
SENAI

CIBERSEGURANÇA

SISTEMAS OPERACIONAIS

PROF. ESP. RENATO OLIVEIRA

Introdução

A cibersegurança é um conjunto de ações e técnicas para proteger sistemas, programas, redes e equipamentos de invasões, ataques cibernéticos ou acessos não autorizados, evitando assim vazamento de informações que são consideradas valiosas ou mesmo que essas informações sejam violadas durante o ataque.

Ataques cibernéticos tem a intenção de acessar servidores ou serviços em rede, roubar senhas, sequestrar dados ou até mesmo fraudar transações financeiras.

Todo dispositivo conectado à internet precisa se preocuprar com a cibersegurança, uma vez que uma pessoa má intencionada pode tentar obter acesso não autorizado as informações deste dispositivo.

Introdução

A segurança de dispositivos digitais vai além de softwares e ferramenta de segurança como antivirus, antimalwares, firewalls e etc.

Um fator muito importante na segurança cibernética é o fator humano, já que este desempenha um dos principais papéis neste cenário.

O ser humano é **o componente chave** de um sistema, pois é ele que irá consumir, utilizar e manipular as informações.

Cibersegurança envolve também processos burocráticos e normas para acesso à informação, tendo até normas internacionais para isso, como a ISO 27000, ISO 27001, ISO 27002 e ISO 27003.

AMEAÇAS

Ameaças

Uma ameça é qualquer coisa que comprometa a informação, pode ser um fator humano, lógico ou alguma ferramenta construída com o intuito de obter acesso não autorizado.

Entre elas existem:

- Cavalos de tróia
- Botnets
- Spyware
- Worms
- Ransomware
- Phishing

AMEAÇAS VIRTUAIS

Spyware

- **Spyware:** É uma forma de malware que se esconde em nosso dispositivo, monitora nossa atividade e pode roubar informações sensíveis como dados bancários, logins e senhas.

- Pode infectar computadores ou celulares, coletar informações sobre nós, nossa navegação e hábitos de uso da Internet.

- É executado silenciosamente em segundo plano, coletando informações ou monitorando nossas atividades.

- Pode capturar pressionamento de teclas, capturas de tela, credenciais de acesso, endereço de e-mail pessoal, dados de formulário da rede, informações pessoais, como números de cartão de crédito, etc.

AMEAÇAS VIRTUAIS

Spyware

- O contágio é da mesma forma que o adware. Através de instalação de programas suspeitos, navegação em sites fraudulentos ou através de dispositivos USB infectados.

- **Forma de remoção**: Através de softwares antivírus e em alguns casos dá para se remover manualmente.

AMEAÇAS VIRTUAIS

Phishing

- O termo phishing foi escolhido devido à semelhança com outra palavra do vocabulário inglês, fishing, que significa pescar. Isso quer dizer a prática de “pescar” as informações e dados secretos dos usuários através de mensagens falsas e atrativas, uma espécie de estelionato.

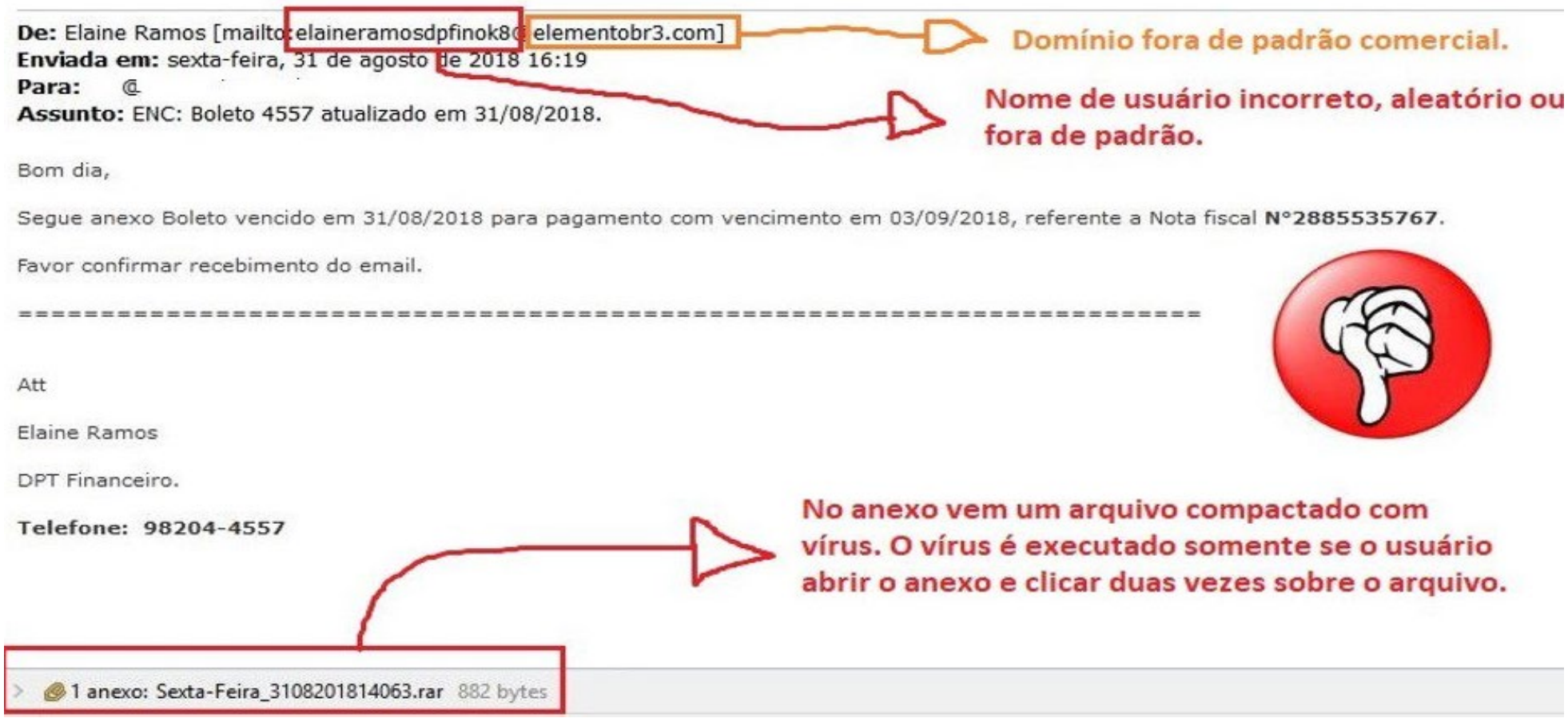
- O criminoso que pratica o phishing consegue estas informações através de uma **isca** lançada aos usuários para então obter as ações que precisam para aplicar os golpes.

- É um crime virtual no qual pessoas comuns são contactadas através de e-mail, telefone ou mensagens de texto (SMS) por uma outra pessoa ou empresa.

- Incluem mensagens falsas e apelativas tais como: "Alguém tentou acessar sua conta", "boleto está vencido", "notificação extrajudicial", "mensagens de whatsapp da Fulana", etc.

AMEAÇAS VIRTUAIS

Phishing



AMEAÇAS VIRTUAIS

Ransomware

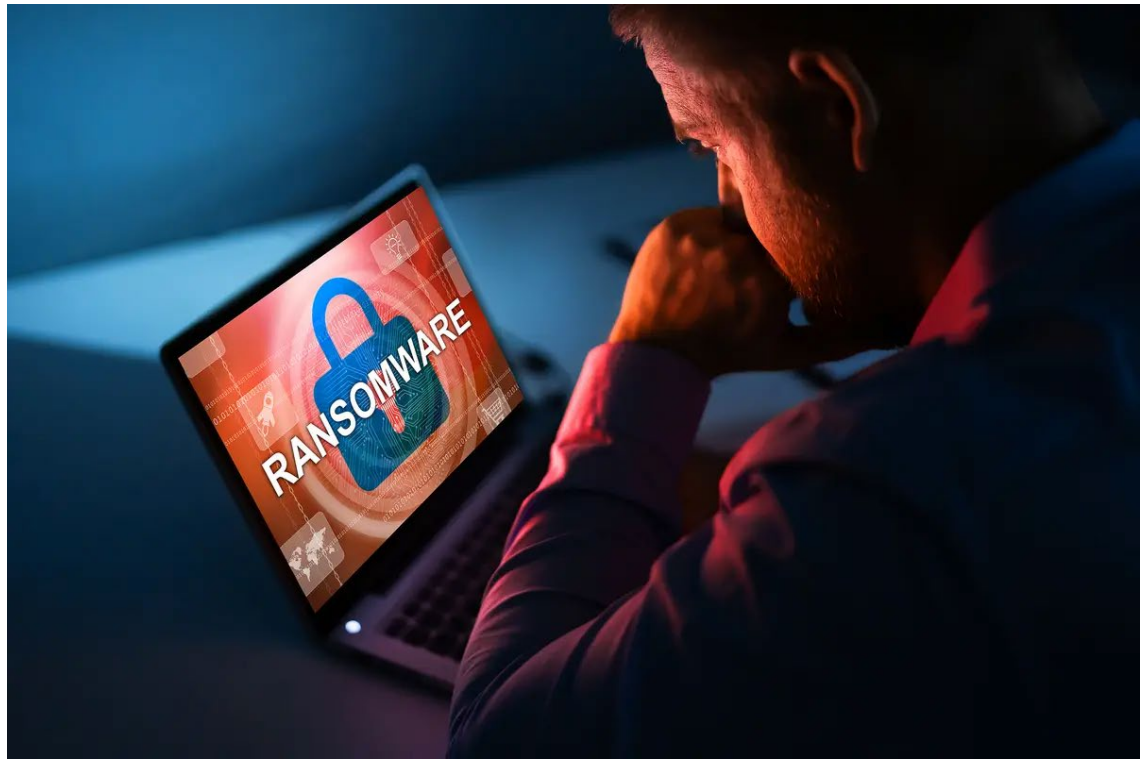
- É um malware que criptografa arquivos do nosso HD ou outros dispositivos de armazenamento e de rede.
- Exige um resgate para descriptografar os arquivos. Os atacantes desenvolvem esse malware para ganhar dinheiro com extorsão digital.
- O objetivo é deixar os usuários sem acesso aos arquivos (porque foram criptografados): planilhas excel, arquivos do Word, arquivos pdf, imagens, fotos, arquivos de bancos de dados, etc.
- Dessa forma os criminosos exigem um pagamento em dinheiro (geralmente bitcoin) para passar a chave que supostamente irá descriptografar os arquivos.

AMEAÇAS VIRTUAIS

Ransomware

- Tipos de arquivos que um ransomware procura criptografar:

- **Microsoft Office:** .xlsx, .docx, .pptx e suas versões antigas
- **Imagens:** .jpeg, .png, .jpg, .gif, .tiff
- **Imagens relacionadas a negócios:** .dwg
- **Bancos de dados:** .sql e .ai
- **Vìdeos:** .avi, .m4a, .mp4



AMEAÇAS VIRTUAIS

Ransomware

- É atualmente a maior ameaça para usuários comuns e empresas, sendo uma fonte enorme de paradas de sistemas, roubo de informações, paralização de operações inteiras.

- Várias instituições são alvos dos atacantes de ransomware: Grandes e pequenas empresas, hospitais, sedes de governos de diversos países.

- https://www.youtube.com/watch?v=nrrty3rMTIM - Ransomware GoldenEye

- https://www.youtube.com/watch?v=aw2IFNwvYmw - Cisco – Bastidores de um ataque phishing + ramsonware.

AMEAÇAS VIRTUAIS

Ransomware

Formas de contágio

- Anexos de e-mails (phishing)
- Download e instalação de softwares suspeitos
- Instalação de softwares "piratas"

Prevenção

- Deixar sistema operacional sempre atualizado
- Ter instalado um bom software antivírus
- E, principalmente, ter backup dos arquivos (de preferência em nuvem)
- Conscientização.

AMEAÇAS VIRTUAIS

Zero-Day Exploit – Falha dia zero

Dia zero é um termo que descreve uma falha de segurança recém descoberta por hackers para atacar um sistema. Isso quer dizer que o fornecedor ou desenvolvedor acabou de conhecer a falha e precisa trabalhar na correção dela, enquanto isso seu sistema está vulnerável ao hacker.

AMEAÇAS VIRTUAIS

Zero-Day Exploit – Falha dia zero

- Uma **vulnerabilidade de dia zero** 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 o ataque ser bem-sucedido.

- Uma **exploração de dia zero** é o método que os hackers usam para atacar os sistemas com uma vulnerabilidade não identificada anteriormente.

- Um **ataque de dia zero** é o uso de uma exploração de dia zero para causar danos ou roubar dados de um sistema afetado por uma vulnerabilidade.

VULNERABILIDADES

Vulnerabilidades

Segundo a OWASP (Open Worldwide Application Security Project), uma vulnerabilidade é uma **falha ou fraqueza** no aplicativo, que **pode ser uma falha de design ou um bug de implementação**, que permite que um invasor cause danos às partes interessadas de um aplicativo. As partes interessadas incluem o proprietário do aplicativo, os usuários do aplicativo e outras entidades que dependem do aplicativo.

Exemplos de vulnerabilidades

- Falta de validação de entrada na entrada do usuário
- Falta de mecanismo de registro suficiente
- Tratamento de erros de falha aberta
- Não fechando a conexão com o banco de dados corretamente

Vulnerabilidades

Uma vulnerabilidade não é apenas de lógica (software), existem alguns tipos de vulnerabilidades, como:

- Vulnerabilidades de Hardware
- Vulnerabilidades de Software
- Vulnerabilidades de Rede
- Vulnerabilidade de Pessoal
- Vulnerabilidade Organizacional

Vulnerabilidades

Uma vulnerabilidade pode ser explorada por um hacker para obter acesso não autorizado a informações de uma empresa ou indivíduo.

As vulnerabilidades de software mais exploradas por hackers em 2023 foram:

- **Buffer Overflow** (Estouro de memória)
- **RCE** (Remote Code Execution, Execução de código remoto)
- **Privilege Escalation** (Escalada de privilégios)
- **Authentication Bypass** (Desvio de Autenticação)

CREDENCIAIS

Credenciais

Credenciais são uma forma de autenticar um usuário para obter acesso a um sistema e suas informações.

O modelo mais básico de credenciais que existe são o **nome de usuário** e **senha**, que ficam salvos em um banco de dados do sistema a ser acessado.

Com o avanço da tecnologia e a conectividade, outras credenciais foram criadas para aumentar a forma de acessar as informações de forma segura.

Credenciais

SENHAS

Senhas foram um dos primeiros tipos de credenciais criadas, e consistem em uma palavra secreta onde somente o dono deve ter acesso.

Ao tentatar acessar uma informação ou serviço confidencial, essa senha seria solicitada ao usuário e depois validada para fornecer o acesso.

Credenciais

SENHAS

Embora existam meios mais seguros de credenciais, a senha ainda é a mais utilizada, é altamente recomendado que a senha seja forte, dificultando assim técnicas de força bruta com objetivo de quebrar essa senha.

Para uma senha ser considerada forte, é necessário que ela possua pelo menos 8 caracteres, incluindo letras maiúsculas e minúsculas, números e caracteres especiais.

Exemplos de senhas fortes

AS3nH@!$2023

C0mpl3xP@$$

C4ch0RRo$LaT3s!

Roxo$Céu#987

Credenciais

BIOMETRIA

Pode ser usado como um tipo de credencial;

É um tipo de credencial que usa dados corporais dos seres humanos para validar o acesso a um sistema;

Por ser

- **Reconhecimento facial**
- **Impressão digital**
- **Reconhecimento ocular**

Credenciais

Autenticação biométrica – Reconhecimento facial

- Como o próprio nome já diz, é o método que transforma em dados as medidas e características de nosso rosto. Nossas características faciais são digitalizadas e assim podem ser comparadas pelos sistemas.

- O software de reconhecimento facial analisa a geometria do rosto, incluindo a distância entre os olhos, a distância entre o queixo e o nariz, etc., para criar um modelo digital criptografado de nossos dados faciais.

- Ao autenticar, a ferramenta de reconhecimento facial digitaliza nosso rosto em tempo real e compara o modelo ao modelo armazenado no sistema.

Credenciais

Autenticação biométrica – Impressão digital

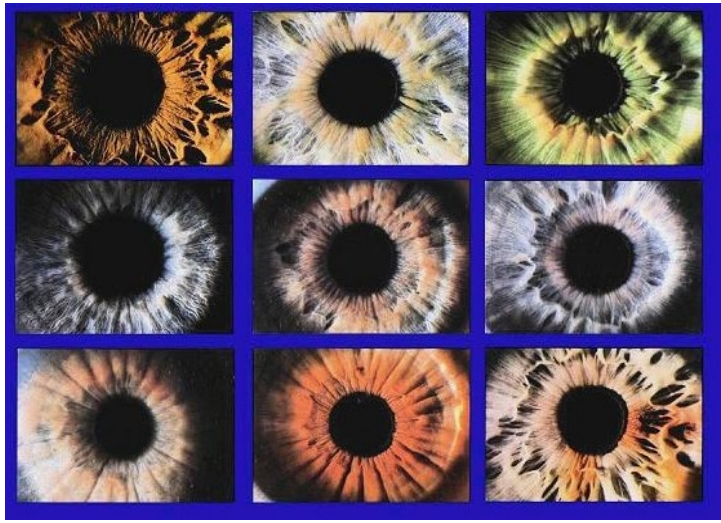
- É o método que digitaliza nossas impressões digitais e compara essa digitalização com a digital colocada em um leitor.

- As impressões digitais são únicas, para cada indivíduo. Assim, analisando os sulcos e o padrão da impressão, os scanners de impressão digital criam um modelo digital que é comparado com tentativas futuras de autenticação.

Credenciais

Autenticação biométrica – Reconhecimento ocular

- É a metodologia de autenticação realizada através da leitura, identificação e digitalização da íris ou retina de nossos olhos.
- No dispositivo verificador ocular é gerada uma breve luz no olho do usuário para iluminar o padrão único de vasos sanguíneos no olho.
- Ao mapear esse padrão, a ferramenta de reconhecimento ocular pode comparar os olhos de um usuário com um original.
- As digitalizações de íris funcionam da mesma forma, mas analisam os anéis coloridos encontrados na íris.



Credenciais

AUTENTICAÇÃO EM DOIS FATORES (2FA)

A autenticação em dois fatores adiciona uma camada adicional de segurança as credencias;

Agora além de digitar seu usuário e senha, é necessário que o usuário interaja com algum mecanismo que valide que é ele mesmo que está tentando obter o acesso.

Dentre os métodos de autenticação em dois fatores mais utilizados, o mais utilizado são aplicativos de MFA como o Google Authenticator e o Microsoft Authenticator, que geram um código de autenticação temporário para acesso a conta.

Credenciais

AUTENTICAÇÃO EM DOIS FATORES (2FA)

O uso desses aplicativos é altamente recomendável, já que, para que um hacker possa acessar sua conta caso ele tenha posse da senha, ele irá precisar interagir com o aplicativo que está instalado no seu telefone, dificultando muito o acesso não permitiado a conta.

Hoje em dia, todo serviço grande na internet oferece a configuração de um aplicativo para verificação em duas etapas.

Se você quer evitar perder fotos e documentos pessoais que estão em algum serviço na internet, recomendo a utilização e configuração dessa aplicativo o mais rápido possível.

Credenciais

AUTENTICAÇÃO EM DOIS FATORES (2FA)

Dependendo do aparelho celular onde o aplicativo está instalado, é possível utilizar o acesso biométrico ao invés do código temporário.

Um exemplo seria a identificação por **impressão digital** em dispositivos Android.

Outro exemplo seria o **reconhecimento facial** do sistema iOS.

Dúvidas

Referências

Cibersegurança: o que é, importância, tipos e carreira na área – **Acessado em 09/05/2024**

https://fia.com.br/blog/ciberseguranca/

O que é cibersegurança? – **Acessado em 09/05/2024**

https://www.sap.com/brazil/products/financial-management/what-is-cybersecurity.html

Vulnerabilities, OWASP – **Acessado em 09/05/2024**

https://owasp.org/www-community/vulnerabilities/#