui uma propriedade importante, de modo que é reversível, muito utilizada em algoritmos criptográficos.

Por exemplo:

	AND	**OR**	**XOR**
Primeiro:	1001	1001	1001
Segundo:	0101	0101	0101
Resultado:	0001	1101	1100

PS: O NOT seria apenas a inversão, por exemplo, 1001 viraria 0110.

Web Crawler e Arquivo robots.txt

Um webcrawler (rastreador web) é um bot (robô) da internet que navega sistematicamente pelas páginas da web com o propósito de indexá-las. Também é conhecido pelo nome de web spider.

O webcrawler utiliza uma lista inicial de URLs para visitar, que são conhecidas como seeds (sementes). Ele identifica todos os hyperlinks nessas URLs, e os adiciona à lista de URLs a visitar. As páginas visitadas são copiadas para serem processadas posteriormente com o intuito de indexá-las. Os motores de busca utilizam webcrawler para manterem seus bancos de dados atualizados. Um exemplo é o webcrawler usado pelo Google para indexar as páginas da web para construir a busca do mesmo, o Googlebot.

Um arquivo robots.txt restringe acesso dos robôs webcrawlers a um site. Os webcrawlers, antes de indexar um novo site descoberto, verificam se ele possui um arquivo robots.txt que os impeçam de acessar determinadas páginas.

A sintaxe de um robots.txt costuma ser essa:

 # Tudo com hashtag é comentário.

*User-agent: **

Disallow: /

No caso acima, ambos são coringas para bloquear geral, no User-agent colocamos os sites de busca especificados, e em Disallow, as pastas que não devem ser indexadas.

O que é a Deep Web

Antes de entendermos a Deep Web. Precisamos entender a Surface Web (web da superfície), que trata-se da web que conhecemos, cujos sites são indexados normalmente pelos motores de busca, como o Google, Yahoo!, Bing, etc. Um site como https://facebook.com/ é um exemplo de site que pertence a Surface Web.

A Deep Web se refere ao conteúdo da web que não é visível na Surface Web, conteúdo esse não-indexado pelos mecanismos de busca convencionais. Acredita-se que a maior parte da informação da web esteja em sites que são gerados dinamicamente, os quais não são encontrados usando-se os mecanismos de busca comuns. Geralmente terminam com .onion ao invés de .com.

Na Deep Web, as páginas são dinâmicas, e são isoladas (portanto, inacessível aos webcrawlers), são privados (protegidos com login e senha), o conteúdo fica em servidores FTP e o acesso é limitado.

A Deep Web opera de tal forma que a navegação pro sua páginas se dá de forma anônima. É muito difícil, quase impossível, rastrear seu conteúdo ou descobrir quem acesso qual página.

Um estudo realizado em 2001 diz que existiam na época cerca de 7500 TB de dados na Deep Web. Em 2004, outro estudo detectou a existência de mais de 300 mil sites na Deep Web ao redor do mundo. Acredita-se que hoje em dia, a Deep Web seja mais de 500 vezes maior que a web da superfície.

A web é como um iceberg, a pontinha que enxergamos é a Surface Web, e a maior parte, escondida, seria a Deep Web.

Em tese, devido ao anonimado ao se procurar algo na Deep Web, é possível visualizar ou adquirir itens e "serviços" ilegais, como armas, drogas e pornografia infantil. Atividades criminosas encontrariam uma forma segura e anônima de proliferar nesse ambiente. Porém, a Deep Web també é utilizada de muitas formas positivas, como a divulgação de violações de diretos humanos em países com altos níveis de censura, por exemplo, ou simplesmente a navegação anônima.

Para acessar a Deep Web você precisará de um software especial habilitado para isso, como navegadores web específicos ou plugins para navegadores convencionais. O exemplo mais conhecido desse tipo de software é o Tor. Ao usar um software como esse, você estará totalmente anônimo e não será possível descobrir quem você é ou onde está localizado, e não é possível monitorar o que você faz na web.

Cifras Simétricas e OTP

Um sistema de cifragem simétrico utiliza a mesma chave para encriptar e desencriptar os dados. Também é conhecido pelos nomes de criptografia de chave privada ou chave compartilhada. Esse sistema pode utilizar cifragem de fluxo ou de bloco.

Uma cifra é definida sobre um parte de algoritmos de encriptação, onde:

$c = E(k, m)$

$m = D(k, c)$

No caso acima, as letras significam:

- *m:* Texto plano (mensagem).

- *c:* Texto cifrado (encriptado).
- *k:* Chave criptográfica.
- *E:* Algoritmo de encriptação.
- *D:* Algoritmo de desencriptação.

Podemos relacionar os dois algoritmos da seguinte forma:

$m = D(k, E(k, m))$

O algoritmo E é frequentemente randomizado, ao passo que o algoritmo D é sempre determinístico.

Um exemplo de algoritmo simétrico é o One Time Pade (OTP). A chave é uma string de bits aleatória, com pelo menos o mesmo tamanho da mensagem em si:

$C = E(k, m) = K \wedge m$

Veja um exemplo de OTP:

$C = E(k, m) = K \wedge m$

Mensagem	1000110
Chave	1100011
Cifrado	0100101

Outro exemplo:

$M = D(k, c) = K \wedge c$

Cifrado	0100101
Chave	1100011
Mensagem	1000110

Exemplo OTP: Prova:

$D(k, E(k, m)) = D(k, k \wedge m) =$

$k \wedge (k \wedge m) = (k \wedge k) \wedge m =$

$0 \wedge m = m$

O algoritmo OTP é muito rápido, porém, necessita de chaves muito longas (do tamanho da mensagem).

Cifras de Fluxo (Stream Ciphers)

A stream cipher trata-se de uma cifra de chave simétrica que combina os bits do texto plano com um fluxo de bits pseudoaleatório, uma a um. Assim, cada dígito da mensagem é encriptado pela

combinação com um dígito do fluxo de bits, originando assim o texto encriptado. Usa-se muito a operação XOR para realizar a combinação.

As cifras de fluxo usam a ideia da cifra OTP (One Time Pad), a qual usa um fluxo de bits (keystream) de dígitos totalmente aleatórios. Porém, uma cifra de fluxo usa uma chave de tamanho muito menos para gerar essa keystream, como 64 ou 128 bits. Essa chave é usada para gerar um keystream pseudoaleatório que será combinado com o texto plano para gerar o texto cifrado.

Veja um exemplo:

Texto Plano	1001 0100 1001 0010 1001
Key Stream	0100 1010 0100 1001 0010
Texto Cifrado Gerado	1101 1110 1101 1011 1011

Alguns exemplos de cifras de fluxo são o RC4, Salsa20 e SEAL.

Cifras de Bloco (Block Ciphers)

Essa cifragem opera sobre blocos de dados, o texto plano é dividido em blocos pelo algoritmo, o qual opera sobre cada bloco de forma independente. Cada bloco recebe uma chave independente e gera diferentes blocos cifrados.

No entanto, a cifra de bloco apresenta um problema: Se o mesmo bloco de texto se repetir, o texto cifrado será igual, o que pode gerar um padrão de repetição, identificável por um invasor. Esse problema pode ser resolvido usando-se um modo de realimentação.

Um modo de realimentação comum é o CBC (Cipher Block Chaining, ou cifra de blocos por encadeamento), a qual funciona fazendo XOR no bloco atual de texto plano com o bloco anterior de texto cifrado.

Para o primeiro bloco (que não tem anterior), é feito XOR com um vetor de inicialização (IV, que significa Initialization Vector).

Alguns dos exemplos de cifras de bloco são IDEA, RC5, RC6, AES, Blowfish, CAST, Rijndael e 3DES.

Encriptar Arquivos com GnuPG no Linux

No Linux, usamos o GnuPG para criptografar dados, colocar assinatura digital e gerenciamento de chaves de criptografia.

Pegue um arquivo comum, como um de texto, e vamos criptografar ele com esse programa, que usa uma chave privada (simétrica) com o algoritmo CAST5.

Vá no terminal do Linux e digite para ler o arquivo no terminal *cat teste.txt*, e para encriptar o arquivo, digite esse comando:

gpg -c teste.txt

Ele cria um diretório, um arquivo de configuração e um “chaveiro” com as chaves e pede para criar uma senha. O arquivo criado terá um .gpg depois da extensão. Se quiser ver o conteúdo do arquivo criptografado, use o cat novamente.

Para desencriptar, digite isso no comando:

gpg teste.txt.gpg

Ele pedirá a senha e desencriptará ele.

Enviando E-mails Criptografados e Assinados

Primeiramente tenha o certificado criado com as chaves públicas e privadas com seu e-mail.

No Thunderbird, instale a extensão Enigmail, que é integrada ao GPG. Ative e reinicie o Thunderbird, ele abrirá a configuração de e-mail, ele achará a chave de criptografia do seu chaveiro, além de opção para criar uma nova.

No seu e-mail no Thunderbird, crie uma nova mensagem qualquer, em cima tem uma mensagem avisando que a mensagem não está assinada nem criptografada, clique em Enigmail e marque as opções criptografar e/ou assinar mensagem. DO lado dele temos os atalhos para criptografar, assinar e anexar chave pública.

Mesmo se o destinatário não tiver chave pública, podemos marcar nosso e-mail remetente e criptografar ou assinar. Podemos criptografar apenas a mensagem ou também os anexos (atenção que a chave pública enviada será como anexo também, e não deve ser criptografada).

No e-mail destinatário, ao clicarmos no e-mail recebido ele pedirá a chave pública e descriptografará normalmente.

A resposta também será criptografada, ao responder o remetente.

Podemos também salvar e adicionar a chave pública ao chaveiro.

SSH – Conceitos Básicos e Conexão por Senha no Linux

SSH (Secure Shell) é um protocolo de comunicação seguro que permite o envio de comandos e o controle remoto de um host por meio de uma conexão criptografada. O SSH possui uma arquitetura cliente/servidor, e está disponível em praticamente todas as plataformas, como Linux, Mac OS X, BSD, Windows, etc.

O protocolo SSH cuida da autenticação, criptografia e integridade dos dados transmitidos em uma rede.

- **Autenticação:** Determina a identidade de alguém de forma confiável.
- **Criptografia:** Os dados são “embaralhados” de modo a se tornarem ininteligíveis para todos, exceto os destinatários.
- **Integridade:** Garantia de que os dados transmitidos cheguem inalterados.

O OpenSSH é uma versão gratuita do SSH. É desenvolvido pelo projeto OpenBSD (mas é disponível para várias plataformas).

Para instalar ele, vamos usar o apt mesmo, digitando isso pro cliente:

sudo apt install openssh-client

E isso pra instalar o servidor:

sudo apt install openssh-server

No servidor, inicie o serviço dele digitando *sudo service ssh start*.

E para conectar a partir do cliente, use o nome de usuário e o IP provado (ou nome do host) dele, assim (em modo root):

ssh -l nomedoservidor 192.168.1.129

PS: Podemos dar um ping antes no IP do servidor, pra ver se ele está respondendo.

Ao tentar fazer a conexão, ele pedirá a senha, e logará no sistema do servidor, que aparecerá no terminal do cliente. Para sair digite *exit* ou *logout*.

PS: Pode ser necessário ter que liberar a porta 22 no Firewall do servidor.

Se olharmos na pasta /etc/ssh do servidor, corretamente configurado, temos os arquivos de configuração ssh_config e sshd_config, que são a configuração do cliente e servidor, respectivamente.

Voltando ao servidor, entre nesse diretório e abra esses arquivos pelo terminal, que vemos as portas, protocolos usados, autenticações, etc.

Quando um cliente SSH se conecta a um servidor, cada um prova sua identidade ao outro. O servidor autentica o cliente e o cliente também autentica o servidor com o uso de criptografia de chave pública. Cada servidor SSH possui uma chave de identificação, chamada de hostkey, usada para identificar-se para os clientes.

Observe no arquivo em /root ou /home, no cliente, que temos um diretório com o nome .ssh, que tem um arquivo com criptografia que identifica os servidores conhecidos pelo cliente, para conexão.

PS: Lembre-se que o cliente é quem acessa, e o servidor que é o acessado.

SSH – Conexão por Chave Pública e Criptografia Assimétrica no Linux

Podemos nos conectar por senha a um servidor SSH. Porém, senhas apresentam problemas como:

- Para que uma senha seja segura, deve ser longa e aleatória (são difíceis de memorizar).
- Senhas podem ser capturadas se o host de destino for comprometido.

- Os sistemas operacionais geralmente só suportam uma senha por conta de usuário, o que é um problema para contas que são compartilhadas por mais de um usuário (root, por exemplo).

Para eliminar esses problemas, o SSH suporta autenticação de chave pública, usando chaves criptográficas.

Esse é o processo de autenticação:

1. O cliente solicita uma conexão com o servidor em uma conta de usuário específica.
2. O servidor responde enviando um desafio ao cliente, para que este prove sua identidade.
3. O cliente recebe o desafio, gera um autenticador usando sua chave privada, e o envia ao servidor.
4. O servidor verifica o autenticador recebido e a conta solicitada usando a chave pública do usuário para determinar a autenticidade da conexão, liberando ou não o acesso.

Para usarmos esse esquema, precisamos de: Um par de chaves e um passphrase para protegê-las, e instalar a chave pública do usuário no servidor.

Entrando no Linux cliente, entre no SSH igual anteriormente, com acesso root, mas com a opção *-v*, que mostrará na tela os passos que está executando:

ssh -vl nomedoservidor 192.168.1.129

Para usar a autenticação criptográfica primeiro devemos gerar um par de chaves. Usaremos o programa ssh-keygen para gerar chaves DSA ou RSA. No cliente basta digitar *ssh-keygen -t rsa*. O programa criará o diretório local ~/.ssh se ele não existir ainda e armazenará as chaves criadas em dois arquivos nele. Por padrão, os nomes das chaves serão id_rsa e id_rsa.pub.

Para isso, no cliente, digite isso:

ssh-keygen -t rsa

Ele gerará a chave RSA e criará o arquivo id_rsa (que pode ser alterado o nome, para não alterar é só dar enter sem escrever nada), digite uma passphrase (frase-chave) e dê enter. Ele gerará uma "imagem" aleatória para isso.

PS: Prefira RSA ao invés de DSA, já que esta última não está mais sendo aceita.

E no cliente, digite isso, na pasta ~/.ssh, para copiar o arquivo do cliente para o servidor:

scp id_rsa.pub nomedoservidor@192.168.1.129:

PS: Se definiu o arquivo pub com nome diferente, coloque esse nome.

No acesso ao servidor (via SSH mesmo), em /home, digite isso:

cat id_rsa.pub»~/.ssh/authorized_keys

cat ~/.ssh/authorized_keys

O primeiro comando escrito acima pega o conteúdo do id_rsa e escreve no arquivo de chave autorizadas para conexão.

Para finalizar, digite *logout* para voltar à máquina cliente. E agora tente logar no servidor novamente com *ssh -l nomedoservidor 192.168.1.129*. Ele não pedirá mais a senha do outro computador, pedirá a passphrase, que é a chave pública que foi criada e adicionada ao servidor.

A autenticação de chave pública é mais segura que autenticação por senha porque são necessários dois componentes secretos (o arquivo de chave no disco e a passphrase), nem a passphrase e nem a chave privada são enviadas ao host remoto, apenas o autenticador gerado com elas, e chaves criptográficas geradas por computador são muito mais difíceis de adivinhar do que chaves criadas por pessoas.

O OpenSSH inclui um programa chamado ssh-copy-id que instala uma chave pública automaticamente em um servidor remoto com um comando, escrevendo no ~/.ssh/authorized_keys ssh-copy-id -i arquivo_chave usuario@servidor, por exemplo, digitamos no cliente *ssh-copy-id -i id_rsa.pub nomedoservidor@192.168.1.129*.

Cada vez que nos conectarmos ao servidor SSH precisamos redigitar a passphrase. Porém, se usarmos um agente SSH poderemos nos identificar apenas uma vez, e o ssh (e o scp) podem se "lembrar" de nossa identidade até efeturarmos logout do cliente, por exemplo.

Um agente é um programa que mantém chaves privadas na memória e fornecem serviços de autenticação a clientes SSH. O agente usado pelo OpenSSH é o ssh-agent.

Voltando ao cliente, digite isso (fora do SSH), para iniciar o ssh-agent no shell que estamos usando:

ssh-agent $SHELL

ssh-add

Ele vai pedir o passphrase, digita ela e aí ele não a pedirá mais até fazermos logout no cliente. Para ver se a chave foi carregada, digite *ssh-add -l* (fora do SSH, no cliente).

Conecte novamente ao servidor, ele não pedirá mais a senha enquanto estivermos nessa sessão.

PS: Não use isso quando tiver fora do acesso da máquina cliente, por questões de segurança.

Pra apagar uma chave da memória, digite fora do SSH, no cliente, *ssh-add -d id_rsa* (ou o nome dela, caso seja outro), para apagar todas, digite *ssh-add -D*.

SSH – Usando SCP Para Transferência de Arquivos entre Hosts Linux

O comando SCP (Secure Copy) é um programa utilizado para copiar arquivos de forma segura entre dois hosts numa rede, usando o SSH para transferência segura dos dados.

Entre no servidor e pegue o IP dele, usando o ifconfig para isso, e o nome do usuário do mesmo.

Na máquina cliente, dê um ping no IP do servidor, e veja se ele está respondendo.

Crie um arquivo qualquer, como um de texto, na máquina cliente. E na máquina cliente, digite isso:

scp arquivo.txt nomedoservidor@192.168.1.129:/home/usuario

No caso, o que vai após o IP do servidor, é a pasta onde será salvo o arquivo.

Ele pedirá a confirmação da conexão, a senha e transferirá o arquivo até lá.

Também podemos transferir do servidor para o cliente, e uso outro arquivo do servidor.

Para baixar algo do servidor, faça isso no cliente:

scp nomedoservidor@192.168.1.129:servidor.txt servidor.txt

ls

cat servidor.txt

mkdir TesteSCP

mv arquivo.txt /TesteSCP/
mv servidor.txt /TesteSCP/

No código acima, o padrão é a pasta /home/nomedoservidor, se for baixar de outro diretório, especifique ele após os dois pontos, o segundo nome é o nome que ele terá no cliente após o download.

Para copiar do cliente para o servidor da pasta criada, fazemos assim:

scp -r TesteSCP nomedoservidor@192.168.1.129:~/Imagens

No servidor, podemos ver, na pasta especificada, que o diretório todo foi transferido, com todos os arquivos juntos.

- *scp -Cv* – Comprimir arquivos antes de enviar.
- *scp -c nomedometodo* – Escolher método de criptografia a ser usado, como 3des, aes-128 e blowfish.
- *scp -P numerodaporta* – Trocar a porta padrão para troca de arquivos.

Tor Browser Bundle – Baixando, Verificando e Rodando no Linux

O projeto Tor é uma organização que conduz pesquisa e desenvolvimento em privacidade e anonimidade online. A ideia central do Tor é impedir que outras pessoas descubram sua localização, seus hábitos de navegação, mascarar sua identidade, etc.

Baixe o Tor e a chave do arquivo dele. Com os dois arquivos na mesma pasta digite isso:

gpg –auto-key-locate nodefault,wkd –locate-keys torbrowser@torproject.org

Depois, assine a chave pública com sua chave privada, assim:

gpg –sign-key 5234758723475247824759 8

Depois, para verificar se o pacote TOR realmente é o original, faça isso:

gpg –verify tor-browser-linux32.tar.xz{.asc,}

Veja se aparece assinatura correta de “The Tor Browser Developers”, que mostrará que o pacote é verídico.

Para instalar, rode esses comandos:

tar -zpvf tor.browser-linux32.tar.xz

Entre no diretório do programa, e vê se aparece o start-tor-browser, que é o que inicializa o navegador, posteriormente, ele pode ser adicionado a um atalho ou ao lançador.

Abrindo o Tor, aparecerá as configurações do navegador, que deverão ser feitas para permitir o acesso.

Quando ele terminar, ele abrirá uma página de boas-vindas, mostrando seu IP anônimo e outras dicas para usar o Tor com segurança.

Hashes – Resumos de Mensagens

Um algoritmo de resumo de mensagem recebe uma mensagem de tamanho variável como entrada e produz um resumo de tamanho fixo como saída, totalmente incompreensível. Essa saída é chamada de Message Digest (Digest) ou hash. E o algoritmo é chamado de One-Way Hash ou simplesmente Algoritmo de Hash.

Para que seja criptograficamente seguro, um algoritmo de hash necessita no mínimo, que:

- Deve ser impossível determinar a mensagem de entrada baseado no seu resumo.
- Deve ser impossível encontrar uma mensagem qualquer que possua um hash em particular ou desejado.
- Deve ser computacionalmente inviável encontrar duas mensagens que tenham o mesmo resumo (colisão).

Adicionalmente, um algoritmo de hash seguro também tem:

- O mapeamento de um hash para a mensagem deve parecer totalmente aleatório.
- A alteração de um bit que seja na mensagem original deve produzir um hash absolutamente diferente (efeito avalanche).

Veja alguns algoritmos de hash comuns:

Algoritmo de Hash	Tamanho do Resumo em Bits

MD2	128
MD4	128
MD5	128
SHA	160
SHA-1	160
SHA-256	256
WHIRLPOOL	512

O MD5 tem 128 bits e 32 caracteres hexadecimais. O SHA-1 é bastante parecido, mas tem 160 bits e 40 caracteres, o que torna mais difícil a quebra. O hash SHA-256 tem 256 bits e 64 caracteres hexadecimais, e é mais difícil ainda a quebra.

Veja os hashs da palavra “Teste” em cada um deles:

Algoritmo	Palavra “Teste” Criptografada
MD5	8e6f6f815b50f474cf0dc22d4f400725
SHA-1	6d7082969a0681db6fe658a26ff16198600f0923
SHA-256	89f308210c7c7820bad0974f31e751bfa433d2066a93e808947c3188dedba6e3

Em sistemas Linux, podemos usar o programa HashID para identificar o tipo de hashs, digitando no terminal *hashid 8e6f6f815b50f474cf0dc22d4f400725*.

Em criptografia, os hashes são usados geralmente para:

- Autenticação.
- Integridade de Mensagens (com MAC/HMAC).
- Assinaturas de Mensagens.
- Detecção de Alteração de Dados.
- Verificação de Senhas.

PS: MAC (Message Autenticator Code) é um tipo de código de autenticação de mensagem, geralmente adicionada ao final dela. O HMAC utiliza um hash para isso.

Há outros usos, fora da criptografia, como detecção de dados duplicados e verificação de corrupção de arquivos.

Vejamos um exemplo de aplicação de hash: Detecção de alteração de dados.

Geraremos o hash de uma imagem, alteraremos um pixel na imagem e depois geraremos outro hash para comparação.

Usaremos um programa chamado md5sum que existe no Linux, que roda no terminal. Para Windows, ele é disponibilizado no GPG4Win, bastando colocar a pasta *C:\Program Files (x86)\Gpg4win\bin* no path.

Para gerar o hash do arquivo, digite *md5sum nomedoarquivo.jpg*.

Vamos fazer isso com uma imagem, para gerar o hash dela, e mantenha o prompt aberto, edite a imagem com uma pequena alteração num editor (pode ser até o Paint), mudando apenas um pixel (aumentando a foto).

Gere o hash novamente, verificará que o hash é diferente, isso é usado para ver se o arquivo foi alterado.

Nos próprios sites de alguns arquivos (como imagens ISO de sistemas operacionais como o Linux), possui os números de hash ao lado para isso.

Autenticação – Paradigmas e Técnicas

O processo de autenticação fornece garantia sobre a identidade de um usuário, verificando se você é quem diz ser.

Podemos chamar de reclamante a pessoa (ou sistema) cuja identidade será verificada.

Credenciais são a evidência que um reclamante apresenta para estabelecer sua identidade.

Assim o sistema de autenticação nos fornece proteção contra ataques como man-in-the-middle, mascaramento e spoofing, por exemplo.

Esses são alguns tipos de autenticação:

- **Autenticação de Entidade:** Um usuário afirma ter uma identidade legítima em um sistema.
- **Autenticação de Origem de Dados:** Fornece evidência de que dados (como uma mensagem de e-mail), foram originados de um usuário legítimo.

A autenticação de entidade pode ainda se subdividir em:

- **Unilateral:** Apenas uma das partes envolvidas na comunicação se autentica.
- **Mútua:** Ambas as partes devem se autenticar.

Esses são alguns dos paradigmas de autenticação:

- **Algo que você sabe:** O reclamante possui uma informação, como uma senha ou um PIN.
- **Algo que você possui:** O reclamante demonstra a posse de algo, como uma chave física, um crachá, um cartão ou uma chave privada em um smart card.
- **Algo que você é:** Baseado em alguma característica imutável do reclamante, como impressão digital, voz, padrão de retina ou geometria das mãos.

Senhas

Senhas são o mecanismo de autenticação mais usados para autenticar um usuário. Neste modelo, o reclamante prova sua identidade apresentando o conhecimento de uma string de caracteres. As senhas são uma das maiores vulnerabilidades de um sistema de autenticação, pois as pessoas tendem a escolher senhas fáceis de memorizar, e por isso, fáceis de adivinhar. O PIN também é um tipo de senha, que contém apenas números em uma pequena quantidade, geralmente de 4 a 6 algarismos. As senhas alfanuméricas geralmente são chamadas de passphrase (palavra-passe).

Muitas senhas são muito comuns, fáceis de serem quebradas por invasores.

Esses são alguns dos tipos de ataques a senhas:

- Pode ser descoberta se for transmitida sem criptografia em uma rede.
- Um intruso entra em um sistema e lê o arquivo de senhas.
- Alguém pode adivinhar facilmente uma senha mal escolhida.
- Pode ser possível quebrar uma senha usando um ataque de dicionário ou bruteforce.
- É possível inclusive enganar um usuário fazendo-o revelar sua senha.

Token

Um reclamante pode fornecer evidência de sua identidade ao demonstrar a posse de um token.

Um token é um objeto físico, como uma chave, um documento de identidade, um dispositivo eletrônico ou um smart cart, por exemplo.

Geralmente os tokens são usados em conjunto com uma senha para fornecer um grau mais elevado de certeza com relação a identidade de um reclamante.

Geradores de números eletrônicos ou um cartão com chip são exemplos disso.

Um smart card é um token do tamanho de um cartão de crédito que contém um microprocessador, memória para armazenar programas e dados, e contatos elétricos usados como interface com um leito de cartões, o qual também fornece energia elétrica ao dispositivo.

Geralmente o smart card possui um valor secreto armazenado, como uma chave privada de assinatura digital ou um número secreto, usado para realizar autenticação do portador do cartão.

Smart cards podem também ser os que se “encostam” num painel, como os cartões de ônibus, e qualquer um que tenha chip, inclusive os chips de celulares são um tipo de smart card.

Temos também tokens desconectados, que é um tipo de token que não possui conexão física nem lógica com o computador cliente.

Possuem um display que mostra um código de autenticação que muda, por exemplo, a cada minuto ou outro período.

O código pode ser usado então, para realizar autenticação em um sistema, geralmente online, como um bankline.

Biometria

A biometria fornece garantia da identidade de um reclamante baseado em características humanas físicas, comportamentais e morfológicas mensuráveis.

A biometria é usada geralmente em combinação de outros paradigmas de autenticação para obtermos um nível mais alto de segurança.

Esses são uns exemplos de biometria:

- **Padrões de Retina:** Testa os padrões únicos de vasos sanguíneos no tecido da retina de uma pessoa.
- **Impressões Digitais:** Padrões únicos de impressão digital do usuário.
- **Formato da Mão:** Exame das medidas geométricas da mão de uma pessoa.
- **Padrões de Voz:** O sistema explora os padrões vocais, acústicos, fonéticos ou até mesmo linguísticos.
- **Assinatura:** Padrões únicos de uma assinatura convencional.

O que são Assinaturas Digitais?

Um esquema de assinatura digital é um esquema matemático utilizado para provar a autenticidade de uma mensagem ou documento digital. Podemos usar assinaturas digitais com qualquer tipo de documento, mesmo criptografados, assim o destinatário da mensagem pode ter a certeza da identidade do remetente e também confiar que a mensagem chegou ao destino intacta.

Uma assinatura digital precisa ter algumas características, como:

- Deve ser simples de produzir para o assinante.
- Verificável com facilidade.
- Extremamente difícil de ser falsificada.
- Quem a usa não pode negar que assinou o documento.

Usa-se então uma assinatura digital quando você envia uma mensagem a alguém e, embora possa não ser importante que a mensagem seja mantida em segredo, é muito importante que o destinatário da mensagem tenha certeza de que essa mensagem realmente partiu de você.

Nesse caso, você pode criptografar a mensagem com sua chave privada, enviá-la, e o destinatário só será capaz de decriptá-la com a sua chave pública (não a dele nem de mais ninguém), provando a autenticidade da mensagem. Sendo assim, uma assinatura digital utiliza alguma forma de criptografia assimétrica para operar.

Porém, uma forma mais eficiente de obter esse mesmo resultado é criptografar um pequeno bloco de bits que seja uma função do documento, e não o documento inteiro. Este bloco é chamado de autenticador (autenticator), e possui a propriedade de que é impossível alterar um bit que seja no documento sem desfigurar totalmente o autenticador. Criptografamos então o autenticado com a chave privada do remetente, e ele servirá para verificar a autenticidade do documento todo. Podemos usar um hash como o SHA-1 para essa função.

Dessa forma, a assinatura digital é enviada anexada à própria mensagem e o conjunto é enviado ao destinatário. O destinatário então calcula o hash da mensagem, decripta a assinatura digital, e compara os dois valores, se forem idênticos, a mensagem é autêntica.

Mas há um problema com esse esquema de assinaturas digitais: Como podemos ter certeza de que um documento assinado foi realmente assinado pelo remetente correto? Em outras palavras, como podemos garantir que um intruso não consiga gerar e assinar um documento em nome de outra pessoa? Para resolver esse problema, devemos utilizar um certificado digital, que pode ser usado para atestar e verificar a validade de uma assinatura digital.

Alguns dos algoritmos mais comuns usados para assinar digitalmente um documento são RSA, DSA, ElGamal e HMAC.

Hash MD5 – Usando no Windows e no Linux

O MD5 (Message Digest 5) é uma função de hash criptográfico muito usada. Produz um valor de hash de 32 caracteres hexadecimais (128 bits).

Um hash MD5 pode ser usado em aplicações como:

- Verificar se um arquivo transferido chegou intacto ao destino (“checksum” – MD5sum).
- Armazenar hashes de senhas (one-way hash).

PS: No mundo real as duas aplicações não são recomendadas com o MD5.

Uma minúscula mudança no texto original produz uma mudança brutal no resultado computador pelo hash, por exemplo:

- raio: 320652e3afe3d17415897504813abf7b
- Raio: 93a6ff559b4a143ff1b6f77c57145951

A segurança do hash MD5 está fortemente comprometida. Ele é vulnerável a ataques de colisão, mesmo usando máquinas comuns com poder de processamento médio.

Um ataque de colisão em um hash criptográfico é um tipo de ataque onde se tenta encontrar duas entradas que produzam o mesmo valor de hash na saída. Outro problema grave, relativo ao uso de hashes MD5 para armazenar senhas, é o uso de rainbow tables para reverter um hash e descobrir a string que o originou. Também não é recomendado usar isso com SHA-1.

No Linux, o gerador de hash já existe, já no Windows, precisaremos usar os programas do GPG4Win.

Para gerar o hash de um arquivo qualquer, usamos o comando *md5sum nomedoarquivo.extensao*. Se quisermos gerar um arquivo com o hash MD5 dele, podemos usar *md5sum nomedoarquivo.extensao>nomedoarquivo.md5*. No Linux, usamos a mesma lógica com hashs SHA-1 e SHA-256, mudando o comando para *sha1sum* e *sha256sum*, respectivamente.

O gerador de hashs do GPG4Win também tem opção para SHA-1 e SHA-256.

PS: Independente do arquivo, o hash sempre terá um tamanho pequeno.

Pra quem usa Windows, o 7-Zip, programa de compactação e descompactação, também oferece um utilitário para verificar hashs SHA-1 e SHA-256, basta clicar com o botão direito no arquivo e verificar.

Hashes e Rainbow Tables – Descobrindo Senhas

Existem algumas técnicas de ataques a hashes, sendo as mais comuns as seguintes:

- Força Bruta.
- Dicionário.

- Colisão.
- Aniversário.
- Rainbow Tables.

Os dois primeiros não são muito efetivos, devido a imensa quantidade de valores que precisam ser testados, principalmente com senhas longas.

Os ataques de força bruta consistem no uso de um programa que tenta várias combinações aleatórias até achar a senha certa. O dicionário age de forma parecida, mas usando um dicionário de palavras num arquivo txt comum, que pode ser feito especialmente para um determinado usuário (um com palavras da Bíblia para obter a senha de alguém religioso ou um com nomes de bebês para obter a senha de uma grávida, por exemplo).

O ataque de colisão é quando encontramos dois textos planos diferentes que tem o mesmo hash, inclusive já chega a comprometer os algoritmos MD5 e SHA-1. Já o ataque de aniversário baseia nas probabilidades matemáticas de encontrar determinada senha.

Uma rainbow table é uma espécie de tabela que contém milhões (ou bilhões) de hashes pré-calculados e as strings (“senhas”) que os originaram. Uma rainbow table é otimizada para armazenar hashes e senhas, permitindo pesquisar entradas de forma muito veloz. São usadas basicamente para quebrar hashes de senhas.

Uma função de hash mapeia textos planos (dados não criptografados) em hashes de forma que não podemos discernir qual texto plano originou qual hash. Para que seja possível descobrir o texto plano a partir de um hash, devemos aplicar a função de hash em cada texto plano possível até encontrarmos o hash idêntico ao procurado. Podemos também armazenar cada hash gerado em uma tabela, de modo que podemos consultá-la mais tarde sem precisarmos efetuar o cálculo de hash outra vez.

Uma forma comum de proteger o hash de nossas senhas contra ataques de rainbow tables é o uso de uma técnica conhecida como salt (“salgar a senha”). Um salt é uma informação aleatória adicionada a entrada da função de hash, tornando a saída da função única, e imune às rainbow tables. Seria algo tipo *funcaoHash(TextoPlano + Salt)*. O “salt” pode ser o nome de usuário, um PIN, um valor aleatório, etc.

Para vermos na prática um funcionamento de uma rainbow table, podemos utilizar sites pra isso.

Coloque uma senha simples como “laranja” (cujo hash é *cf75ceb29197f57b19dcb8b4757368e8*), e pegue o hash dela e jogue no site, pra ver se ele encontra algo. Da mesma forma, teste senhas de todo tipo, das mais fáceis até as mais complexas.

Isso é útil para sabermos se uma senha é fraca ou mais forte.

Além do MD5, o rainbow table também pode quebrar outros tipos de senhas, como SHA-1.

O que são Cifras de Feistel

A maioria dos algoritmos de criptografia simétrica de bloco possuem uma estrutura descrita por Horst Feistel, da IBM, em 1973.

As entradas do algoritmo são blocos de texto plano de comprimento 2x bits e um chave K. O bloco de texto plano é dividido em duas metades, L_0 e R_0. Essas duas metades passam por n rodadas de processamento e então se combinam para produzir o bloco de texto cifrado.

Cada rodada r recebe como entrada L_{r-1} e R_{r-1}, derivadas da rodada anterior, assim como uma subchave K_r, derivada da chave geral K. Essas subchaves são diferentes de K entre si pois são geradas a partir de K com um algoritmo de geração de chaves. As interações possuem todas a mesma estrutura. Uma substituição é realizada na metade esquerda dos dados, por meio da aplicação de uma função F na metade direita dos dados com a chave e então obtendo-se o XOR da saída desta função e da metade esquerda dos dados.

Em outras palavras, o texto plano é dividido em dois, o que está no lado direito (o -1) é o bloco anterior de ambos na função f que é aplicada a criptografia com uma chave, a saída recebe o que está do lado esquerdo e a saída vai pro lado direito, e o que estava no lado direito vai pro esquerdo. Isso é feito várias vezes, formando uma rede Feistel.

Muitos algoritmos de criptografia utilizam uma ideia baseada em redes Feistel.

Como a cifra de Feistel será aplicada depende da escolha de alguns parâmetros, como:

- **Tamanho do bloco:** Geralmente 64 bits.
- **Tamanho da chave:** Chaves maiores significam maior segurança, porém, menor velocidade de execução do algoritmo.
- **Número de rodadas:** Tamanho típico 16.
- **Algoritmo de geração de subchaves:** Quanto mais complexo, melhor.
- **Função F (função principal do algoritmo):** Quanto mais complexa, melhor.

O processo de descriptografia de uma cifra de Feistel é igual a criptografia. Usa-se, nesse caso, o texto cifrado como entrada do algoritmo, e as subchaves K_n em ordem reversa.

As cifras de Feistel são usadas nos algoritmos de criptografia DES, Blowfish, RC5, Twofish, 3DES, entre outros.

Steghide – Esteganografia no Linux – Ocultando Mensagens em Imagens

A esteganografia é a ocultação de arquivos (como uma mensagem) em outro arquivo, como uma imagem, vídeo ou áudio.

Para usarmos a esteganografia, primeiro crie um arquivo de texto com alguma mensagem qualquer.

Depois, instale, caso já não tenha instalado, o Steghide.

O Steghide suporta vários formatos de arquivos, como JPEG, BMP, WAV e AU. Para ver o manual dele, digite *man steghide*.

Esses são os comandos do Steghide:

Para ocultar uma mensagem em um arquivo de imagem ou som, usamos o comando embed seguido dos argumentos apropriados. Os principais argumentos são os seguintes:

- *-ef*: Especificar o arquivo que será incorporado, ou seja, o arquivo que contém a mensagem secreta. Se este argumento for omitido ou o nome do arquivo for o caractere “-”, os dados secretos serão lidos diretamente da entrada padrão (teclado).
- *-cf*: Especificar o arquivo portador que será usado para incorporar os dados secretos. Esse arquivo deve estar em um dos formatos a seguir: AU, BMP, JPEG ou WAV. Se este argumento for omitido ou o nome do arquivo for o caractere “-”, o Steghide lerá o arquivo portador a partir da entrada padrão.

Para extrairmos uma mensagem oculta de um arquivo esteganografado usamos o comando extract, cujo argumento principal é esse:

- *-sf*: Especificar o arquivo esteganografado (que contém os dados secretos embutidos). Se este argumento for omitido ou o nome do arquivo for o caractere “-”, o Steghide lerá o arquivo esteganografado a partir da entrada padrão.

Primeiramente, pegue uma imagem grande em JPEG, e crie um arquivo de texto com uma mensagem.

Pra ocultar a mensagem dentro da imagem, digitamos esse comando, no diretório onde estão os arquivos:

steghide embed -cf imagem.jpg -ef mensagem.txt

Ele pedirá para criar uma senha, e o arquivo é modificado, visualmente ela estará igual antes, mas terá a mensagem oculta. Para especificar um algoritmo de criptografia, use a opção -e seguida do algoritmo, por exemplo *-e rc2*.

Para mostrar informações do arquivo, fazemos assim:

steghide info imagem.jpg

No caso acima, ele mostrará os dados da imagem, e mostrará a opção de tentar obter dados do arquivo embutido, aí ele pedirá a senha pra mostrar estes dados.

E para extrair a mensagem, fazemos isso:

steghide extract -sf imagem.jpg

Ele pedirá a senha, e extrairá a mensagem.

Para mostrar informações sobre os algoritmos de criptografia, use esse comando:

steghide encinfo

Kali Linux – Coletando Informações com Dmitry

O Dmitry (Deepmagic Information Gathering Tool) é uma aplicação open source de linha de comandos que nos permite coletar diversos tipos de informações sobre um host em uma rede. A ferramente, que é codificada em linguagem C, é capaz de coletar dados sobre subdomínios, endereços de e-mail, efetuar escaneamento de portas TCP (port scan), lookups whois e mais algumas funções.

No Kali Linux, a ferramenta está presente por padrão, não sendo necessário baixá-la e instalá-la. De acordo com o site do desenvolvedor, o Dmitry pode ser executado em várias plataformas, incluindo FreeBSD, Mac OS X, SuSE Linux e OpenBSD, entre outras. Ele lembra um pouco o Nmap, mas é um pouco mais simples.

Vamos começar executando o software sem usar nenhuma opção. Para isso, execute o comando a seguir no terminal:

dmitry

Ele mostrará a saída que explica as funções das opções do programa.

Exemplo de um lookup whois num host:

dmitry -w www.google.com.br

Podemos realizar um TCP port scan no endereço 192.168.1.1:

dmitry -p 192.168.1.1

E um TCP port scan no endereço 192.168.1.110:

dmitry -p -f 192.168.1.110

E para salvar a saída do comando anterior em um arquivo:

dmitry -p -f 192.168.1.110 -o portas-escaneadas

O Kali Linux traz outras ferramentas para coleta de informações sobre hosts, muitas delas bem mais completas que o Dmitry, que é uma ferramenta bem simples.

Kali Linux – Manipulando Endereços MAC com Macchanger

O utilitário de linha de comandos Macchanger (GNU Mac Changer), escrito por Álvaro Lopez Ortega, permite visualizar e manipular o endereço MAC (Media Access Control) das interfaces de rede do computador. Esse utilitário está presente nativamente no Kali Linux.

A sintaxe básica dele é macchanger opções dispositivo.

PS: Todos os comandos deverão ser utilizados como root, então dê *sudo su* caso não esteja no Kali. Pode ser necessário também dar um down na interface antes de fazer alterações nela.

Vamos visualizar o endereço MAC (MAC Address) atual da interface eth0:

macchanger -s eth0

Vamos alterar o endereço MAC da interface eth0 sem no entanto, alterar os bytes do fabricante, criando um endereço aleatório:

macchanger -e eth0

Podemos também configurar um endereço MAC totalmente aleatório na interface eth0:

macchanger -r eth0

Ou configurar um endereço MAC específico, como 12:34:56:78:90:AB, na interface eth0:

macchanger -m 12:34:56:78:90:ab eth0

E podemos também resetar o endereço MAC para o valor original na interface eth0:

macchanger -p eth0

Acessando um Desktop Linux via VNC com Android

Primeiro logue dentro do Linux e baixe o servidor VNC, e depois inicie o serviço digitando *x11vnc --forever* (deixe o terminal aberto, não execute como root).

PS: Caso ele termine a aplicação abruptamente, vá no arquivo em /etc/gdm3/custom.conf (pode ser lightdm também) e tire a hashtag de comentário da linha *# WaylandEnable=false*. Reinicie e tente novamente.

No Android, vá na Play Store e baixe o aplicativo VNC Viewer, que tornará nosso Android um cliente VNC.

Dentro do APP Android, colocamos em Address o IP privado do servidor seguido da porta, e o nome de usuário dele em Name, ele mostrará a conexão sem criptografia (que não pede a senha). Dentro do Android mostrará inclusive a interface gráfica do Linux acessado.

Podemos também acessar um Windows pelo Android, nesse caso instalamos no Windows o Real VNC e usamos ele como servidor no PC, o restante permanece da mesma forma.

PS: Pode ser necessário ter que liberar a porta do VNC (especificada no terminal) no Firewall do Linux.

Esteganografia – Ocultando Mensagens em Arquivos no Windows

A esteganografia é uma técnica utilizada para “esconder” ou ocultar mensagens, imagens ou arquivos dentro de outros arquivos.

A esteganografia tem origem na Grécia antiga, na qual escreviam com uma tinta “invisível” que só podia ser vista com uma técnica especial. Em informática, usamos dois arquivos, a mensagem e o portador (carrier).

Lembrando que no exemplo usaremos texto em uma imagem, mas qualquer arquivo pode ser inserido em qualquer arquivo.

Existem vários programas disponíveis para esteganografia, no exemplo, vamos usar o OpenPuff para Windows.

Abra a pasta e execute o aplicativo dentro dela. Ele demora um pouco enquanto, veja que ele tem várias opções como, além da esteganografia, tem marca d’água (pra proteger os direitos autorais de imagens e arquivos).

Clique no botão “Hide” e ele abrirá a tela para isso. Na tela que abrir, vá na parte 1 e insira até três senhas diferentes nos campos, a primeira é requerida, para criptografar, as outras são recomendadas, mas opcionais, a segunda é pro gerador de números aleatórios e a terceira é o embaralhamento da mesma.

Coloque num txt uma mensagem qualquer e selecione uma imagem (para query).

Na parte dois, clique em “Browse” e selecione o txt da mensagem (que será o arquivo a ser escondido).

Na parte três, coloque os arquivos em “ADD” (vamos trabalhar só com um no caso, se a mensagem for grande, pode ser dividida em vários portadores).

Na parte quatro é opcional, é mais para escolher a qualidade do arquivo ou dos algoritmos utilizados, etc.

Depois é só salvar o novo arquivo clicando em “Hide Data”. Veja que, aparentemente, nada da imagem parece alterada.

Para descobrir a mensagem, pegue o arquivo esteganografado e faça o mesmo procedimento no OpenPuff, escolhendo a opção “Unhide”. Carrega ela em “ADD Carries” e em “Unhide”. A mensagem oculta será salva como um novo arquivo.

Dependendo do tamanho do arquivo a ser escondido, a imagem poderá ter tamanhos diferenciados, se uma imagem tiver tamanho muito grande, é provável que tenha alguma coisa escondida, principalmente malwares.

Criptografia com GnuPG no Windows – Apresentação

Abra o Kleopatra, clique em file e em new certificate, as escolhas de formato será aberto, as opções são OpenPGP (que é um padrão aberto e são criadas localmente, sem uma autoridade de certificação, podendo ser certificadas pelos amigos e conhecidos), e a X.509 (que precisará verificar a chave com uma autoridade de certificação, que terá um custo). No caso, criaremos OpenPGP.

Ao abrir o Kleopatra e escolher OpenPGP, coloque o nome, e-mail e comentário para o qual será enviado.

Tem um botão escrito Advanced Settings, que tem algumas opções avançadas como as de algoritmos (escolha RSA de preferência), tamanhos de chaves e validades. Quanto maior a chave, mais difícil de quebrar a criptografia, porém, mais recursos de hardware serão consumidos. Marque a opção autenticação para configurar a validade dela.

No próximo, ele mostrará os dados, e depois pedirá para você inserir uma senha para descriptografar posteriormente.

Ele criará a chave, exibirá o fingerprint, terá as opções de fazer um back-up dela também.

Na chave pronta, clique com o botão direito para ver as opções deles para alteração e criação de certificados. Temos opções para exportar as chaves públicas e privadas, gerar certificados de revogação, etc.

Para encriptar um arquivo com essa chave, basta ir em file, sign/encrypt files, adicionar o arquivo, escolher a chave criada, e confirmar, será gerado um arquivo criptografado. Também podemos encriptar um arquivo com uma senha.

Para desencriptar, faça da mesma forma, insira a senha (caso seja criptografado com uma, se foi criptografado com sua chave pública, ele pedirá a senha da sua chave privada) e ele será descriptografado.

O Kleopatra também fornece um autenticador de chaves, basta colocar o arquivo e a chave dele na mesma pasta e clicar diretamente na chave, que abrirá o Kleopatra e verificará a autenticidade do arquivo (podendo também pesquisar a chave dele num servidor, importar e certificar a mesma). Podemos também assinar arquivos com nossa chave privada, indo em sign/encrypt files. Também é possível usar a maioria dos comandos do GPG do Linux pelo CMD do Windows.

Introdução ao Registro do Windows

O registro é um banco de dados hierárquico do Windows que armazena informações importantes sobre hardware do sistema, programas instalados e configurações, além de perfis de cada uma das contas de usuário no computador.

O registro foi introduzido no Windows 3.1, e foi expandido ao longo do tempo para armazenar mais informações e configurações do sistema e programas. Antes de existir o registro, as configurações dos programas eram armazenados em arquivos de texto com extensão .ini, que ainda existe, mas é bem menos usado que antigamente, praticamente tudo é feito no registro, hoje em dia.

Para abrir o registro, procure no executar ou no iniciar “regedit.exe”, ele será executado como administrador.

Os dados do registro são armazenados em chaves (compartimentos, como se fossem “pastinhas”), e dentro dele tem subchaves, que funcionam da mesma forma. As configurações que aparecem do lado

direito são chamados de valores. Os valores sempre possuem um nome, o tipo de dados e o conteúdo dos dados (como se fossem variáveis). Tudo isso são parâmetros que ficam armazenados dentro das chaves, e os valores são itens de configurações.

Esses são os tipos de dados mais comuns em entradas de registro, que são utilizados para configurar os valores que guardamos dentro das chaves:

ID do Tipo	Nome Simbólico	Significado
0	REG_NONE	Sem tipo definido
1	REG_SZ	Valor de cadeia de caracteres UTF-16
2	REG_EXPAND_SZ	Valor de cadeia de caracteres expansível
3	REG_BINARY	Dados binários
4	REG_DWORD	Valor DWORD, inteiro sem sinal de 32 bits
7	REG_MULTI_SZ	Cadeia de caracteres múltipla (lista ordenada)
11	REG_QWORD	Valor QWORD, inteiro de 64 bits

O registro tem cinco chaves principais (chaves raiz ou de alto nível), que são essas:

- HKEY_CLASSES_ROOT
- HKEY_CURRENT_USER
- HKEY_LOCAL_MACHINE
- HKEY_USERS
- HKEY_CURRENT_CONFIG

PS: Podem existir também outras, dependendo da versão do Windows.

A chave *HKEY_CLASSES_ROOT* contém informações relativas a associações de nomes de arquivos, objetos OLE, associações com objetos COM, e associações de arquivos de classe. Parâmetros contidos nessa chave são na verdade um link (atalho) para a chave HKEY_LOCAL_MACHINE\SOFTWARE\Classes. Abreviada normalmente como HKCR.

A chave *HKEY_CURRENT_USER* contêm as configurações do usuário logado no sistema no momento, incluindo variáveis de ambiente, configurações de desktop, de redes e de aplicações. É um link para HKEY_USERS\<SID-DO-USUÁRIO-ATUAL>. Abreviada normalmente como HKCU.

A chave *HKEY_LOCAL_MACHINE* contêm todas as informações globais de hardware e sistema operacional. A informação nessa chave é aplicável a todos os usuários que se logam no sistema local. Abreviada normalmente como HKLM.

A chave *HKEY_USERS* contêm dados de todos os perfis de usuários no sistema, incluindo HKEY_CURRENT_USER e o perfil de usuário padrão. No geral, usamos a chave HKCU para configuração do usuário atual. Abreviada normalmente como HKU.

A chave *HKEY_CURRENT_CONFIG* armazena todos os dados sobre a configuração atual de hardware da máquina. É um link para HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Hardware\Profiles\Current. Não é muito utilizada no geral. Abreviada normalmente como HKCC.

Uma das coisas que podemos fazer no registro é exportar ele (fazer um backup), apenas indo em arquivo e exportar, escolhendo a ramificação selecionada ou tudo. Da mesma forma, você importa os dados.

Para criar uma chave, podemos fazer isso clicando com o botão direito no local onde ela será inserida (por exemplo, em HKEY_LOCAL_MACHINE\SOFTWARE), podemos escolher uma nova chave (pasta) ou diretamente os valores. No exemplo, criaremos a chave Teste, ele já terá um valor padrão não definido dentro dela (ou seja, está vazia), basta clicar duas vezes nele, colocar os valores na janela que abre e dar OK, ele já será salvo (em alguns casos pode ser necessário reiniciar o PC. Da mesma forma, podemos criar novos valores dentro da mesma chave, clicando com o botão direito dentro dela.

Caso você entre muito numa chave de difícil localização que precise mexer com frequência, clique nela e adicione aos favoritos, logo acima do editor de registro, nesse mesmo local terá o link de acesso direto à ela. Da mesma forma, podemos remover os favoritos.

A seguir, veremos um exemplo de configuração de registro do Windows que você pode testar em seu sistema (de preferência, teste numa máquina virtual).

Para desabilitar o painel de controle, vamos em HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer e criar o valor NoControlPanel do tipo DWORD, e o valor será 1 (pra habilitar restrição), pra desabilitar o valor é 0 (de preferência hexadecimal). Depois o valor criado pode ser excluído.

PS: Os nomes não podem ter erros, e eles não são inventados, são nomes que o sistema e/ou os programas reconhecem. E tome muito cuidado para mexer no registro.

Como Funciona a Cifra de César

A cifra de César é uma técnica de criptografia bastante simples e provavelmente a mais conhecida de todas. Trata-se de um tipo de cifra de substituição, na qual cada letra de um texto a ser criptografado é substituída por outra letra, presente no alfabeto porém deslocada a um certo número de posições à esquerda ou à direita. A cifra de César recebe esse nome, pois, segundo o escritor Suetônio, foi utilizada por Júlio César para se comunicar com seus generais, protegendo mensagens militares.

Sendo uma cifra de substituição monoalfabética, cada letra do texto plano é substituída por uma outra letra do alfabeto no texto criptografado (cifrado), de forma constante (sempre as mesmas letras são utilizadas). Por conta disso, ele acaba sendo extremamente simples de ser decifrada e nunca é utilizada na prática, pois não possui absolutamente nenhuma segurança. Como o texto cifrado acaba tendo exatamente o mesmo número de caracteres do texto plano, também classificamos a cifra de César como monogrâmica, sendo então classificada mais corretamente como cifra de substituição monoalfabética monogrâmica.

Essas são algumas formas de funcionamento:

- Atribuindo valores numéricos às letras do alfabeto (A = 1, B = 2, C = 3).
- Escolhendo o valor de rotação (deslocamento das letras), como por exemplo 4, e calculando e substituindo as letras de acordo com o deslocamento (A = 1 + 4 = 5 = E, B = 2 + 4 = 6 = F), quando chegar no Z, as últimas letras são atribuídas às primeiras (W = 23 + 4 = 1 = A, X = 24 + 4 = 2 = B, etc.).

Utilizando o exemplo anterior, vamos ver a cifra de César na prática, com rotação à esquerda de quatro posições:

- **Alfabeto Normal:** ABCDEFGHIJKLMNOPQRSTUVWXYZ
- **Alfabeto Cifrado:** EFGHIJKLMNOPQRSTUVWXYZABCD

Veja um exemplo de mensagem cifrada nesse método:

- VAMOS APRENDER CRIPTOGRAFIA
- ZEQSW ETVIRHIV GVMTXSKVEJME

O Que é um Ataque Zero Day?

Uma vulnerabilidade de dia zero (ou zero day) é uma vulnerabilidade de software descoberta por invasores antes que o fornecedor tome conhecimento dela. Como os fornecedores não a conhecem, não existe correção para vulnerabilidades de dia zero, o que aumenta a probabilidade de um ataque bem-sucedido. Uma exploração de dia zero é o método usado pelos crackers para atacar sistemas com essas vulnerabilidades não-identificadas anteriormente.

Um ataque zero day (ataque de dia zero) se aproveita das falhas de um software que os desenvolvedores desconhecem para atacar as vítimas sem aviso prévio.

Um ataque zero day, nada mais é do que uma violação de segurança que tem como alvo uma vulnerabilidade de dia zero. Crackers criam malware especial, mais chamado de malware zero day ou malware de dia zero, que ataca essas falhas de segurança recém-descobertas. Após o ataque zero day, os desenvolvedores precisam se esforçar para identificar a violação, para descobrir o que aconteceu e criar uma solução antes que ocorram mais ataques.

Os ataques zero day são realizados por “atores” maliciosos que se dividem nas seguintes categorias: Criminosos virtuais, crackitivistas, espionagem corporativa e guerra virtual.

Um ataque zero day pode explorar vulnerabilidades de diversos sistemas, como, sistemas operacional, navegadores da web, aplicativos, componentes que possuem código aberto, hardware e firmware, IoT (internet das coisas) e isso amplia o leque de possibilidades de vítimas em potencial para os cibercriminosos.

Usuários que fazem o uso de um sistema vulnerável, como por exemplo, um navegador ou sistema operacional, nesse caso, cibercriminosos podem utilizar das vulnerabilidades de segurança para comprometer o dispositivo e construir grandes botnets.

Um botnet é uma rede de computadores, que é comandada por uma única pessoa (muitas vezes de forma remota), com vários computadores destinados a fazer uma única tarefa ou várias tarefas com o mesmo objetivo. Na teoria, muitas redes poderiam ser classificadas assim, como as da internet, com seus roteadores e servidores, no entanto, os botnets são usados muitas vezes com más intenções, como por exemplo, enviar e-mails de spam, arquivos maliciosos ou outros tipos de ataques, como por exemplo, de negação de serviço (DoS).

O que é Ransomware e Como se Proteger Dessa Ameaça

Ransomware é um tipo de software malicioso que bloqueia o acesso aos dados da vítima até que um resgate seja pago, e exibe na tela uma mensagem de requisição de pagamento. No geral, criptografam os arquivos da vítima, tornando-os totalmente inacessíveis e só podem ser decriptados após o pagamento do resgate. Alguns ransomwares criptografam todo o HD da máquina, outros criptografam arquivos e pastas específicos. Trata-se de uma grande ameaça a indivíduos e organizações.

O ransomware funciona num sistema de extorsão criptoviral:

- Ransomware infecta máquina da vítima
- Arquivos são criptografados com uma chave pública.
- Chave privada é gerada e armazenada em um local oculto na internet.
- Resgate é solicitado para liberar a chave privada.
- Vítima paga o resgate, usualmente em bitcoin.
- Atacante envia chave privada para vítima.

- Vítima decripta seus arquivos e os recupera.

No caso, geralmente é usado uma chave assimétrica (pública) para isso.

No geral, ransomwares infectam as máquinas das vítimas por meio de cavalos-de-troia (trojans). Podem infectar quaisquer tipos de equipamentos, como PCs e notebooks, smartphones, smart TVs, tablets e dispositivos IOT. Basicamente qualquer equipamento com sistema operacional.

Os principais vetores de infecção de ransomware são, basicamente, os mesmos da maioria dos malwares existentes:

- E-mails de phishing.
- Anexos de e-mail maliciosos.
- Links em documentos (Office, etc.).
- Download de programas e arquivos.
- Navegação em sites específicos (drive-by).
- Pen-drives e mídias removíveis (menos comum).

Os sinais de que seu sistema está sendo infectado por ransomware incluem:

- Lentidão atípica da máquina.
- Tráfego de rede desconhecido.
- Arquivos sendo renomeados automaticamente.
- Extensões estranhas em nomes de arquivos.
- O mais óbvio, mensagem de pedido de resgate (no sistema já comprometido).

As formas de pagamento do resgate costumam ser essas:

- Bitcoin (modo preferido).
- Serviços de voucher.
- Transferências eletrônicas.
- Popcorn ransomware (infecte outras máquinas e ganhe sua decriptação).

Para se proteger do ransomware, siga esses métodos:

- Manter o sistema operacional sempre atualizado.
- Possuir back-ups dos dados importantes em local seguro.
- Utilizar softwares antimalware e mantê-los atualizados.
- Se detectado ataque em curso, agir imediatamente, desconectando as máquinas da rede, e desligar as máquinas infectadas.
- Desabilitar WSH (Windows Scripting Host).
- Impedir que aplicativos sejam executados em %AppData% e %LocalAppData%.

- Impor UAC (User Account Control).
- Sempre exibir as extensões dos arquivos no Explorer.
- Usar AppLocker para bloquear a execução de programas.

E para se livrar dele:

- Identificar e conter a propagação da infecção.
- Identificar o ransomware.
- Eliminar o ransomware das máquinas com ferramentas apropriadas (antivírus, antirransomware).
- Tentar usar ferramentas de decriptação.
- Reinstalar o SO.
- Restaurar back-up dos arquivos criptografados.
- Como último recurso, pagar o resgate.

O que é um Firewall?

O Firewall é um sistema de hardware/software cuja função é proteger uma rede local de ameaças provenientes de uma rede externa (como a internet) e de hosts na própria rede. O firewall controla o tráfego de dados entre as redes interconectadas de acordo com regras preestabelecidas (políticas de segurança).

Veja como um firewall funciona:

- Todo o tráfego que entra e sai da rede deve passar pelo firewall. O acesso a LAN deve ser bloqueado fisicamente usando-se o firewall entre as redes.
- Apenas o tráfego autorizado (definido pelas regras de segurança) poderá atravessar o firewall.
- O firewall deve ser imune a penetração. Ou seja, deve-se usar um software confiável com um SO seguro.

O firewall protege a rede em ambos os sentidos, como o nome já diz, é como uma parede “corta-fogo”.

Mas tem coisas que um firewall não faz, como podemos ver abaixo:

- Não protege contra ataques que o atravessem, por exemplo, advindos de uma conexão VPN estabelecida.
- Não protege contra ameaças internas, como funcionários.
- Não protege contra infecção de vírus e outros tipos de malware, principalmente entre máquinas da rede interna.

Esses são alguns dos tipos de firewall que existem:

- Filtro de pacotes.
- Filtro de estado de sessão (inspeção de estado).

- Gateway de aplicação (proxy).
- UTM (gerenciamento unificado de ameaças).

Num filtro de pacotes, as regras são aplicadas a cada pacote IP que chega e então o pacote é encaminhado ou descartado. Esse firewall filtra os pacotes em ambas as direções (incoming e outgoing). As regras de filtragem são baseadas no conteúdo do pacote, como IPs de origem e destino, Nº de portas de comunicação, tipo de protocolo e interface de rede.

As regras são verificadas em sequência quando um pacote é analisado. Se houver correspondência entre uma regra e um pacote, a regras é aplicada e as subsequentes são ignoradas. Se nenhuma regra for encontrada para tratar o pacote, então uma regra padrão pode ser aplicada. As regras padrão pode ser descartas (drop/block/deny) e permitir (allow).

Os filtros de pacote apresentam alguns problemas:

- Não examinam dados das camadas superiores, assim não são efetivos contra ataques que explorem vulnerabilidades das aplicações.
- Log é limitado devido a pouca quantidade de informações em um pacote.
- Geralmente não suportam esquemas de autenticação de usuários.

Também podemos usar um outro tipo de firewall, o de filtro de estado de sessão, que funciona dessa forma:

- Aprimoramento do sistema de filtro de pacotes.
- Examina o status das conexões de redes ativas e determina quais pacotes aceitar ou não.
- Permite ou bloqueia tráfego de acordo com o estado, a porta e o protocolo.
- Monitora toda atividade a partir do momento em que uma conexão é aberta até que ela seja fechada.

Temos também o firewall pessoal, funcionando dessa forma:

- Um firewall pessoal é instalado no sistema operacional da máquina do usuário.
- Geralmente é implementado pelo S.O.
- Protege a máquina contra ameaças na rede externa e de outras máquinas na rede interna.
- Pode ser implementado como software de terceiros, incluindo pacotes de antivírus do tipo “Internet Security”.

Esses são alguns exemplos de firewalls pessoais:

- Firewall do Windows com Segurança Avançada.
- Linux Iptables.

- Norton Internet Security.
- Comodo Firewall.
- Karpersky Internet Security.
- Mc Afee Personal Firewall.

E temos também os firewalls de hardware (usando aparelhos físicos):

- Um firewall de hardware é um appliance dedicado, que consiste em um hardware específico com um software de firewall instalado.
- No geral, possui uma performance maior do que um firewall de software instalado em um servidor comum.

No firewall do Windows, podemos adicionar novas regras de entrada e saída, clicando com o botão direito na regra especificada, escolhendo o tipo de regra (como programa, porta, predefinida ou personalizada), a ação (permitir, permitir apenas se for segura ou bloquear a conexão), o escopo e o nome. Para excluir uma regra existente, basta clicar com o botão direito e excluir ela.

Podemos também usar firewall no Linux, no Ubuntu, por exemplo, podemos habilitar ele digitando *sudo ufw enable*. Para permitir tráfegos como por exemplo, os TCP e UDP na porta 22 (SSH), digitamos *sudo ufw allow 22* (ou para apenas os TCP, *sudo ufw allow 22/tcp*), e para verificar a porta requerida do SSH, *sudo ufw allow ssh*. Para excluir um deles use algo tipo *sudo ufw delete allow 22*, pra verificar todas as especificações, *sudo ufw status*, e para resetar tudo (e desativar) *sudo ufw reset*. Podemos também baixar uma interface gráfica para ele, digitando *sudo apt install gufw*.

O que é Proxy e VPN

Muita gente confunde o que é proxy com a definição de uma VPN. Embora ambos sirvam para mascarar o seu IP e impedir que você seja identificado na internet, a forma como atuam é bem diferente.

Um proxy é um serviço que age como um intermediário entre o usuário e a internet, recebe e repassa todas as suas requisições ao site que você está acessando. Dessa forma, o IP registrado nessas páginas acessadas é o do proxy e não o seu. Assim, sua identidade não fica exposta na rede, dificultando que você seja rastreado.

Neste ponto, muita gente pensa que um proxy e uma VPN são a mesma coisa, pois ambos possuem a mesma função, que é proteger a identidade do usuário na internet, mas, não é bem assim.

Embora uma VPN (Virtual Private Network) também possa ser usada para acessar serviços de outros países, e mascarar seu IP, ela

cria uma rede privada criptografada, blindando totalmente os dados entre o computador do usuário e o servidor VPN. Já o proxy é apenas um intermediário entre você e a internet e não criptografa nada.

Por isso mesmo, é normal utilizar mais de um proxy para realizar uma conexão realmente anônima, com cada servidor escondendo o IP do servidor anterior, dificultando o rastreio do usuário.

Assim como as VPNs, existem as versões pagas dos serviços de proxies, desenvolvidas por empresas confiáveis e que são mais seguras. Há também as versões gratuitas, mais vulneráveis a ataques e que podem acessar e repassar seus dados a terceiros, bem mais facilmente que uma VPN gratuita, dada a falta de criptografia. Por isso, tome muito cuidado com qual serviço você vai usar e proteja bem os seus dados.

PS: A rede Tor não deve ser confundida com nenhum dos dois, apesar da rede Tor usar proxies aleatórios com vários nós.

Como Desenvolver um Aplicativo Seguro

A segurança de aplicativos é mais predominante do que você poderia ter imaginado. Vamos falar sobre algumas ameaças comuns em segurança da aplicação e segurança do aplicativo, vulnerabilidades das quais você precisa estar ciente.

As principais vulnerabilidades em dispositivos são essas:

- **Spyware e Malwares**: Depois de instalado, ele pode comprometer todos os outros aplicativos no dispositivo do usuário, incluindo os baixados de fontes confiáveis.
- **Vazamento de Dados**: Em casos como os de dispositivos móveis, um usuário geralmente permite que um aplicativo baixado acesse outros dados no dispositivo, um malware pode transportar dados confidenciais sem serem detectados.
- **Software ou Sistema Operacional Obsoleto**: Softwares e sistemas mais antigos não conseguem identificar e interromper os ataques mais recentes, por não receber os patches de segurança.
- **Senhas Comprometidas ou Fracas**: Usar a mesma senha em várias contas é um risco, além de uso de senhas fáceis de serem quebradas ou adivinhadas.
- **Wi-Fi Público Inseguro**: A rede wi-fi pública pode estar sem criptografia ou mesmo ter algum malware ou monitoramento maliciosos. E nunca devem ser usadas para acessar serviços privados ou confidenciais, como dados bancários e cartões de crédito.
- **Ataques de Phishing e Smishing**: E-mails falsos podem te redirecionar para sites falsos visando roubar seus dados com

a técnica do phishing. O smishing concentra o ataque em mensagens de texto, que também contém um link que redireciona para sites falsos.
- **Engenharia Reversa**: Usando essa técnica, os invasores podem alterar o código-fonte, revelar os algoritmos de criptografia em uso e muito mais. Um exemplo de uso disso são os programas crackeados, que podem ser perigosos.
- **Dispositivos Roubados ou Perdidos**: A perda ou roubo de dispositivos (principalmente móveis) é outro risco sério, pois alguém com acesso físico ao dispositivo pode tentar passar pela tela de bloqueio.

E para garantir a segurança de aplicativos:

- **Criptografia de Dados**: Sempre que os dados são transferidos por meio do aplicativo, eles devem ser criptografados, para minimizar ataques de invasores e de engenharia reversa. Uma dica é criptografar o código-fonte.
- **Autenticação Forte de Alto Nível**: As autenticações fracas são o erro mais comum cometido ao projetar aplicativos, eles devem ser desenvolvidos de forma que apenas senhas fortes sejam aceitas. Uma outra dica é uma autenticação multifator, utilizando biometria.
- **Uso de Técnicas de Criptografia Atualizadas**: Algoritmos populares como MD5 e SHA-1 estão comprometidos. É aconselhável empregar técnicas mais confiáveis. Também deve-se realizar testes de penetração manuais e modelagem de ameaças antes dos aplicativos serem lançados.
- **Conexões de Rede Seguras**: O aplicativo deve ter medidas de segurança para impedir o acesso não-autorizado e proteger os dados se o aplicativo usar algum servidor. Podemos usar HTTPS (SSL ou de preferência, TLS) e VPN para isso.
- **Minimizar Permissões**: Você deve sempre evitar dar ao seu aplicativo muitas permissões, que nem sempre são necessárias. Lembre-se de que cada permissão solicitada pelo aplicativo é outra conexão que pode ser vulnerável.
- **Fique Alerta com Tecnologias de Detecção de Adulteração e Bibliotecas de Terceiros**: Você pode ativar as notificações usando métodos de quando um código nocivo é inserido. Devemos também implantar repositórios internos estruturados e empregar controles de política para proteger o sistema contra problemas de segurança.
- **Pratique Testes Repetidos**: A segurança do aplicativo deve passar por um processo contínuo e sem fim. Revise o código constantemente para encontrar falhas de segurança e corrija-as antes de publicá-las. Encontrar brechas no sistema é uma necessidade vital, pois podem se transformar em perigos reais.
- **Crie um Plano de Back-Up e Restauração**: A tecnologia está se desenvolvendo rapidamente e os invasores estão criando maneiras inteligentes de comprometer aplicativos e roubar

dados críticos. Precisamos proteger os aplicativos dos efeitos graves de uma violação com um plano de back-up e restauração. É altamente recomendado que os desenvolvedores forneçam aos usuários a opção de back-up de dados mais frequentes e armazenamento secundário.

O que é Bitcoin

Uma criptomoeda é uma forma de dinheiro digital, ou moeda virtual, desenvolvido para ser seguro e anônimo. Associadas a internet, as criptomoedas utilizam criptografia forte para gerenciar transferências de valores e pagamentos. Não são controladas por bancos, governos ou outras instituições. As criptomoedas usam tecnologia descentralizada para permitir que usuários realizem pagamentos seguros e enviem, recebam e armazenem dinheiro sem precisar usar seu nome ou passar por um banco ou outra instituição financeira, permitindo dessa forma a criação de moedas virtuais (crypyocurrencies).

O termo moeda virtual foi definido pelo Banco Central Europeu em 2014 como sendo “Uma representação digital de valor que não é emitida nem por um banco central ou autoridade pública, e nem é necessariamente ligada a uma moeda fiat (fiduciária), mas é aceito por pessoas naturais ou legais como meio de pagamento e pode ser transferida, armazenada ou negociadas eletronicamente”.

Antes do surgimento da primeira criptomoeda descentralizada, o Bitcoin, algumas tentativas de implementar um sistema de moeda digital foram realizados, como por exemplo:

- **B-Money**: Sistema de pagamentos eletrônico distribuído e anônimo, proposto por Wei Dai em 1998.
- **Bit Gold**: Moeda digital projetada por Nick Szabo em 1998.
- **Hashcash**: Sistema baseado em funções de hash criptográfico, com algoritmo Proof-of-Work (PoW)), proposto por Adam Back em 1997. O conceito de PoW foi reutilizado no processo de mineração de Bitcoins posteriormente.
- **RPOW**: Primeiro sistema de moeda baseado em PoW reutilizável, apresentado por Hal Finney em 2004. Hal Finney se tornou posteriormente o primeiro usuário de Bitcoin após Satoshi Nakamoto, recebendo a primeira transação em Bitcoin do próprio Nakamoto.

São baseadas em um registro digital (livro-razão) distribuído chamado de blockchain, que é um registro de todas as transações em moeda virtual atualizadas e mantidas pela rede de detentores de moedas. As criptomoedas são criadas por meio de um processo chamado de mineração, que envolve o uso do poder de processamento de computadores para resolver problemas complexos de matemática que validam as transações e geram moedas. De acordo com a Universidade de Cambridge, há em 2017 entre 2,9 e 5,8 milhões de

usuários distintos utilizando carteiras de criptomoeda, a maioria Bitcoin.

Muitas centenas de criptomoedas foram criadas, algumas com duração muito curta, outras criadas apenas com propósitos fraudulentos, outras ainda trazendo inovações tecnológicas adicionais e sendo negociadas ativamente nos mercados especializados. Existem hoje, literalmente, centenas de criptomoedas disponíveis na internet, das quais apenas um punhado é efetivamente negociada. No geral, os mecanismos de funcionamento e princípios básicos de operação da maioria das criptomoedas são derivadas do protocolo original Bitcoin, com modificações mais ou menos extensas sendo adicionadas.

Dois conceitos importantes para o entendimento do funcionamento das criptomoedas são o conceito de transação e o conceito de endereço:

- Endereço é uma string (conjunto) de caracteres que identifica uma carteira de criptomoedas e que permite realizar uma transação.
- Transação é o processo de transferir unidades monetárias de um endereço para outro, ou seja, enviar ou receber dinheiro ou efetuar um pagamento em criptomoeda. Esse processo da origem aos Blocos de Transações.

As criptomoedas, como o famoso Bitcoin e outras moedas relacionadas são baseadas em dois tipos distintos de estrutura de dados: Transações, que são agrupadas em blocos. Os blocos são encadeados usando hashes dos blocos anteriores na cadeia, formando uma estrutura de dados mais complexa autenticada chamada de blockchain. As transações e os blocos são distribuídas entre todos os nós participantes da rede por meio de um protocolo que roda sobre uma rede peer-to-peer (P2P). Um novo bloco é adicionado ao blockchain se um nó na rede consegue fornecer uma “prova de trabalho” (proof of work ou POW) para ele. O algoritmo PoW age como uma defesa contra ataques específicos e também permite que uma assinatura digital sem chave autentique os novos blocos, assim como o blockchain completo. Se um nó não considerar um bloco como válido, então esse bloco não será adicionado ao blockchain.

As transações, dessa forma, ficam armazenadas de forma definitiva no blockchain, imutável para sempre, e os usuários armazenam suas criptomoedas (na verdade, códigos que representam as criptomoedas) em softwares específicos denominados carteiras (wallets), que podem ser instaladas em um computador, smartphone, ou ainda serem hardwares especializados para armazenamento offline.

A principal criptomoeda em “circulação” atualmente é o Bitcoin, mas existem literalmente centenas de outras criptomoedas disponíveis. Classificamos essas outras moedas como “altcoins” (alternative coins, ou moedas alternativas) por serem alternativas à moeda dominante, que é o próprio Bitcoin. Alguns exemplos de

criptomoedas (altcoins) mais conhecidas são: Litecoin, Bcash, Peercoin, Namecoin, Dash, Dogecoin, Ripple e Ethereum.

O que é SAST e DAST

Uma preocupação que atinge todas as empresas refere-se a segurança dos seus sistemas e dados. Principalmente agora com a expansão dos aplicativos e soluções em nuvem.

E o SAST (Static Application Security Testing) e o DAST (Dynamic Application Security Testing) são soluções bem diferentes, indicadas para momentos diferentes, com benefícios variados e dentro do DevSecOps.

Elas são duas ferramentas muito importantes e usadas para localizar vulnerabilidades em um software, automatizando algumas barreiras de segurança e evitando que o fluxo de trabalho se torne lento.

O SAST, ou análise estática, é um teste de segurança que analisa o código-fonte para localizar vulnerabilidades que fazem com que os aplicativos fiquem vulneráveis a ataques. Ele pode ser definido como um software estático de teste de segurança de aplicativos. Deve ser utilizado mais no início e de preferência nos arquivos que possuem o código-fonte. Contudo, o método não consegue identificar fragilidades que surgem com a aplicação em produção.

O DAST, ou análise dinâmica, é um teste de segurança na qual um aplicativo em execução é testado de fora, o tratando como uma caixa preta. Ou seja, um testador que usa o modelo DAST examina um aplicativo quando ele está em execução e tenta “hackeá-lo”, simulando o que um invasor faria. Ele pode ser definido como um software dinâmico de teste de segurança de aplicativos.

O que é SSL e o Certisign

Novas tecnologias estão sendo cada vez mais usadas e implementadas para controles de acesso, tais como assinaturas digitais que garantem que o acesso vem mesmo da pessoa em questão.

A segurança também é um fator decisivo na aquisição e retenção de possíveis clientes dos vários sites online.

A segurança na transmissão de dados é um dos empecilhos para concretização de compras na rede pelo internauta e na divulgação de seus dados pessoais, como RG, CPF e número do cartão de crédito.

Um dos recursos mais utilizados para realização de negócios na internet entre comerciantes e clientes é a criptografia.

Um recurso de segurança muito popular é o Secure Socket Layer (SSL), comercializado pela Certisign, no Brasil. Esse protocolo garante a privacidade da transação, pois as informações transmitidas são criptografadas e somente o usuário e o servidor da empresa envolvidos no processo podem decodificar seu conteúdo.

Secure Socket Layer (SSL) é um padrão global em tecnologia de segurança desenvolvida pela Netspace em 1994. Ele cria um canal criptografado entre um servidor web e um navegador (browser) para garantir que todos os dados transmitidos sejam sigilosos e seguros. Milhões de consumidores reconhecem o “cadeado dourado” que aparece nos navegadores quando estão acessando um website seguro.

Quando escolher ativar o SSL no seu servidor web, você terá que responder algumas questões sobre a identidade do seu site (ex. a URL) e da sua empresa (ex. a Razão Social e o endereço). Seu servidor web então criará duas chaves criptográficas – a Chave Privada (Private Key) e a Chave Pública (Public Key). Sua chave privada não possui esse nome a toa – ela deve ser mantida privada e segura. Já a chave pública não necessita ser secreta e deve ser colocada na CSR (Certificate Signing Request) – um arquivo de dados contendo os detalhes do site e da empresa. Você deverá enviar esta CSR através do formulário de solicitação no site da certificadora, seu dados serão validados e se estiverem corretos, seu certificado digital será emitido.

Seu servidor web irá associar o certificado emitido com a sua chave privada. Seu servidor irá estabelecer um link criptografado entre seu website e o navegador do seu consumidor.

Em resumo, SSL é um tipo de segurança digital que permite a comunicação criptografada entre um site e um navegador. Atualmente a tecnologia se encontra depreciada e está sendo completamente substituída pelo TLS.

TLS é a sigla de Transport Layer Security, ou seja, um protocolo de segurança cuja finalidade é facilitar a segurança e privacidade de dados na internet.

Isso ocorre a partir do momento em que o TLS criptografa a comunicação entre os computadores e o servidor de hospedagem no momento em que um site é acessado. Contudo, sua aplicação também pode ser feita para criptografar mensagens de e-mail, Voip, entre outros meios de comunicação.

HTTPS é o uso de HTTP protegido por TLS/SSL.

Existem outros sites que geram certificados SSL para sites, incluindo as próprias hospedagens, que podem ser pagas ou gratuitas.

Como Instalar o Nmap e Zenmap no Linux

O Nmap é um software scanner de rede que é empregado para descobrir portas, serviços, computadores ativos, etc., ele faz isso enviando determinados pacotes para rede e avaliando as respostas recebidas.

Para instalar ele no Linux, digitamos simplesmente esses comandos:

sudo apt update

sudo apt install nmap

Para usarmos ele, no terminal digite *nmap 192.168.1.1* (substituindo pelo IP/site desejado).

Para instalarmos a interface gráfica Zenmap, digite esse comando:

sudo apt install zenmap

Indo nos programas do sistema, procure o Zenmap e execute ele como root.

Na caixa do alvo, colocamos o IP ou site desejado, o tipo de scanner. Colocamos o mesmo endereço do roteador como exemplo e um scan rápido (quick scan).

PS: Podemos digitar o comando no Zenmap também.

Também existe Nmap e Zenmap para outros sistemas Linux, além do Windows e Mac.

O que é um Backdoor?

O backdoor é um recurso utilizado por diversos malwares para garantir acesso remoto ao sistema ou à rede infectada. Para esse fim, os códigos maliciosos podem explorar falhas críticas não documentadas existentes em programas instalados, falhas características de software desatualizados ou do firewall, para abrir portas do roteador. Alguns backdoors podem ser explorados por sites maliciosos, através de vulnerabilidades existentes nos navegadores. As falhas podem garantir acesso completo ou parcial ao sistema por um cracker, sendo utilizadas para a instalação de outros malwares ou para o roubo de dados.

Em outras palavras, backdoor é um método de entrada deixado pelo cracker para que ele possa acessar livremente o sistema novamente com mais facilidade, já que ele já o explorou anteriormente.

O NetBus é um exemplo clássico de backdoor, sendo usado por diversos crackers na década de 1990 e início do século XXI. Nos últimos anos, uma das pragas do tipo mais disseminadas é o backdoor Brifost. Outros famosos backdorrs são o c99Shell, WebShell e RST.

Para proteger-se, mantenha atualizados os sistemas e os módulos que compõem todos os serviços, e deixe o firewall ativo. Outra forma de proteção de computadores pessoais é o IDS, sistema de detecção de intrusão, na sigla em inglês.

O que é o Shouder Surfing

O surfe de ombro, ou shoulder surfing em inglês, é uma técnica utilizada por pessoas mal-intencionadas para roubar informações valiosas de uma determinada pessoa ou organização.

Essa prática conhecida como visual hacking, é um ato utilizado para coletar informações por meios visuais e que não requer habilidades com computadores ou qualquer outro tipo de tecnologia.

Imagine o seguinte cenário, você precisa da segunda via de um boleto e entra em contato com a empresa para solicitar, imediatamente será necessário confirmar algumas informações para emitir o documento.

Enquanto você fornece os dados, alguém por perto pode escutar sua conversa. Mesmo que não esteja ouvindo a pessoa do outro lado da ligação, é possível deduzir a pergunta através da sua resposta. Após essa coleta de informações, o mal-intencionado pode se passar por você, com o seu nome, CPF, telefone, e-mail e endereço. Em posse destas informações já é possível ter uma conduta maliciosa, fingir ser outra pessoa e fraudar algum serviço oficial que seja utilizado por você com frequência.

Este exemplo esclarece as possibilidades de fraudes que podem ocorrer. Esta solicitação da segunda via do boleto poderia ser efetuada através de outro meio como app, website, etc., porém em uma análise mais aprofundada, percebemos os riscos em fornecer dados pessoais (sensíveis) em ambientes públicos ou em locais onde não conhecemos quem nos cerca. Por isso é crucial ter cuidados ao fornecer informações.

Ser observado enquanto digita no celular é uma sensação que todos nós já passamos, o problema é quando isso deixa de ser impressão e passa a ser real.

Muitos observadores fazem isso em filas, transporte público ou até na rua, basta uma brecha para ter seus dados escutados ou lidos.

Em um cybercafé, no trabalho ou local público, ter alguém de olho na sua tela é comum, seja por pura curiosidade ou má intenção. Fique atento ao se logar e evite clicar na “descoberta de senha” após inserir a password, pois isso facilita o trabalho do invasor.

Seja na fila, no trabalho ou no banco, evite ao máximo a exposição de suas informações, fique atento ao ambiente e observe ao seu redor. E se possível, prefira fornecer informações suas em locais reservados. Isso irá mitigar esse tipo de ataque, pois a maior vulnerabilidade está em como os usuários utilizam os sistemas e não nos próprios sistemas.

O que é Phishing

Phishing se refere a um conjunto de técnicas empregadas por bandidos digitais com o intuito de enganar usuários para que eles forneçam inadvertidamente informações sigilosas e valiosas. Geralmente, este tipo de ataque começa com o recebimento de um e-mail falso, ou ainda outra forma de comunicação cujo intuito seja enganar a vítima, como uma mensagem instantânea.

A mensagem enviada é forjada para se parecer com uma mensagem legítima, proveniente de uma fonte confiável ao usuário. Caso a vítima caia na armadilha, poderá ter informações confidenciais roubadas, comumente fornecendo esses dados em um website falso. Algumas vezes também é feito o download de software malicioso para o computador da vítima.

O phishing é um exemplo clássico de técnica de engenharia social empregada para enganar usuários de sistemas de computador.

Existem várias formas de se realizar ataques de phishing, dependendo de como é realizado e de quem são os alvos. Os mais comuns são os seguintes:

- **Whaling:** Quando um ataque de phishing tem por alvo uma figura de grande importância, como o diretor de uma grande empresa, o ataque é também conhecido como “whaling”, que significa basicamente “pesca à baleia”, pelo porte do usuário-alvo e alta possibilidade de retorno da “operação”. Este é um ataque de periculosidade elevada, devido à categoria de informações que podem ser obtidas.
- **Pharming:** Uma outra forma de phishing bastante comum é chamada de “pharming”, na qual os usuários são redirecionados a um website falso, mas que aparenta ser legítimo. Às vezes nem é necessário que o usuário clique em um link malicioso – é possível alterar registros DNS na máquina da vítima ou no servidor de hospedagem do site de modo a redirecionar as requisições de acesso ao site para uma página falsa, mesmo que o endereço correto do website seja digitado no navegador. É preciso tomar muito cuidado e sempre inspecionar minuciosamente o endereço que está sendo acessado, pois normalmente um endereço falso difere de um legítimo por diferenças mínimas, como um simples caractere.
- **Spear Phishing:** Também existe o conceito de spear phishing (“pesca com arpão”), no qual o alvo são indivíduos específicos, em vez de um grande grupo de pessoas aleatórias. Para tal, os atacantes podem pesquisar informações sobre o alvo em redes sociais e em outros locais, de modo a coletar informações suficientes para personalizar a comunicação empregada no ataque – o que a torna muito mais autêntica, e passível de êxito.
- **Clone Phishing:** Neste tipo de ataque, um e-mail legítimo, recebido anteriormente e contendo um anexo ou link tem seu conteúdo e endereços de destinatários recebidos alterados para criar um e-mail praticamente idêntico ou ainda totalmente clonado. O anexo ou link enviado no e-mail é substituído por uma versão maliciosa e, enviado a partir de um endereço de e-mail falsificado para que pareça ser proveniente do remetente original.

Na maior parte dos casos, meliantes querem obter vantagens financeiras, e fazem isso roubando números de cartão de crédito, senhas de acesso a bancos ou outros tipos de dados do gênero. Algumas vezes o phishing é empregado para obter dados de acesso a uma corporação, obtendo esses dados de funcionários incautos, como por exemplo dados de login em sistemas.

Além disso, é possível que um ataque de phishing seja escalado para um ataque mais elaborado, como por exemplo, a implantação de ransomware nos computadores de uma empresa.

O que é Malware

Malware é qualquer software ou trecho de código escrito com o intuito de ser prejudicial a sistemas, indivíduos e organizações.

No geral, os malwares são criados para:

- Roubar dados e informações importantes.
- Extorquir dinheiro.
- Danificar sistemas e prejudicar o funcionamento de dispositivos.
- Causar prejuízos a uma empresa.
- Testar a segurança.
- Como armas cibernéticas.

Esses são os tipos mais conhecidos de malware:

- Vírus.
- Cavalos-de-troia.

- Spyware.
- Worms;
- Ransomware.
- Bootnets.
- Rootkit.
- Keylogger.
- Adware.
- Cryptojacking (Cripto Mineração Maliciosa).
- Exploits.

No geral, malwares infectam as máquinas das vítimas por meio de cavalos-de-troia (trojans), links em e-mail de phishing e downloads fraudulentos.

Podem infectar quaisquer tipos de equipamento, como:

- PCs e Notebooks.
- Smartphones.
- Smart TVs.
- Tablets.
- Dispositivos IoT.

Os principais vetores de infecção dos malwares são:

- E-mails de phishing.
- Anexos de e-mail maliciosos.
- Links em documentos (tipo Office).
- Download de programas e arquivos.
- Navegação em sites específicos (drive-by).
- Pen-drives e mídias removíveis (menos comum).

Essas são algumas estatísticas:

- 38% dos malwares se escondem em arquivos do pacote MS Office.
- Um vazamento de dados causado por malware pode custar 3,86 milhões de Dólares pra empresas.
- Este ano (2019) as empresas devem pagar 11,5 bilhões de Dólares em resgates de ransomware.
- Prejuízo global com malware deve chegar a 6 trilhões de Dólares em 2021.
- Cerca de 24000 apps maliciosos são bloqueados por dia nas lojas de apps para smartphones.
- 70% das empresas não estão preparadas para enfrentar sequer o mais leve ataque.
- 60% dos ataques são direcionados a pequenas empresas.
- 90% dos ataques se iniciam com um e-mail de phishing.

Como detectar infecções:

- Lentidão “inexplicável” no sistema.
- Antivírus para de funcionar ou ser atualizado.
- Travamentos constantes.
- Arquivos que somem ou aumentam de tamanho.
- CPU com alta % de uso/ventoinha.

- Aumento na atividade de rede/internet.
- Desligamentos repentinos.
- Página inicial do navegador muda, e links não levam ao destino esperado.

Como se proteger de malware:

- Não confiar em desconhecidos online.
- Tomar cuidado com ataques de engenharia social.
- Verificar cuidadosamente tudo o que você baixa em sua máquina.
- Somente instalar softwares provenientes de fontes confiáveis.
- Cuidado triplo com os sites que visita.
- Não clicar em links de e-mail que sejam suspeitos ou não-solicitados.
- Sempre manter o firewall ativado.
- Possuir sempre back-up de seus arquivos importantes.
- Manter o sistema operacional sempre atualizado.
- E claro, usar antivírus sempre atualizado no computador.

Como se livrar de malwares:

- Identificar e conter a propagação da infecção.
- Identificar o malware.
- Eliminar o malware das máquinas com ferramentas apropriadas (antivírus/antimalware).
- Escanear o sistema completamente.
- Se necessário, instalar ferramentas para remoção de malware específico.
- Após remover o malware, trocar todas as suas senhas, do computador e de serviços online.
- Reinstalar o SO (se totalmente infectado).
- Restaurar back-up dos arquivos.

Podemos escanear os arquivos pra verificar se eles tem malwares passando o antivírus, mas também temos outras opções como sites voltados pra isso, tipo o Vírus Total.

Chaveiro Digital e Assinaturas com GPG no Linux

O GnuPG é um programa de software de criptografia híbrida, porque usa uma combinação de criptografia de chave simétrica (privada), e criptografia de chave assimétrica (pública) para facilitar a troca segura de chaves.

As chaves públicas resultantes podem ser trocadas com outros usuários de diversas maneiras. Elas devem sempre ser trocadas cuidadosamente para evitar falsificação de identidade. Também é possível adicionar uma assinatura digital à mensagem, para que a integridade e o remetente da mensagem possam ser validados.

Como sabemos, para criptografar um arquivo com senha, fazemos assim e ele pedirá a senha:

gpg -c arquivo.txt

Para descriptografar um arquivo, basta isso:

gpg arquivo.txt.gpg

PS: Se quiser ver o conteúdo de algum arquivo ao invés de salvá-lo descriptografado, use o comando *gpg -d arquivo.txt.gpg*.

Se ele for criptografado com sua chave pública, ele pedirá a senha de sua chave privada. Se for criptografado com senha, ele pedirá esta.

O chaveiro digital de um usuário é a reunião de todas as chaves de interesse de tal usuário. Esse chaveiro, geralmente, contém o par de chaves do usuário (pública e privada) e as chaves públicas de outros usuários. O chaveiro digital de cada usuário fica armazenado em *~/.gnupg* e pode ser visto com esse comando:

gpg –list-keys

PS: Se quiser listar apenas as chaves públicas, use *–list-public-keys*, assim como para listar as privadas, use *–list-secret-keys*.

Para criar um par de chaves (pública e privada), utilize esse comando:

gpg –gen-key

Para criar um par de chaves completo, utilize esse comando:

gpg –full-generate-key

Para listar as assinaturas existentes em uma chave, utilize esse comando (substituindo pelo número da chave, o mais comprido em hexa:

gpg –list-sigs 5A4F5F4F5452677F32E55A17D0ACBC71C8C023AB

Para exportar a sua chave pública como asc (para disponibilizar na internet, por exemplo), utilize o comando:

gpg -a –export 5A4F5F4F5452677F32E55A17D0ACBC71C8C023AB > arquivo.asc

Para exportar a sua chave privada (perigoso) como asc, utilize o comando:

gpg -a –export-secret-keys 5A4F5F4F5452677F32E55A17D0ACBC71C8C023AB > arquivo.asc

Para importar uma chave pública ou privada de um arquivo, fazemos assim:

gpg –import chave.asc

Para importar uma chave pública do servidor, é assim:

gpg –keyserver pool.sks-keyservers.net –recv-keys 0x416F061063FEE6

Podemos também procurar uma chave usando o e-mail associado a ela, assim:

gpg –auto-key-locate nodefault,wkd –locate-keys email@servico.com

Para criar um certificado de revogação:

gpg –gen-revoke 5A4F5F4F5452677F32E55A17D0ACBC71C8C023AB > cert.rev

PS: Sempre crie o arquivo de revogação de chave após criar a chave.

Para revogar uma chave, basta importar ela:

gpg –import cert.rev

Para remover uma chave privada do chaveiro:

gpg –delete-secret-keys 5A4F5F4F5452677F32E55A17D0ACBC71C8C023AB

Para remover uma chave pública do chaveiro:

gpg –delete-keys 5A4F5F4F5452677F32E55A17D0ACBC71C8C023AB

Para alterar a frase-senha de uma chave, utilize o comando:

gpg –edit-key 5A4F5F4F5452677F32E55A17D0ACBC71C8C023AB password

Depois digite *save* e dê enter.

Colocar chave pública no servidor online:

gpg –keyserver pool.sks-keyservers.net –send-key 5A4F5F4F5452677F32E55A17D0ACBC71C8C023AB

Para determinar a confiabilidade de cada chave, execute o comando:

gpg –update-trustdb

Para alterar a confiabilidade de uma chave, digite isso:

gpg –edit-key user@email.com

Digite *trust* para modificar a confiabilidade, para sair do gpg digite *save* (ou *quit*) e *help* para ajuda.

A opção edit-key também pode ser usada para renovar a data de expiração de uma chave, incluindo as já expiradas, usando os comandos *expire* para alterar os dados, e depois *save*.

Para listar as chaves, mostrando as assinaturas de cada chave, utilize o comando:

gpg –list-sigs

Para listar as impressões digitais de cada chave (fingerprint):

gpg –fingerprint

Para assinar uma chave pública de outra pessoa com sua chave privada, utilize o comando:

gpg –sign-key 5A4F5F4F5452677F32E55A17D0ACBC71C8C023AB

Para assinar arquivos digitalmente (no caso, arquivos de texto), usamos esse comando (com uma chave privada criada, obviamente):

gpg -s –clearsign arquivo.txt

Para assinar arquivos binários, usamos esse comando (com uma chave privada criada também):

gpg –detach-sign arquivo.tar.xz

Para checar a assinatura de um arquivo de texto, usamos esse comando:

gpg –verify arquivo.txt.asc

No caso de arquivos binários, no entanto, fazemos assim:

gpg –verify arquivo.tar.xz{.sig,}

Você pode atualizar as informações de chaves digitando:

gpg –refresh-keys

Você pode puxar informações de um servidor de chaves específico usando:

gpg –keyserver pool.sks-keyservers.net –refresh-keys

Para criptografar um arquivo com a chave pública de outro usuário, faça assim:

gpg -er usuario@email.com arquivo.txt

O comando que segue, pode ser usado para assinar seu arquivo com sua chave privada e, em seguida, criptografá-lo com a chave pública do destinatário:

gpg -ser usuario@email.com arquivo.txt

O Que é Biometria

Esses são os conceitos básicos de biometria:

- **Identidade Pessoal:** Conjunto de atributos de uma pessoa.
- **Gerenciamento de Identidade:** Permite estabelecer a associação entre um indivíduo e sua identidade pessoal.

Uma pessoa pode ser reconhecida com base em três métodos básicos:

- O que ela sabe.
- O que ela possui (extrinsecamente).
- O que ela é (intrinsecamente).

O roubo ou fraude de identidade ocorre quando uma pessoa se apossa da identidade de outro indivíduo ou afirma uma identidade falsa de modo a acessar recursos ou serviços para os quais ela não tem direito.

O reconhecimento biométrico pode ser definido como a ciência empregada para estabelecer a identidade de um indivíduo com base em características físicas e/ou comportamentais da pessoa, de forma total ou semiautomatizada. Características biométricas constituem uma ligação forte e razoavelmente permanente entre uma pessoa e sua identidade.

Um sistema biométrico é essencialmente um sistema de reconhecimento ou comparação de padrões que consiste em quatro blocos básicos de construção:

- **Sensor:** Interface de usuário que mede ou registra os dados biométricos brutos do usuário.
- **Extrator de Características:** Realiza pré-processamento nos dados brutos lidos do sensor.
- **Banco de Dados:** Repositório das informações biométricas e identidade pessoal.
- **Comparador (Sistema de Correspondência):** Módulo que compara amostras biométricas com dados armazenados no banco, para validar ou recusar uma identidade alegada.

A ciência do reconhecimento biométrico é baseada em duas premissas fundamentais dos traços biométricos: Singularidade e permanência.

- Um identificador biométrico é único (singular) apenas se duas pessoas no mundo podem ser diferenciadas com base nesse identificador.
- Já um traço biométrico é permanente se ele não muda ao longo do tempo de vida de um indivíduo.

Raramente essas duas premissas são totalmente válidas em sistemas biométricos reais.

Algumas das características biométricas mais comuns empregadas em sistemas incluem:

- Impressões digitais.
- Impressão da palma da mão.
- Íris.
- Rosto.
- Geometria da mão.
- Voz.
- Modo de andar.
- Retina.
- Assinatura.
- DNA.

Impressão digital é o padrão de cristas e sulcos na superfície da ponta de um dedo, cuja formação é determinada durante os primeiros sete meses do desenvolvimento do feto. As impressões digitais têm sido usadas em aplicações forense por mais de 100 anos.

As palmas das mãos contém padrões de cumes e vales como as impressões digitais. A área da palma é bem maior que a área de um dedo, e, por conta disso, as impressões de palmas podem ser mais distintivas que as impressões digitais. Também é possível explorar os padrões das veias nas palmas das mãos, que é diferente em todas as pessoas, mesmo em gêmeos idênticos.

Íris é a região anular do olho entre a pupila e a esclera (branco do olho). A textura visual da íris é formada durante o desenvolvimento fetal e se estabiliza durante os dois primeiros anos de vida (a cor continua a mudar por mais tempo). Como essa textura é muito complexa, pode ser usada para reconhecimento pessoal.

A vasculatura da retina é rica em estruturas e aparentemente distinta para cada indivíduo e cada olho. Alega-se que é o tipo de biometria mais seguro de todos, pois é praticamente impossível alterar ou replicar o padrão de veias na retina. Porém pode revelar condições médicas, como hipertensão. A taxa de erro de um scanner de retina é de cerca de 1 em 10 milhões.

Reconhecimento facial é um método não-intrusivo, e os atributos faciais são as características biométricas mais comuns empregadas pelos humanos para se reconhecerem entre si. Envolve a análise de características e padrões faciais para verificação e autenticação de um indivíduo. Pode empregar recursos avançados em IA.

Geometria da mão é um sistema baseado em um número de medidas tiradas da mão humana, incluindo formato, tamanho da palma, comprimentos e largura dos dedos, entre outras. A geometria das mãos não é muito distintiva, e por isso não pode ser escalonada para sistemas que necessitem identificar um indivíduo em uma população grande.

Modo de andar é um dos poucos traços biométricos que podem ser usados para reconhecer uma pessoa à distância. Consiste em uma câmera de vídeo que captura imagens de uma pessoa caminhando, considerando características como ângulos entre as articulações e silhuetas do indivíduo. É útil em cenários de vigilância onde a identidade de um indivíduo pode ser estabelecida de forma secreta.

A voz é a combinação de características biométricas físicas e comportamentais. As características físicas são invariantes para um indivíduo, pois dependem de suas cordas vocais, boca, nariz, etc., mas os aspectos comportamentais podem mudar ao longo do tempo, devido à idade, condição de saúde, estado emocional, etc. Não é apropriada para identificação em grande escala.

A forma como uma pessoa assina seu nome é uma característica do indivíduo. Uma assinatura requer contato físico com o instrumento de escrita (e esforço do usuário), e é uma técnica aceita em transações legais, governamentais e comerciais como forma de autenticação. Traço biométrico comportamental que pode mudar com o tempo, e ser influenciado por estados físicos e emocionais do assinante. Falsificadores são capazes de forjar uma assinatura e enganar um sistema de verificação.

Ácido Desoxirribonucleico (DNA), molécula que contém a informação genética necessária para o desenvolvimento e funcionamento de organismos vivos. Código unidimensional único para cada indivíduo, até mesmo em gêmeos idênticos. Usado em aplicações forenses para identificar suspeitos e vítimas, ou verificar a existência de laços familiares entre pessoas. Suscetível à contaminação, necessita de métodos químicos, e pode revelar informações privadas, como a existência de doenças no indivíduo.

Uma forma de melhorar a precisão de um sistema biométrico é usar mais de um traço em uma aplicação de reconhecimento, tornando-os mais confiáveis devido ao emprego de múltiplas peças de evidência. Esse tipo de sistema é denominado sistema multibiométrico ou ainda biometria multimodal. Combinando-se mais de uma forma de identificação biométrica, obtém-se um sistema de identificação ultra-seguro.

Estabelecer a identidade de uma pessoa com alto grau de confiabilidade é crítico em diversas aplicações. Alguns exemplos:

Forense	Governamental	Comercial
Identificação de cadáveres	Documentos para identificação de cidadãos	Controle de acesso a edifícios
Investigação criminal	Distribuição de benefícios	Caixas eletrônicos (ATM)
Testes de paternidade	Controle de fronteiras	E-commerce e e-banking
Localização de pessoas desaparecidas	Aplicações militares	Login em sistemas de computador

Sobre os sistemas de segurança:

- É importante perceber que um sistema de biometria é apenas um componente em uma solução geral de segurança, pois ele cuida apenas do aspecto da autenticação.
- Outras tecnologias como criptografia, assinaturas digitais, etc. são necessárias para atender aos critérios de confidencialidade, integridade e disponibilidade do sistema de informação como um todo.
- Assim, o sistema de biometria pode ser considerado como um subsistema no sistema de informação completo.

Em resumo, a biometria traz diversas vantagens quando comparada a sistemas de autenticação baseados em tokens ou informações conhecidas:

- Desencoraja a fraude e aumenta a segurança.
- Detecta duplicação de identidades.
- Não pode ser transferido, esquecido, perdido ou copiado com facilidade.
- Elimina alegações de repúdio.
- Aumenta a conveniência para o usuário.

Assim, sistemas de reconhecimento por biometria são reconhecidos como uma ferramenta poderosa e necessária para o gerenciamento de identidades.

O que é Engenharia Social

A engenharia social se define assim:

- Manipulação de alvos humanos em vez de tecnológicos ou outros mecanismos.
- Ataque não-técnico, que envolve interação humana com o objetivo de tentar enganar ou coagir a vítima a revelar informações sigilosas ou violar práticas de segurança.
- Inclui diversas atividades, geralmente maliciosas.
- Emprega regularmente técnicas de manipulação psicológica para enganar os usuários.

Roubo ou fraude de identidade ocorre quando uma pessoa se apossa da identidade de outro indivíduo ou emprega uma identidade falsa para acessar recursos ou serviços aos quais ela não tem direito.

E isso funciona pelos seguintes motivos:

- Falta de tecnologias apropriadas que possa combatê-la.
- Políticas de segurança insuficientes nas organizações.
- Difícil detecção e, por conseguinte, prevenção.
- Falta de treinamento de funcionários e usuários.

Ataques de engenharia social podem ter efeitos diversos em uma organização, impactando-a de diversas formas:

- Perdas econômicas.
- Terrorismo.
- Perda de privacidade.
- Processos judiciais.
- Encerramento temporário ou permanente.
- Perda de confiança.

Engenheiros sociais são bons em reconhecer sinais ou comportamentos que podem ser úteis na extração de informação, como:

- Obrigação moral.
- Confiança.
- Ameaça.
- Algo por nada.
- Ignorância.

Agressores costumam procurar alvos oportunos ou vítimas em potencial que tenham algo a oferecer. Alguns alvos comuns incluem:

- Recepcionistas.
- Pessoal de help desk.
- Administradores de sistemas.
- Executivos.
- Usuários em geral.

Ataques de engenharia social são realizados de diversas formas. Algumas técnicas de ataques comuns incluem os seguintes:

- Baiting (Isca de Links).
- Cavalos-de-troia.
- Scareware (Software Enganoso).
- Pretexting (Situação Inventada).
- Phishing.
- Spear Phishing.
- PNL (Programação Neurolinguística).

Para evitar esses ataques, é importante que os usuários sejam treinados em detectar determinados padrões. Alguns dos sinais que denunciam um ataque de engenharia social incluem:

- Uso de autoridade pelo atacante.
- Não fornecer informações de contato válidas.

- Fazer requisições informais ou fora de contexto.
- Usar repetidamente nomes de pessoas supostamente conhecidas.
- Uso excessivo de elogios (bajulação).
- Mostras de desconforto ou inquietação pelo atacante, quando questionado.

Algumas dicas para ajudar a se prevenir contra golpes:

- Não abra e-mails nem tampouco anexos vindos de fontes suspeitas.
- Fique esperto com ofertas muito tentadoras.
- Use autenticação baseada em mais de um fator.
- Confirme a identidade do suspeito antes de tomar ações.
- Peça um endereço de contato e diga que retorna posteriormente.
- Mantenha antivírus e softwares de segurança atualizados.

Casos interessantes:

- Partido Democrata dos Estados Unidos, 2016.
- Ubiquiti Networks, 2015.
- RSA, 2011.
- Kevin Mitnick, 1979.
- Sony Pictures, 2014.

Em resumo:

- Engenharia social se refere a um conjunto de técnicas de persuasão para obtenção de informações.
- O elemento humano é sempre altamente vulnerável e propenso a cometer erros.
- Causa grandes prejuízos a indivíduos e organizações.
- Políticas de segurança adequadas são necessárias para mitigar seus efeitos nefastos.
- Técnicas de segurança combinadas aumentam a proteção contra essa ameaça.

Como as Senhas são Descobertas

Como sabemos, as senhas podem ser descobertas por ataques como força-bruta ou dicionário, no entanto, senhas podem ser descobertas usando apenas a lógica.

Essas são algumas características de senhas bem óbvias:

- Área de trabalho ou estudo.
- Comportamento, como tipo de humor.
- Pessoas próximas (como amigos, familiares), ou animais de estimação.
- Características e gostos pessoais (como musical, esportivo, religioso).
- Números que podem ser obtidos baseados em datas, idade, documentos e outros.
- Senhas como “qwerty”, “12345678”, “password” e variações das mesmas também devem ser consideradas.
- Combinações mais fracas geralmente tem letras de palavras comuns combinadas com números (geralmente algo como “nomequalquer23” ou “exemplo55”), raramente com símbolos especiais.

Algumas formas de criar senhas fortes é combinar números, letras e símbolos (como por exemplo, “password” pode virar “Pa$sW0rD”).

Algumas das senhas mais comuns e fáceis de serem descobertas são essas:

- 12345
- senha
- qwerty
- password
- iloveyou
- abc123
- admin
- lovely
- qwertyuiop
- 12345678
- 654321
- welcome
- princess
- dragon
- login

Além das adivinhações usando a lógica, força bruta e dicionário, uma senha pode ser “farejada” por um programa sniffer caso a transmissão não seja criptografada, e também temos programas espiões como os keyloggers, que leem tudo que o usuário digita e envia ao hacker.

As senhas são salvas nos bancos de dados usando um algoritmo de criptografia, mas um hash pode ser descoberto por uma rainbow table, por isso podemos “salgar” a senha usando um valor aleatório junto ao hash para gerar um hash único.

No Windows, as senhas são armazenadas em *C:\Windows\System32\config* e *C:\Windows\repair*, em arquivos SAM criptografados (algumas versões antigas não criptografam). No Linux, as senhas são criptografas e guardadas em */etc/passwd* e */etc/shadow*.

PS: Não adianta nada usarmos senhas fortes se não se preocuparmos com a segurança dos sistemas, rede e programas.

Os Vários Tipos de Malware

Há uma variedade de ameaças que podem atacar os computadores. Em geral, todas elas podem ser classificadas como malwares. Por exemplo, um vírus de computador é um tipo de malware. Conheça vários tipos de malware:

- **Vírus:** Para atacar o computador, o vírus age se anexando a um programa hospedeiro já existente. Em seguida, altera o começo do programa para executar o código malicioso que foi inserido no programa original. O vírus infecta outros arquivos, inclusive pelo compartilhamento de rede, e pode criar novos executáveis. Com a alteração do registro do Windows, um vírus pode forçar a sua execução ao ser reinicializado o computador.

- **Worm:** Se o vírus necessita de um programa hospedeiro, o worm não precisa. Ele se propaga pela rede e infecta o computador explorando uma falhas de segurança (exploit) do sistema operacional ou de algum aplicativo.
- **Trojan:** O cavalo-de-troia é um tipo de malware que exige uma ação do usuário para se instalar, seja executando um anexo de e-mail ou realizando o download de um programa. Em grande parte das vezes, técnicas como phishing levam qualquer usuário a executar esse malware acreditando ser um programa inofensivo com alguma utilidade para o computador.
- **Rootkit:** É um software criado para permitir que hackers tenham controle sobre um computador ou rede, oferecendo ferramentas que podem roubar arquivos e informações sensíveis do usuário.
- **Backdoor:** O backdoor permite que um hacker comande o computador de forma remota e execute determinadas ações, como o download de outros malwares, o envio de dados do usuário e spams, além de ataques de negação de serviço (Denial of Service).
- **Botnet:** Uma botnet é um número de dispositivos conectados à internet, cada um executando um ou mais bots. As redes de bots podem ser usadas para executar ataques DDoS, roubar dados, enviar spam e permitir que o invasor acesse o dispositivo e sua conexão.
- **Adware:** Esse tipo de malware tem por característica exibir vários anúncios indesejados, levando, em alguns casos, o navegador a abrir sites com anúncios.
- **Spyware:** O spyware recolhe informações do computador, como os sites visitados pelo usuário, e os envia ao hacker. O principal objetivo desse tipo de malware é o roubo de senhas. Para isso, pode ser usado o keylogger, que captura senhas a partir do que é teclado pelo usuário. Ou o screenlogger, que captura a imagem ao redor do mouse quando o usuário clica, permitindo ao hacker o roubo de senhas dos teclados virtuais.
- **Downloaders:** Esses programas maliciosos, quando usados, instalam outros malwares.
- **Ransomware:** É um tipo de malware que restringe o acesso do usuário ao seu computador ou a arquivos até que seja pago um “resgate” para o hacker.

Com tantas ameaças, é bom manter o seu antivírus (ou antimalware) sempre atualizado.

O que é Hooking?

Hooking, do inglês enganchar, é um conceito que permite modificar o comportamento de um programa. É a chance que um código te dá para alterar o comportamento original de alguma coisa sem alterar seu código.

O aspecto prático de utilização dos hooks varia muito de ferramenta para ferramenta. A construção de módulos do drupal, por exemplo, é toda baseada em hooks. Quando vai salvar um post, exibir um bloco, exibir ajuda, deletar um comentário, em todas estas ocasiões o que o drupal faz é verificar se os módulos disponibilizam funções com determinado nome para acrescentes ou retirar alguma coisa do que será feito.

A principal vantagem dos hooks é não alterar o código original. Em todos os manuais de boas práticas de todas as ferramentas open-source que tem atualizações periódicas o mantra que se repete é não altere o core. Além de impossibilitar atualizações, quem vier depois para fazer manutenção não saberá da mudança e quem fica mal falado com isso é você e não a ferramenta.

O hooking também pode ser usado por código malicioso, como por exemplo, rootkits. As técnicas comumente utilizadas por rootkits para esconder ou alterar estruturas internas do sistema

operacional atacado podem inviabilizar sua detecção e monitoração por mecanismos de segurança ou outros métodos de análise, como no caso, o hooking.

O que é IDS e IPS

O IDS (Intrusion Detection System) e o IPS (Intrusion Prevention System), traduzindo, significam Sistema de Detecção de Intrusão e Sistema de Prevenção de Intrusão, respectivamente.

São recursos que examinam o tráfego na rede, para detectar e prevenir os acessos não autorizados na mesma, protegendo-a da exploração das vulnerabilidades.

IDS e IPS são tecnologias que fazem parte da segurança da informação, desenvolvidas para agregar a frente da proteção de dados, uma necessidade urgente para as empresas. Afinal, os ataques estão ocorrendo com muita força e em grandes proporções.

Já abordamos o significado das siglas IDS e IPS, mas existem mais questões que precisam ser compreendidas a respeito dos recursos.

Basicamente, ambos são partes da infraestrutura de rede. Eles comparam pacotes da rede em um banco de dados de ameaças cibernéticas (que contém assinaturas conhecidas), e sinalizam todos os pacotes correspondentes.

A principal diferença entre eles é que o IDS é um sistema de monitoramento, enquanto o IPS é um sistema de controle de intrusão, que impede que o pacote seja entregue com base em seu conteúdo, da mesma forma como um firewall impede o tráfego por endereço IP.

O que é RDP

RDP é o serviço disponibilizado pelo Windows para acesso remoto, o Microsoft Terminal Services. O acesso remoto possibilita que acessos externos sejam feitos a equipamentos, que, muitas vezes, estão na rede interna da empresa. Isso facilita atividades como administração remota ou suporte remoto, porém abre uma brecha significativa que pode ser explorada em ataques. O firewall tem que liberar a porta TCP 3389 para que o RDP funcione, e, já que o firewall possibilita essas conexões, os ataques passam diretamente pelo firewall.

O firewall bloqueia tráfegos baseado em suas regras, que são basicamente as origens, os destinos e os serviços/portas liberadas pela empresa. No caso do RDP (porta TCP 3389), a regra deve definir quem pode fazer o acesso remoto a quais equipamentos da empresa. Uma vez liberado o tráfego desse protocolo, o suporte técnico, por exemplo, pode acessar os equipamentos via Microsoft Terminal Services, em que uma senha de acesso é solicitada. O hacker também pode explorar esse acesso ao serviço para realizar os ataques.

Uma vez descoberta a senha de acesso ao equipamento via RDP, o hacker passa para o passo posterior, que visa ao domínio do equipamento ou servidor. Ele desabilita o antivírus e o firewall, além de criar contas adicionais e descobrir outras credenciais da rede. Outra medida dele é a instalação de backdoor, que abre uma porta no servidor para que acessos posteriores possam ser feitos diretamente pelo atacante.

Caso a empresa precise utilizar o RDP, é recomendável que a porta padrão seja alterada. Porém, isso apenas minimiza a possibilidade de ataque. Outra medida importante é habilitar controles de autenticação, como o travamento em caso de tentativa de ataque de força bruta.

Definição do Ataque Man-in-the-Middle

O objetivo da maioria dos hackers, independente de seus negócios, é roubar informação do usuário. Seja através de ataques discretos e individuais ou em grande escala por meio de sites populares e bancos de informação financeira. Quase sempre os invasores começa tentando inserir algum malware na máquina do usuário para depois percorrer um curto caminho até você e sua informação. Se por alguma razão este plano der errado, eles poderão utilizar-se de outro ataque popular conhecido como man-in-the-middle. Como o próprio nome sugere, nesta modalidade o hacker coloca suas armadilhas entre a vítima e sites relevantes, como sites de bancos e contas de e-mail. Estes ataques são extremamente eficientes e difíceis de detectar, especialmente por usuário inexperientes ou desavisados.

O conceito por trás do ataque MITM é bastante simples e não se restringe ao universo online. O invasor se posiciona entre duas partes que tentam comunicar-se, intercepta mensagens enviadas e depois se passa por uma das partes envolvidas. O envio de contas e faturas falsas poderia ser um exemplo desta prática no mundo offline, o criminoso as envia ao correio das vítimas e rouba os cheques enviados como forma de pagamento. No universo online, os ataques são mais complexos. Apesar de basear-se na mesma ideia, o invasor deve permanecer inadvertido entre a vítima e uma instituição verdadeira para que o golpe tenha sucesso.

Na forma mais comum de MITM o golpista usa um roteador wi-fi como mecanismo para interceptar conversas de suas vítimas, o que pode se dar tanto através de um roteador corrompido quanto através de falhas na instalação de um equipamento. Numa situação comum o agressor configura seu laptop, ou outro dispositivo wireless, para atuar como ponto de wi-fi e o nomea com um título comum em redes públicas. Então quando um usuário se conecta ao roteador e tenta navegar em sites delicados como de online banking ou comércio eletrônico, o invasor rouba suas credenciais.

Num caso recente, um hacker usou debilidades na implementação de um sistema criptográfico de uma rede wi-fi real e a usou para capturar informações. Este é a situação mais incomum mas também a mais lucrativa. Se o agressor for persistente e acessar o equipamento hackeado por dias e horas a fio, terá a possibilidade de espiar as sessões de seus usuários silenciosamente fazendo com que deixando as vítimas à vontade para usar informações delicadas durante a navegação.

Uma versão mais recente do ataque MITM é chamada man-in-the-browser. Nesta variável o agressor usa um dos inúmeros métodos para implementar um código daninho no browser do computador de suas vítimas. O malware silenciosamente grava informações enviadas a vários sites harcodeados. Esta modalidade tem se popularizado ao longo dos anos porque possibilita atacar a um grande volume de usuários por vez e mantém o criminoso a uma distância segura (para ele) de suas vítimas.

Existem diferentes maneiras de defender-se dos ataques MITM, mas a maioria delas deve ser instalada nos roteadores/servidores e não são 100% seguras. Existe também a técnica que aplica uma criptografia complicada entre o cliente e o servidor. Neste caso o servidor pode identificar-se apresentando um certificado digital para que o cliente possa estabelecer uma conexão criptográfica e envie informação delicada através da mesma. Mas esta possibilidade de defesa depende de que ambos os servidores tenham tal criptografia habilitada. Por outro lado, usuários podem proteger-se

de ataques MITM evitando conectar-se a wi-fi livres ou instalando plugins como HTTPS Everywhere ou ForceTLS em seu navegador, tais programas selecionarão apenas conexões seguras, sempre que estas estejam disponíveis. De todas as maneiras, todas as estratégias de defesa possuem limitações e há provas de que vírus como SSLStrip ou SSLSniff podem driblar a segurança de conexões SSL.

Entendendo os Exploits

A definição geral de exploits é que eles são programas ou códigos projetados para abusar de vulnerabilidades de software ou hardware e causar efeitos indesejados pelos desenvolvedores ou fabricantes. Para melhor entendimento, pense nas falhas de programas como uma fruta no alto de uma árvore, e no exploit como a escada que você usa para alcançar o alimento.

Os exploits podem ser usados para muitas coisas, como permitir que jogos piratas funcionem em consoles de videogames, instalação de sistemas operacionais customizados em celulares e, claro, infecção de dispositivos com agentes maliciosos.

Como os exploits se aproveitam de vulnerabilidades nos sistemas e aparelhos, a responsabilidade pelo bloqueio de suas funcionalidades é dos desenvolvedores, normalmente através de atualizações de firmware e software.

Normalmente, desenvolvedores de software e fabricantes de hardware classificam exploits de duas formas:

- **Exploits Conhecidos:** São todos aqueles já descobertos pelos pesquisadores de segurança cibernética, e que já podem ter sido corrigidos pelos desenvolvedores e fabricantes responsáveis, por meio de atualizações de segurança.
- **Exploits Desconhecidos:** Normalmente, são aqueles feitos a partir de falhas de dia zero e fazem com que os desenvolvedores de software e fabricantes de hardware corram para liberar uma atualização inutilizando-os. Enquanto a correção não sai, é comum que criminosos virtuais foquem a maioria de seus golpes ao redor deles.

Para um ataque de exploit acontecer, os criminosos precisam conhecer vulnerabilidades do sistema que pretendem invadir, para assim desenvolver métodos que aproveitem característica para penetrar no dispositivo.

Como muitas vezes o desenvolvimento do código de um exploit pode ser demorado, muitos criminosos optam por comprarem krits prontos em lugares como a Dark Web e a Deep Web, que permitem a exploração de vulnerabilidades de sistema, conhecidas ou desconhecidas, sem precisar da expertise em programação.

Outra forma de ataque exploit utiliza um código que se espalha por uma rede em busca de máquinas com vulnerabilidades, sem precisar de nenhuma interação com o usuário. Esse tipo é considerado um dos mais preocupantes, possibilitando que ameaças como o WannaCry, ataque virtual que se destacou em 2017, infectem milhões de computadores pelo mundo.

Independente do ataque de exploit usado, os próximos passos do golpe dependerão dos objetivos dos criminosos, como vazamento de dados, ataque de sequestro virtual (ransomware) e espionagem virtual são só alguns exemplos do que pode acontecer após uma invasão desse tipo.

SQL Injection e Falhas XSS

A injeção de SQL ocorre quando dados inseguros são enviados ao interpretador como parte de um comando ou consulta. Os dados alterados são enviados pelo invasor visando enganar o interpretador para que este execute os comandos maliciosos ou permita o acesso a dados não autorizados. Considerado um dos grandes desafios das aplicações web, o SQL injection tomou o posto principal em uma análise realizada pela OWASP, quando um ataque obtém sucesso, o invasor poderá ter acesso ao banco de dados da aplicação.

Os vetores de ataque são simples, baseados em textos enviados pelos atacantes, visando explorar a sintaxe do interpretador onde praticamente qualquer fonte de dados pode ser considerada como um vetor de injeção, inclusive fontes internas. Já as vulnerabilidades de segurança exploradas no SQL injection, quando uma aplicação envia dados não confiáveis a um interpretador, os impactos técnicos poderão resultar em perda ou corrupção de dados, negação de acesso e, em alguns casos, poderá acarretar no comprometimento completo do servidor. Finalmente, os impactos no negócio são que a reputação e as atividades da empresa poderão ser totalmente prejudicadas, já que os dados podem ser roubados, modificados ou excluídos, perdente a confidencialidade, integridade e até mesmo disponibilidade das informações.

Uma aplicação está suscetível a SQL injection se os interpretadores não separam dados não confiáveis dos comandos ou consultas, para se proteger de tal ação deve-se utilizar variáveis de ligação nos procedimentos armazenados e instruções preparadas buscando também não realizar consultas dinâmicas. Analisar o código-fonte é uma forma eficaz de se identificar se os interpretadores estão sendo utilizados de maneira segura, os testes de invasão por meio de exploits podem ajudar a confirmar se tal vulnerabilidade está presente.

A prevenção do SQL injection deve ocorrer buscando manter os dados inseguros separados das consultas e comandos, a forma preferida de prevenção é por meio de interfaces de programação de aplicativos (API) que buscam evitar totalmente o uso de interpretadores, o seu uso deve ser cuidadosamente avaliado pois podem ocorrer injeções em segundo plano se utilizados incorretamente, caso não seja utilizado um API deve-se efetuar a filtragem dos caracteres especiais utilizados para tal finalidade maliciosa.

Já as falhas de XSS residente ocorrem sempre que uma aplicação recebe dados não confiáveis e os envia ao navegador sem validação ou filtro adequados. Permite aos agentes de ameaça executarem scripts no navegador da vítima que podem obter sessões do usuário, desfigurar sites, ou redirecionar o usuário para sites maliciosos.

Diferente da injeção de SQL que busca executar instruções SQL maliciosas em consultas no banco de dados, ocorrendo fora da vista dos usuários, o XSS residente busca executar marcações maliciosas ou códigos Javascript em valores que serão mostrados em uma página web. Este tipo de ataque busca enganar o usuário que tem confiança em um site levando-o a executar uma ação ou exibição de informações para um outro site não confiável.

As vulnerabilidades relacionadas ao XSS residente estão ligadas a não filtragem de todas as entradas enviadas pelos usuários bem como a não avaliação da segurança das informações na entrada antes que seja incluídas na página de saída. Sem um filtro apropriado, as entradas fornecidas serão consideradas conteúdos ativos no navegador, existem algumas ferramentas que podem localizar algumas falhas de XSS automaticamente, entretanto cada aplicação possui páginas de saída diferenciadas utilizando interpretadores diversos juntamente com o navegador, como Javascript, Flash, Silverlight e ActiveX, causando maior dificuldades para uma detecção

automatizada, assim necessitando de uma análise manual, bem como testes de invasão para análise das vulnerabilidades. Prevenir os ataques por XSS consistem na separação de dados inseguros do conteúdo ativo do navegador, assim deve-se efetuar uma filtragem total dos dados inseguros baseados no contexto HTML (corpo, atributo, CSS ou URL).

Como o Spoofing Funciona

O spoofing (falsificação) funciona assim: Um cibercriminoso se finge ser outra pessoa ou entidade para enganar alguém. Assim que o cibercriminoso ganha a confiança da vítima, o perigo é iminente. Spoofers de e-mail, telefone e SMS enganam as vítimas para que elas entreguem informações pessoais, que podem levar a fraudes financeiras ou roubo de identidade.

Cibercriminosos usam frequentemente spoofing de e-mail para iludir as vítimas em golpes de phishing. Outros tipos de spoofing visam redes em vez de indivíduos, com o objetivo de espalhar malware, roubar dados, contornar sistemas de segurança ou preparar ataques subsequentes.

Como o spoofing se baseia em enganação, impedir e detectar esses ataques pode ser complicado. Por isso, é muito importante se proteger com uma segurança de internet forte e confiável. O antivírus escaneia constantemente se há ameaças e protege contra os tipos de ataque de phishing e malware que os spoofers adoram.

A diferença entre spoofing e phishing é que, embora o spoofing use a identidade de outra pessoa, os ataques de phishing tentam acessar informações confidenciais. Golpes de phishing comuns envolvem “atrair” as vítimas com uma isca, como e-mails falsos, e fazer com que elas forneçam dados pessoais que podem ser usados para roubo de identidade.

Ataques de spoofing fazer parecer que as comunicações do cibercriminoso são confiáveis, porque imitam a aparência de fontes confiáveis. Muitos phishers usam o spoofing para fazer com que as vítimas acreditem que o e-mail que usam é legítimo. Esse tipo de engenharia social manipuladora é usada pelos golpes de phishing para convencer as vítimas a divulgar informações pessoais.

Como mencionamos, há vários tipos de spoofing. Spoofing no nível de DNS ou endereço IP é diferente de phishing, pois envolve métodos técnicos para enganar um computador ou um sistema. Por exemplo, “typosquatting” é um tipo de ataque de spoofing que usa erros comuns que as pessoas cometem ao digitar URLs para fazer com que pensem que acessaram o site correto.

Porém, spoofing de e-mail e phishing são muito parecidos e muitas vezes são usados juntos.

Cibercriminosos mais inteligentes usam spoofing para tornar os e-mails de phishing ou as mensagens SMS muito mais convincentes e aumentar as chances de sucesso.

O spoofing de site ocorre quando um cibercriminoso cria um site falso que parece legítimo. Ao fazer login, o cibercriminoso obtém suas credenciais.

Às vezes, spoofers mal-intencionados usam um URL disfarçado, que redireciona você para o sistema deles e coleta suas informações pessoais. Eles podem até disfarçar o verdadeiro URL de destino, inserindo caracteres de controle especiais que contêm um significado diferente dos caracteres exibidos. Frequentemente, como no “typosquatting”, o URL é tão parecido com o endereço pretendido que você pode não notar a diferença.

Spoofing de IP acontece em um nível mais profundo da internet do que o spoofing de e-mail. Quando um cibercriminoso usa o spoofing de IP, ele está lidando com um dos protocolos web mais básicos. Todo dispositivo se conecta à internet de um endereço IP, uma cadeia de números que informa aos outros onde ele está. Quando o dispositivo envia e recebe informações, ele usa pacotes de dados que podem encontrar o endereço IP do dispositivo.

Muitas redes fechadas são configuradas para aceitar apenas pacotes de um intervalo pré-aprovado de endereços IP. Essa medida de segurança impede o ingresso de dispositivos desconhecidos. Um cibercriminoso pode usar um ataque de spoofing de IP para alterar o endereço IP do seu dispositivo e enganar uma rede segura para permitir a invasão. Você pode ocultar seu endereço IP para evitar que ele seja usado como disfarce.

Buffer Overflow: O Que é Como Funciona

Um buffer overflow (ou transbordamento de dados) ocorre quando um programa em execução tenta gravar dados além do que o buffer de memória permite, sobrecarregando o sistema operacional. Este tipo de falha é usada por cibercriminosos para executar código arbitrário em um computador, de modo que em muitos caso eles conseguem obter o controle do dispositivo da vítima ou executar um ataque de negação de serviço (DoS).

Na verdade, um buffer overflow ocorre quando um aplicativo não conta com os controles de segurança necessários em seu código de programação. Deve-se destacar que, para realizar um transbordamento de dados, é necessário ter conhecimentos de programação, bem como noções básicas de arquitetura de sistemas operacionais.

O princípio operacional de um buffer overflow anda de mãos dadas com a arquitetura do processador no qual um aplicativo vulnerável é executado, seja ele de 32 bits ou 64 bits. Os dados inseridos em um aplicativo são armazenados na memória de acesso aleatório, em uma área conhecida como buffer. Um programa devidamente projetado estipula um tamanho máximo para os dados de entrada e garante que esse valor não seja excedido.

As instruções e os dados de um programa em execução são armazenados temporariamente na memória, em uma área chamada de pilha. Os dados que ficam depois do buffer contêm um endereço de retorno (chamado de ponteiro de instruções) que permite que o programa continue seu tempo de execução. Se o tamanho dos dados for maior que o buffer, o endereço de retorno é sobrescrito e o programa lerá um endereço de memória inválido, causando uma violação de segmento no aplicativo. Qual é o risco de segurança nisso?

Um cibercriminoso com sólidos conhecimentos técnicos pode garantir que o endereço de memória sobrescrito corresponda a um endereço real, por exemplo, um que esteja localizado no mesmo buffer. Ao inserir as instruções no buffer (o código arbitrário), torna-se fácil executar essa instrução. Desta forma, é possível incluir instruções no buffer que permitem a abertura de um intérprete de comandos (como um shell), o que pode fazer com que um atacante assuma o controle do sistema. Este código arbitrário que permite a execução do intérprete de comandos é conhecido como código de shell ou shellcode.

Como vimos anteriormente, essa falha pode ser encontrada em sistemas operacionais, em outros tipos de aplicativos de terceiros e até mesmo em protocolos. Nestes casos, o ideal é realizar a leitura das falhas que são corrigidas através de atualizações dos aplicativos e sistemas operacionais – a instalação de atualizações corrige este tipo de erro, fechando brechas que podem facilitar a ocorrência de um vazamento de dados.

A adoção de uma política de atualizações, em conjunto com uma solução de segurança, ajuda a evitar exploração desses bugs na programação de aplicativos.

O Que é HoneyPot

Essa expressão típica brasileira está ligada diretamente ao honeypot em segurança digital. Ao traduzir para o português, honeypot significa “pote de mel”, algo doce e gostoso que pode atrair predadores. Essa é a função básica do honeypot, atrair os invasores para uma armadilha.

O honeypot é um sistema conectado à rede e configurado como chamariz para atrair os ataques cibernéticos detectando, desviando e estudando as tentativas dos hackers em obter acesso não autorizado aos sistemas de informação.

A função de um honeypot é se apresentar na internet como um alvo potencial para invasores – geralmente, um servidor ou outra fonte de alto valor – e coletar informações, notificando os defensores – white hats – sobre quaisquer tentativas de acesso à isca por usuários não autorizados.

Basicamente, o hacker atua roubando dados e informações, mas ao cair no honeypot, ele estará dando informações para os defensores do sistema. Se o usuário, por exemplo, fosse responsável pela segurança de TI de um banco, poderia configurar um sistema honeypot que, para que mestá de fora, se parece com a rede do banco.

Ao monitorar o tráfego para esses sistemas isca, pode-se entender melhor de onde vêm os criminosos, como operam e o que desejam. Mias importante, pode-se determinar quais medidas de segurança estão funcionando – e quais podem precisar de melhorias – simplesmente como estão praticando a invasão. É um verdadeiro “raio-X” sobre a forma de agir do determinado hacker.

Usualmente, esse tipo de ferramenta vem sendo utilizada em sistemas de alto poder de destruição na mão dos hackers, principalmente envolvendo o público e risco de vida, onde a ação de um invasor pode tornar um ataque terrorista em potencial.

Pesquisadores e defensores – white hats – usam honeypots para expor vulnerabilidades com dispositivos médicos, postos de gasolina, sistemas de controle industrial usados para atividades como controle de redes de energia elétrica, abertura de comportas de hidrelétricas, etc.

Dada toda a atenção que os bandidos recebem por seus esforços de invasão e violação de dados, é bom saber que os protetores de sistemas têm alguns truques para ajudar na proteção contra os ataques cibernéticos. Ao passo que mais dispositivos e sistemas se conectam à internet, a importância de lutar contra aqueles criminosos que usam a rede como uma arma só vai aumentar, os honeypots podem ajudar na proteção dos sistemas.

Como Criar e Armazenar Senhas Seguras e PINs e Passphrases

Contas e senhas são atualmente o mecanismo de autenticação mais usados para o controle de acesso a sites e serviços oferecidos na internet. É por meio das suas contas e senhas que os sistemas conseguem saber quem é o usuário (autenticação) e definir as ações que ele pode (ou não) realizar (autorização).

Uma senha é um dado secreto, geralmente uma sequência de caracteres, empregada para confirmar a identidade de um usuário em um sistema. Sendo assim, é um mecanismo de autenticação baseado em algo que somente você sabe – um segredo, portanto. As senhas são comumente empregadas em conjunto com um nome de usuário, constituindo desta forma um par de valores para autenticação em um sistema.

Se os caracteres que compõe a senha são obrigatoriamente apenas numéricos, a senha é comumente chamada de PIN – Personal Identification Number. Um exemplo clássico são as senhas de autorização de transação de cartão de crédito ou de contas bancárias.

Já uma sequência de palavras ou de cadeias de caracteres separadas por espaços é chamada de passphrase (ou frase secreta), funcionando de forma similar à de uma senha, porém geralmente mais seguras (por serem mais longas).

Técnicas empregadas para descobrir senhas:

- Palpites inteligentes.
- Ataques de dicionário.
- Ataques de força bruta.
- Rainbow tables.
- Engenharia social.
- Softwares, como keyloggers e sniffers.
- Exploração de vulnerabilidades em sistemas.

Podemos usar sites para testar a segurança de senhas.

Como escolher uma senha segura e memorizável?

Algumas técnicas que empregamos para criar senhas seguras incluem:

- Combinar duas ou mais palavras não relacionadas entre si, e alterar algumas das letras para caracteres especiais ou números (como exemplo: *C@qu1_P1ngu1m_$0rt&10*). Preferencialmente empregue palavras relacionadas a assuntos que você não costuma ter interesse.
- Pense em uma frase, e tome a primeira letra de cada palavra tomando o cuidado de alterar algumas das letras para símbolos e números (exemplo: *ePc0mdcCmN@lDp*, retirada da frase “Eu posso calcular o movimento dos corpos celestes, mas não a loucura das pessoas”, de Isaac Newton.

O que evitar ao criar uma senha:

- Nome do seu animal de estimação, de membros da família, amigos, pessoas famosas.
- Datas de aniversário em geral e local de nascimento.
- Algo relacionado ao seu time favorito (de futebol ou outro esporte qualquer).
- A palavra “senha” ou sequências como “123” ou similares.
- Palavras relacionadas a hobbies que você tenha.

Os Pilares da Segurança da Informação

Basicamente, temos cinco pilares na segurança da informação, que são estes:

Confidencialidade

Esse é o mais importante dos pilares, um dos exemplos disso era a cifra de César. Ou seja, se gerarmos dados, queremos que eles não sejam disponíveis para todas as pessoas. Absolutamente ninguém pode ter acesso a 100% dos seus dados, nem mesmo um banco, parente ou etc., e vale pra tudo, não apenas a informática. Resumindo, é algo que nós queremos que ninguém saiba (como senhas, por exemplo, como as de redes sociais ou de bancos, por exemplo).

Integridade

Quando enviamos uma mensagem ou dados pra alguém (como um banco), devemos manter a integridade desses dados, de modo de que eles não sejam alterados por ninguém além do remetente e do destinatário, para isso podemos usar um algoritmo de criptografia que ninguém além das duas partes que se comunicam, terá acesso.

Disponibilidade

É quando temos disponível o acesso aos dados para utilizarmos em ambos os lados da comunicação, mesmo criptografados pra quem não tem acesso aos mesmos, como a de um cliente e um servidor. Quando alguém tira um site do ar, por exemplo, temos a afetação desse pilar. É diferente de quando roubam dados de um servidor como a de um cartão de crédito, pois este afeta a confidencialidade.

Autenticidade

É você provar que você é você mesmo, ou que algo é realmente verdadeiro. Um exemplo disso são os “captchas” que verificam se alguém realmente é humano, por exemplo. As senhas são um exemplo popular de autenticidade, mas também um dos mais fracos. Biometria é outro exemplo disso.

Legalidade

Existe uma lei sobre crimes cibernéticos que punem tudo ilegal envolvendo dados de pessoas físicas ou jurídicas, visando proteger dados de todos. Isso vale pra tudo e todos, não apenas para informática ou dispositivos eletrônicos. Por exemplo, se guardamos os dados de alguém (como telefone e CPF) num caderninho e trancamos no cofre, e esse caderninho some, devemos obrigatoriamente avisar essa mesma pessoa, o mesmo acontece com sistemas informáticos.

PS: A sigla desses pilares é conhecida como “CIDAL”.

Termos de Segurança da Informação

O termo hacker geralmente é usado por leigos para falar dos invasores de sistemas e programas, até porque quando um computador, conta ou relacionado é invadido, falamos que eles foram “hackeados”. Existe sim a diferença entre os tipos de hacker, já que nem sempre o hacker é o que faz o “mal” na informática (estes costumam ser chamados de crackers).

Existem vários tipos de hackers, os mais conhecidos são esses (todos esses abaixo tem basicamente o mesmo conhecimento avançado):

- **White Hat:** É o hacker “bonzinho” ou ético, que procura falhas em sistemas e programas visando corrigir as mesmas.
- **Black Hat:** É o hacker “do mal”, que usa seu conhecimento para crimes e coisas ilegais.
- **Gray Hat:** É um meio-termo entre os dois anteriores, um hacker que age dos dois lados.

O cracker, também conhecido como “black hat”, é o que usa seu conhecimento para o mal, inclusive, o termo é muito usado em alterações de softwares pagos para torná-los ativos, como por exemplo “Windows crackeado”.

O newbie é o hacker iniciante, inclusive é deste nome que vem a palavra “noob” (geralmente com uso pejorativo.

O lammer é quem conhece muito pouco sobre hacking, basicamente é o cara que usa ferramentas prontas pra invadir sistemas e crackear programas.

O phreaker são os hackers voltados aos sistemas telefônicos, principalmente analógicos, menos comuns hoje em dia. Um exemplo é quando se burla o sistema telefônico pra fazer uma ligação internacional de graça, se usando de códigos secretos e até sons específicos.

PS: Um invasor de smartphones não é considerado um phreaker, até porque os atuais celulares temos sistemas mais próximos dos computadores (os dois sistemas mais usados são baseados em sistemas computacionais, como o Android que é baseado no Linux e o ISO no BSD) do que dos telefones analógicos.

Computadores

Um computador é algo que realiza a computação, e não engloba só computadores em si, mas também tudo que tenha algum sistema operacional, como smartphones, smart TVs, tables, etc.

Um computador pessoal (PC) geralmente tem uma grande quantidade de dados armazenados e é usado geralmente para acesso a internet banking, comércio eletrônico, redes sociais, etc.

PS: Evite uso de internet banking pelo computador, pelo menos no Windows. Dê a preferência para os aplicativos mobile oficiais dos bancos.

Manter o computador seguro é essencial para proteger dos riscos envolvidos no uso da internet.

Pode ser um grande erro acreditar que seu computador:

- Não apresenta atrativos.
- Dificilmente será localizado na internet.
- Sentindo-se seguro, você pode acreditar que não precisa se prevenir (a ilusão termina quando os problemas aparecem).

Sempre tem atacantes interessados em acessar grande quantidade de computadores, independente de quais são e das configurações que possuem.

Seu computador pode ser invadido ou infectado por meio:

- Da ação direta de atacantes.
- Da autoexecução de mídias removíveis infectadas.
- Do acesso a páginas web maliciosas (utilizando navegadores vulneráveis).
- Da exploração de vulnerabilidades existentes nos programas instalados ou no sistema operacional.
- Da exploração de contas de usuário (principalmente sem senha ou com senha fraca).
- Do meio da ação de códigos maliciosos recebidos pela rede ou obtidos em anexos de mensagens eletrônicas, outros computadores, páginas web e mídias removíveis.

Principais Riscos

Se seu computador for comprometido, você pode vir a enfrentar problemas como:

- Ficar sem acesso ao computador.
- Vazamento de informações.
- Invasão de privacidade.
- Furto de identidade.
- Perda de dados.
- Perdas financeiras.

Seu computador pode ser usado para atividades maliciosas, como:

- Infectar, invadir e atacar outros computadores.
- Esconder a real identidade e localização de um atacante.
- Servir de repositório para dados fraudulentos.
- Aplicar golpes em outros usuários.
- Propagar códigos maliciosos.
- Disseminar spam.

Cuidados a Serem Tomados

As principais dicas de cuidados são essas, pra qualquer sistema:

- Mantenha os programas atualizados e veja o motivo da atualização (sempre existe).
- Remova as versões antigas dos programas.
- Remova os programas que você não utiliza mais (programas não usados tender a ser esquecidos e ficar com versões antigas e potencialmente vulneráveis).
- Habitue-se a verificar a existência de novas versões, por meio de opções disponibilizadas pelos programas ou acessando diretamente os sites dos fabricantes.
- Configure os programas para serem atualizados automaticamente.
- Programe as atualizações automáticas para serem baixadas e aplicadas em um horário que o computador esteja ligado e conectado à internet.
- Cheque periodicamente por novas atualizações usando as opções disponíveis nos programas.
- Use apenas programas originais. Evite ao máximo programas crackeados.
- Ao comprar um computador pré-instalado, certifique-se de que os programas instalados são originais, solicitando ao revendedor as licenças de uso.

- Ao enviar seu computador pra manutenção, não permita a instalação de programas não-originais.
- Caso deseje um programa proprietário, mas não possa adquirir a licença, procure por alternativas gratuitas, mais baratas e com funcionalidades semelhantes às desejadas.
- No Android, apenas verifique se o acesso remoto está desativado, a instalação de aplicativos fora do Google Play está desativada e passar o antivírus. O reset de navegadores pode ser feito diretamente no gerenciador de aplicativos do Android.
- Ao navegar, cuidado com os links suspeitos.
- Se o link estiver encurtado, copie e ele e verifique num site com o URLXRay.

Aplicativos de Terceiros

Ao instalar aplicativos de terceiros:

- Verifique se as permissões de instalação e execução são coerentes (como se um aplicativo de texto queira permissão pra acessar seus contatos, por exemplo).
- Seja cuidadoso ao permitir que os aplicativos acessem seus dados pessoais.
- Seja cuidadoso ao selecionar os aplicativos, escolhendo os com grande quantidade de usuários e bem avaliados.

Use mecanismos de proteção, como esses:

- Instale um antivírus/antimalware e mantenha-o atualizado, incluindo o arquivo de assinaturas e configure-o para verificar todos os formatos de arquivos.
- Sempre verifique os arquivos recebidos antes de abri-los.
- Assegure-se de ter um firewall pessoal instalado e ativo.
- Crie um disco de recuperação do seu sistema e certifique-se de tê-lo por perto em caso de emergências.
- Crie um disco de emergência de seu antivírus e use-o se desconfiar que o antivírus instalado está desabilitado ou comprometido ou o comportamento do computador está estranho (usando muito disco e RAM, lentidão, etc.).
- Seja cuidadoso ao clicar em links, independente de como foram recebidos e de quem os enviou.
- Antes de clicar em um link curto, use complementos que permitam visualizar o link de destino.
- Lembre-se que mensagens de conhecidos nem sempre são confiáveis, o campo de remetente pode ter sido falsificado, ou podem ter sido enviadas de contas falsas ou invadidas.
- Desabilite a autoexecução de mídias removíveis e arquivos anexados.

Contas e Senhas

Crie uma conta padrão e use-a nas tarefas rotineiras. Use a conta de administrador somente quando necessário e pelo menor tempo possível. Use a opção de “executar como administrador” quando necessitar de privilégios administrativos. Mantenha a conta de convidado desabilitada.

Assegure-se de que:

- Todas as contas de acesso existentes tenham senha.
- Não existam contas de uso compartilhado.

- A opção de login automático esteja desabilitada.

Seja cuidadoso ao elaborar suas senhas:

- Use senhas longas, com diferentes tipos de caracteres.
- Não utilize sequências de teclado, dados pessoais como nome, sobrenome e dados, e dados que possam ser facilmente obtidos sobre você.

Ao usar o computador em locais públicos, use travas que dificultem que ele seja aberto ou furtado, mantenha-o bloqueado para evitar que seja usado quando você não estiver por perto. E utilize criptografia de disco (em caso de perda ou furto isso dificultará o acesso aos seus dados).

Ao entrar nas contas posteriormente, num dispositivo confiável, verifique os logins recentes, e encerre os mesmos, verifique também e-mails e telefones vinculados. Troque periodicamente a senha.

Dicas na Utilização de Computadores de Terceiros

Ao utilizar computadores de terceiros:

- Utilize opções de navegar anonimamente.
- Não efetue transações bancárias ou comerciais.
- Não utilize opções como “lembre-se de mim” e “continuar conectado”.
- Limpe os dados pessoais salvos no navegador.
- Não permita que senhas sejam memorizadas pelo navegador.
- Assegure-se de sair (logout) de suas contas de usuários.
- Seja cuidadoso ao conectar mídias removíveis.
- E ao retornar ao seu computador, altere as senhas usadas e verifique seu pendrive com um antivírus.

Outros cuidados a tomar:

- Faça regularmente backup dos seus dados.
- Mantenha a data e a hora corretas.
- Verifique as configurações de segurança oferecidas pelos programas instalados em seu computador.
- Ao compartilhar recursos do seu computador, estabeleça senhas para os compartilhamentos, permissões de acesso adequadas e compartilhe seus recursos pelo tempo mínimo necessário.
- Ao enviar seu computador para serviços de manutenção, selecione empresas com boas referências, pesquise na internet sobre a empresa (à procura da opinião de clientes sobre elas).
- Não permita a instalação de programas não-originais e se possível, faça backup dos dados antes de enviá-lo.

Dispositivos Móveis

Dispositivos móveis são qualquer dispositivo que são portáteis, como tablets, smartphones, celulares (inclusive os mais antigos). O notebook, apesar de ser portátil, ele está mais próximo aos

computadores de mesa e por isso ele não é considerado móvel. Dispositivos móveis estão cada vez mais populares.

Os dispositivos móveis, principalmente os mais modernos, executam ações realizadas em computadores, como navegação web, internet banking, acesso a e-mails, redes sociais, etc.

As principais características dos dispositivos móveis são essas:

- Auxílio em tarefas cotidianas.
- Grande quantidade de informações pessoais e profissionais.
- Agenda, contatos, chamadas realizadas, mensagens recebidas.
- Conectividade wi-fi e 3G.
- Leves e de tamanho reduzido, fáceis de serem carregados em bolsas, bolsos.
- Diversas funcionalidades integradas, como GPS e câmera.

Principais Riscos nos Dispositivos Móveis

Dispositivos móveis e computadores pessoais tem funcionalidades similares e também riscos similares, como por exemplo:

- Códigos maliciosos.
- Phishing.
- Acesso a conteúdos impróprios ou ofensivos.
- Contato com pessoas mal-intencionadas.
- Perda de dados.
- Dificuldade de manter sigilo.

Os dispositivos móveis ainda possuem características que os tornam ainda mais atraentes para atacantes e pessoas mal-intencionadas. Como por exemplo, vazamento de informações, pelo seguinte:

- Grande quantidade de informações pessoais armazenadas.
- Rápida substituição de modelos sem a devida exclusão das informações gravadas.
- Informações que podem ser indevidamente coletadas, como mensagens SMS, lista de contatos, calendários, histórico de chamadas, fotos e vídeos, senhas, números de cartão de crédito, etc.

Dispositivos Móveis – Parte 2

Outros riscos que temos com dispositivos móveis são esses:

- Maior possibilidade de perda e furto, pelo tamanho reduzido, alto valor financeiro, representar status, atrair atenção de assaltantes, estarem constantemente em uso, usados em locais públicos e são facilmente esquecidos e perdidos.
- Invasão de privacidade, seja intencional, pelo dispositivo estar sempre à mão, uso generalizado e alguém pode tirar uma foto sua sem sua autorização.
- Localização fornecida por aplicativos de geolocalização (GPS).
- Dados pessoais coletados por códigos maliciosos ou atacantes.
- Excesso de informações pessoais sendo fornecidas, como locais que frequenta, horários, rotina, hábitos e bens pessoais.

- Instalação de aplicativos maliciosos, grande quantidade de aplicativos sendo desenvolvidos, de diferentes autores, funcionalidades, e dificuldade de manter controle. Podem existir aplicativos não confiáveis, com erros de implementação e especialmente desenvolvidos para executar atividades maliciosas e coletar dados dos aparelhos.
- Propagação de códigos maliciosos, recebidos por meio de mensagens SMS, e-mails, redes sociais, etc. Dispositivos infectados podem ter os dados coletados ou apagados, participar de ataques na internet, fazer parte de botnets, e contribuir para a disseminação de spam.

Cuidados com os Dispositivos Móveis

Antes de adquirir um dispositivo móvel:

- Observe os mecanismos de segurança disponibilizados pelos diferentes modelos e fabricantes e escolha o que considerar mais seguro.
- Caso opte por um modelo já usado, restaure as configurações de fábrica/originais.
- Não adquira um dispositivo que foi ilegalmente desbloqueado (jailbreak/root), com permissões de acesso alteradas (ação ilegal, violação dos termos de garantia ou comprometimento da segurança e do funcionamento).

Ao usar seu dispositivo:

- Mantenha seu dispositivo seguro com a versão mais recente dos programas instalados e com todas as atualizações aplicadas.
- Não siga links recebidos via mensagens eletrônicas.
- Instale e mantenha atualizados mecanismos de segurança, como antivírus, antispam, antimalware, firewall pessoal, etc.
- Mantenha controle físico, principalmente em locais de risco, procure não deixá-lo sobre a mesa, cuidado com bolsos/bolsas em ambientes públicos, etc.
- Proteja suas senhas, cadastre senhas de acesso bem elaboradas e, se possível, configure-o para aceitar senhas complexas, use senhas longas, com diferentes tipos de caracteres, e não utilize sequências de teclado, dados pessoais como nome, sobrenome e datas, dados que possam ser facilmente obtidos sobre você, etc.
- Proteja seus dados, configure senha de bloqueio na tela inicial, código PIN, faça backups periódicos, mantenha informações sensíveis em formato criptografado, use conexão segura quando a comunicação envolver informações confidenciais, como senhas e números de cartões de crédito.

Cuidado com APPs e Venda, Troca e Furto

Ao instalar aplicativos:

- Procure obter aplicativos de fontes confiáveis, como lojas confiáveis e site do fabricante.
- Escolha aplicativos bem avaliados e com grande quantidade de usuários.
- Verifique com seu antivírus antes de instalar o aplicativo.
- Observe as permissões para execução, elas devem ser coerentes com a finalidade do aplicativo, por exemplo, um aplicativo de jogos não necessariamente precisa ter acesso a sua lista de chamadas.

Ao acessar redes:

- Seja cuidadoso ao usar redes wi-fi públicas, desabilite a opção de conexão automática.
- Mantenha interfaces de comunicação desativadas, como bluetooth, infravermelho e wi-fi, e somente as habilite quando necessário.
- Configure o bluetooth para que o dispositivo não seja identificado ou “descoberto” por outros aparelhos.

Ao desfazer do seu aplicativo:

- Apague todas as informações neles contidas.
- Restaure as configurações de fábrica.

Em caso de perda ou furto:

- Configure-o previamente, se possível, para que seja localizado/rastreado e bloqueado remotamente por meio de serviços de geolocalização, uma mensagem seja mostrada na tela para aumentar as chances dele ser devolvido, o volume seja aumentado ou que saia do modo silencioso para facilitar a localização, os dados seja apagados após um determinado número de tentativas de desbloqueio sem sucesso (cuidado principalmente se você tiver filhos que gostam de “brincar” com o seu dispositivo).
- Informe a sua operadora, solicite o bloqueio do seu número (chip), a empresa onde você trabalha caso haja dados se senhas profissionais.
- Altere as senhas que possam estar nele armazenadas.
- Bloquei cartões de crédito cujo número esteja nele armazenado.
- Ative a localização remota, caso a tenha configurado, e se necessário, apague remotamente os dados gravados.

Redes Sociais

Redes sociais são as redes de relacionamento que permitem que os usuários forneçam informações sobre si, acessem informações sobre outros usuários, utilizem mecanismos de comunicação, se agrupem, de acordo com afinidades, características, interesses e objetivos em comum. O conteúdo é totalmente (ou quase) gerado pelos próprios usuários.

Alguns as utilizam como uma espécie de diário público, como quem você é, onde você está, o que você curte, quem você conhece, o que está acontecendo, no que você está pensando, o que seus amigos dizem sobre você, onde você tem estado, etc.

Características Principais das Redes Sociais

As principais características das redes sociais são:

- Facilidade de acesso.
- Rápida velocidade de propagação de informações.
- Grande quantidade de usuários e informações pessoais.
- Dificuldade de exclusão de informações e controle sobre as informações.
- Tempo que as informações ficam disponíveis.
- Alto grau de confiança que os usuários depositam entre si.

- Novas oportunidade de negócios.
- Presente em diversos meios.

Principais Riscos das Redes Sociais

Os principais riscos das redes sociais são esses:

- Furto de identidade.
- Invasão de perfil.
- Uso indevido de informações.
- Invasão de privacidade.
- Danos à imagem e à reputação.
- Recebimento de mensagens maliciosas.
- Contato com pessoas mal-intencionadas.
- Acesso a conteúdos impróprios ou ofensivos.

Cuidados com as Redes Sociais

Dentro de uma rede social, proteja o seu perfil seguindo essas etapas:

- Seja cuidadoso ao elaborar suas senhas, use senhas longas, com diferentes tipos de caracteres e não utilize dados pessoais como nome, sobrenome e datas.
- Seja cuidadoso ao usar as suas senhas, evite usar a mesma senha para acessar diferentes sites, evite usar sua senha em computadores de terceiros.
- Habilite notificações de login e verificação em duas etapas.
- Se desconfiar que seu perfil foi indevidamente usado, verifique o registro de atividades, ou solicite o arquivo com suas informações.
- Evite cadastrar perguntas de segurança que possam ser facilmente descobertas (na verdade evite cadastrar quaisquer perguntas do tipo).
- Cadastre um e-mail de recuperação que você acesse regularmente.
- Use opções como silenciar, bloquear e denunciar, caso identifique abusos como imagens indevidas, perfis falsos, alguém o esteja incomodando, spam, etc.
- Certifique-se de usar conexões seguras ao acessar os sites (alguns indícios apresentados pelo navegador web são que o endereço começa com “https”, o desenho de um cadeado é mostrado na barra de endereço, ao clicar nele são exibidos detalhes sobre a conexão e o certificado digital. Podemos ver também o nome do servidor em “verdinho” ao lado do https.

Mantendo os Equipamentos Seguros

É importante manter os equipamentos seguros, e pra isso, siga essas dicas:

- Mantenha seu computador e dispositivos móveis com todos os programas instalados nas versões mais recentes e todas as atualizações aplicadas.
- Utilize e mantenha atualizados mecanismos de segurança, como antispam, antivírus/antimalware, firewall pessoal, etc.

- Desconfie de mensagens recebidas, mesmo que tenham sido enviadas por conhecidos, pois podem ter sido enviadas de contas falsas ou invadidas.
- Seja cuidadoso ao acessar links reduzidos, use complementos que permitam que você expanda o link, antes de clicar sobre ele.
- Considere que você está em um lugar público.
- Pense bem antes de divulgar (não há como voltar atrás).
- Use as opções de privacidade oferecidas pelos sites, procure ser o mais restritivo possível.
- Mantenha seu perfil e seus dados privados.
- Restrinja o acesso ao seu endereço de e-mail.
- Cuidado ao confirmar sua presença em eventos públicos organizados via redes sociais.
- Seja seletivo ao aceitar seus contatos, ao se associar a grupos.
- Não acredite em tudo que você lê.
- Não confie na promessa de anonimato oferecida por algumas redes sociais e aplicativos. De acordo com as informações divulgadas é possível inferir a sua identidade e a identidade de outras pessoas.
- Seja cuidadoso ao fornecer a sua localização, cuidado ao divulgar fotos e vídeos (ao observar onde foram gerados pode ser possível deduzir sua localização). Não divulgue planos de viagens e por quanto tempo ficará ausente de sua residência.
- Ao usar redes sociais baseadas em geolocalização, faça check-in apenas em locais movimentados, e ao sair do local, ao invés de quando chegar.
- Evite falar sobre as ações, hábitos e rotina de outras pessoas.
- Não divulgue, sem autorização, imagens em que outras pessoas apareçam, e mensagens ou imagens copiadas do perfil de usuários que restrinjam o acesso.
- Tente imaginar como a outra pessoa se sentiria ao saber que aquilo está se tornando público.

Proteja seus Filhos e sua Vida Profissional

Tome cuidado com os seus filhos no mundo virtual, seguindo esses passos:

- Informe-os sobre os riscos de uso das redes sociais.
- Respeite os limites de idade estipulados pelos sites.
- Não exponha excessivamente seus filhos. Muitos pais criam perfis em nomes dos filhos e postam sobre eles ou como se fossem eles, isso pode confundir e desagradar as crianças. Evite constranger seus filhos divulgando fotos ou comentários que posam embaraçá-los. Seja cuidadoso ao divulgar imagens de seus filhos, para você pode ser algo inocente, para outras pessoas pode ter uma conotação diferente.
- Oriente-os para não se relacionarem com estranhos, para nunca fornecerem informações pessoais, e para não divulgarem informações sobre hábitos familiares e localização geográfica (atual ou futura).
- Oriente-os para não marcarem encontros, sobre os riscos de uso da webcam (ela não deve ser usada para se comunicar com estranhos), e para usar opções como silenciar, bloquear e denunciar, caso alguém os esteja incomodando.

Cuide da sua imagem profissional:

- Ao usar redes sociais profissionais, procure ser formal e evite tratar de assuntos pessoais.
- Antes de divulgar uma informação, avalie se ela pode atrapalhar o seu emprego atual ou um processo seletivo futuro. Lembre-se que ela poderá ser acessada por seu chefes e colegas de trabalho. Observe se ela não fere o código de conduta da sua empresa.

- Cuidado ao permitir que seus filhos use o mesmo computador ou dispositivo móvel que você usa para tratar de assuntos profissionais (alguns aplicativos, como jogos, divulgam automaticamente nas redes sociais, dependendo de suas configurações).

Senhas

Sobre as senhas, saiba que:

- Servem para autenticar um usuário (asseguram que você é realmente quem diz ser, e possui o direito de acessar o recurso em questão).
- Um dos principais mecanismos de autenticação usados na internet.
- Proteger suas senhas é essencial para se prevenir dos riscos envolvidos no uso da internet. É o segredo das suas senhas que garante a sua identidade, ou seja, que você é o dono das suas contas de usuário.

Sua senha pode ser descoberta:

- Quando usada em computadores infectados, computadores invadidos e sites falsos (phishing).
- Por meio de tentativas de adivinhação.
- Ao ser capturada enquanto trafega na rede.
- Por meio do acesso ao arquivo onde foi armazenada.
- Com o uso de técnicas de engenharia social.
- Pela observação da movimentação (dos seus dedos no teclado, e dos cliques do mouse em teclados virtuais).

Principais Riscos das Senhas

De posse da sua senha, um invasor pode acessar a sua conta de correio eletrônico e:

- Ler e/ou apagar seus e-mails.
- Furtar sua lista de contatos e enviar e-mails em seu nome.
- Pedir o reenvio de senhas de outras contas, e assim conseguir acesso a elas.
- Trocar a sua senha, dificultando que você acesse novamente a sua conta.
- Enviar mensagens contendo spam, boatos, phishing, códigos maliciosos, etc.

De posse da sua senha, um invasor também pode acessar o seu computador e:

- Apagar seus arquivos.
- Obter informações sensíveis, inclusive outra senhas.
- Instalar códigos e serviços maliciosos.
- Usar seu computador para desferir ataques contra outros computadores.
- Esconder a real identidade desta pessoa (o invasor).

De posse da sua senha, um invasor pode acessar a sua rede social e:

- Denegrir a sua imagem.
- Explorar a confiança de seus amigos/seguidores.

- Alterar as configurações feitas por você, tornando públicas suas informações privadas.
- Trocar a sua senha, dificultando que você acesse seu perfil.
- Enviar mensagens em seu nome, contendo spam, boatos, phishing, códigos maliciosos, etc.

De posse da sua senha, um invasor pode:

- Acessar a sua conta bancária e verificar o seu extrato e seu saldo bancário.
- Acessar o seu site de comércio eletrônico e alterar as informações de cadastro, fazer compras em seu nome e verificar informações sobre suas comprar anteriores.
- Acessar o seu dispositivo móvel e furtar sua lista de contatos e suas mensagens, acessar e/ou copiar fotos e vídeos, e bloquear o acesso ao dispositivo.

Cuidado com as Senhas

Para elaborar sua senha, evite usar:

- Dados pessoais (nome, sobrenome, contas de usuário, datas, números de documentos, de telefones ou de placas de carros).
- Dados disponíveis em redes sociais e páginas web.
- Sequências de teclado (tipo “qwertyuiop” ou “123zxcvb”).
- Palavras presentes em listas publicamente conhecidas (músicas, times de futebol, personagens de filmes, dicionário de diferentes idiomas, etc.).

E use:

- Números aleatórios (quanto mais ao acaso forem os números, melhor, principalmente em sistemas que aceitem exclusivamente caracteres numéricos).
- Grande quantidade de caracteres (quanto mais longa for sua senha, melhor).
- Diferentes tipos de caracteres (quanto mais “bagunçada” for sua senha, melhor).

Dicas práticas para elaborar boas senhas:

- Escolha uma frase e selecione a primeira, a segunda ou a última letra de cada palavra.
- Escolha uma frase longa, fácil de ser memorizada e com diferentes tipos de caracteres.
- Invente um padrão de substituição próprio (como substituir “o” por “0” e duplicar as letras “r” e “s”).

Como Usar sua Senha Corretamente

Sobre o uso de senhas:

- Não exponha suas senhas. Certifique-se de não estar sendo observado ao digitá-las. Não as deixe anotadas em locais onde outros possam ver (como um papel sobre sua mesa). Evite digitá-las em computadores e dispositivos móveis de terceiros.
- Não forneça suas senhas para outras pessoas (cuidado com e-mails/telefonemas pedindo dados pessoais).
- Use conexões seguras quando o acesso envolver senhas.

- Evite salvar as suas senhas no navegador web, usar opções como “lembre-se de mim” e “continuar conectado”. E usar a mesma senha para todos os serviços que acessa (basta ao atacante conseguir uma senha para ser capaz de acessar as demais contas onde ela seja usada).
- Não use senhas de acesso profissional para acessar assuntos pessoais e vice-versa. Respeite os conceitos.
- Crie grupos de senhas, de acordo com o risco envolvido. Crie senhas únicas, fortes, e use-as onde haja recursos valiosos envolvidos. Únicas, um pouco mais simples, e use-as onde o valor dos recursos protegidos é inferior. E simples e reutilize-as para acessos sem risco.
- Armazene suas senhas de forma segura: Use programas gerenciadores de contas/senhas. Anote-as em um papel e guarde-o em local seguro. Grave-as em um arquivo criptografado.

Alterações de Senhas

Altere suas senhas:

- Imediatamente, se desconfiar que tenham sido descobertas ou usadas em computadores invadidos ou infectados.
- Rapidamente, se perder um computador onde elas estejam gravadas, se usar um padrão de formação e desconfiar que alguma tenha sido descoberta, uma mesma senha em mais de um lugar e desconfiar que ela tenha sido descoberta em algum deles, e adquirir equipamentos acessíveis via rede (eles podem estar configurados com senha padrão).
- Regulamente, nos demais casos.

Configure opções de recuperação de senhas:

- Um endereço de e-mail alternativo.
- Uma pergunta de segurança.
- Uma dica de segurança.
- Um número de telefone celular.

Ao usar perguntas de segurança:

- Evite escolher questões cujas respostas sejam facilmente adivinhadas.
- Procure criar suas próprias questões, de preferência com respostas falsas.

Ao usar dicas de segurança, escolha aquelas que sejam:

- Vagas o suficiente para que ninguém consiga descobri-las.
- Claras o bastante para que você consiga entendê-las.

Ao solicitar o envio de suas senhas por e-mail:

- Procure alterá-las o mais rápido possível.
- Cadastre um e-mail que você acesse regularmente.

Phishing e Códigos Maliciosos

Para se prevenir de phishing e códigos maliciosos:

- Desconfie de mensagens recebidas, mesmo que enviadas por conhecidos (elas podem ter sido enviadas de contas falsas ou invadidas).
- Evite clicar/seguir links recebidos via mensagens eletrônicas (procure digitar a URL diretamente no navegador).
- Evite usa sites de busca para acessar serviços que requeiram senhas, como seu webmail e sua rede social.
- Seja cuidadoso ao acessar links reduzidos: Use complementos que permitam expandir o link antes de clicar sobre ele.

Sobre os computadores:

- Mantenha seu computador seguro, com todos os programas instalados nas versões mais recentes, e todas as atualizações aplicadas, principalmente as de segurança.
- Utilize e mantenha atualizados mecanismos de segurança, como antispam, antimalware e firewall pessoal.
- Crie contas individuais para todos os usuários, e assegure-se de que todas as contas tenham senhas.
- Configure seu computador para solicitar senha na tela inicial.
- Nunca compartilhe a senha de administrador, use-a o mínimo necessário.

Sobre os dispositivos móveis:

- Cadastre uma senha de acesso bem elaborada (se possível, configure-o para aceitar senhas complexas (alfanuméricas)).
- Em caso de perda ou furto, altere as senhas que possam estar nele armazenadas.

E sobre os computadores de terceiros:

- Certifique-se de fechar a sua sessão (logout) ao acessar sites que requeiram o uso de senhas.
- Utilize opções de navegação anônima.
- Evite efetuar transações bancárias e comerciais.
- Ao retornar ao seu computador, altere as senhas que tenha utilizado.

Como Funciona a Verificação em Duas Etapas

Efetivamente, sobre a verificação em duas etapas:

- Também chamada de two-factor authentication, aprovação de login, verificação ou autenticação em dois fatores/passos.
- Recurso opcional oferecido por diversos serviços: Webmail, redes sociais, internet banking, armazenamento em nuvem, etc.
- Ao ser habilitada, permite aumentar a segurança da sua conta, e pode ser desabilitada caso não seja mais desejada.
- Dificulta o acesso indevido de contas de usuário.
- Para que o acesso ocorra é necessário que o atacante realize com sucesso duas etapas: A senha do usuário, e as informações adicionais.

Segunda etapa pode envolver:

- Algo que apenas você sabe (outra senha, perguntas de segurança, número PIN, alguma informação pessoal, etc.
- Algo que apenas você possui (código de verificação, cartão de senhas bancárias, token gerador de senhas, acesso a um determinado computador ou dispositivo móvel, etc.
- Algo que você é (informações biométricas, como impressão digital, palma da mão, rosto, olho, etc.).

Cuidados com a Verificação em Duas Etapas

Sobre o código individual:

- É criado pelo serviço.
- Enviado de forma que apenas você possa recebê-lo (como e-mail, chamada de voz e SMS para o telefone cadastrado).
- Pode ser gerado por um aplicativo autenticador instalado no seu dispositivo móvel.

Esses são os cuidados a serem tomados:

- Mantenha atualizados seus dados para recebimento (como telefones alternativos).
- Tenha certeza de estar de posse de seu telefone celular, caso tenha configurado o envio de SMS ou uso de aplicativo autenticador.
- Aplicativo autenticador deve ser usado em casos onde não é possível receber SMS.
- Tarifas de recebimento de SMS podem ser aplicadas por sua operadora.
- Temos também o código de verificação específico, gerado para aplicativos que não suportam a verificação em duas etapas.
- Caso perca o acesso ao seu dispositivo móvel, revogue os códigos específicos gerados para os acessos realizados por meio dele.

Formas de Verificação em Duas Etapas

Sobre o token gerador de senhas:

- Chave eletrônica.
- Tipo de dispositivo eletrônico que gera códigos usados na verificação da sua identidade.
- Cada código é válido por um determinado período, geralmente alguns segundos, após esse tempo um novo código é gerado. Código pode ser gerado automaticamente ou necessitar que você clique em um botão para ativá-lo.

Cuidados a serem tomados:

- Guarde seu token em um local seguro.
- Nunca informe o código mostrado no token por e-mail ou telefone.
- Caso perca seu token ou ele seja furtado, avise imediatamente o responsável pelo serviço no qual ele é usado.

Já o cartão de segurança, é um cartão com diversos códigos numerados e que são solicitados quando você acessa a sua conta. Esses são os cuidados a serem tomados:

- Guarde seu cartão em um lugar seguro.

- Nunca forneça os códigos do cartão por e-mail ou telefone.
- Forneça apenas uma posição do seu cartão a cada acesso.
- Verifique se o número de identificação do cartão apresentado pelo serviço corresponde ao que está no seu cartão. Caso sejam diferentes entre em contato com o serviço.
- Desconfie caso, em um mesmo acesso, seja solicitada mais de uma posição do cartão.

Dispositivos Confiáveis

O dispositivo confiável é o computador ou dispositivo móvel usado para acessar suas contas.

No primeiro acesso pode ser necessário inserir um código de segurança, ele não será necessário nos demais acessos, pois seu dispositivo será “lembrado”, caso você assim o configure.

Cuidados a serem tomados:

- Não esqueça de excluir seus dispositivos confiáveis caso eles sejam trocados ou você perca o acesso a eles.
- Pode ser necessário habilitar a opção de cookies em seu navegador web para que seu dispositivo seja memorizado.

Já as listas de código reserva/backup, são listas de códigos que devem ser usadas de forma sequencial e uma única vez.

Cuidados a serem tomados:

- Anote ou imprima a lista e a mantenha em um local seguro.
- Não a armazene em seu dispositivo confiável pois ela pode vir a ser acessada por atacantes, caso não esteja criptografada.
- Caso perca a lista ou desconfie que alguém a acessou você deve gerá-la novamente ou revogá-la, anulando assim a anterior.

Já a chave de recuperação, é um número gerado pelo serviço quando você ativa a verificação em duas etapas.

Permite que você acesse o serviço mesmo que perca sua senha ou seus dispositivos confiáveis.

Cuidados a serem tomados:

- Anote ou imprima a chave e a mantenha em um local seguro.
- Não a deixe anotada em seu dispositivo confiável pois ela pode vir a ser acessada por atacantes, caso não esteja criptografada.
- Caso peca a chave ou desconfie que alguém a acessou você deve gerá-la novamente.

Outros Cuidados com a Verificação em Duas Etapas

Sobre os dados pessoais, mantenha seu cadastro atualizado:

- Dados pessoais podem ser solicitados aleatoriamente para checar a sua identidade.

- Seu endereço de correspondência pode ser usado para envio de tokens e cartões de segurança.
- Dados pessoais e perguntas de segurança podem ser solicitados, caso você desabilite a verificação em duas etapas.

Sobre os dispositivos móveis:

- Instale um programa antivírus.
- Mantenha o sistema operacional e as aplicações instaladas sempre com a versão mais recente e com todas as atualizações aplicadas.
- Em caso de perda ou furto, remova-os da lista de dispositivos confiáveis, revogue autorizações concedidas para aplicativos instalados, cadastre um novo número de celular, se tiver configurado a localização remota, apague remotamente os dados armazenados.

O que é Privacidade (Parte 1)

Sua privacidade pode ser exposta na internet:

- Independentemente da sua vontade.
- Sem aviso ou consentimento prévio.
- Quando alguém divulga informações sobre você ou imagens onde você está presente.
- Quando um site altera as políticas de privacidade, ou coleta hábitos e preferências de navegação e repassa a terceiros.
- Ou quando um impostor cria uma conta/perfil em seu nome e a usa para se passar por você.

O que é Privacidade (Parte 2)

Sua privacidade pode ser exposta na internet:

- Independentemente da sua vontade.
- Sem aviso ou consentimento prévio.
- Quando um atacante e/ou código malicioso acessa dados que você digita ou que estejam armazenados em seu computador.
- Quando invadem uma conta sua e acessam informações restritas, invade um computador no qual seus dados estão armazenados, coletam informações não criptografadas que trafegam na rede.
- Quando um aplicativo instalado em seu dispositivo coleta dados pessoais e os envia ao desenvolvedor/fabricante, ou você compartilha recursos do seu computador sem configurar restrições de acesso adequadas, elabora senhas fracas, facilitando a invasão de suas contas, acessa suas contas em computadores potencialmente infectados, e não mantém a segurança do seu computador ou dispositivo móvel.

Principais Riscos a sua Privacidade

Divulgação e coleta indevida de informações pessoais pode:

- Comprometer a sua privacidade, de seus amigos e familiares.
- Facilitar o furto da sua identidade. Quanto mais dados você divulga mais fácil é para um impostor criar uma identidade falsa sua e usá-la em ações maliciosas, como acessar sites,

efetuar transações financeiras, enviar mensagens eletrônicas, abrir empresas fantasmas, criar contas bancárias ilegítimas, etc.
- Facilitar a invasão de suas contas de usuário. Senhas e respostas a dicas/perguntas de segurança podem ser adivinhadas caso usem dados pessoais.
- Fazer com que propagandas direcionadas sejam apresentadas.
- Colocar em risco sua segurança física.
- Favorecer o recebimento de spam.
- Causar perdas financeiras, perda de reputação e falta de crédito.

Cuidados a Serem Tomados com E-mail

Esses são os cuidados a serem tomados ao acessar/armazenar e-mails:

- Configure seu programa leitor de e-mails para não abrir mensagens que não estejam na própria mensagem. O acesso a imagem pode confirmar que o e-mail foi lido.
- Use programas leitores de e-mails que permitam que as mensagens sejam criptografadas. Mensagens criptografas somente poderão ser lidas por quem decodificá-las.
- Use conexão segura ao acessar e-mails via navegadores. Isto pode evitar que eles sejam interceptados.
- Armazene e-mails confidenciais em formato criptografado. Isso dificulta que sejam lidos por atacantes e códigos maliciosos, você pode decodificá-los sempre que desejar lê-los.
- Use criptografia para conexão entre seu leitor de e-mails e os servidores de e-mail do seu provedor.
- Seja cuidadoso ao acessar seu webmail. Digite a URL diretamente no navegador, e tenha cuidado ao clicar em links recebidos por meio de mensagens eletrônicas.

Cuidados ao Navegar na Web

Ao navegar na web, seja cuidadoso ao usar cookies:

- Use uma ou mais das seguintes opções: Defina um nível de permissão superior ou igual a “médio”. Configure para que os cookies sejam apagados quando o navegador for fechado e que cookies de terceiros não sejam aceitos. Você pode também configurar para que, por padrão, os sites não possam definir cookies e criar listas de exceções, liberando os sites considerados confiáveis e onde o uso é realmente necessário, e os sites possam definir cookies e criar listas de exceções, bloqueando os sites indesejados.
- Quando disponível, procure utilizar navegação anônima, principalmente ao usar computadores de terceiros, informações sobre navegação não serão armazenadas. Opções que indiquem que você não quer ser rastreado, “do not track” e lista de proteção contra rastreamento.

Cuidados ao Divulgar Informações

Ao divulgar informações na web:

- Avalie com cuidado as informações divulgadas em sua página web, rede social ou blog, elas podem ser usadas para atentar contra a segurança do seu computador, atentar contra a sua segurança física, aplicar golpes de engenharia social e obter informações sobre você.

- Considere que você está em um local público.
- Pense bem antes de divulgar algo, não é possível voltar atrás.
- Divulgue a menor quantidade possível de informações, tanto sobre você como sobre seus amigos e familiares, e oriente-os a fazer o mesmo.
- Sempre que alguém solicitar dados sobre você ou ao preencher algum cadastro, reflita se é realmente necessário que aquela empresa ou pessoa tenha acesso àquelas informações.
- Ao receber ofertas de emprego pela internet, limite as informações disponibilizadas no currículo, e só forneça mais dados quando estiver seguro de que a empresa e a oferta são legítimas.
- Fique atento a mensagens eletrônicas pelas quais alguém solicita informações pessoais, inclusive senhas.
- Seja cuidadoso ao divulgar a sua localização geográfica, com base nela, é possível descobrir a sua rotina, deduzir informações e tentar prever os seus próximos passos.
- Verifique a política de privacidade dos sites que você usa, fique atento às mudanças, principalmente aquelas relacionadas ao tratamento de dados pessoais.
- Use as opções de privacidade oferecidas pelos sites, procure ser o mais restritivo possível.
- Mantenha seu perfil e seus dados privados.
- Seja seletivo ao aceitar seus contatos.
- Seja cuidadoso ao se associar a grupos e comunidades.

Cuidado ao Manipular Dados e Recursos

Ao manipular dados e recursos:

- Armazene dados sensíveis em formato criptografado.
- Cifre o disco do seu computador e dispositivos removíveis.
- Ao compartilhar recursos do seu computador, estabeleça senhas para os compartilhamentos, e compartilhe pelo tempo mínimo possível.
- Mantenha backups em locais seguros e com acesso restrito.
- Ao usar serviços de backup online, considere a política de privacidade e de segurança do site.

Contas e Senhas

Sobre contas e senhas:

- Evite reutilizar suas senhas.
- Não forneça suas senhas para outra pessoa.
- Ao usar perguntas de segurança, evite escolher questões cujas respostas sejam facilmente adivinhadas.
- Seja cuidadoso ao elaborar suas senhas, use senhas longas com diferentes tipos de caracteres, e não utilize dados pessoais, como nome, sobrenome e datas, e dados que posam ser facilmente obtidos.

Sobre o computador e dispositivos móveis:

- Mantenha o seu computador/dispositivo móvel seguro, com a versão mais recente de todos os programas instalados e com todas as atualizações aplicadas.

- Utilize e mantenha atualizados mecanismos de segurança, como antispam, antimalware e firewall pessoal.
- Ao instalar aplicativos desenvolvidos por terceiros, seja cuidadoso ao permitir o acesso aos seus dados pessoais, verifique se as permissões necessárias são coerentes, e seja seletivo ao selecionar os aplicativos (escolha aqueles bem avaliados e com grande número de usuários).

Proteção de Dados

Sobre a importância dos seus dados:

- Dados de cadastros, biográficos, profissionais, financeiros e de navegação são apenas alguns exemplos de dados armazenados referentes a você que, diariamente circulam por diversas redes, e são armazenados em diferentes sistemas, dispositivos e mídias.
- Infelizmente, há situações em que seus dados podem ser perdidos, indevidamente acessados, coletados e vendidos sem que você tenha ciência disso.
- Exemplos dessas situações incluem quando você perde o celular, computador ou mídia removível, seus dados são interceptados ao trafegarem na rede, há um vazamento envolvendo seus dados, suas contas de usuário e sistemas onde seus dados estão armazenados são invadidos, e seus dados de navegação são coletados de forma não transparente e compartilhados seu seu consentimento.

A Importância dos Seus Dados

Continuando sobre a importância dos seus dados:

- Para proteger seus dados e assegurar que eles sejam tratados de forma adequada há um conjunto de mecanismos de segurança que podem ser usados, por exemplo: O uso de senhas fortes impedem o acesso indevido às contas, e a criptografia dificulta que seus dados seja acessados e alterados indevidamente.
- Há situações em que os mecanismos de segurança sozinhos não protegem seus dados, por exemplo, quando eles são passados deliberadamente a outros sem sua autorização, e coletados sem necessidade.
- Adotar uma postura preventiva, tentando reduzir a quantidade de dados fornecida por você, é essencial.
- Para coibir abusos, garantir seus direitos e agir adequadamente é importante conhecer a legislação vigente.

Como seus Dados podem ser Abusados

Veja como seus dados podem ser abusados:

- O abuso de seus dados pode acarretar prejuízos financeiros, restrição a direitos ou benefícios, invasão de privacidade.
- Pode ocorrer de diversas formas, acesso indevido, perda de dados, invasão de contas e golpes, coleta excessiva.

Seus dados podem ser indevidamente acessados:

- Por aplicativos e sites que processem seus dados além das finalidades informadas.

- Por atacantes ou códigos maliciosos que consigam acesso às suas contas, equipamentos ou mídias.
- Em casos de vazamento de dados.

Seus dados podem ser perdidos:

- Pela ação de códigos maliciosos, como ransomware.
- Pela ação de atacantes que consigam invadir seus equipamentos e mídia e venham a apagá-los.

Seus dados podem ser usados:

- Para adivinhas suas senhas e responder perguntas de segurança.
- Em tentativas de golpes, como phishing direcionado e personalizado (spear phishing), furto de identidade ou extorsão.

Sobre a coleta excessiva:

- Muitos aplicativos e sites coletam dados extras sem o seu conhecimento e os utilizam para elaboração de perfis de comportamento (profiling).
- Seu perfil pode, então, ser usado sem o consentimento de forma discriminatória, e para fins como propagandas.

Cuidado com os Seus Dados

Backups protegem seus dados em caso de mau funcionamento de equipamentos, da perda de dispositivos e da ação de códigos maliciosos, especialmente ransomware:

- Faça regularmente backup dos seus dados.
- Programe seus backups para serem feitos automaticamente.
- Teste periodicamente seus backups, para ter certeza de que estão sendo feitos corretamente.
- Mantenha pelo menos um backup offline.

Sobre os arquivos:

- Evite colocar na nuvem arquivos contendo dados confidenciais ou que considere privados.
- Crie uma partição criptografada ou use recursos de criptografia para armazenar seus arquivos de forma segura.
- Seja cuidadoso ao abrir arquivos enviados por terceiros.

Cuidados com os Seus Dados – Parte 2

A criptografia ajuda a tornar as transmissões de dados mais seguras, detectar alterações em seus dados e impedir que sejam lidos indevidamente:

- Use criptografia para proteger os dados armazenados em seus equipamentos e mídias. Em caso de perda ou furto será mais difícil deles serem acessados.
- Ative as configurações de criptografia em seus discos e mídias, como pen-drives e discos externos.

Sobre as contas e senhas:

- Crie senhas fortes e não repita senhas.
- Habilite verificação em duas etapas, especialmente em sistemas de armazenamento em nuvem, notificações de login, para ser mais fácil perceber acessos indevidos, e configurações de privacidade e segurança.
- Ao usar equipamentos compartilhados, lembre-se de sair de suas contas (logout).

Cuidado com os Aplicativos

Instale aplicativos somente de fontes e lojas oficiais, e também:

- Antes de instalar, verifique as telas e o nome do aplicativo.
- Muitos falsos aplicativos se assemelham aos oficiais.

Observe:

- Se o desenvolvedor do aplicativo é confiável.
- Quantas pessoas instalaram o aplicativo.
- Qual a opinião delas sobre o aplicativo.

Fique atento às permissões:

- Forneça apenas aquelas que considerar necessárias.
- Limite quais aplicativos podem acessar o microfone, a câmera, seus contatos e sua localização (exemplo: Um aplicativo de teste de velocidade não precisa ter acesso aos seus contatos para funcionar).

Apague os aplicativos que você não usa mais.

Sobre os equipamentos e mídias:

- Atualize o sistema e os aplicativos.
- Utilize mecanismos de segurança.
- Cuidado para não perder pen-drives e discos externos.
- Antes de se desfazer de seus equipamentos e mídias apague os dados armazenados.
- Ao enviar equipamentos para manutenção escolha empresas com boa reputação.
- Seja cuidadoso ao usar equipamentos de terceiros ou potencialmente infectados.

Sobre os e-mails e mensagens eletrônicas:

- Desconfie de links ou pedidos de pagamentos recebidos via mensagens eletrônicas, mesmo que vindos de pessoas conhecidas, pois podem ter sido enviadas de perfis falsos ou invadidos.
- Seja cuidadoso ao acessar seu webmail, digite a URL diretamente no navegador.
- Armazene e-mails confidenciais em formato criptografado, para evitar que sejam lidos por atacantes ou códigos maliciosos, você pode decodificá-los sempre que desejar lê-los.

Como Reduzir a Quantidade de Dados sobre Você

Você sabia que todas as vezes que acessa seus equipamentos e “entra na internet” alguns de seus dados são de alguma forma fornecidos?

Cada vez que acessa um site, assiste a um vídeo ou compra algo, deixa marcas de sua passagem, essas marcas são chamadas vestígios, rastros ou pegadas digitais, permite criar sua reputação online e definir seu perfil comportamental.

Sobre os dados que você divulga:

- Pense bem antes de divulgar algo, depois será difícil de excluir.
- Seja seletivo ao aceitar seus contatos nas redes sociais.
- Ao preencher cadastros questione-se sobre a necessidade de fornecer todos os dados solicitados, e da instituição retê-los.

E sobre os dados coletados sobre você:

- Use conexões seguras.
- Seja seletivo ao baixar aplicativos.
- Observe as configurações de privacidade de seus aplicativos e navegadores.
- Ao acessar sites, procure limitar a coleta de dados por cookies, preferencialmente, autorize somente aqueles essenciais ao funcionamento da sessão.
- Limpe frequentemente o histórico de navegação.

Lei Geral de Proteção de Dados

Criada para que:

- O indivíduo tenha controle sobre seus dados pessoais.
- Saiba como esses dados são tratados por organizações públicas, privadas e terceiros.

Dados pessoais, segundo a LGPD:

- Informações relacionadas a pessoa natural identificada ou identificável.

Como titular de dados pessoais você tem diversos direitos garantidos pela LGPD, como os definidos no Art. 18.

A LGPD:

- Dá a você o direito de saber como seus dados são exatamente tratados, quais os dados são coletados e o porquê e com quem seus dados são compartilhados. Traz maior segurança jurídica ao fornecer mecanismos para que você tenha controle sobre quais dados seus são coletados e como são usados.

Organizações públicas e privadas deve disponibilizar informações claras que o ajudem a compreender:

- Os termos de consentimento.
- As bases legais que apoiam o tratamento dos seus dados.

Caso a instituição responsável pelo tratamento de seus dados pessoais não atenda a um de seus direitos de titular sem uma justificativa legal:

- Você tem o direito de peticionar uma reclamação para a Autoridade Nacional de Proteção de Dados – ANPD.

Vazamento de Dados – Parte 1

Ocorrem quando dados são indevidamente acessados, coletados e divulgado na internet, ou repassados a terceiros.

Com a disseminação dos serviços online, seus dados estão cada vez mais expostos e sendo coletados pelos diferentes serviços disponíveis.

Pode ser originado:

- Do furto de dados por atacantes e códigos maliciosos que exploram vulnerabilidades em sistemas.
- Do acesso a contas de usuários, por meio de senhas fracas ou vazadas.
- Da ação de funcionários ou ex-funcionários que coletam dados dos sistemas da empresa e os repassam a terceiros.
- Do furto de equipamentos que contenham dados sigilosos.
- De erros ou negligência de funcionários, como descartas mídias (discos e pen-drives), sem os devidos cuidados.

Vazamento de Dados – Parte 2

Exemplo de dados que podem vazar:

- Credenciais de acesso, como nomes de usuário e senhas.
- Informações financeiras, como números de contas bancárias e de cartões de crédito.
- Documentos, como CPF, RG e carteira de habilitação.
- Informações de contato, como endereços e números de telefone.
- Registros de saúde, como resultados de exames e prontuários médicos.
- Outros dados, como data de nascimento e nomes de familiares.

Para evitar vazamentos é importante que todos contribuam. Você pode ajudar reduzindo a quantidade de dados expostos sobre você. Fique atento e, no caso de um vazamento envolvendo seus dados, procure agir rapidamente para reduzir os danos.

Após um vazamento é esperado um aumento nas tentativas de golpes por diferentes meios, como e-mails, mensagens de texto e ligações telefônicas.

Furto de Identidade e Tentativas de Golpes

Sobre o furto de identidade e invasão de contas online:

- Abertura de contas em seu nome.
- Tentativas de adivinhação de senhas.

- Responder perguntas de segurança.
- Uso das senhas vazadas para invadir os serviços onde foram criadas, invadir outros serviços onde a mesma senha seja usada, e mecanismos adicionais não estejam ativados (verificação em duas etapas e autorização prévia de dispositivos).

Furto de identidade levando a prejuízos financeiros:

- Criação de cartões de crédito, contas bancárias e empréstimos, levando a dívidas e transações ilícitas em seu nome.
- Movimentações financeiras indevidas em suas contas bancárias ou cartões de crédito.
- Transferência de bens móveis ou imóveis.

Informações privadas podem ficar expostas na internet, como:

- Dados médicos.
- Conversas particulares.

E sobre as tentativas de golpes:

- Extorsão, onde o atacante faz chantagem para não expor os seus dados.
- Quanto mais informações um atacante tiver, mais convincente ele será, e mais facilmente enganará outras pessoas.
- Dados vazados podem ser usados em tentativas de phishing direcionado e personalizado (spear phishing), para convencê-lo a revelar mais informações, para induzi-lo a efetivar transações, e para se passar por você.

O que Fazer em Caso de Vazamento de Dados – Parte 1

Se receber notificações ou souber pela mídia de algum vazamento envolvendo seus dados pessoais, informe-se sobre o ocorrido e tente identificar:

- Quais dados vazaram (isso ajuda a saber quais medidas tomar).
- Quais medidas de mitigação foram ou serão tomadas pela organização.
- Quais medidas devem ser tomadas por você.
- As datas do potencial vazamento.
- Comunicados e notícias a respeito.

Evite acessar sites e abrir arquivos que supostamente confirmem ou exibam os dados do vazamento. Em caso de dúvida, contate diretamente as organizações envolvidas e busque mais informações.

O que Fazer em Caso de Vazamentos de Dados – Parte 2

O que fazer em caso de credenciais de acesso vazadas:

- Troque imediatamente as senhas expostas.
- Ative a verificação de duas etapas nas contas que ofereçam esse recurso, caso ainda não tenha feito.
- Use os mecanismos disponíveis para analisar os registros de acesso e denunciar tentativas/acessos indevidos.

O que fazer em caso de cartões de crédito ou débito vazados:

- Informe as instituições emissoras dos cartões.
- Revise o extrato dos seus cartões e da sua conta bancária.
- Conteste os eventuais lançamentos irregulares que identificar (use os canais oficiais das respectivas instituições).

Fique Atento ao Utilizar a Internet

Monitore sua vida financeira e sua identidade:

- Ative alertas e monitore o extrato dos seus cartões e da sua conta bancária (preste atenção a movimentações “estranhas”).
- Acompanhe outros registros financeiros, por meio de serviços específicos, como o oferecido pelo Banco Central (Serviço Registrado).
- Verifique no “Cadastro Pré” se alguma linha pré-paga de celular foi ativada usando seu CPF (mantido por empresas do setor de telecomunicações).
- Busque saber mais se receber notificações de instituições de proteção ao crédito, e ao tentar se cadastrar em algum serviço ou benefício, for informado que seu cadastro já existe.

Cuide de suas contas e senhas:

- Não forneça códigos de verificação a terceiros.
- Ative notificações.
- Monitore tentativas de login, recuperação de senhas e trocas de senhas.

Se constatar que alguma conta foi invadida ou criaram um perfil em seu nome:

- Efetue os procedimentos disponíveis nas plataformas para recuperação do acesso ou denúncia do perfil falso.
- Informe seus contatos para que não caiam em golpes.

Previna-se contra golpes:

- Não clique em links recebidos por e-mail ou mensagens de texto, mesmo que pareçam enviados por alguém que você conhece, pois pode ser um spear phishing.
- Não efetive transações financeiras sem antes confirmar a identidade das partes envolvidas.

A quem Recorrer em Caso de Vazamentos

Quem contatar, caso você verifique que seus dados foram usados de maneira fraudulenta ou foi prejudicado:

- **Fraude Financeira:** Contate as instituições envolvidas, e siga as orientações recebidas.
- **Furto de Identidade:** Registre boletim de ocorrência junto à autoridade policial, para viabilizar a apuração e resguardar-se. E contate as instituições envolvidas.

Se comprovadamente ocorrer um vazamento envolvendo seus dados pessoais:

- Busque informações junto a instituição responsável, também chamada “controladora de dados”.

Caso sua solicitação não seja atendida ou não saiba qual instituição está envolvida:

- Denuncie no site da Autoridade Nacional de Proteção de Dados, informando quais os dados vazados, quando teve ciência do vazamento, se acredita que seus dados pessoais foram indevidamente usados em alguma ação criminosa (como estelionato, fraude ou comércio ilegal de dados pessoais), e quais evidências possui para comprovar essa hipótese).

Não incentive vazamentos e abusos:

- Não compre lista de dados (essa prática incentiva que mais vazamentos ocorram, e coloca todos em risco, inclusive você).
- Evite acessar sites e abrir arquivos que supostamente confirmem ou exibam os dados vazados (eles podem ter sido criados com fins maliciosos para expor ainda mais seus dados).

Como se Prevenir

Procure reduzir a quantidade de dados que possam ser divulgados sobre você:

- Seus dados pessoais são valiosos.
- Instituições têm interesse em obtê-los para fins comerciais.
- Atacantes têm interesse em obtê-los para ações maliciosas.

Cadastros e sites:

- Ao preencher cadastros, questione-se sobre a real necessidade de fornecer todos os dados, e da instituição reter seus dados.
- Leia as políticas de privacidade dos serviços que usa.
- Ao acessar sites, procure limitar a coleta de dados por cookies, preferencialmente, autorize somente aqueles essenciais ao funcionamento da sessão, e limpe frequentemente o histórico de navegação.
- Use conexões seguras para evitar que seus dados sejam interceptados e coletados.

Links e aplicativos:

- Desconfie de links recebidos via mensagens eletrônicas, mesmo que vindos de pessoas conhecidas (as mensagens podem ter sido enviadas de perfis falsos ou invadidos).
- Observe as configurações de privacidade de seus equipamentos e dos softwares instalados (limite quais aplicativos podem acessar o microfone, a câmera, seus contatos e sua localização).
- Apague os aplicativos que você não usa mais.

Contas e senhas:

- Crie senhas fortes.
- Não repita suas senhas.
- Habilite a verificação em duas etapas, sempre que possível.
- Habilite notificações de login, sempre que esse recurso estiver disponível.

Arquivos e equipamentos:

- Mantenha seus equipamentos seguros, com o sistema e os aplicativos atualizados e utilize mecanismos de segurança.
- Verifique no monitor de atividades de seu equipamento a lista de programas em execução e desconfie de processos “estranhos”.
- Evite colocar na nuvem arquivos contendo dados pessoais que considere confidenciais, como fotos e cópias de documentos.
- Use criptografia, sempre que possível, para proteger os dados armazenados em seus equipamentos.