Cibersegurança – Ataques Cibernéticos à Rede de Dados e Códigos Maliciosos

Seminários – DI

Prof. Anderson Oliveira da Silva, phD

Engenheiro de Computação

Gestor de Segurança da Informação

Encarregado de Dados Pessoais

anderson@inf.puc-rio.br

linkedin.com/in/anderson-oliveira-da-silva-58221680

Departamento de Informática

PUC-Rio

Ementa

Cibersegurança – Ataques Cibernéticos à Rede de Dados e Códigos Maliciosos:

- Segurança da Informação x Cibersegurança
- Proteção dos ativos de Informação
- Dados x Informação x Conhecimento
- Conceitos de Cibersegurança
  - Ciberespaço
  - Segurança Ofensiva e Segurança Defensiva
  - Red Team e Blue Team
  - Hacking e Pen Test

Ementa

Cibersegurança – Ataques Cibernéticos à Rede de Dados e Códigos Maliciosos:

- Vulnerabilidade, Ameaça e Ataque
- Tipos de Vulnerabilidades
  - vulnerabilidade no design ou na especificação;
  - vulnerabilidade na implantação; e
  - vulnerabilidade na operação e no gerenciamento.
- Classificação de Ameaças
  - Ameaças Acidentais
  - Ameaças Intencionais

Ementa

Cibersegurança – Ataques Cibernéticos à Rede de Dados e Códigos Maliciosos:

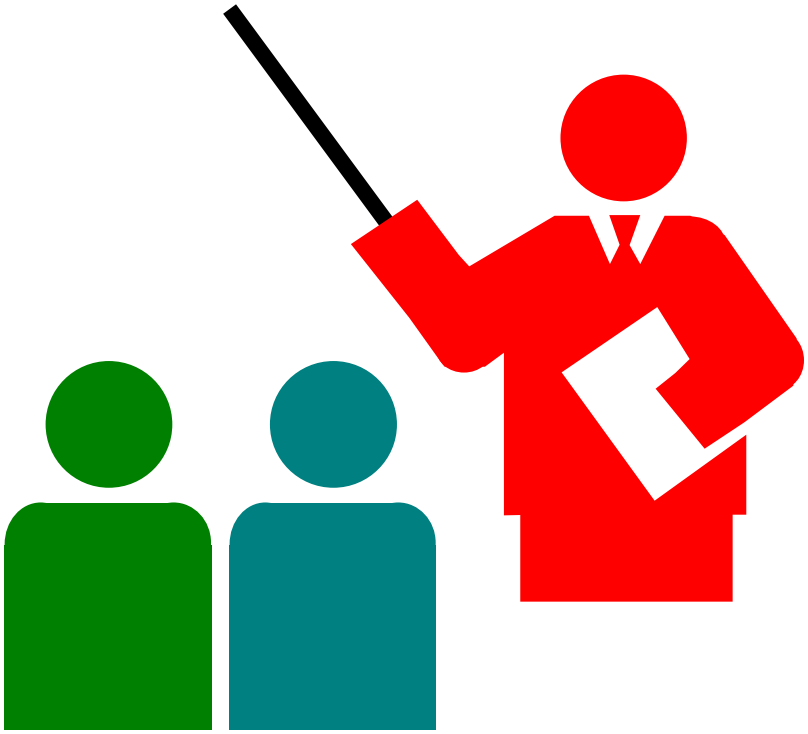
- Classificação de Ataques
  - Ataque interno (inside attack)
  - Ataque externo (outside attack)
  - Ataques passivos
    - Inspeção de Conteúdo
    - Análise de Tráfego
  - Ataques ativos
    - Interceptação com Modificação da Mensagem
    - Disfarce (Masquerade ou Spoofing)
    - Repetição (Replay)
    - Negação de Serviço (DoS - Denial of Service) - Botnets

Ementa

Cibersegurança – Ataques Cibernéticos à Rede de Dados e Códigos Maliciosos:

- Código Malicioso (Malware)
  - Vírus
  - Worm
  - Cavalo de Tróia
  - Backdoor
  - Keylogger
  - Screenlogger
  - Downloader
  - Injector
  - Flooder
  - Ransomware
  - Spyware e Adware
  - Formjacker

Cibersegurança



Segurança da Informação x Cibersegurança

Qual é a diferença entre segurança da informação e cibersegurança?

- **Segurança da informação**
  - Visa assegurar a **proteção dos ativos de informação** da organização através da **seleção** e da **aplicação de salvaguardas** apropriadas e alinhadas com o **objetivo do negócio** e a **missão da organização**.
    - Os **ativos de informação** podem estar presentes ou ser acessados em diferentes **tipos de meios**, **software** ou **hardware**.

- **Cibersegurança (Segurança Cibernética)**
  - Visa assegurar a **proteção dos ativos de informação** das organizações que **operam no ciberespaço (espaço cibernético)** contra as **ameaças cibernéticas** para manter um **nível aceitável** de **estabilidade**, **continuidade** e **segurança**.

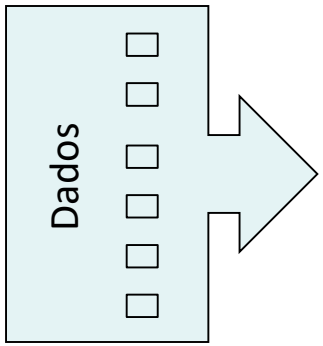
Proteção dos ativos de Informação

Por que precisamos proteger os ativos de informação da organização?

Dados x Informação x Conhecimento

Precisamos entender a diferença e a relação entre dados, informação e conhecimento...

- **As empresas diariamente produzem uma enorme quantidade de dados...**



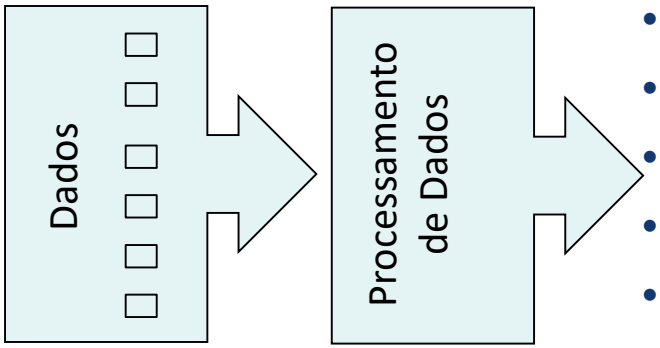
matéria-prima

- **Dados são elementos básicos, sem contexto ou significado específico, que podem ser quantificados, medidos ou observados.**
  - **Números: 55, 21, 3527, 1500, 225, 3, 15.000, ...**
  - **Palavras: Anderson, Silva, Marquês, São, Vicente, Brasil, Rio, Janeiro, PUC, INF, Gávea, Rua, ...**
  - **Símbolos: $, %, #, @, &, ...**

Dados x Informação x Conhecimento

Precisamos entender a diferença e a relação entre dados, informação e conhecimento...

- **...que servem como matéria-prima para o processamento de dados...**



matéria-prima

organização ou estruturação dos dados

- **Nome:** Anderson da Silva
- **Idade:** 55
- **Telefone:** 21 3527-1500
- **Local:** Rua Marquês de São Vicente, 225
- **Bairro:** Gávea
- **Cidade:** Rio de Janeiro
- **Empresa:** PUC-Rio
- **Departamento:** INF
- **E-mail:** anderson@inf.puc-rio.br
- **Salário-base:** R$ 15.000,00
- **Anuênio:** 3,0%

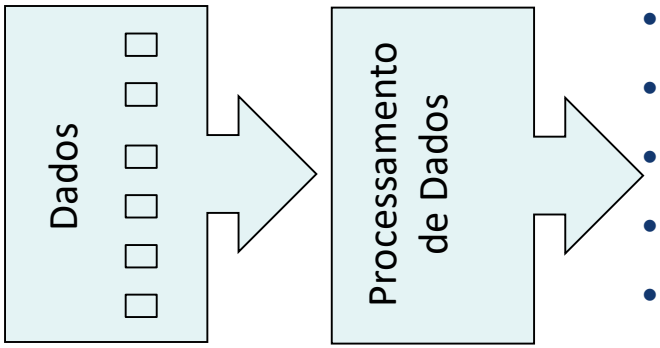
DEPARTAMENTO DE INFORMÁTICA PUC-RIO

PUC RIO

Dados x Informação x Conhecimento

Precisamos entender a diferença e a relação entre dados, informação e conhecimento...

- **...que servem como matéria-prima para o processamento de dados...**



matéria-prima

organização ou estruturação dos dados

- **Exportador: Anderson & Silva**
- **Código do item: 55-21-3527**
- **Quantidade: 1500**
- **Destino: Rua Marquês de São Vicente, 225**
- **Bairro: Gávea**
- **Cidade: Rio de Janeiro**
- **Importador: PUC-Rio**
- **Departamento: INF**
- **E-mail: anderson@inf.puc-rio.br**
- **Valor do item: R$ 15.000,00**
- **Taxa de frete: 3,0%**

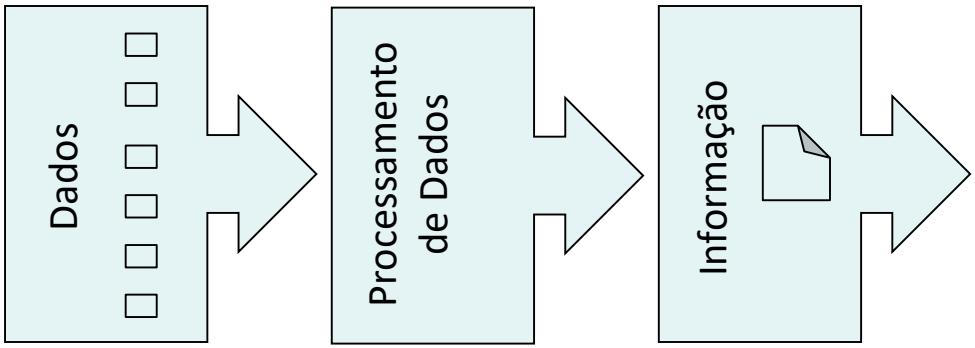
DEPARTAMENTO DE INFORMÁTICA PUC-RIO

PUC RIO

Dados x Informação x Conhecimento

Precisamos entender a diferença e a relação entre dados, informação e conhecimento...

- **...que produz informação (produto intermediário)...**



matéria-prima

organização ou estruturação dos dados

produto intermediário

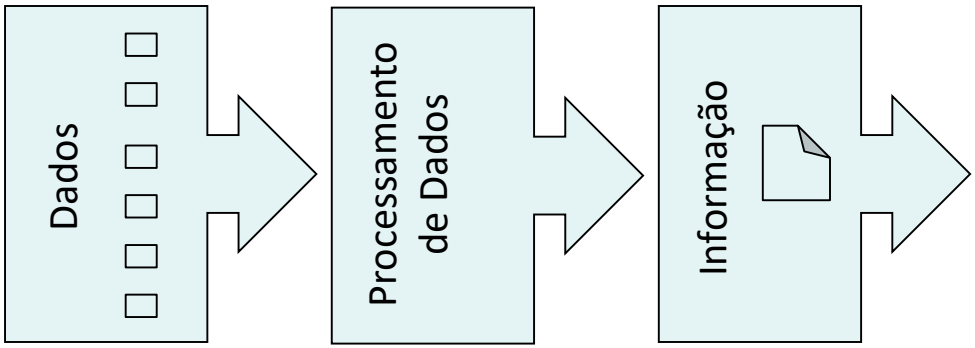
- **Informação de identificação pessoal**

  - **Nome:** Anderson da Silva
  - **Idade:** 55
  - **Telefone:** 21 3527-1500
  - **Local:** Rua Marquês de São Vicente, 225
  - **Bairro:** Gávea
  - **Cidade:** Rio de Janeiro
  - **Empresa:** PUC-Rio
  - **Departamento:** INF
  - **E-mail:** anderson@inf.puc-rio.br
  - **Salário-base:** R$ 15.000,00
  - **Anuênio:** 3,0%

Dados x Informação x Conhecimento

Precisamos entender a diferença e a relação entre dados, informação e conhecimento...

- **...que produz informação (produto intermediário)...**



matéria-prima

organização ou estruturação dos dados

produto intermediário

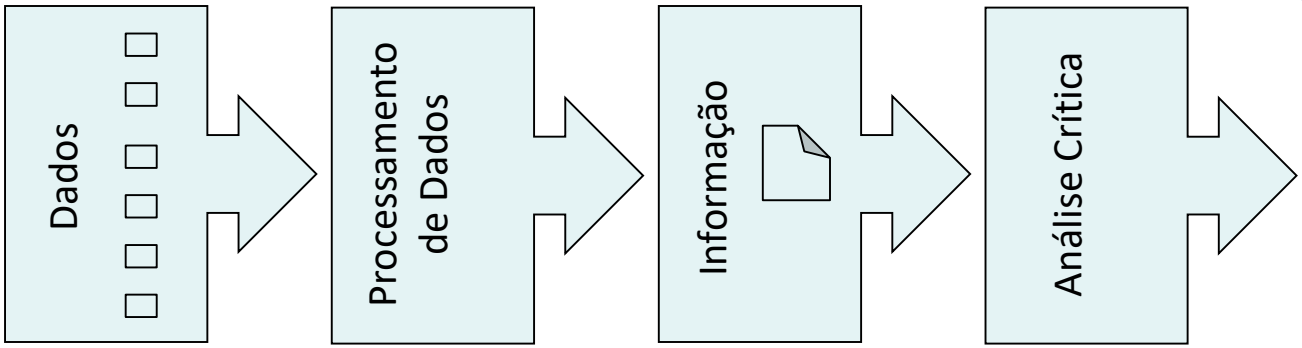
- **Informação de importação de produto**

  - Exportador: Anderson & Silva
  - Código do item: 55-21-3527
  - Quantidade: 1500
  - Destino: Rua Marquês de São Vicente, 225
  - Bairro: Gávea
  - Cidade: Rio de Janeiro
  - Importador: PUC-Rio
  - Departamento: INF
  - E-mail: anderson@inf.puc-rio.br
  - Valor do item: R$ 15.000,00
  - Taxa de frete: 3,0%

Dados x Informação x Conhecimento

Precisamos entender a diferença e a relação entre dados, informação e conhecimento...

- **Quando realizamos a análise crítica da informação num determinado contexto...**



matéria-prima

organização ou estruturação dos dados

produto intermediário

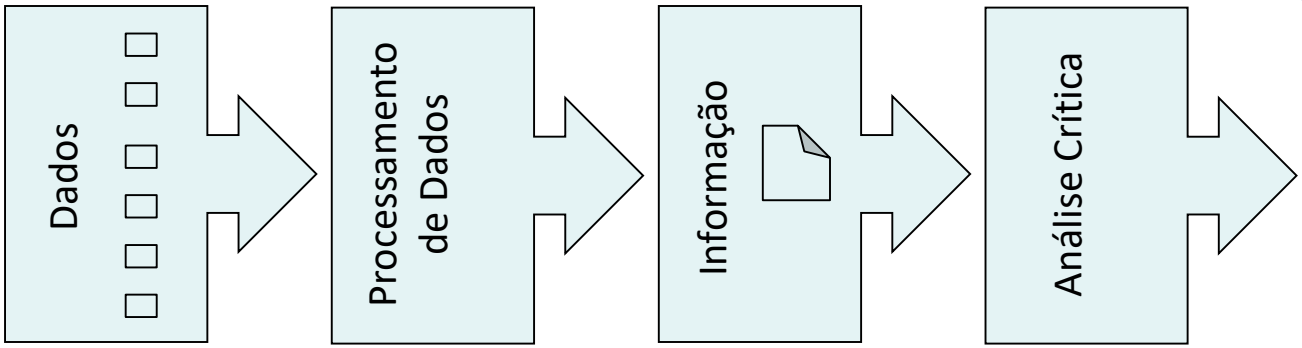
tratamento da informação em determinado contexto

- **Existem funcionários bem avaliados com salário inferior à média do mercado?**

Dados x Informação x Conhecimento

Precisamos entender a diferença e a relação entre dados, informação e conhecimento...

- **Quando realizamos a análise crítica da informação num determinado contexto...**



matéria-prima

organização ou estruturação dos dados

produto intermediário

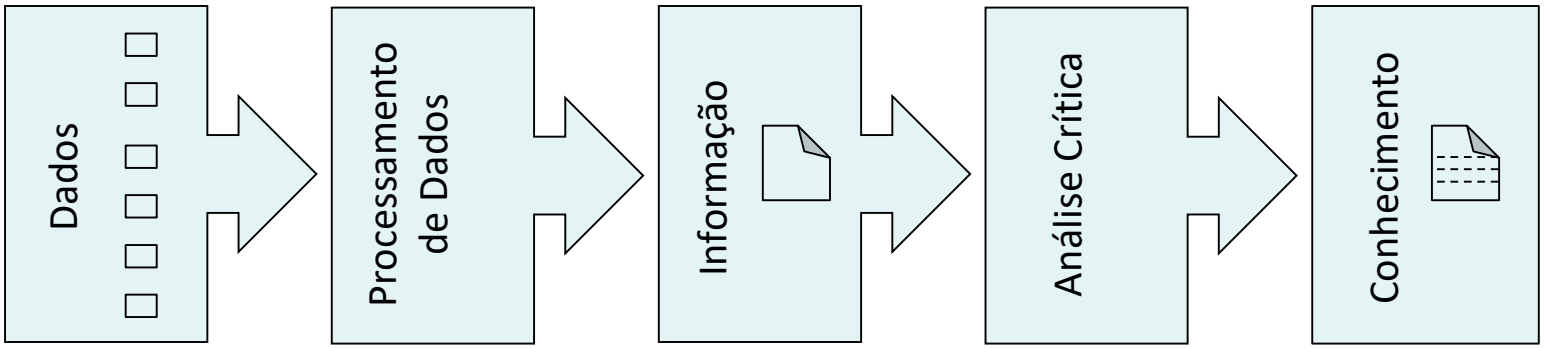
tratamento da informação em determinado contexto

- **Quais são as opções de importação que podem reduzir a taxa de frete para o cliente?**

Dados x Informação x Conhecimento

Precisamos entender a diferença e a relação entre dados, informação e conhecimento...

- **...produzimos conhecimento.**



matéria-prima

organização ou estruturação dos dados

produto intermediário

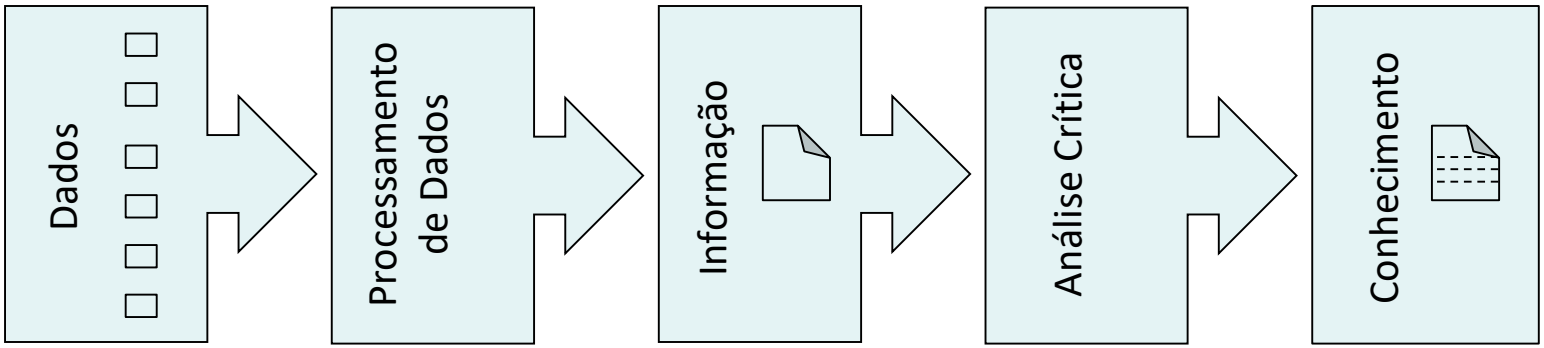
tratamento da informação em determinado contexto

produto final

Valor dos ativos de informação

Por que os ativos de informação são valiosos para uma empresa?

- **Informação e conhecimento são fundamentais para a tomada de decisão e resolução de problemas.**



matéria-prima

organização ou estruturação dos dados

produto intermediário

tratamento da informação em determinado contexto

produto final

Cibersegurança – Conceitos Básicos

Conceitos básicos: Ciberespaço (Espaço Cibernético)

- **É o espaço formado pela interligação de computadores e sistemas eletrônicos do mundo inteiro, onde as informações circulam e são compartilhadas globalmente.**

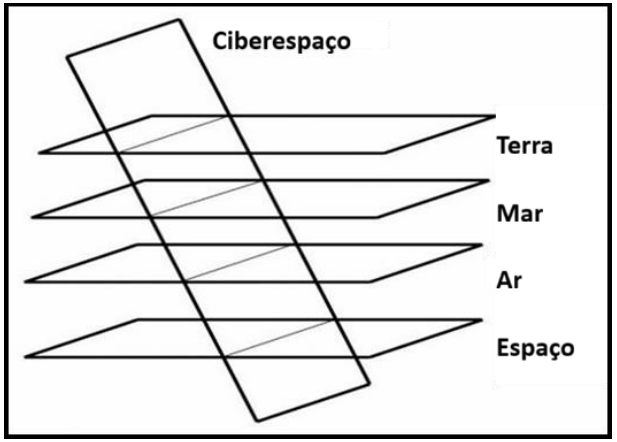
Fonte: Defesa Cibernética e Segurança Cibernética: Diferenças e Semelhanças. Security Information News. URL: https://securityinformationnews.wordpress.com/2019/07/27/defesa-cibernetica-e-seguranca-cibernetica-diferencas-e-semelhancas/

- **Ciberespaço é o termo cunhado pelo escritor norte-americano William Gibson em 1984, no livro de ficção científica Neuromancer.**

Cibersegurança – Conceitos Básicos

Conceitos básicos: Ciberespaço (Espaço Cibernético)

- **Não é um espaço natural como a terra, o mar, o ar e o espaço sideral, mas, sim, um espaço criado pelo próprio homem.**
- **Transpassa todos os demais espaços e possibilita interações entre os espaços.**
- **Ações em meio virtual podem gerar consequências em meios físicos!**



(VENTRE, 2011, p.35, apud PORTELA, 2016, p.4)

Cibersegurança – Conceitos Básicos

Conceitos básicos: Ciberespaço (Espaço Cibernético)

- **Ataque Worm em 2010 à Usina de Enriquecimento de Urânio de Natanz, Irã.**
- **O malware infectou sistemas Siemens, destruindo cerca de 1.000 centrífugas (quase 20% do total).**
- **Alterou a velocidade de operação enquanto enviava dados falsos de funcionamento normal aos operadores.**

BBC

Ataque nuclear iraniano: Mistério envolve sabotagem nuclear em Natanz. BBC URL: https://www.bbc.com/news/world-middle-east-56722181

Cibersegurança – Conceitos Básicos

Conceitos básicos: Ciberespaço (Espaço Cibernético)

- **Ataque Ransomware em Maio/2021 à Colonial Pipeline, EUA.**
- **Operações interrompidas para conter o ataque.**
- **Escassez de combustível, corrida aos postos e aumento de preços na Costa Leste dos EUA.**
- **Pagamento de resgate: ~75 bitcoins (US$ 4,4 milhões).**

BBC NEWS BRASIL

O ataque de hackers a maior oleoduto dos EUA que fez governo declarar estado de emergência. BBC NEWS Brasil. URL: https://www.bbc.com/portuguese/internacional-57055618

Cibersegurança – Conceitos Básicos

Conceitos básicos: Segurança Ofensiva e Segurança Defensiva

- **Segurança Ofensiva**
  - Compreende as **táticas**, **técnicas** e **procedimentos** (TTP – Tactics, Techniques, and Procedures) adotadas pelos adversários contra o sistema-alvo.

- **Segurança Defensiva**
  - Compreende o **estabelecimento** e a **manutenção** das **medidas de proteção** (controles de segurança) do sistema-alvo.

Cibersegurança – Conceitos Básicos

Conceitos básicos: Red Team e Blue Team

- **Red Team (grupo de ataque da organização)**
  - **Profissionais focam na segurança ofensiva e buscam conhecimento de técnicas e ferramentas usadas para encontrar falhas nas defesas das organizações.**

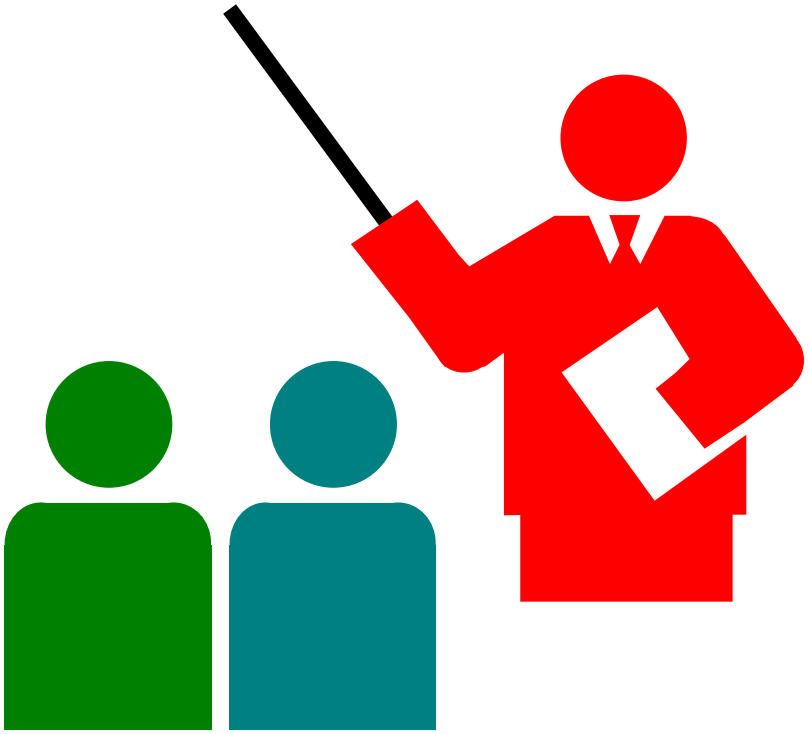
- **Blue Team (grupo de defesa da organização)**
  - **Profissionais focam na segurança defensiva e buscam conhecimento de técnicas e ferramentas usadas para proteger os sistemas da organização.**

Cibersegurança – Conceitos Básicos

Conceitos básicos: Hacking e Pen Test

- **Hacking**
  - É a habilidade de explorar os limites dos sistemas, geralmente em busca de falhas.
  - Quando feito sem autorização e com más intenções, é ilegal e chamado de cibercrime.
  - Quando feito com autorização para encontrar e corrigir falhas, é chamado de hacking ético.
- **Pen Test (Teste de Penetração)**
  - É uma tarefa específica e estruturada dentro do campo do hacking ético.
  - É uma simulação controlada de um ataque para testar a segurança de um alvo específico, com permissão para identificar falhas e recomendar soluções.

Ataques Cibernéticos à Rede de Comunicação de Dados



Conceitos Básicos e Definições
Recomendação X.800 ITU-T - IETF RFC 4949

Conceitos básicos: Vulnerabilidade

- **Qualquer fraqueza que possa ser explorada para violar um sistema ou a informação contida nele.**

- **Tipos de vulnerabilidades:**
  - ***vulnerabilidade no design ou na especificação*;**
  - ***vulnerabilidade na implantação*; e**
  - ***vulnerabilidade na operação e no gerenciamento*.**

- **Muitos sistemas possuem uma ou mais vulnerabilidades, mas isso não significa necessariamente que eles são demasiadamente falhos a ponto de não poderem ser usados.**

Conceitos Básicos e Definições
Recomendação X.800 ITU-T - IETF RFC 4949

Conceitos básicos: Ameaça

- **Potencial para violação da segurança**
  - **Quando há uma entidade, circunstância, capacidade, ação ou evento que pode causar mal ao sistema.**
- ***Ameaças Acidentais***
  - **Quando não há intenção premeditada para sua ocorrência.**
    - **Ex: o mau funcionamento do sistema, os erros operacionais graves, os erros em software (bugs) ou os desastres naturais (incêndio, inundação, terremoto, etc).**
- ***Ameaças Intencionais***
  - **Quando envolvem a possibilidade de se fazer uma simples inspeção de conteúdo com ferramentas de monitoramento ou ataques sofisticados usando conhecimentos especiais do sistema.**
    - **Ex: transmissão de dados em uma rede de comunicação sem proteção contra a exposição dos dados.**

DEPARTAMENTO DE INFORMÁTICA PUC-RIO

PUC RIO

Conceitos Básicos e Definições
Recomendação X.800 ITU-T - IETF RFC 4949

Conceitos básicos: Ataque

- **Um ato intencional no qual uma entidade procura evadir serviços de segurança e violar a política de segurança de um sistema.**
- **Pode ser caracterizado de acordo com o ponto de origem:**
- ***Ataque interno (inside attack)***
  - **É aquele iniciado por uma entidade no lado de dentro do perímetro de segurança, isto é, uma entidade que está autorizada a acessar os recursos do sistema, mas faz uso desses recursos de forma não aprovada pela parte que garantiu a autorização.**
- ***Ataque externo (outside attack)***
  - **É aquele iniciado no lado de fora do perímetro de segurança por um usuário não autorizado ou não legítimo do sistema.**

Conceitos Básicos e Definições
Recomendação X.800 ITU-T - IETF RFC 4949

Conceitos básicos: Ataque

- Pode ser dividido em duas categorias de ataque.
- *Ataques passivos*
  - Quando **não resultam na modificação** de qualquer informação contida no sistema e não ocorre mudança na operação e no estado do sistema;
    - Ex: a coleta de informação a partir da observação do fluxo de dados transmitido na linha de comunicação.
- *Ataques ativos*
  - Quando **implicam na alteração** da informação contida no sistema ou mudam a operação e o estado do sistema.
    - Ex: a mudança maliciosa das tabelas de rotas de um sistema por um usuário não autorizado.

Conceitos Básicos e Definições
Recomendação X.800 ITU-T - IETF RFC 4949

Conceitos básicos: Ataque

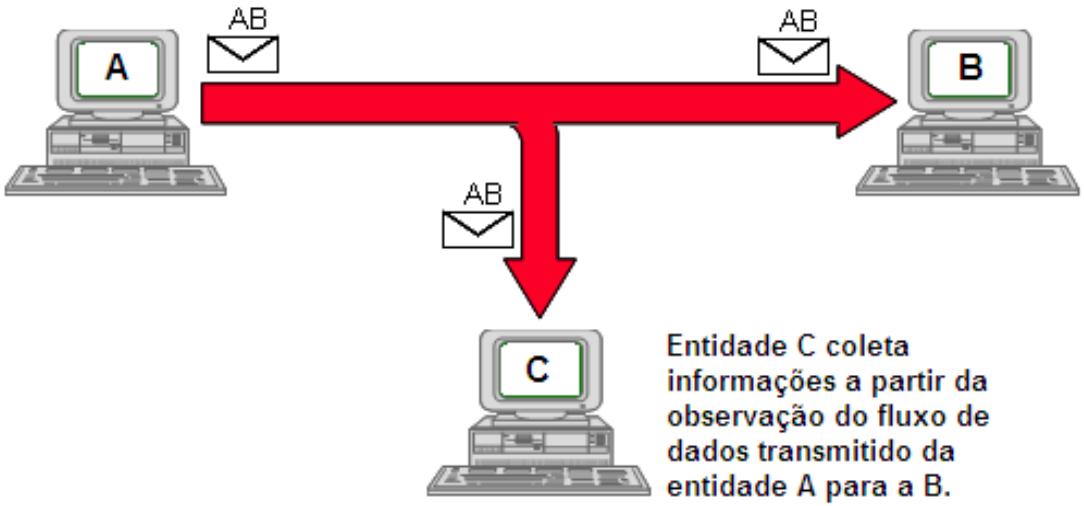
- Os *ataques ativos* podem ser caracterizados em função do método de execução.

- *Ataque direto*
  - A entidade hostil executa o ataque a(s) vítima(s) direcionando o fluxo de dados malicioso para a(s) vítima(s).

- *Ataque indireto*
  - A entidade hostil comanda um terceiro na execução do ataque a(s) vítima(s) fazendo com que o fluxo de dados malicioso seja direcionado à(s) vítima(s) pelo terceiro.

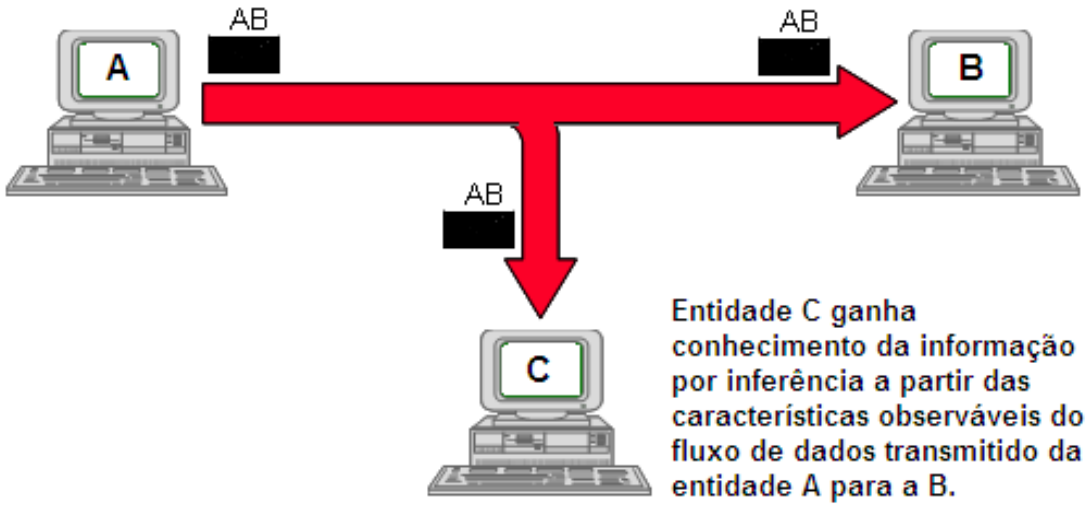
Conceitos Básicos e Definições
Recomendação X.800 ITU-T - IETF RFC 4949

Conceitos básicos: Ataque Passivo – Inspeção de Conteúdo



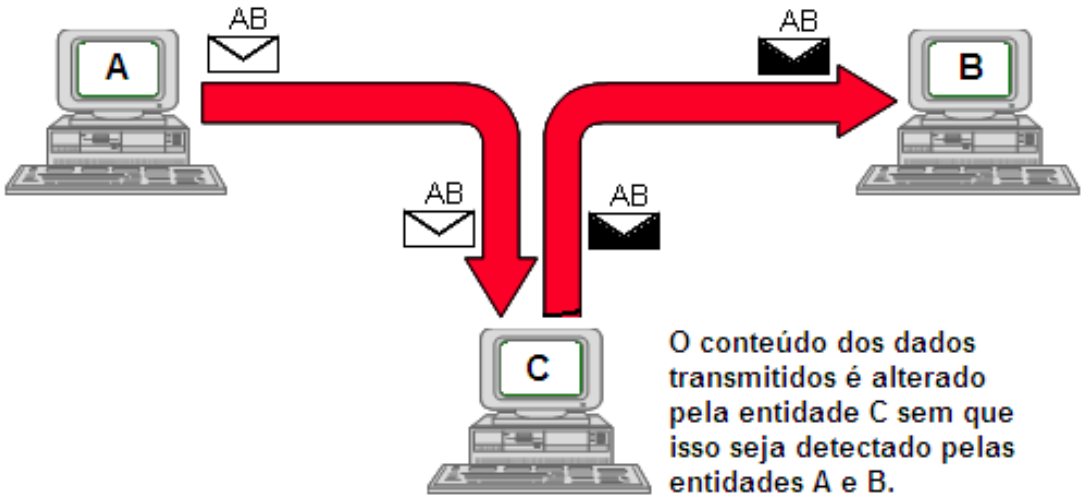
Conceitos Básicos e Definições
Recomendação X.800 ITU-T - IETF RFC 4949

Conceitos básicos: Ataque Passivo – Análise de Tráfego



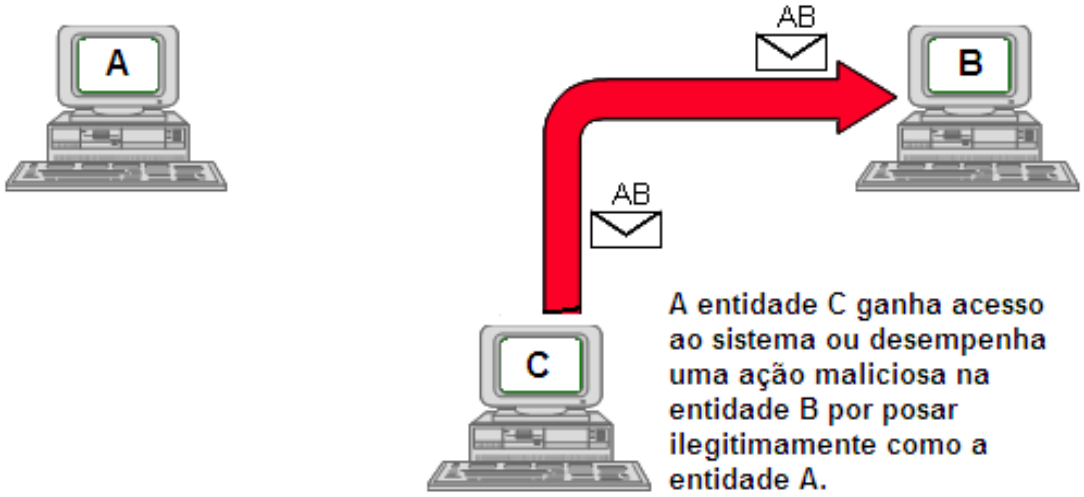
Conceitos Básicos e Definições
Recomendação X.800 ITU-T - IETF RFC 4949

Conceitos básicos: Ataque Ativo – Interceptação com Modificação da Mensagem



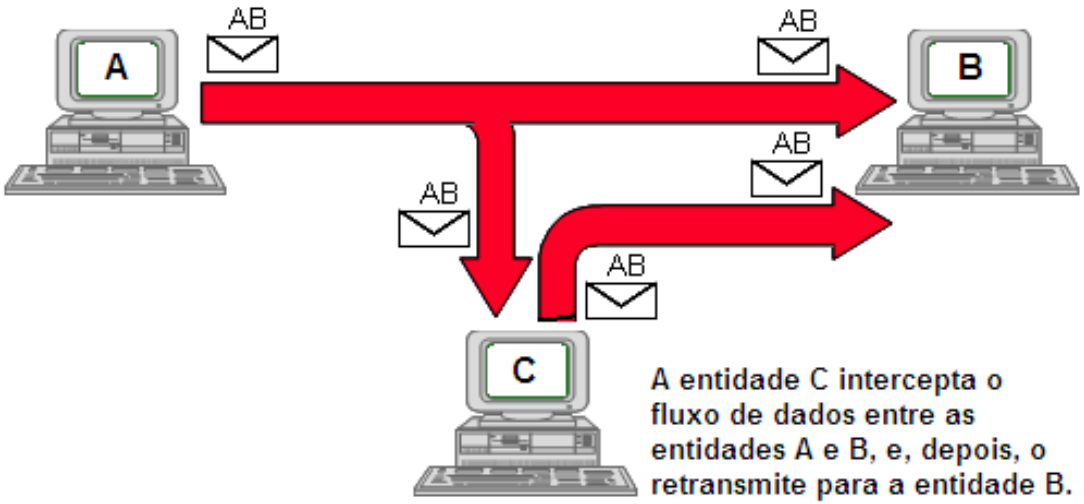
Conceitos Básicos e Definições
Recomendação X.800 ITU-T - IETF RFC 4949

Conceitos básicos: Ataque Ativo – Disfarce (Masquerade ou Spoofing)



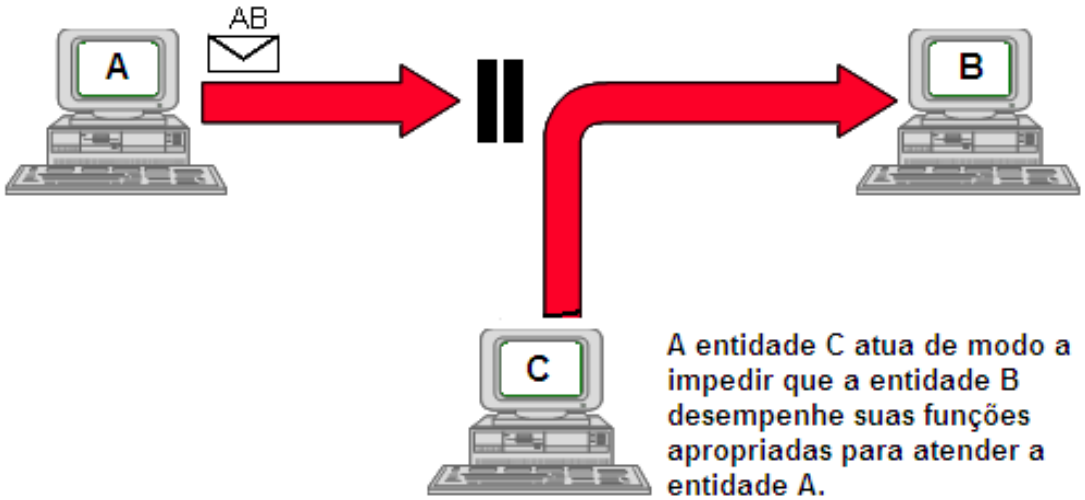
Conceitos Básicos e Definições
Recomendação X.800 ITU-T - IETF RFC 4949

Conceitos básicos: Ataque Ativo – Repetição (Replay)



Conceitos Básicos e Definições
Recomendação X.800 ITU-T - IETF RFC 4949

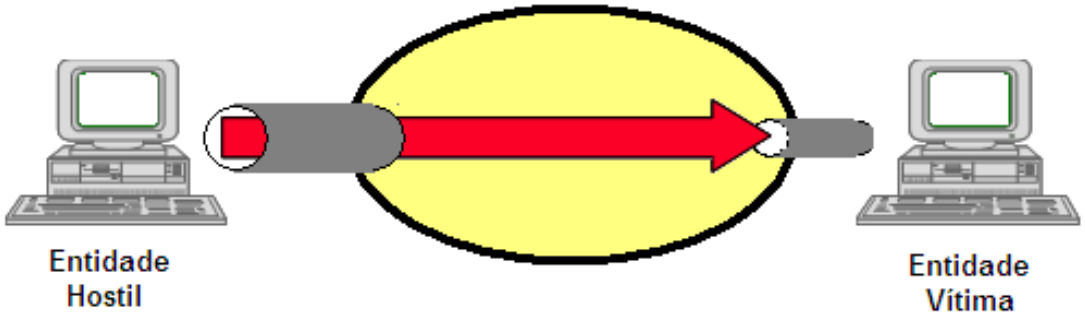
Conceitos básicos: Ataque Ativo – Negação de Serviço (Denial of Service)



Conceitos Básicos e Definições
Recomendação X.800 ITU-T - IETF RFC 4949

Conceitos básicos: Ataque Ativo – Negação de Serviço (Denial of Service) – Inundação

- **Cenário 1: Inundação Direta**

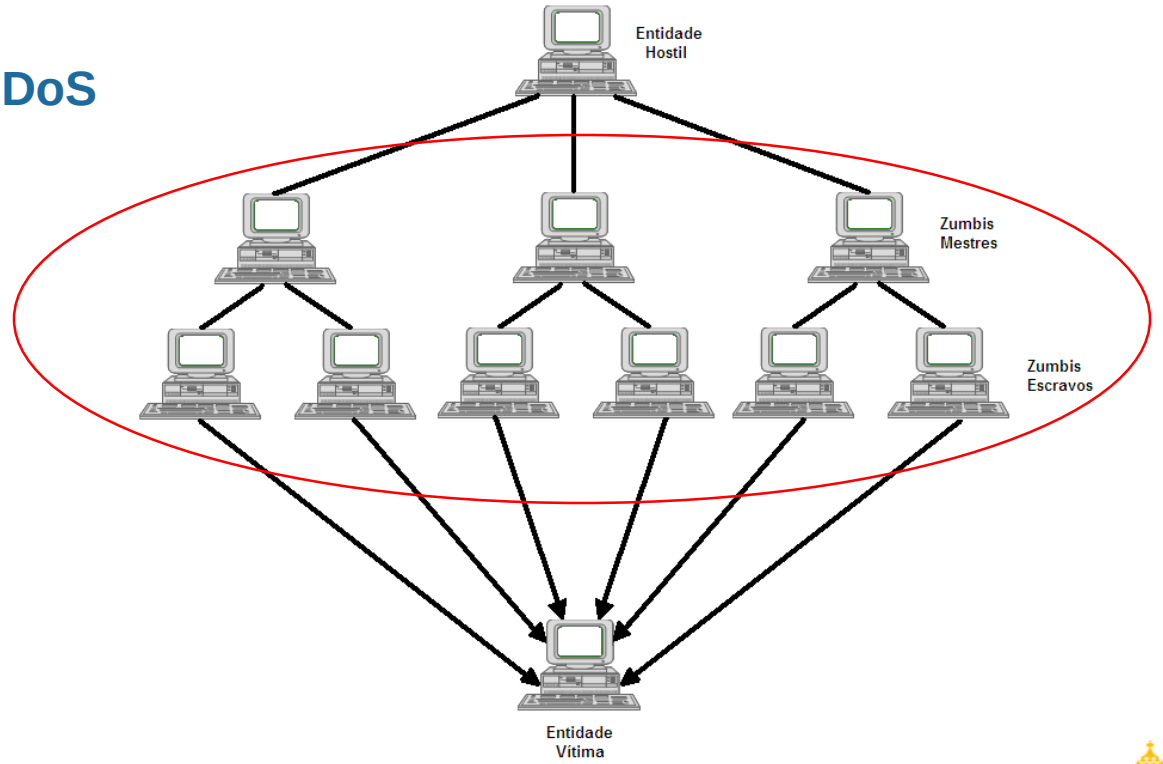


Conceitos Básicos e Definições
Recomendação X.800 ITU-T - IETF RFC 4949

Conceitos básicos: Ataque Ativo – Negação de Serviço (Denial of Service) – Inundação

- **Cenário 2:**
  Inundação Indireta - DDoS

robot network

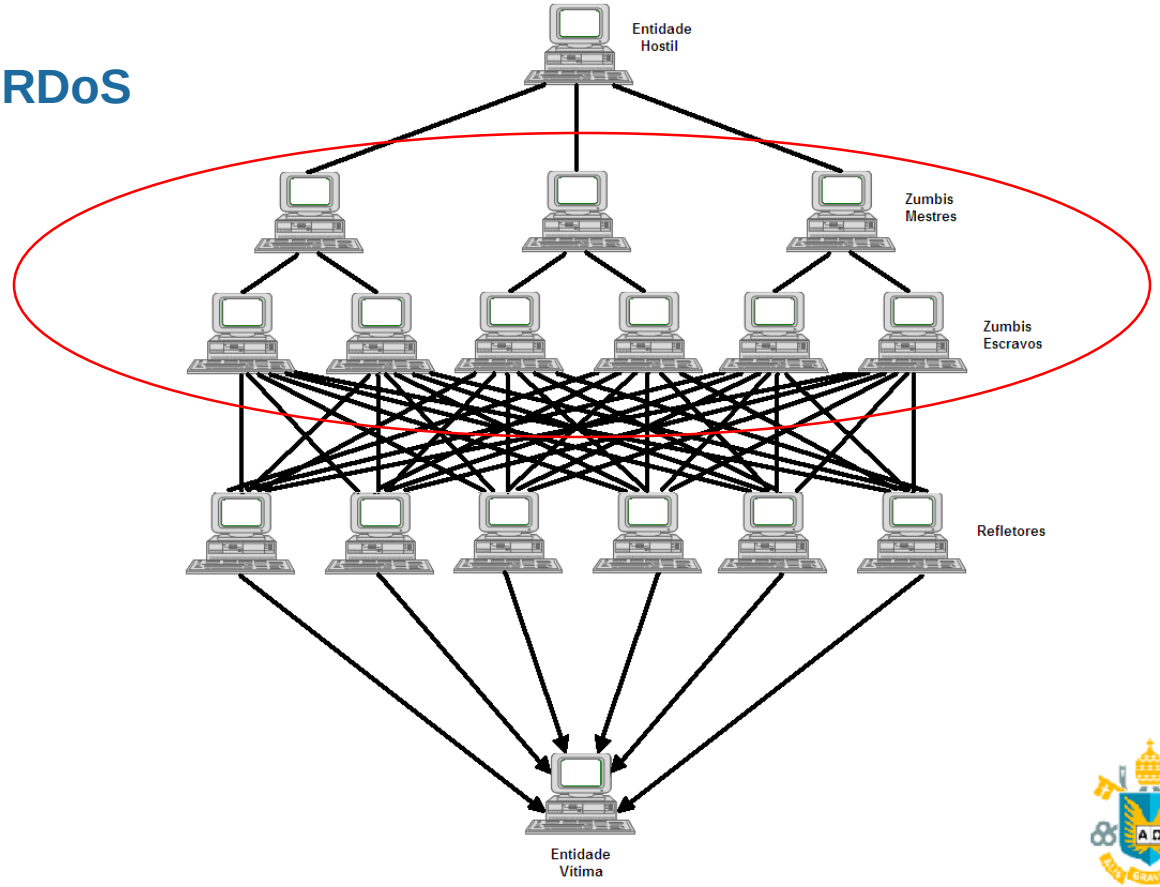


Conceitos Básicos e Definições
Recomendação X.800 ITU-T - IETF RFC 4949

Conceitos básicos: Ataque Ativo – Negação de Serviço (Denial of Service) – Inundação

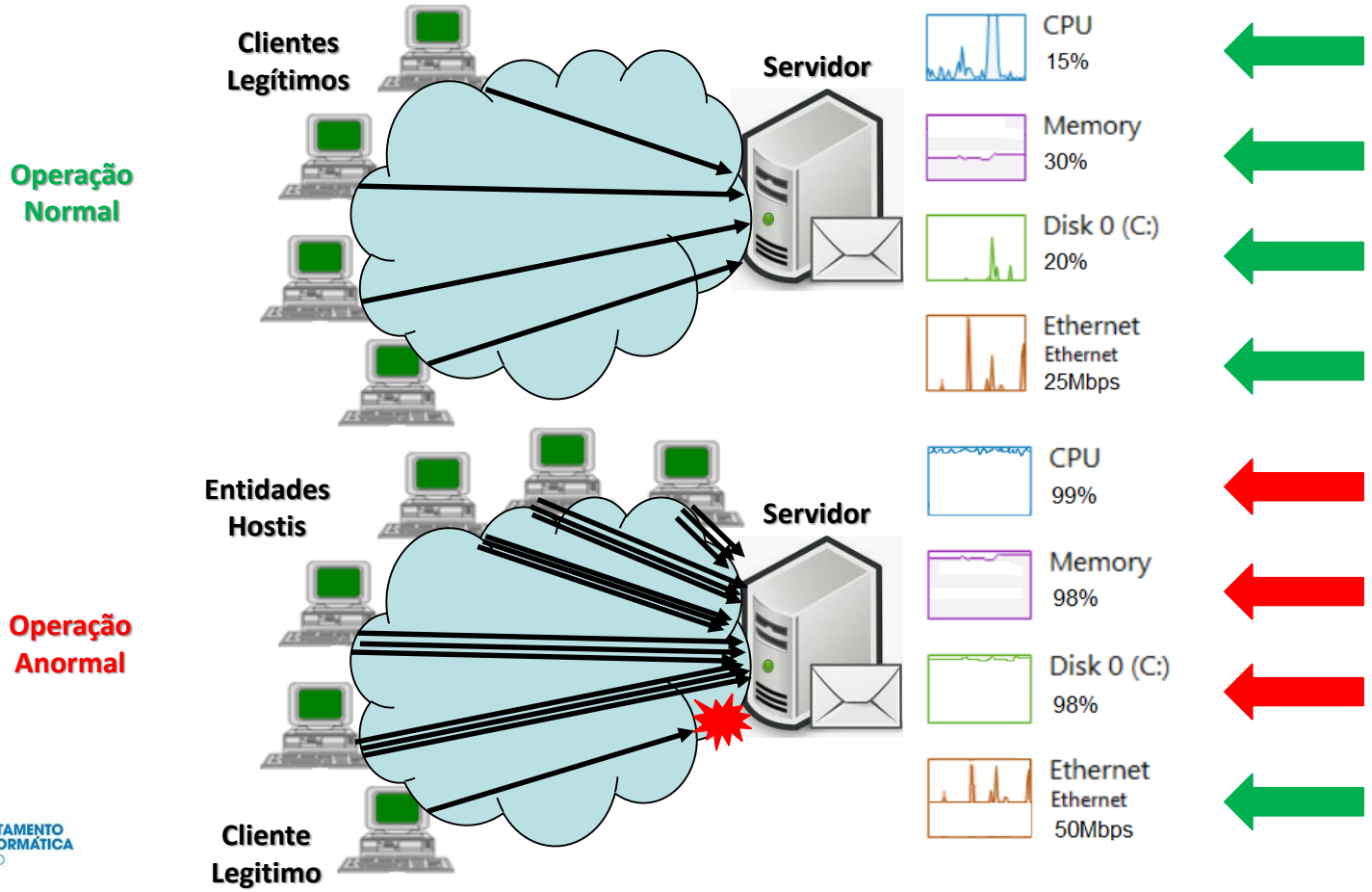
- **Cenário 2:**
  Inundação Indireta - DRDoS

robot network



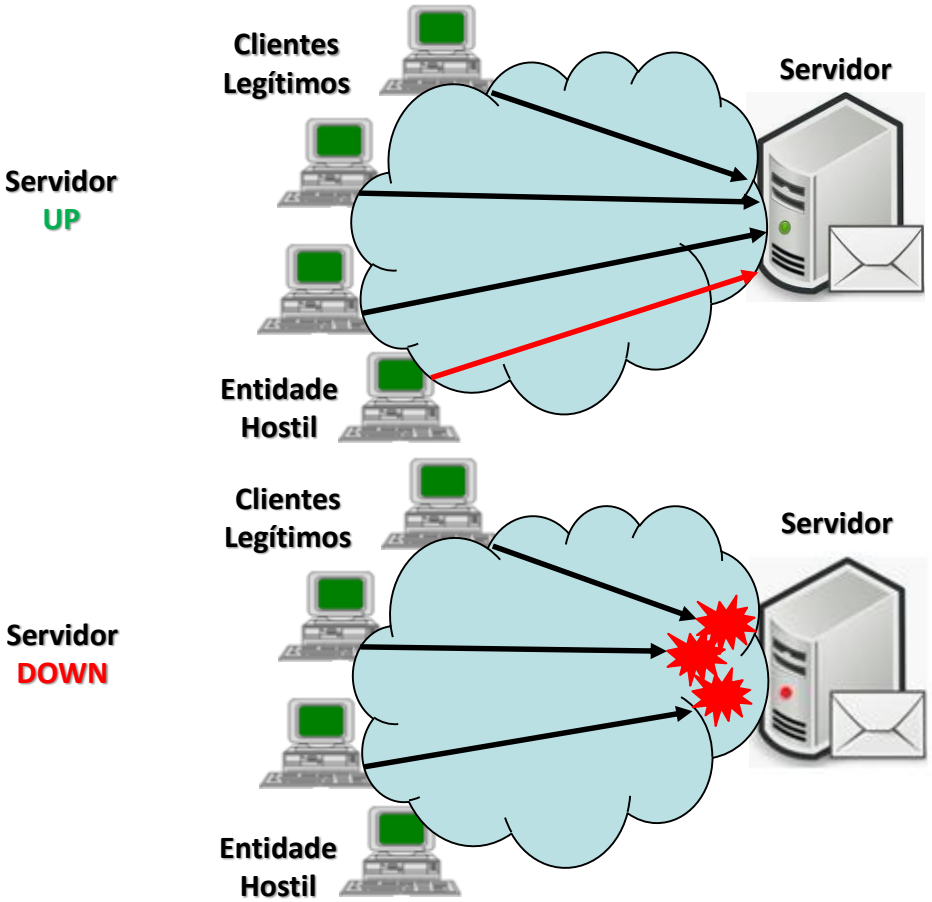
Conceitos Básicos e Definições
Recomendação X.800 ITU-T - IETF RFC 4949

Conceitos básicos: Ataque Ativo – Negação de Serviço (Denial of Service) – Inanição de Recursos



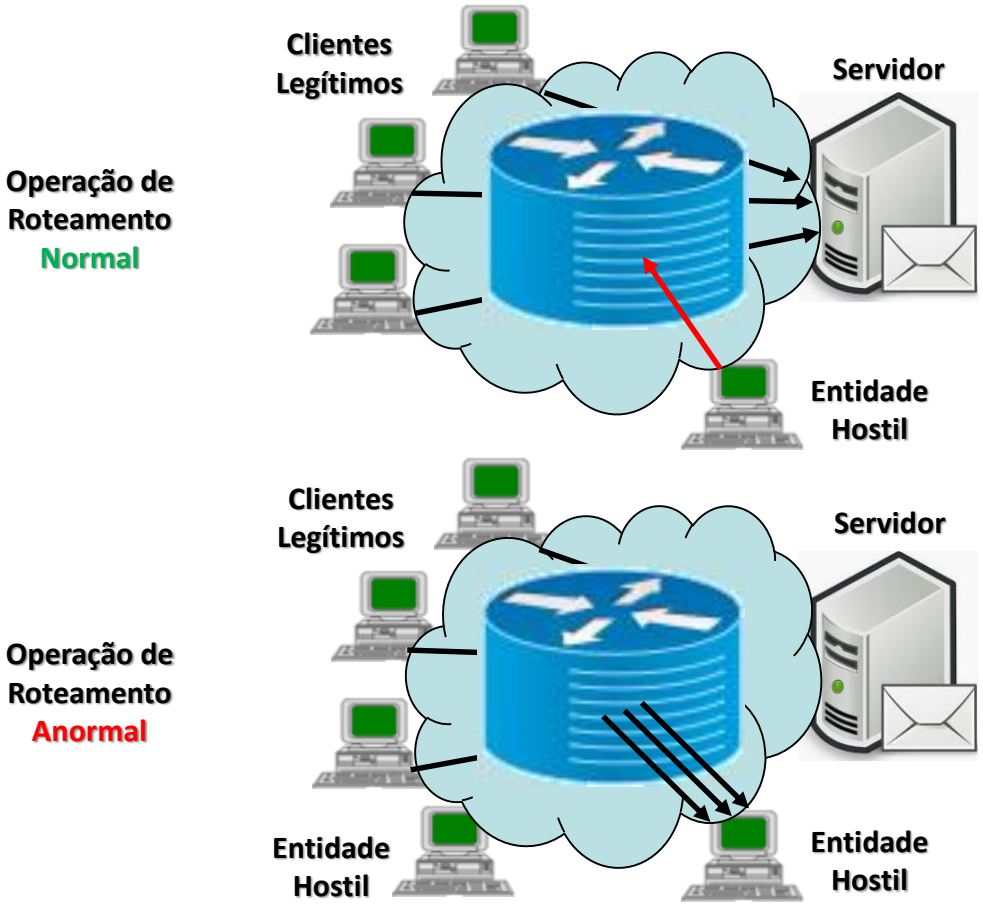
Conceitos Básicos e Definições
Recomendação X.800 ITU-T - IETF RFC 4949

Conceitos básicos: Ataque Ativo – Negação de Serviço (Denial of Service) – Interrupção de Serviços



Conceitos Básicos e Definições
Recomendação X.800 ITU-T - IETF RFC 4949

Conceitos básicos: Ataque Ativo – Negação de Serviço (Denial of Service) – Manipulação de Tráfego



Prof. Anderson Oliveira da Silva - anderson@inf.puc-rio.br

Ataques Cibernéticos com Códigos Maliciosos (Malware)

Conceito:

- **Código malicioso (mal intencionado) com o potencial de danificar sua vítima, porém nem sempre age desta forma.**

- **Qualquer código que execute em um sistema, consumindo recursos, sem prévia autorização, pode ser considerado malicioso.**

- **Sua instalação e execução varia em função do tipo de malware e normalmente ocorre sem que a vítima perceba ou autorize.**

Ataques Cibernéticos com Códigos Maliciosos (Malware)

Conceito: Vírus

- **Programa malicioso com o poder de proliferação, que depende de um hospedeiro para ser executado.**

- **Embutido em programas executáveis, documentos que suportam macros (Documentos Word, Planilhas Excel, etc) e no setor de boot dos discos.**

(CERT.BR, 2025, p.15)

CERT.BR. NIC.BR. CGI.BR. Cartilha de Segurança para Internet. Fascículo Códigos Maliciosos. https://cartilha.cert.br/fasciculos/codigos-maliciosos/fasciculo-codigos-maliciosos.pdf. Acessado em Janeiro/2025.

Ataques Cibernéticos com Códigos Maliciosos (Malware)

Conceito: Verme (Worm)

- **Programa malicioso com o poder de proliferação, que não depende de um hospedeiro para ser executado.**

- **Utiliza a rede de dados como forma de disseminação, normalmente explorando vulnerabilidades em sistemas remotos.**

(CERT.BR, 2025, p.23)

CERT.BR. NIC.BR. CGI.BR. Cartilha de Segurança para Internet. Fascículo Códigos Maliciosos. https://cartilha.cert.br/fasciculos/codigos-maliciosos/fasciculo-codigos-maliciosos.pdf. Acessado em Janeiro/2025.

Ataques Cibernéticos com Códigos Maliciosos (Malware)

Conceito: Cavalo de Tróia (Trojan Horse)

- Código malicioso **camuflado em um software de interesse** do usuário com o objetivo de se instalar na máquina do usuário e executar uma ação maliciosa sem conhecimento do mesmo.

- Famoso "**Presente de Grego**".

(CERT.BR, 2025, p.20)

CERT.BR. NIC.BR. CGI.BR. Cartilha de Segurança para Internet. Fascículo Códigos Maliciosos. https://cartilha.cert.br/fasciculos/codigos-maliciosos/fasciculo-codigos-maliciosos.pdf. Acessado em Janeiro/2025.

Ataques Cibernéticos com Códigos Maliciosos (Malware)

Conceito: Porta dos Fundos (Backdoor)

- Código malicioso que **permite conexões remotas a sistemas**, funcionando como um controle remoto.
- Usa **porta de comunicação** da rede de dados do sistema hospedeiro.

(CERT.BR, 2025, p.21)

CERT.BR. NIC.BR. CGI.BR. Cartilha de Segurança para Internet. Fascículo Códigos Maliciosos. https://cartilha.cert.br/fasciculos/codigos-maliciosos/fasciculo-codigos-maliciosos.pdf. Acessado em Janeiro/2025.

Ataques Cibernéticos com Códigos Maliciosos (Malware)

Conceito: Registrador de Teclas (Keylogger)

- Código malicioso que **captura o pressionamento das teclas** num sistema comprometido, coletando informação sensível para o atacante.

- Tais informações sensíveis podem incluir **nomes, senhas, PINs, data de nascimento, número do seguro social,** ou **números de cartão de crédito.**

(CERT.BR, 2025, p.18)

CERT.BR. NIC.BR. CGI.BR. Cartilha de Segurança para Internet. Fascículo Códigos Maliciosos. https://cartilha.cert.br/fasciculos/codigos-maliciosos/fasciculo-codigos-maliciosos.pdf. Acessado em Janeiro/2025.

Ataques Cibernéticos com Códigos Maliciosos (Malware)

Conceito: Registrador de Tela (Screenlogger)

- Código malicioso que registra a posição do cursor do mouse e captura e armazena toda a tela ou uma região específica da tela, quando o usuário clica no mouse num sistema infectado.

- Usado para capturar teclas digitadas em teclados virtuais.

(CERT.BR, 2025, p.18)

CERT.BR. NIC.BR. CGI.BR. Cartilha de Segurança para Internet. Fascículo Códigos Maliciosos. https://cartilha.cert.br/fasciculos/codigos-maliciosos/fasciculo-codigos-maliciosos.pdf. Acessado em Janeiro/2025.

Ataques Cibernéticos com Códigos Maliciosos (Malware)

Conceito: Baixador (Downloader)

- Código malicioso que **baixa conteúdo malicioso de um servidor remoto** controlado pelo atacante para a máquina infectada.

(CERT.BR, 2025, p.18)

CERT.BR. NIC.BR. CGI.BR. Cartilha de Segurança para Internet. Fascículo Códigos Maliciosos. https://cartilha.cert.br/fasciculos/codigos-maliciosos/fasciculo-codigos-maliciosos.pdf. Acessado em Janeiro/2025.

Ataques Cibernéticos com Códigos Maliciosos (Malware)

Conceito: Injetador (Injector)

- Código malicioso que **injeta código malicioso** na memória de um processo em execução na máquina atacada.
- O código injetado, em geral, é executado no sistema remoto vulnerável (Remote Code Execution – RCE) com os **mesmos privilégios do processo em execução**.

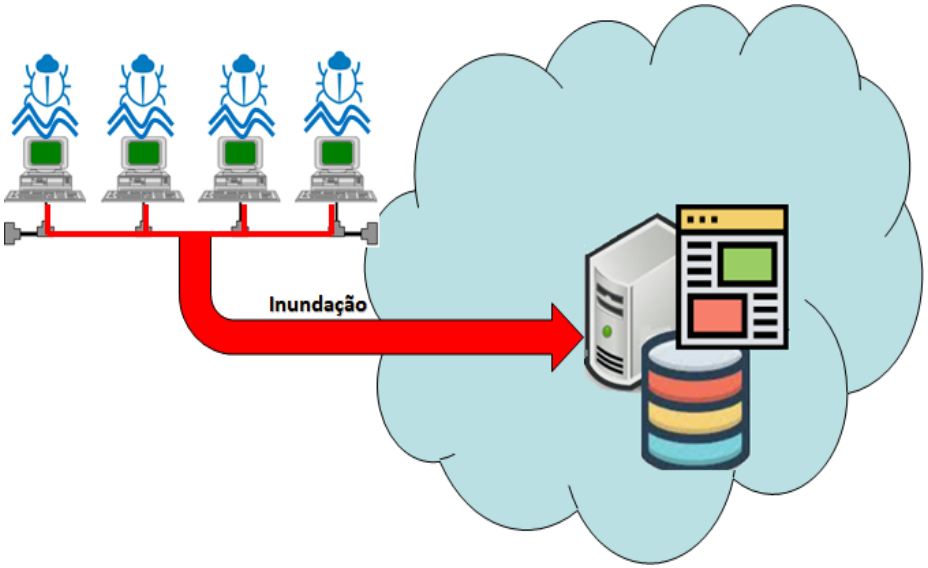
https://www.shutterstock.com/pt/search/code-injection

CERT.BR. NIC.BR. CGI.BR. Cartilha de Segurança para Internet. Fascículo Códigos Maliciosos. https://cartilha.cert.br/fasciculos/codigos-maliciosos/fasciculo-codigos-maliciosos.pdf. Acessado em Janeiro/2025.

Ataques Cibernéticos com Códigos Maliciosos (Malware)

Conceito: Inundador (Flooder)

- Código malicioso que **sobrecarrega o sistema-alvo** com uma **quantidade de tráfego de rede muito superior ao suportado** de modo que os usuários legítimos não conseguem ter suas requisições atendidas, configurando uma situação conhecida como **negação de serviço (Denial of Service – DoS)**.



CERT.BR. NIC.BR. CGI.BR. Cartilha de Segurança para Internet. Fascículo Códigos Maliciosos. https://cartilha.cert.br/fasciculos/codigos-maliciosos/fasciculo-codigos-maliciosos.pdf. Acessado em Janeiro/2025.

Ataques Cibernéticos com Códigos Maliciosos (Malware)

Conceito: Ransomware

- Código malicioso que **danifica o computador da vítima** de alguma forma e **exige pagamento para reverter esse dano**.
- Uma ação maliciosa comum é **tornar inacessíveis os dados armazenados no dispositivo**, geralmente usando **criptografia**, e **exigir pagamento de resgate** para restabelecer o acesso ao usuário e não vazar os dados".

(CERT.BR, 2025, p.16)

CERT.BR. NIC.BR. CGI.BR. Cartilha de Segurança para Internet. Fascículo Códigos Maliciosos. https://cartilha.cert.br/fasciculos/codigos-maliciosos/fasciculo-codigos-maliciosos.pdf. Acessado em Janeiro/2025.

Ataques Cibernéticos com Códigos Maliciosos (Malware)

Conceito: Spyware e Adware

- O Spyware é um código malicioso que **monitora as atividades** de um sistema e **envia as informações coletadas** para terceiros.

(CERT.BR, 2025, p.17)

- Um Adware, em particular, **coleta informações** sobre o **perfil de utilização da rede** feito pelo usuário para apresentar **propagandas direcionadas** ao mesmo através, por exemplo, de mensagens em pop-ups.

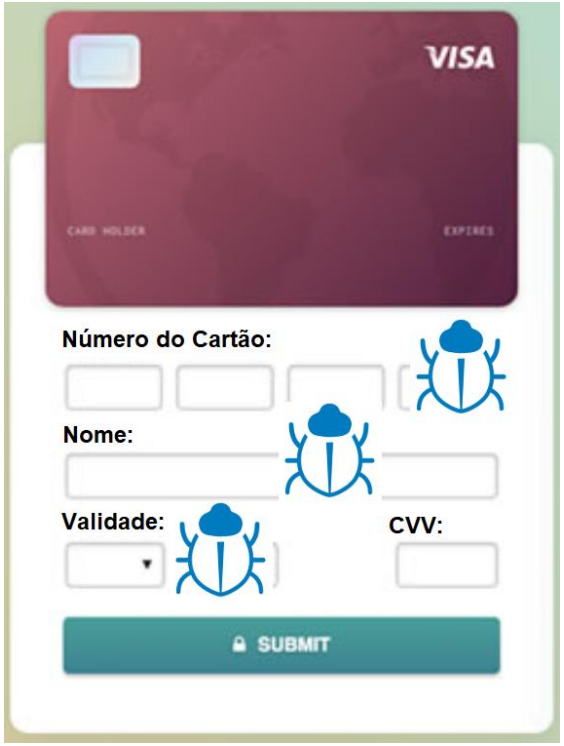
(CERT.BR, 2025, p.19)

CERT.BR. NIC.BR. CGI.BR. Cartilha de Segurança para Internet. Fascículo Códigos Maliciosos. https://cartilha.cert.br/fasciculos/codigos-maliciosos/fasciculo-codigos-maliciosos.pdf. Acessado em Janeiro/2025.

Ataques Cibernéticos com Códigos Maliciosos (Malware)

Conceito: Sequestrador de Formulários (Formjacker)

- Código malicioso que executa uma ação conhecida como **formjacking**, que **furta os dados de cartão de crédito** e outras **informações sensíveis** preenchidas pelo usuário no **formulário de pagamento** de um site de comércio eletrônico (eCommerce) no momento da sua submissão para o servidor Web.



CERT.BR. NIC.BR. CGI.BR. Cartilha de Segurança para Internet. Fascículo Códigos Maliciosos. https://cartilha.cert.br/fasciculos/codigos-maliciosos/fasciculo-codigos-maliciosos.pdf. Acessado em Janeiro/2025.

Obrigado!

Prof. Anderson Oliveira da Silva, phD

Engenheiro de Computação

Gestor de Segurança da Informação

Encarregado de Dados Pessoais

anderson@inf.puc-rio.br

Departamento de Informática

PUC-Rio