Segurança da Informação– GBC083

Prof. Rodrigo Sanches Miani – FACOM/UFU

Aula passada

Segurança da Informação– GBC083

Informações básicas

- Email: miani@ufu.br
- Página do curso:
  - Teams – procurar por "GBC083 - 2024/01" (chave de acesso: fq49gh2)
- Horário de atendimento – sala 1B-148:
  - Terça-feira – 15:00 – 16:30 ou Quarta-feira – 14:00 – 14:50;
  - Outros horários são possíveis! Basta enviar um email para marcar atendimento fora do horário acima.

Avaliação – Trabalhos práticos

- Entrega eletrônica usando o Microsoft Teams;
- Tarefas atrasadas serão penalizadas:
  - 1 dia – 10% da nota;
  - 2 a 3 dias – 20% da nota;
  - Entre 4 a 21 dias – 50% da nota;
  - Mais de 21 dias – o TP não será pontuado.

Datas importantes

Semana	Data	Conteúdo
1	06/ago	Apresentação da disciplina
1	07/ago	Tópico 1 - Conceitos de Segurança - Parte 1
2	13/ago	Tópico 1 - Conceitos de Segurança - Parte 2
2	14/ago	Tópico 2 - Princípios de Criptografia
3	20/ago	Defesa de Mestrado - Não haverá aula
3	21/ago	Tópico 3 - Criptoanálise e ataques
4	27/ago	Evento IA x Cybersecurity - Google - Não haverá aula
4	28/ago	Tópico 5 - Criptografia simétrica - Cifra de bloco - Parte 1
5	03/set	Tópico 5 - Criptografia simétrica - Cifra de bloco - Parte 2
5	04/set	Tópico 6 - Criptotrafia simétrica - DES - Parte 1
6	10/set	Tópico 6 - Criptotrafia simétrica - DES - Parte 2
6	11/set	Tópico 7 - AES - Parte 1
7	17/set	SBSeg 2024 - Não haverá aula
7	18/set	SBSeg 2024 - Não haverá aula
8	24/set	Tópico 7 - AES - Parte 2
8	25/set	Tópico 8 - Modos de cifra de bloco
9	01/out	Discussão da primeira parte da disciplina - Dúvidas
9	02/out	P1
10	08/out	Tópico 9 - Criptografia de chave pública
10	09/out	Tópico 10 - RSA - Parte 1
11	15/out	Tópico 10 - RSA - Parte 2
11	16/out	Tópico 11 - Funções de Hash
12	22/out	Tópico 12 - Integridade, autenticação e não repúdio
12	23/out	Tópico 13 - Infraestrutura de chaves públicas - Parte 1
13	29/out	Tópico 13 - Infraestrutura de chaves públicas - Parte 2
13	30/out	Tópico 14 - Segurança na camada de transporte - Parte 1
14	05/nov	Tópico 14 - Segurança na camada de transporte - Parte 2
14	06/nov	Aula extra - Tópico a decidir
15	12/nov	Discussão da segunda parte da disciplina - Dúvidas
15	13/nov	P2
16	19/nov	Recuperação
16	20/nov	Feriado - Não haverá aula

Tópicos da aula

Segurança da Informação– GBC083

Tópicos

1. Motivação para o estudo de segurança da informação
2. Pilares da segurança da informação
3. Ataques
4. Mecanismos de defesa

Motivação

Segurança da Informação– GBC083

Motivação – importância da segurança

- A **importância** das redes e o caráter **sensível** de dados e transações chamam atenção de indivíduos e grupos mal intencionados:
  - Muitos destes grupos estão buscando formas de obter vantagens financeiras;
  - Alguns destes grupos buscam notoriedade.

Motivação – importância da segurança

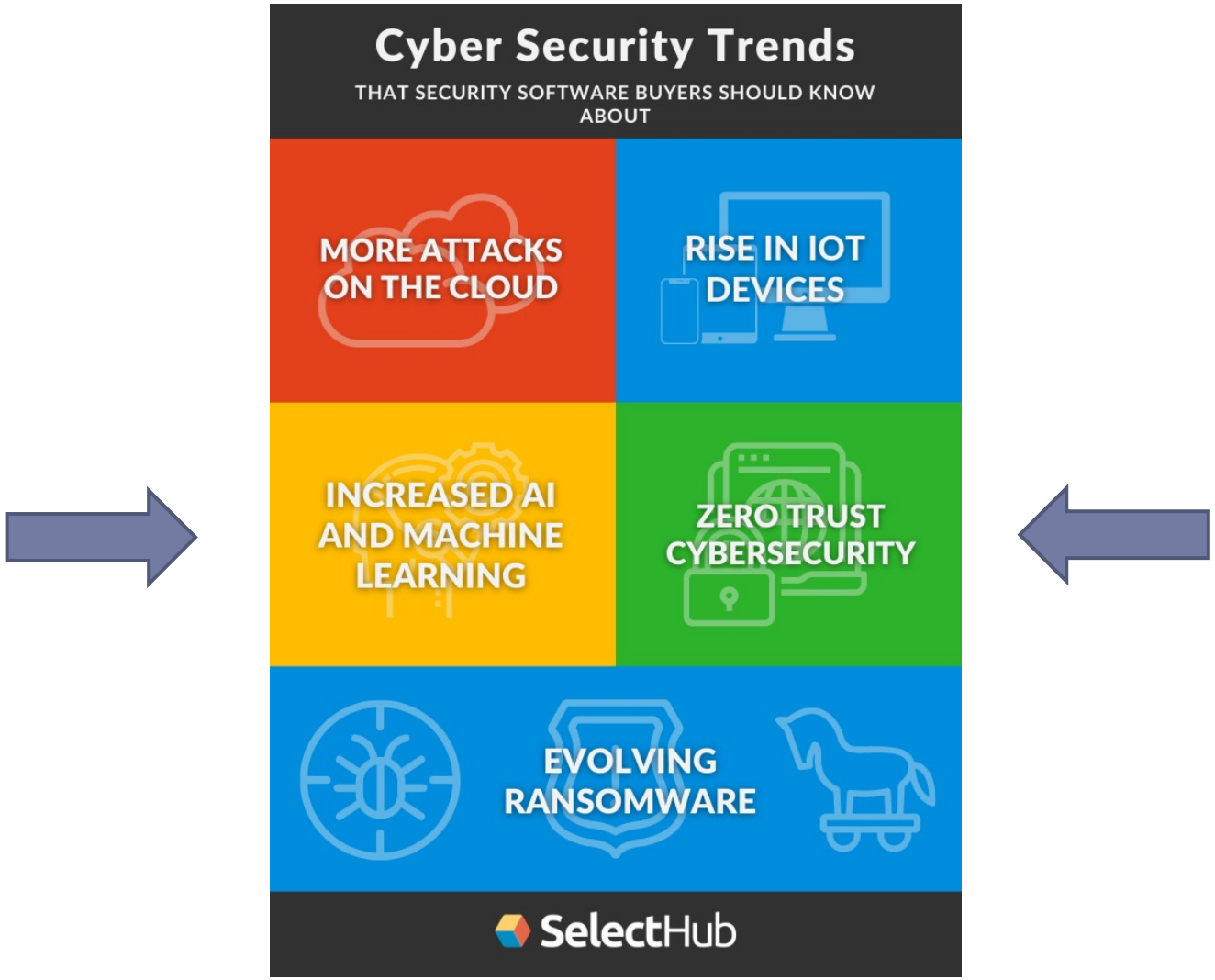
É comum ler nos noticiários relatos de ataques provocados por grupos de *cibercriminosos*:

- Hackers invadem sistemas críticos (cyberwarfare);
  - https://www.washingtonpost.com/technology/2023/12/11/china-hacking-hawaii-pacific-taiwan-conflict/
- Vazamento de dados – Facebook, LinkedIn;
  - https://www.upguard.com/blog/biggest-data-breaches-us
- Vazamento e compilação de senhas;
  - https://g1.globo.com/economia/tecnologia/blog/altieres-rohr/post/2021/06/09/entenda-por-que-o-suposto-vazamento-de-84-bilhoes-de-senhas-nao-esta-preocupando-especialistas.ghtml
  - https://haveibeenpwned.com
- Ataques de ransomware;
  - https://www.cisoadvisor.com.br/dona-da-vans-e-north-face-e-atingida-por-ataque-de-ransomware/

Motivação – importância da segurança

- Problemas de segurança podem:
  - Causar perdas financeiras;
  - Sujar a reputação da empresa;
  - Causar problemas com a justiça;
  - O que mais?
  - Matar!
    - https://www.kaspersky.com.br/blog/stuxnet-as-origens/4391/
    - https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Tendências...



https://www.selecthub.com/endpoint-security/cyber-security-trends/

O que fazer?

Pergunta:

E aí? Como tratar os inúmeros problemas discutidos anteriormente?

O que fazer?

Pergunta:

E aí? Como tratar os inúmeros problemas discutidos anteriormente?

Uma **parte** da resposta envolve planejar e implementar MECANISMOS DE SEGURANÇA.

Implementando segurança

- Computadores atuais são ricos em funcionalidades e complexos;
- Maioria dos usuários são leigos;
  - Atacantes tentam aproveitar essa brecha;
- Vontade de tornar tudo disponível o tempo todo e em qualquer lugar aumenta os problemas;
- Outro ponto importante: a segurança costuma ser implementada usando uma visão reativa;

Pilares

Segurança da Informação– GBC083

Pilares da segurança

- Um modelo de segurança simples mas largamente aplicado é conhecido como a tríade CID - Confidencialidade, Integridade e Disponibilidade;

- Os três conceitos acima envolvem os **objetivos fundamentais** da segurança tanto para dados quanto para serviços de informação e computação;

- Veremos que a violação de qualquer um dos três princípios implica em sérias consequências para os envolvidos.

https://www.informationsecuritybuzz.com/isbuzz-expert-panel/cia-triad-and-new-emerging-technologies-big-data-and-iot/

Pilares da segurança

Confidencialidade:

- Garante que as informações não serão acessadas por agentes não autorizados.

Objetivos da segurança

Integridade:

- Garante que sistemas e informações só sejam modificados dentro das condições previstas;

Objetivos da segurança

Disponibilidade:

- Garante que os dados e sistemas estejam disponíveis para aqueles que tem o direito de utilizá-los;

Objetivos da segurança – Outra referência

Ref. - https://www.doc.ic.ac.uk/~ajs300/security/CIA.htm

Ataques

Segurança da Informação– GBC083

Ataques - Definição

- Qualquer ação que comprometa algum dos três princípios mostrados anteriormente:
  - Confidencialidade, integridade e disponibilidade

Ataques – Tipos

- Ataques passivos
  - Obter informações a partir do monitoramento de comunicações;
  - Tipos: vazamento de conteúdo de mensagem e análise de tráfego.

- Ataques ativos
  - Envolvem alguma modificação do fluxo de dados ou a criação de fluxo falso;
  - Tipos: disfarce, repasse, modificação de mensagem e negação de serviço.

Alguns exemplos de ataques...

- Força bruta: atacante testa exaustivamente diferentes possibilidades até encontrar um código ou senha;

- Negação de serviço:
  - Atacante tenta esgotar recursos do servidor enviando grande volume de requisições;
  - Pode acarretar de perda de desempenho a indisponibilidade do serviço;
  - Variação: ataque distribuído de negação de serviço.

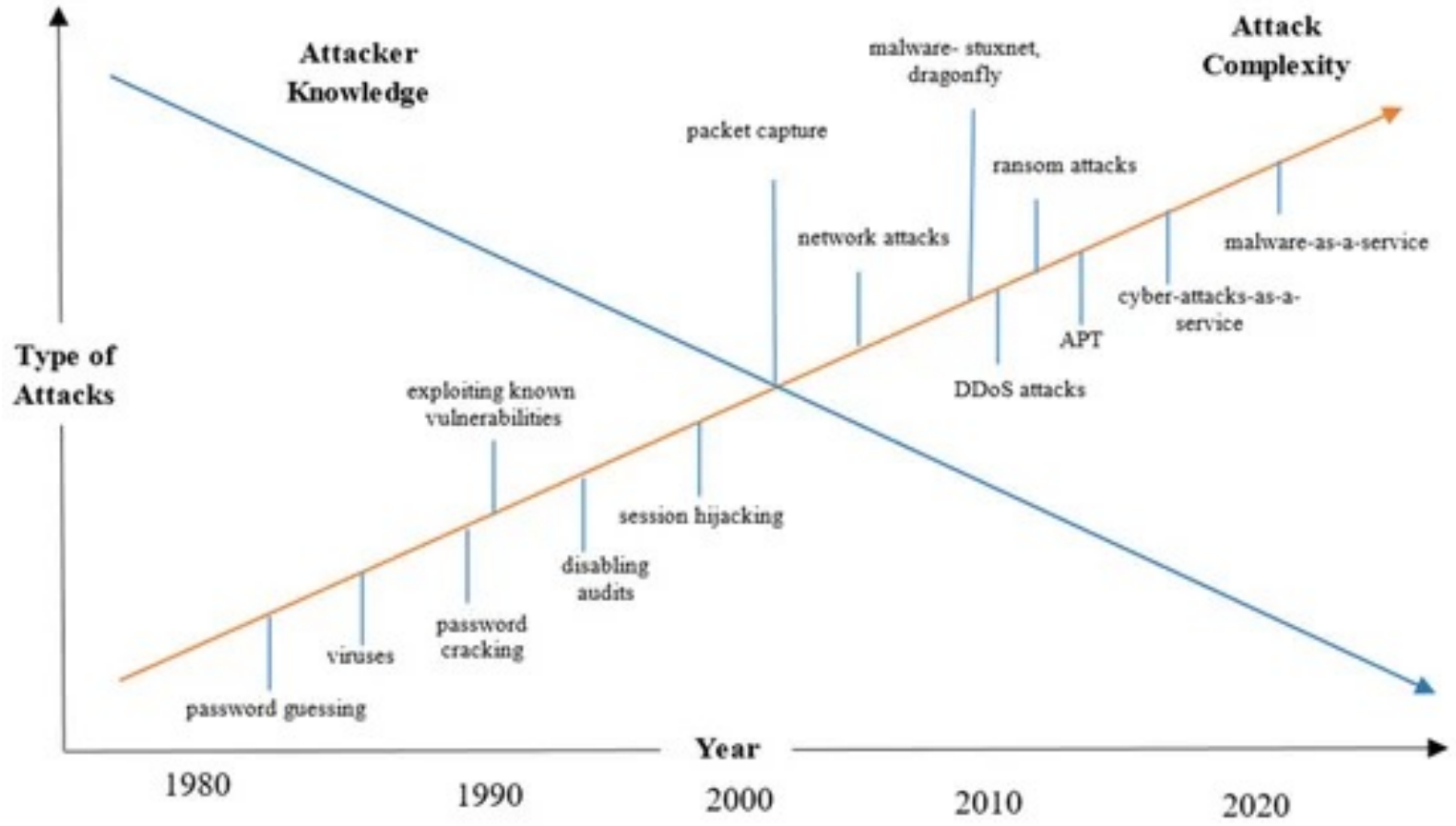
Ataques

- Malwares (malicious softwares):
  - Vírus:
  - Spywares;
  - Worms (vermes);
  - Cavalos de tróia;
  - Botnets.

Ataques

- Engenharia Social:
  - Técnica que explora as fraquezas humanas e sociais;
  - Tem como objetivo enganar e ludibriar pessoas, a fim de conseguir informações;
  - Ataque clássico consiste em se fazer passar por um alto funcionário que tem problemas urgentes de acesso ao sistema;
  - Ataque muito difícil de prevenir ou detectar;
  - Kevin Mitnick, famoso *hacker*, afirmou que utilizava técnicas de Engenharia Social em mais de 80% de seus ataques.

Ataques – Conhecimento x Complexidade



Aslan, Ö.; Aktuğ, S.S.; Ozkan-Okay, M.; Yilmaz, A.A.; Akin, E. A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. *Electronics* **2023**, *12*, 1333.

Mecanismos de defesa

Segurança da Informação– GBC083

Defesas

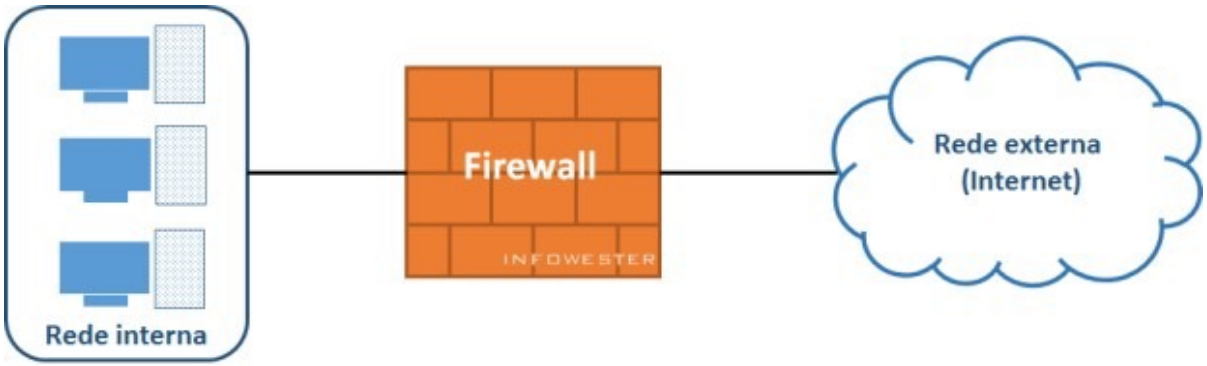
- Protocolos de segurança:
  - TLS (Transport Layer Security):
    - Segurança na camada de transporte;
    - Oferece canal seguro para camada de aplicação;
    - Navegadores e servidores HTTP implementam o TLS;
    - Muito utilizado em transações na Web que envolvem, por exemplo, pagamento com cartão de crédito;
    - SSL implementa os mais famosos e importantes algoritmos de criptografia como RSA e AES.

Defesas

- Protocolos de segurança:
  - IPSEC:
    - Autenticação e cifragem de pacotes IP (mecanismo de segurança na camada de rede);
    - Construção de Virtual Private Networks (VPNs)
    - Authentication Header (AH): autenticação e integridade;
    - ESP (Encapsulating Security Payload): autenticação, integridade e sigilo.

Defesas

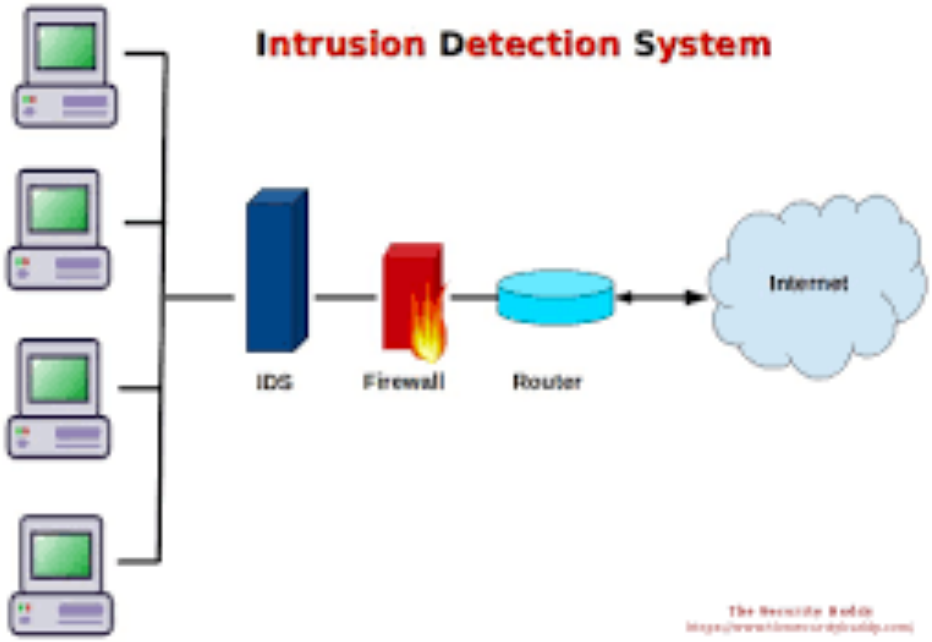
- Firewall:
  - Delimitam o perímetro de defesa da rede;
  - Ponto por onde todo o tráfego que entra e sai da rede deve passar;
  - Analisa todo o tráfego e bloqueia pacotes que não atendam a regras;
  - Possibilita, por exemplo, bloquear acesso externo a sistemas que só devem ser acessados por agentes internos da rede.



http://helpdigitalti.com.br/blog/o-que-e-firewall-conceito-tipos-e-arquiteturas

Defesas

- Sistemas de detecção de intrusão (Intrusion Detection System – IDS):
  - Detecção de situações nas quais há acesso (ou tentativa) não autorizado aos sistemas;
  - Baseados em assinaturas;
  - Baseados no comportamento normal;
  - Problema: alarmes falsos
  - Exemplo: Snort.



Defesas

- Antivírus:
  - Detecção, identificação e remoção de vírus;
  - Várias soluções disponíveis no mercado:
    - AVG;
    - Avast;
    - Mcafee;
    - Norton;
    - Symantech;
    - Panda.

Defesas

- Políticas de segurança:
  - Diz respeito às regras que devem ser elaboradas e seguidas pelos utilizadores dos recursos de informação de uma empresa. Exemplos:
    a) Backups – frequência? Quais dados? Onde armazenar...;
    b) Segurança no acesso físico – Quem pode entrar? Quando?;
    c) Conscientização de usuários quanto a comportamento adequado que evita problemas;
    d) Atualizações constantes de antivírus, bases de assinaturas, etc;
    e) Estudo de incidentes ocorridos;
    f) Análise de métricas de segurança.

Defesas - Políticas

Extraído de https://www.tecmundo.com.br/seguranca/220645-lgpd-lei-geral-protecao-dados-pessoais.htm

Criptografia

- A criptografia permite:
  - Que o emissor da informação use uma chave para embaralhar a informação de maneira que só o destinatário com a mesma chave a entenderá;
  - Que o emissor da informação seja autenticado;
  - Que a informação não seja alterada durante o seu percurso (que o destino consiga verificar se houve alguma alteração).

Discussões

GBC083 - Segurança da Informação

Organizações totalmente seguras?

Com base no que foi discutido, é possível afirmar que uma organização é 100% segura?

Organizações totalmente seguras?

Com base no que foi discutido, é possível afirmar que uma organização é 100% segura?

- Não! Não existe um modelo de segurança à prova de ataques;
- Um sistema que está seguro hoje pode não estar seguro amanhã;

Organizações totalmente seguras? - Exemplo

- A segurança envolve:
  - Aspectos tecnológicos – um sistema de autenticação robusto;
  - Aspectos técnicos – um administrador de segurança experiente e com vastos conhecimentos na área;
  - Aspectos sociais/humanos – funcionários que seguem políticas e boas práticas;
  - Aspectos educacionais – fornecer treinamento aos envolvidos – funcionários e terceiros.

Organizações totalmente seguras? – Conclusão

- O objetivo não é construir uma rede 100% segura, mas sim um **sistema confiável**:
  - Capaz de anular os ataques mais casuais;
  - Tolerar acidentes! Ter um plano de contingência (famoso plano B).

- Uma tendência de pesquisa nos últimos anos envolve o uso de **técnicas de aprendizado de máquina** para identificar diferentes tipos de ataque.

IA x Cybersecurity

- Aplicações de IA para problemas de *cybersecurity* estão atraindo muita atenção da indústria e academia;

- Estimativas indicam que o mercado de IA para cybersecurity irá crescer de 1 bilhão de dólares em 2016 para **34.8 bilhões de doláres até 2025**;

- Diferentes tarefas tradicionais de segurança podem ser potencializadas com o uso de IA*:
  - desenvolvimento de IDSs baseados em detecção de anomalias,
  - análise de malware,
  - identificação de phishing e URLs maliciosas,
  - construção de SIEMs (Security Information and Event Management - Gerenciamento e Correlação de Eventos de Segurança).

* "Cybersecurity data science: an overview from machine learning perspective"

IA x Cybersecurity

- Contudo, o uso de IA para resolver tarefas de *cybersecurity* possui **vantagens** e **desvantagens;**

- Apesar de melhorar substancialmente diferentes práticas de *cybersecurity*, também facilita novas formas de ataques às próprias soluções de IA*:
  - Envenenamento de dados (*data poisoning*)
  - Evasão (*tempering of categorization model*)

- *Trusting artificial intelligence in cybersecurity is a double-edged sword

Roteiro de Estudos

1. Leitura do Capítulo 1 (Introdução) – "Criptografia e segurança de redes. Princípios e práticas". William Stallings;
2. Estudo da vídeo-aula referente ao Tópico 1;
   - https://www.youtube.com/@criptografia

Roteiro de Estudos

Materiais complementares:

1. Estudo da vídeo-aula 1 do curso de Segurança da Informação da UNIVESP
   - https://www.youtube.com/watch?v=JrVS7YsGw8w&list=PLxI8Can9yAHenoHipBXp9XuJY4BBxBUPQ&index=2
2. Leitura dos capítulos 1, 2, 3 e 7 (são curtinhos!!) da Cartilha de Segurança para Internet do Cert.br:
   - https://cartilha.cert.br/livro/
3. Assistir os seguintes vídeos:
   - https://www.youtube.com/watch?v=KZC7vQOTuEw&t=5s
   - https://www.youtube.com/watch?v=erCAp_Bd0AQ