TÓPICOS ESPECIAIS EM DEFESA CIBERNÉTICA

Professor Me. Vladimir Geraseev Junior

Fatec Centro Paula Souza Governo de São Paulo

Curso: TECNOLOGIA EM DEFESA CIBERNÉTICA

Disciplina: Tópicos Especiais em Defesa Cibernética

Sejam Bem Vindos!

Prof. Vladimir Geraseev Junior

PROF VLADIMIR GERASEEV JUNIOR

- **GRADUAÇÃO EM CIÊNCIAS DA COMPUTAÇÃO**
- **MESTRADO EM ENGENHARIA - UNITAU**

- EXPERIÊNCIA PROFISSIONAL:

- COMPANHIA DE INFORMÁTICA DE JUNDIAÍ – ARQUITETO DE REDES
- EMBRAER – GRUPO DE ENGENHARIA
- INSTITUTO NACIONAL DE PESQUISAS ESPACIAIS – INPE – ANALISTA DE REDES E SEGURANÇA
- IMPLEMENTAÇÃO DOS REQUISITOS DE SEGURANÇA CIBERNÉTICA PARA EQUIPAMENTOS PARA TELECOMUNICAÇÕES (ATO 77) – ANATEL
- CONSULTORIA EM CONDUÇÂO DE PENTESTS

PROF VLADIMIR GERASEEV JUNIOR

- EXPERIÊNCIA PROFISSIONAL ACADÊMICA.

- PROFESSOR NA FATEC TAUBATÉ
- PROFESSOR NA ETEC JACAREÍ
- PROFESSOR EM UNIVERSIDADES PARTICULARES (UNIP, UNIVAP, FAPI)

EMENTA DA DISCIPLINA

- Panorama atual de cybersegurança
- Inteligência de Ameaças – Cyber Threat Intelligence
- Defesa preditiva
- Next Generation Firewall

EMENTA DA DISCIPLINA

- Zero Trust e segurança baseada em identidade
- SOC, SIEM e monitoramento de segurança
- Automação, SOA
- XDR (Extended Detection and Response), EDR (Endpoint Detection and Response) e NDR (Network Detection and Response)
- Segurança de APIs e aplicações modernas

OBJETIVOS DA DISCIPLINA

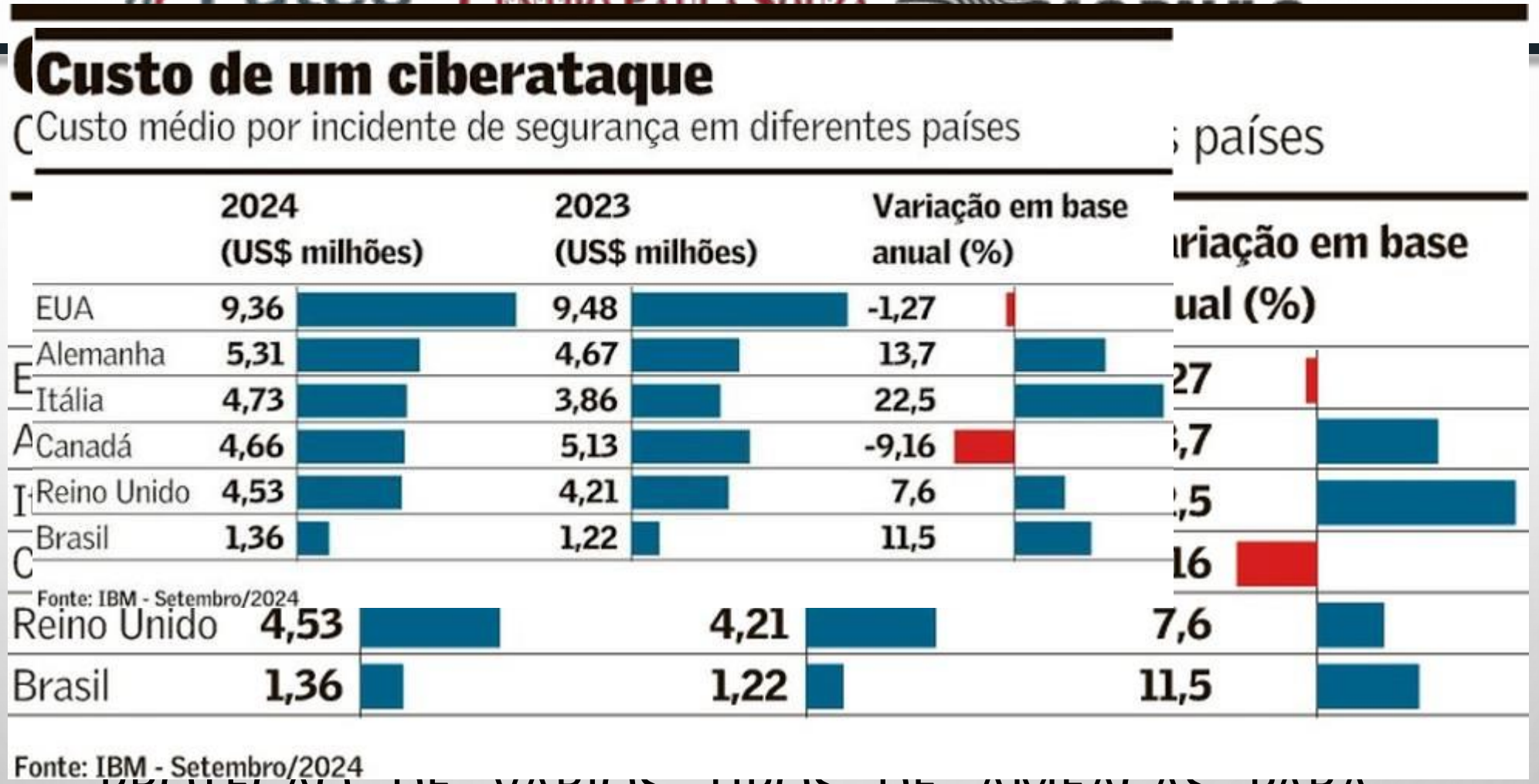
- Analisar, identificar e implementar tecnologias emergentes que auxiliem na solução de defesa cibernética.
- Manter atualizado com o estado da arte nas tecnologias que envolvem o ambiente de defesa cibernética;
- Identificar Tecnologias Inovadoras e suas aplicações para defesa cibernética.

BIBLIOGRAFIA BÁSICA

- FONTES, E. **PRATICANDO A SEGURANÇA DA INFORMAÇÃO**. BRASPORT, 2008.
- STALLINGS, W. **CRIPTOGRAFIA E SEGURANÇA DE REDES**. 4 ED. SÃO PAULO: PEARSON, 2008.

BIBLIOGRAFIA COMPLEMENTAR

- MORAES, ALEXANDRE FERNANDES DE. SEGURANÇA EM REDES: FUNDAMENTOS. SÃO PAULO: ÉRICA, 2010.
- MORAES, ALEXANDRE FERNANDES DE. FIREWALLS: SEGURANÇA NO CONTROLE DE ACESSO. SÃO PAULO: ÉRICA, 2015.



PROTEÇÃO DE VÁRIOS TIPOS DE AMEAÇAS PARA GARANTIR A CONTINUIDADE DO NEGÓCIO.

INTRODUÇÃO

A informação é algo que contém um significado e causa impacto em diferentes graus, tornando-a o elemento chave da extração e criação do conhecimento. O conhecimento só poderá ser formado quando o indivíduo for exposto à informação, deste modo é possível afirmar que poderá até haver informação sem conhecimento, mas não conhecimento sem informação.

DADO

E QUALQUER ELEMENTO IDENTIFICADO EM SUA FORMA BRUTA QUE, POR SI SÓ, NÃO CONDUZ UMA COMPREENSÃO DE UM DETERMINADO FATO OU SITUAÇÃO.

“DADOS SÃO ÁTOMOS DA INFORMAÇÃO ”

EX: 1024

INFORMAÇÃO

SÃO OS RESULTADOS DOS DADOS DEVIDAMENTE TRATADOS, COMPARADOS, CLASSIFICADOS, RELACIONÁVEIS ENTRE OUTROS DADOS SERVINDO PARA TOMADAS DE DECISÕES .

“SÃO OS DADOS TRABALHADOS, GERANDO A INFORMAÇÃO”

EX: **1024 CLIENTES ATIVOS**

CONHECIMENTO

É O CONJUNTO DE FERRAMENTAS CONCEITUAIS E CATEGORIAS USADA PARA CRIAR, COLECIONAR, ARMAZENAR E COMPARTILHA A INFORMAÇÃO.

“SÃO AS INFORMAÇÕES TRABALHADAS ”

VALOR DA INFORMAÇÃO.

O VALOR DA INFORMAÇÃO É DETERMINADO PELO QUE A ORGANIZAÇÃO OU USUÁRIO DÁ À ELA.

INTRODUÇÃO

No mundo atual a posse e o uso do conhecimento passou a ser um fator estratégico decisivo para muitas empresas. Estamos vivendo a época batizada como "Era da Informação". Mas a informação é volátil, frágil. Hoje, ela pode desaparecer na velocidade de um pulso elétrico.

Atualmente, as informações constituem o objeto de maior valor para as empresas. Por esse e outros motivos a segurança da informação é um assunto tão importante para todos, pois afeta diretamente todos os negócios de uma empresa ou de um indivíduo.

Importância da Informação para o Negócio - A informação é um elemento essencial para a geração do conhecimento, para a tomada de decisões, e que representa efetivamente valor para o negócio.

CONCEITOS

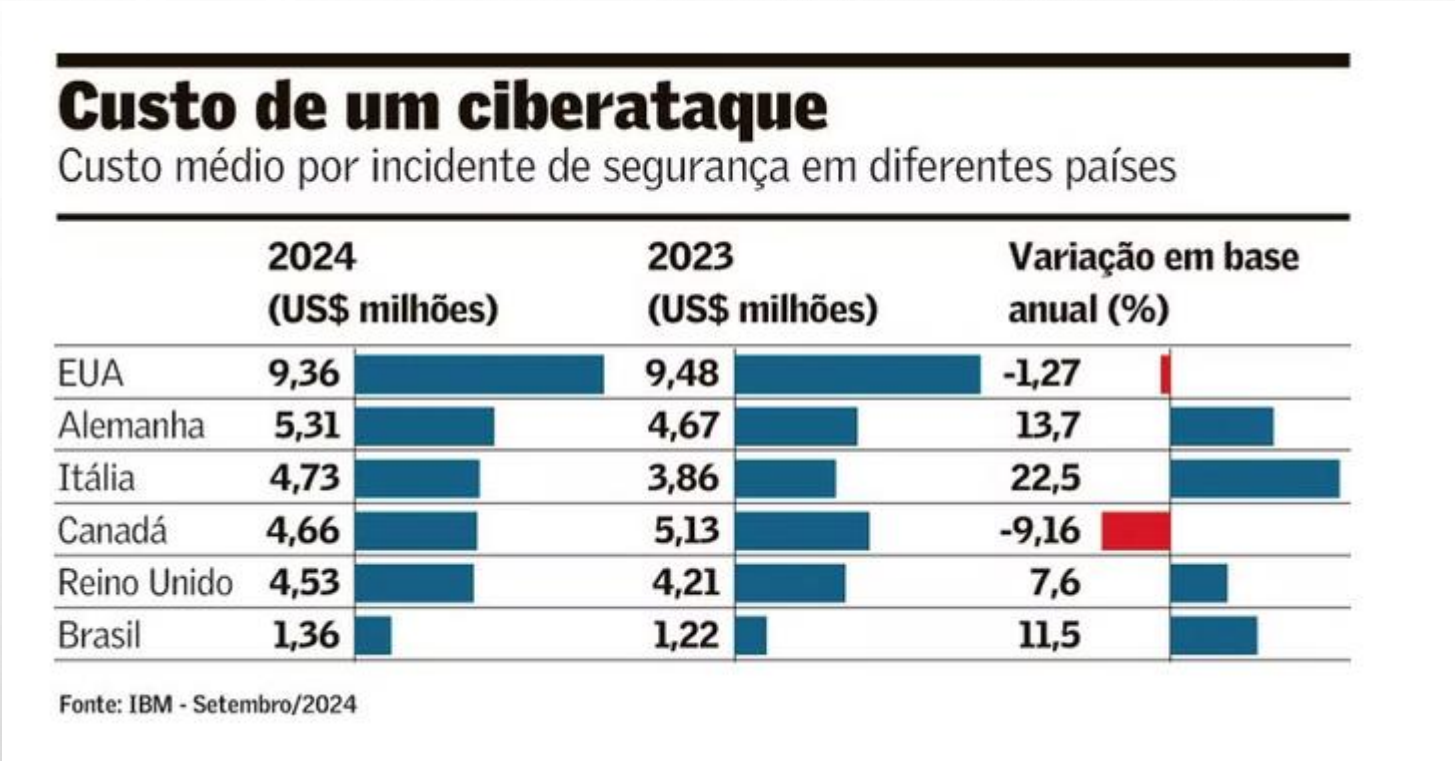
- **Ativo de Informação:** Qualquer elemento que tenha valor para uma organização.
- **Valor do Ativo:** Quantificação de perda de determinado ativo quando esse tem sua confidencialidade, integridade ou disponibilidade (Princípios Básicos da SI) afetadas.
- **Vulnerabilidade:** Falha no ambiente que ameace algum ativo.
- **Ameaça:** Possibilidade de exploração de uma vulnerabilidade.
- **Impacto:** Resultado da concretização de uma ameaça contra a vulnerabilidade de um ativo.

O PESO FINANCEIRO E GEOGRÁFICO DO RISCO

Trilhões de dólares: Custo projetado do cibercrime para a economia global.

Liderança regional: O Brasil se mantém como um dos países mais visados por ataques na América Latina.

Prejuízo reputacional: O custo médio de uma violação de dados corporativos local ultrapassa milhões de reais por incidente.



O PESO FINANCEIRO E GEOGRÁFICO DO RISCO

Trilhões de dólares: Custo projetado do cibercrime para a economia global.

Liderança regional: O Brasil se mantém como um dos países mais visados por ataques na América Latina.

Prejuízo reputacional: O custo médio de uma violação de dados corporativos local ultrapassa milhões de reais por incidente.

Países	Ataques semanais por organizações (primeiro trimestre de 2024)	Variação ano a ano
Argentina	994	-52%
Brasil	2.202	+38%
Canadá	935	+23%
Chile	1.497	+5%
Colômbia	2.484	+5%
México	2.296	+43%
Estados Unidos	925	-4%

A NOVA ERA DAS AMEAÇAS – IA COMO ARMA

Phishing hiper-realista: Golpes customizados em massa, sem erros gramaticais e usando engenharia social avançada.

Ataques autônomos: Criação e modificação de exploits em tempo real por algoritmos automatizados.

Deepfakes corporativos: Uso de voz e vídeo falsificados para fraudes financeiras de alta liderança (CEO Fraud).

A IDENTIDADE É O NOVO ALVO PRINCIPAL

Abuso de credenciais: Atacantes preferem "fazer login" com acessos legítimos roubados a forçar a entrada na rede.
Extorsão sem criptografia: Roubo puro e simples de dados confidenciais sem a necessidade de paralisar sistemas com ransomware tradicionais.
Risco de terceiros: Vulnerabilidades na cadeia de suprimentos e fornecedores de software como porta de entrada.

A RESPOSTA DEFENSIVA – IA E MONITORAMENTO CONTINUO

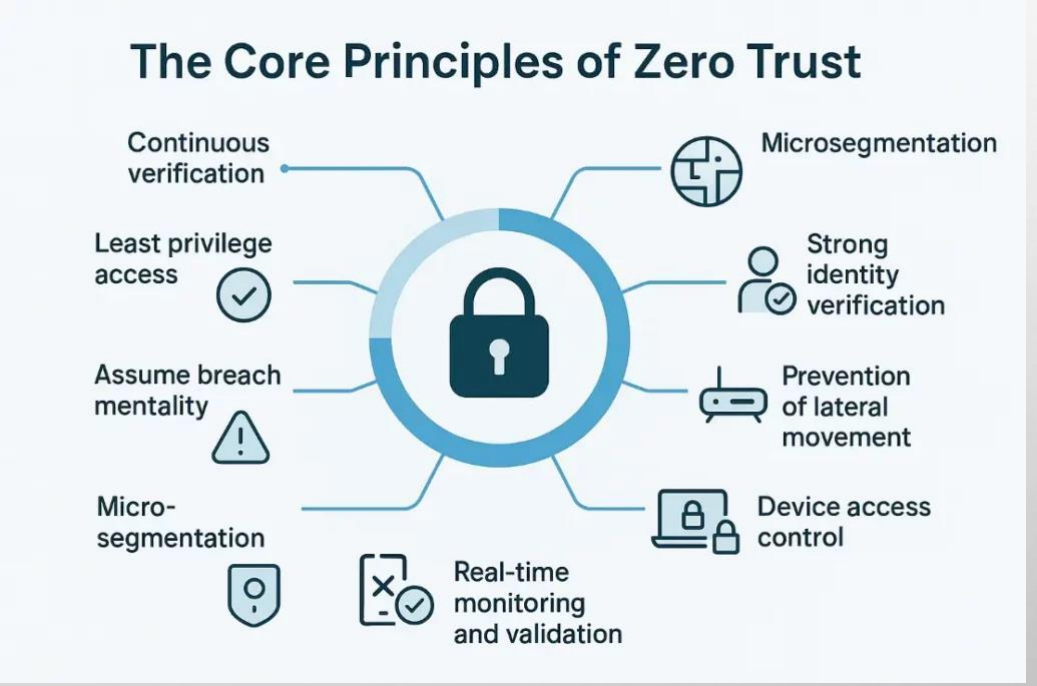
IA defensiva: Detecção comportamental automatizada para conter ameaças antes que elas se espalhem pela rede.

Zero Trust: Filosofia de "nunca confiar, sempre verificar" aplicada a cada usuário, dispositivo e transação.

SOC e SIEM: Monitoramento e resposta a incidentes gerenciados 24 horas por dia, 7 dias por semana.

A RESPOSTA DEFENSIVA – IA E MONITORAMENTO CONTINUO

Zero Trust: Filosofia de "nunca confiar, sempre verificar" aplicada a cada usuário, dispositivo e transação.



A RESPOSTA DEFENSIVA – IA E MONITORAMENTO CONTINUO

SOC e SIEM: Monitoramento e resposta a incidentes gerenciados 24 horas por dia, 7 dias por semana.