EAD

EDUCAÇÃO A DISTÂNCIA

UNIDADE I

Segurança no Ambiente *Web*

Prof. Me. Michel Fernandes

Segurança em ambiente *Web*

- Segundo NIST (1995), o termo “segurança computacional” pode ser definido como a proteção oferecida a um sistema de informações automatizado, a fim de atingir os objetivos aplicáveis de preservar a integridade, a disponibilidade e a confidencialidade dos recursos do sistema de informações.
- Inclui *hardware*, *software*, *firmware*, informações/dados e telecomunicações.

O que é a segurança cibernética?

- Proteção do sistema em rede e dos dados, contra o uso não autorizado ou os danos.

Dados pessoais

Identidade *off-line*:

- Sua identidade que interage regularmente em casa, na escola ou no trabalho.

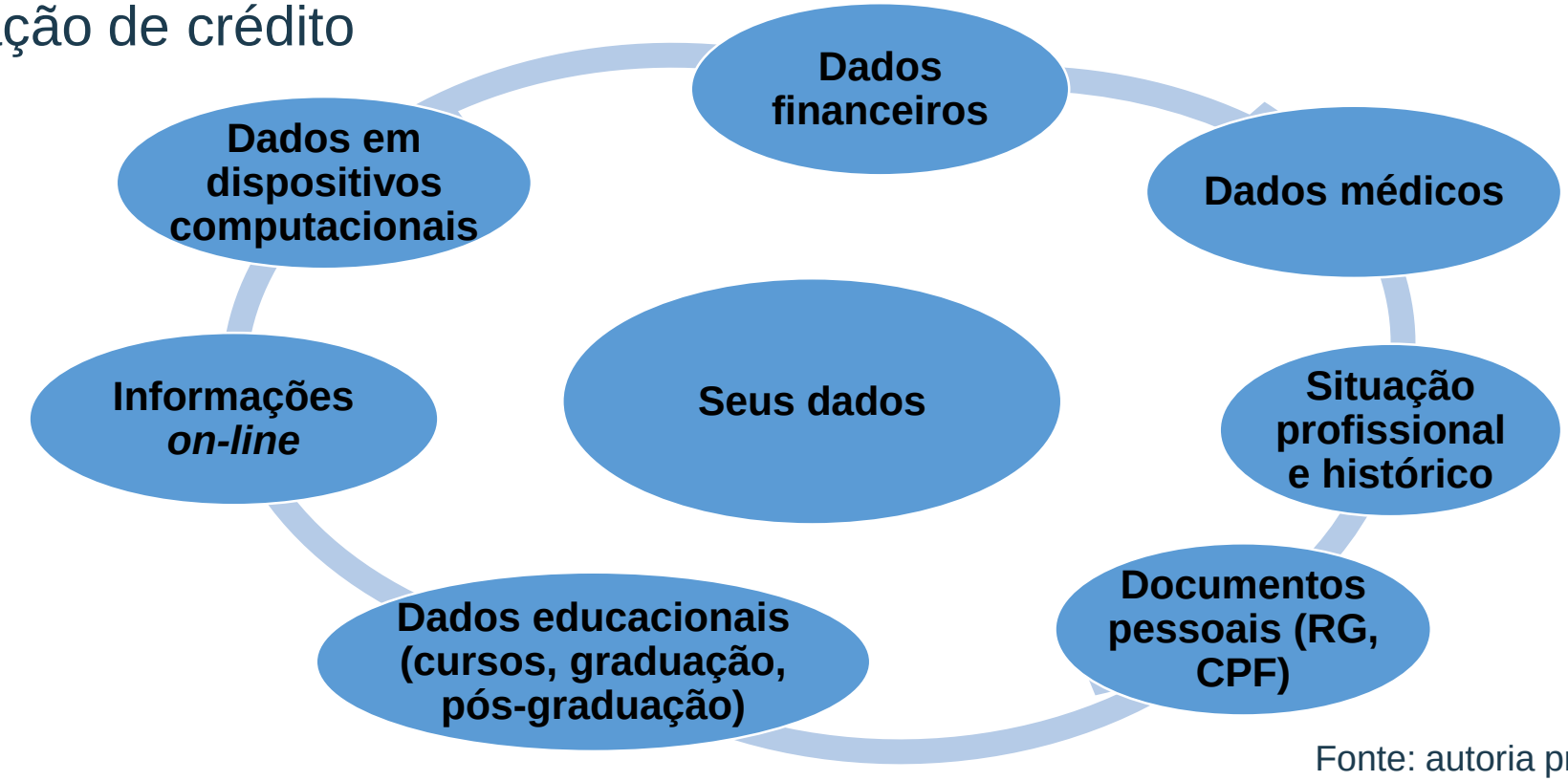
Identidade *on-line*:

- Sua identidade enquanto você está no ciberespaço;
- Só deve revelar uma quantidade limitada de informações sobre você.

Dados pessoais

Seus dados:

- Registros médicos: registros de saúde eletrônicos, receitas médicas;
- Registros de educação: notas, pontuações de testes, cursos realizados, prêmios e graus concedidos, presença, relatórios disciplinares;
- Registros de empregos e financeiros: rendimentos e gastos, registros fiscais, faturas de cartão de crédito, classificação de crédito e extratos bancários;
- Situação profissional.



Fonte: autoria própria.

Dados corporativos

Tipos dos dados corporativos:

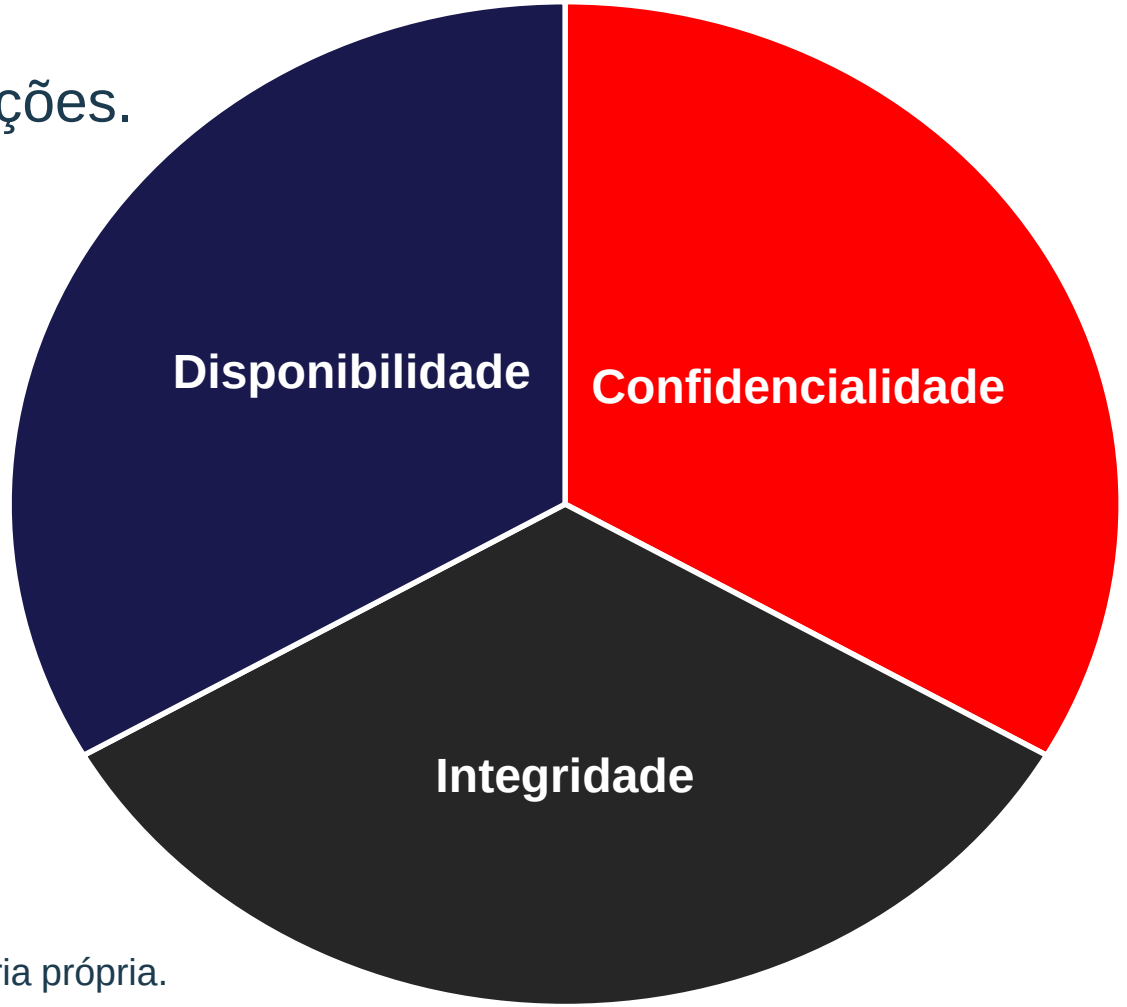
Dados tradicionais:

- Pessoal: materiais de vagas, folha de pagamento, carta de oferta, contratos de funcionários;
- Intelectual: patentes, marcas registradas, planos de produtos, segredos comerciais;
- Financeiro: declarações de renda, balanços patrimoniais, extratos de fluxo de caixa.

Confidencialidade, integridade e disponibilidade

- Tríade da segurança de informação.

- Confidencialidade: privacidade.
- Integridade: precisão e confiabilidade das informações.
- Disponibilidade: a informação é acessível.

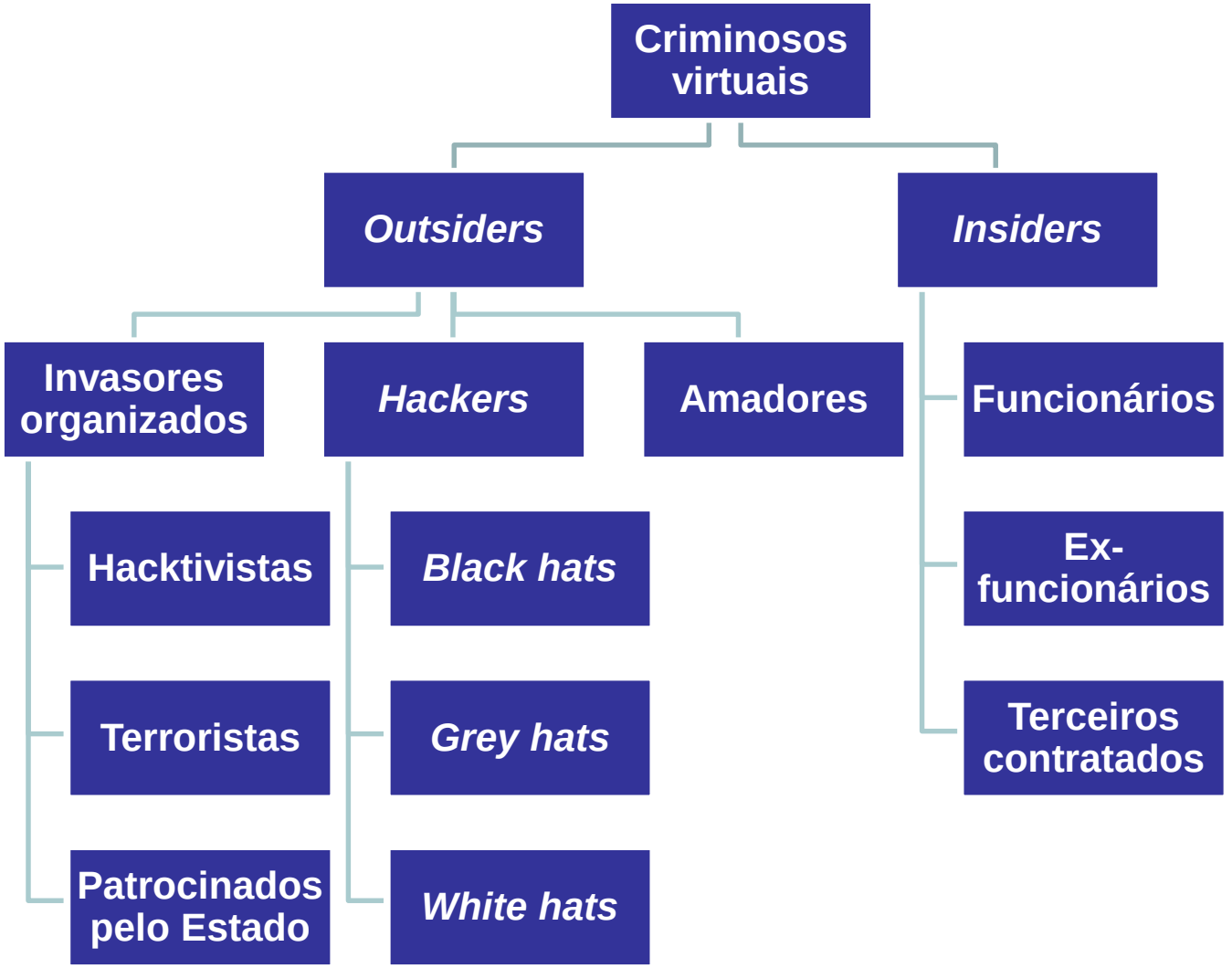


Fonte: autoria própria.

Tipos de invasores

- Divisão de tipos de invasores diferentes.
- Ameaças internas e externas.

Fonte: autoria própria.



Tipos de invasores

Amadores:

- Utilizam ferramentas ou instruções atuais encontradas *on-line* para os ataques.

***Hackers*:**

- Entram em computadores ou redes para obter o acesso. Dividem-se em:
  - ***White hats***: entram no sistema com permissão para descobrir fraquezas, com o objetivo de melhorar a segurança;
  - ***Grey hats***: comprometem os sistemas sem permissão;
  - ***Black hats***: utilizam qualquer vulnerabilidade para o ganho ilegal pessoal, financeiro ou político;
    - ***Hackers* organizados**: empresas de criminosos virtuais, hacktivistas, terroristas e *hackers* patrocinados pelo Estado.

Interatividade

Qual é o nome do tipo de *hackers* que são éticos e usam as suas habilidades de programação para fins legais?

a) *Black hat*.
b) *Grey hat.*
c) *White hat*.
d) Hacktivista.
e) *Hater*.

Resposta

Qual é o nome do tipo de *hackers* que são éticos e usam as suas habilidades de programação para fins legais?

a) *Black hat*.
b) *Grey hat.*
c) *White hat*.
d) Hacktivista.
e) *Hater*.

Ativos passivos

- Natureza de monitoramento e bisbilhotagem de transmissões, com o foco na obtenção das informações quando são transmitidas.

Tipos de ataques passivos:

- **Liberação de conteúdo da mensagem;**
- **Análise de tráfego.**

- Ataque de difícil detecção, já que não há nenhuma alteração no sistema.

Ativos passivos

Liberação de conteúdo da mensagem:

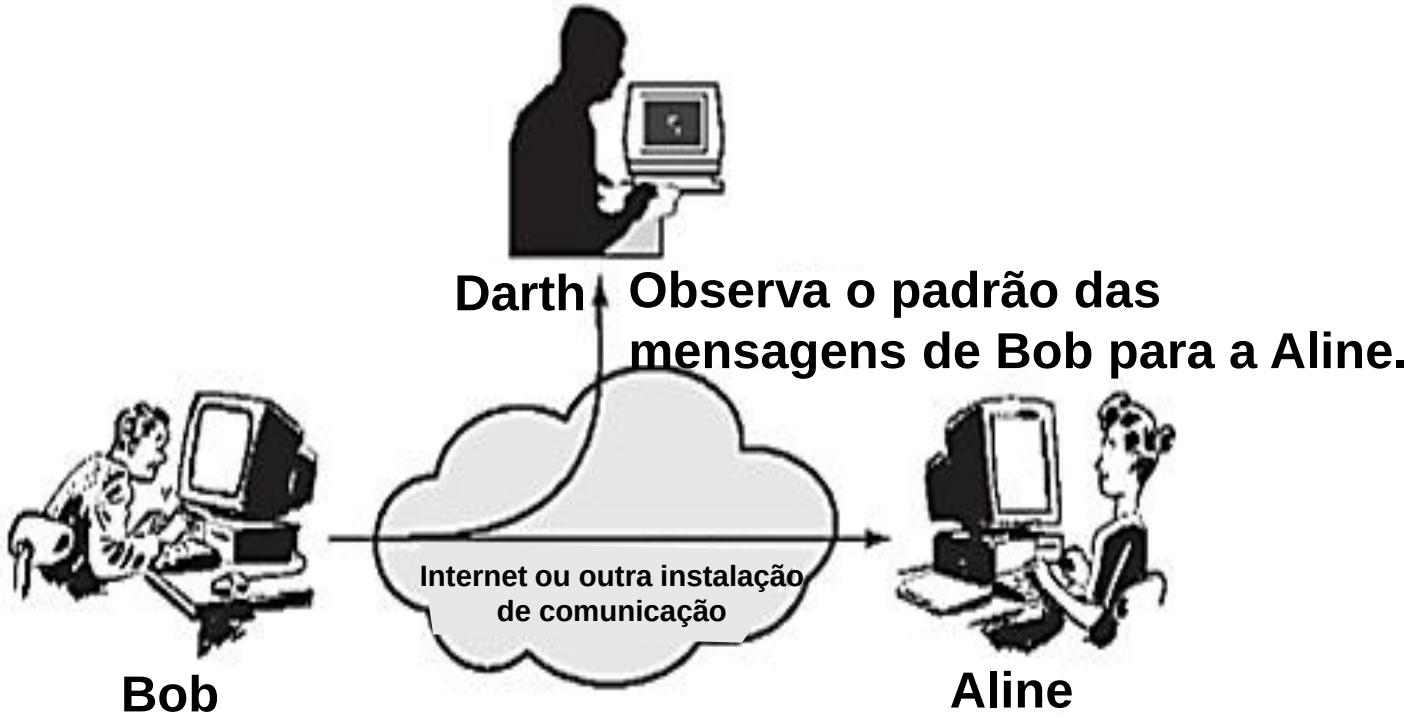
- Informações da mensagem não estão protegidas.

Fonte: STALLINGS, 2008, p. 6.

Ativos passivos

Análise de tráfego:

- Informações estão protegidas, de forma que o oponente não irá conseguir extrair as informações, mesmo se capturar a mensagem;
- Informações do padrão de mensagens, como a frequência de envio, o tamanho da mensagem, os envolvidos na comunicação.



Fonte: STALLINGS, 2008, p. 6.

Ataques ativos

- Ocorre a modificação no fluxo de dados ou a criação de um fluxo falso.

Podem ser agrupados em 4 categorias:

- Repetição;
- Disfarce;
- Modificação de mensagens; e
- Negação de serviço.

- Aproveitam-se das vulnerabilidades físicas, de *software* e da rede.

Ataques ativos

Ataque de repetição:

- Inicialmente, há a captura passiva de dados;
- Posteriormente, os dados serão retransmitidos para produzir um efeito não autorizado.

Fonte: STALLINGS, 2008, p. 7.

Ataques ativos

Disfarce ou *Masquerading*:

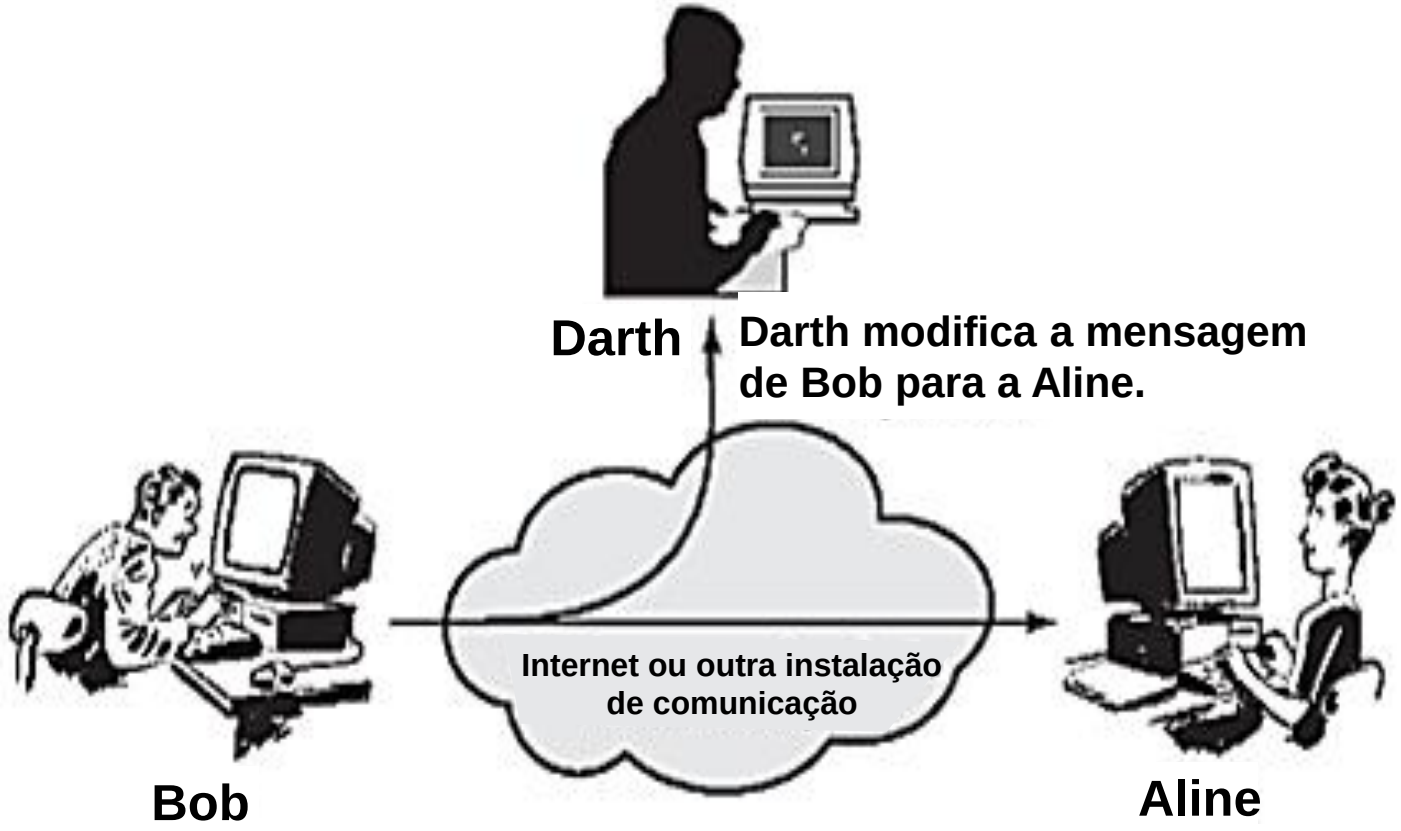
- Uma entidade finge ser outra entidade, visando permitir ao atacante a execução de ações em nome desta entidade;
- Após a autenticação na rede de forma disfarçada, obterá alguns privilégios extras, que não teria antes.

Fonte: STALLINGS, 2008, p. 7.

Ataques ativos

Modificação de mensagens:

- Parte da mensagem originalmente transmitida é alterada, adiada ou reordenada, visando à produção de um efeito não autorizado.

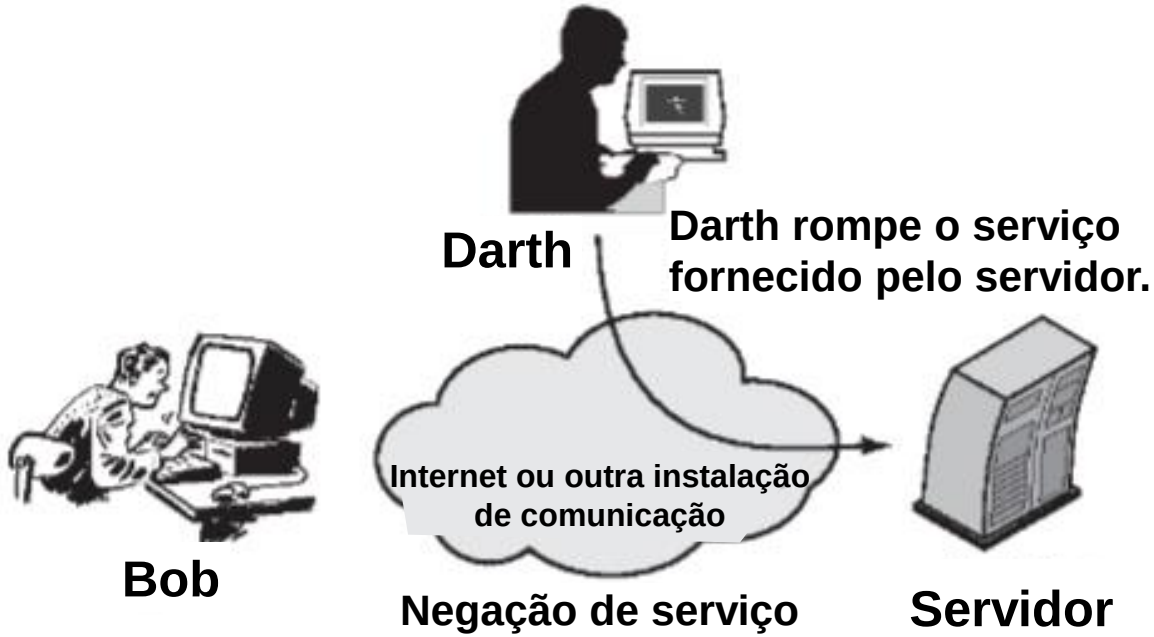


Fonte: STALLINGS, 2008, p. 8.

Ataques ativos

Negação de serviço ou *Denial of Service* (DoS):

- Ocorre um impedimento ou uma inibição, para a utilização ou o gerenciamento das instalações de comunicação;
- Pode possuir um alvo específico ou perturbar a rede como um todo, de modo a sobrecarregá-la com mensagens ou desativá-la, com o intuito de prejudicar o seu desempenho.



Fonte: STALLINGS, 2008, p. 8.

Interatividade

Qual é o nome do ataque quando um pacote formatado, de forma mal-intencionada, é enviado para um *host* ou um aplicativo, e o receptor não consegue contê-lo?

a) Liberação de conteúdo da mensagem.
b) Repetição.
c) Disfarce.
d) Modificação de mensagens.
e) Negação de serviço.

Resposta

Qual é o nome do ataque quando um pacote formatado, de forma mal-intencionada, é enviado para um *host* ou um aplicativo, e o receptor não consegue contê-lo?

a) Liberação de conteúdo da mensagem.
b) Repetição.
c) Disfarce.
d) Modificação de mensagens.
e) Negação de serviço.

Incidente de segurança

- Qualquer evento adverso, seja este confirmado ou sob suspeita, relacionado à segurança de sistemas computacionais ou de redes de computadores.

Exemplos:

- Tentativas, com sucesso e sem sucesso, de obter o acesso não autorizado para um sistema;
- Utilização ou acesso não autorizado a um sistema;
- Interrupção indesejada de serviço por ataques de negação de serviço;
- Desrespeito à política de segurança de uma empresa;
- Incidentes devem ser reportados ao CERT.br: Grupo de Resposta a Incidentes de Segurança para a Internet no Brasil.

Vulnerabilidades de segurança

- Um *exploit* é o termo usado para descrever um programa escrito para tirar proveito de uma vulnerabilidade conhecida.
- Um ataque é o ato de usar um *exploit* contra uma vulnerabilidade.
- Vulnerabilidade de *software*: erros no código do sistema operacional ou aplicativo.
- Vulnerabilidade de *hardware*: falhas de projeto de *hardware*.

Fonte: http://ibyte.com.br/ciencia-e-tecnologia/principios-gerais-para-seguranca-pessoal-na-internet/

Vulnerabilidades de segurança

- *Buffer overflow*: os dados são gravados além dos limites de um *buffer*.
- Entrada não validada: força os programas a se comportarem de forma não intencional.
- Condição de corrida: eventos indevidamente ordenados ou cronometrados.
- Fragilidade nas práticas de segurança: protege os dados confidenciais através de autenticação, autorização e criptografia.

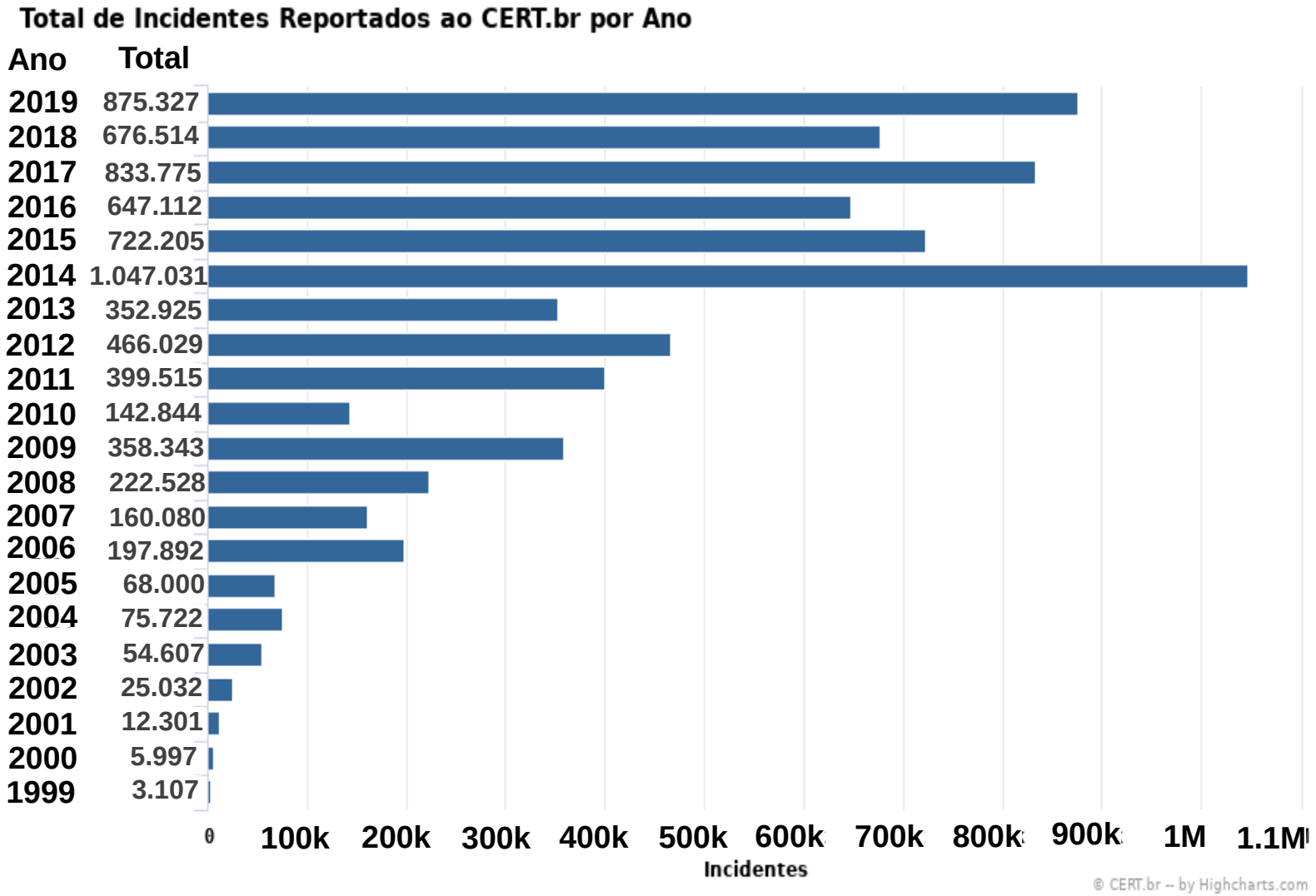
Problemas de controle de acesso:

- Controle de acesso a equipamentos físicos e a recursos;
- Práticas de segurança.

Fonte: https://www.muyseguridad.net/2016/11/08/ransomware-cerber-bases-datos/

Incidentes de segurança

- CERT.br possui estatísticas em relação aos incidentes de segurança.

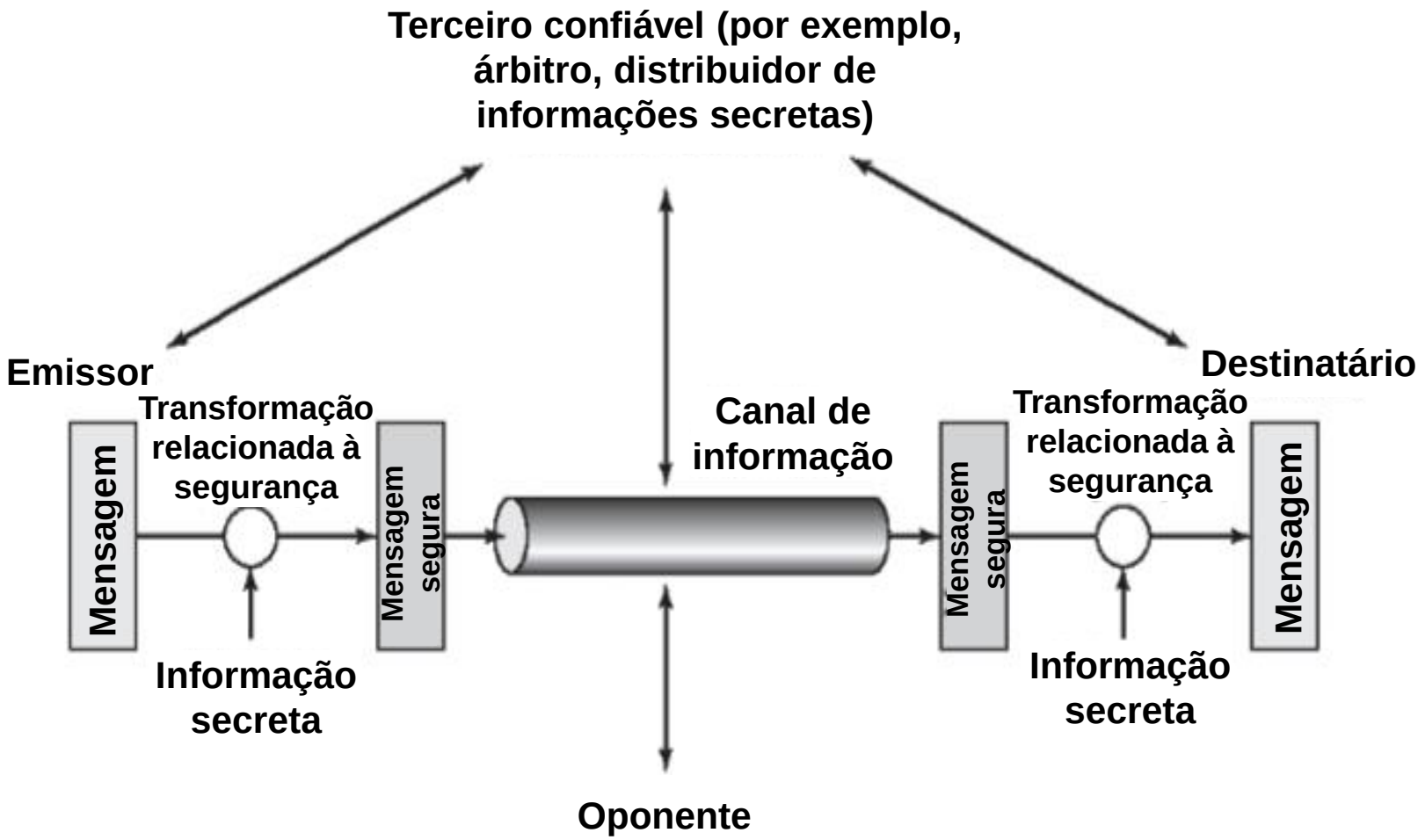


Fonte: https://www.cert.br/stats/incidentes/

Modelo de segurança para a rede

Componentes do modelo:

- Emissor;
- Mensagem;
- Canal de informação;
- Terceiro confiável;
- Oponente;
- Informação secreta;
- Transformação relacionada.



Fonte: STALLINGS, 2008, p. 12.

Estimativa de custo do cibercrime

De acordo com estudo da empresa McAfee, a estimativa de custos de cibercrime em 2018 foi de:

Região do mundo	PIB da região (em US$ trilhões)	Custo do crime cibernético na região (em US$ bilhões)	Custo do crime cibernético como % do PIB
América do Norte	20,2	140 a 175	0,69% a 0,87%
Europa e Ásia Central	20,3	160 a 185	0,79% a 0,89%
Leste Asiático e Ásia-Pacífico	22,5	120 a 200	0,59% a 0,89%
Sul da Ásia	2,9	7 a 15	0,24% a 0,52%
América do Sul e Caribe	5,3	15 a 30	0,28% a 0,57%
África Subsaariana	1,5	1 a 3	0,07% a 0,20%
Oriente Médio e Norte da África	3,1	2 a 5	0,06% a 0,16%
Mundo	**75,8**	**445 a 608**	**0,59% a 0,80%**

Fonte: https://www.mcafee.com/enterprise/en-us/solutions/lp/economics-cybercrime.html

Interatividade

Qual é o nome do órgão que coleta as informações de ataques na internet no Brasil?

a) CERT.br.
b) Hackers.br.
c) Defesa.gov.br.
d) Internet.br.
e) Google.br.

Resposta

Qual é o nome do órgão que coleta as informações de ataques na internet no Brasil?

a) CERT.br.
b) Hackers.br.
c) Defesa.gov.br.
d) Internet.br.
e) Google.br.

Consequências de violação de segurança

As consequências de uma violação de segurança:

- Não é viável prevenir todos os ataques;
- Os invasores sempre encontrarão novas maneiras;
- Reputação arruinada, vandalismo, roubo, receita perdida, propriedade intelectual danificada.

Fonte: autoria própria.

Impactos de violação de segurança

Exemplo de violação de segurança: Vtech (EUA)

- VTech é um fabricante de brinquedos de alta tecnologia para as crianças;
- Expôs informações confidenciais, incluindo nomes de clientes, endereços de *e-mail*, senhas, fotos e registros de bate-papo;
- VTech não protegeu as informações corretamente;
- Os *hackers* podem criar contas de *e-mail*, pedir créditos e cometer crimes usando as informações das crianças;
- Os *hackers* também podem assumir as contas *on-line* dos pais.

Impactos de violação de segurança

Exemplo de violação de segurança – Equifax:

- A Equifax é uma agência de geração de relatório de crédito ao consumidor;
- Os invasores exploraram uma vulnerabilidade no *software* de aplicativo da *web*;
- A Equifax montou um *site* dedicado com um novo nome de domínio, que permitiu aos criminosos criar *sites* não autorizados para o esquema de *phishing*.

Guerra cibernética

O que é a guerra cibernética?

- Conflito usando o espaço cibernético.

Malware Stuxnet:

- Concebido para danificar a planta de enriquecimento nuclear do Irã;
- Codificação modular usada;
- Certificados digitais roubados usados.

Guerra cibernética

Utilizada para ganhar uma vantagem sobre os adversários, as nações ou os concorrentes:

- Pode sabotar a infraestrutura de outras nações;
- Oferece aos invasores a capacidade de chantagear funcionários governamentais;
- Os cidadãos podem perder a confiança na capacidade do governo de protegê-los;
- Afeta a confiança dos cidadãos no governo, sem nunca, fisicamente, invadir a nação do alvo.

Interatividade

O que o termo “vulnerabilidade” significa?

a) Um alvo conhecido ou uma máquina vítima.
b) Um método de ataque para explorar um alvo.
c) Uma ameaça em potencial criada por um *hacker*.
d) Uma fraqueza que torna um alvo suscetível a um ataque.
e) Um computador que contém informações confidenciais.

Resposta

O que o termo “vulnerabilidade” significa?

a) Um alvo conhecido ou uma máquina vítima.
b) Um método de ataque para explorar um alvo.
c) Uma ameaça em potencial criada por um *hacker*.
d) Uma fraqueza que torna um alvo suscetível a um ataque.
e) Um computador que contém informações confidenciais.

Referências

- CERT.BR. *Cartilha de Segurança para a Internet, versão 4.0*/CERT.br. São Paulo: Comitê Gestor da Internet no Brasil, 2012.
- CERT.BR. *Estatísticas de incidentes na internet*. Disponível em: https://www.cert.br/stats/incidentes/.
- CISCO. *Curso de Cibersegurança*. Disponível em: http://www.netacad.com.
- KIM, D.; SOLOMON, M. G. *Fundamentos de segurança da informação*. 1 ed. Rio de Janeiro: LTC, 2014.
- MCAFEE. CSIS*. Economic Impact of Cybercrime - No Slowing Down*. 2018. Disponível em: https://www.mcafee.com/enterprise/en-us/solutions/lp/economics-cybercrime.html.
- NIST. National Institute of Standards and Technology. 1995.
- STALLINGS, W. *Criptografia e Segurança de Redes.* 4 ed. São Paulo: Pearson, 2008.

ATÉ A PRÓXIMA!