Prof. Esp. Thalles Canela

- **Graduado:** Sistemas de Informação - Wyden Facimp
- **Pós-graduado:** Segurança em redes de computadores - Wyden Facimp

- **Consultor de Tecnologia - [aXR6] Cyber Security e NtecSoftware**
- **Professor no Senac (contratado)**
- **Professor na Wyden Facimp (contratado)**
  - **Pós-graduação:** Segurança em redes de computadores - Wyden Facimp
- **Professor na Wyden Facimp (Efetivado)**
  - **Graduação:** Análise e desenvolvimento de sistemas - Wyden Facimp

Redes sociais:

- **Linkedin:** https://www.linkedin.com/in/thalles-canela/
- **YouTube:** https://www.youtube.com/aXR6CyberSecurity
- **Facebook:** https://www.facebook.com/axr6PenTest
- **Instagram:** https://www.instagram.com/thalles_canela
- **Github:** https://github.com/ThallesCanela
- **Github:** https://github.com/aXR6
- **Twitter:** https://twitter.com/Axr6S

PRINCÍPIOS E CONCEITOS DE SEGURANÇA CIBERNÉTICA

ROTEIRO

1. EVOLUÇÃO DA SEGURANÇA CIBERNÉTICA
2. VALOR DA INFORMAÇÃO ALINHAMENTO ESTRATÉGICO DA SEGURANÇA AOS NEGÓCIOS
3. INVESTIMENTO NECESSÁRIO PARA GARANTIR A PROTEÇÃO DOS DADOS
4. PLANO DE CIBERSEGURANÇA (CYBERSECURITY PLAN)

O que é segurança cibernética e por que é importante?

- Conjunto de boas práticas;
- Proteção informação armazenada: computadores e aparelhos de computação transmitidos através das redes de comunicação;

A EVOLUÇÃO DOS ATAQUES CIBERNÉTICOS

=

EVOLUÇÃO DA SEGURANÇA CIBERNÉTICA

EVOLUÇÃO DA SEGURANÇA CIBERNÉTICA

- **Os ataques cibernéticos nas empresas têm se tornado um grande problema** (relatórios, informações de clientes, dados fiscais, planejamentos, entre outros);
- **Em geral, os ataques são feitos em plataformas com excelência em coletar um grande volume de informações** (sites de instituições financeiras, bancos, grandes varejistas, organizações médicas, entre outros)

O Creeper e o Reaper, 1971

- O Creeper, considerado o primeiro vírus do mundo;
- Código portátil que podia viajar entre sistemas;
- Ele tinha como alvo os computadores mainframe PDP-10 da Corporação de Equipamentos Digitais (DEC) conectados ao Arpanet;
- Ele não afetou nenhum efeito destrutivo de longo prazo nos dispositivos afetados;

O primeiro congelamento de rede, 1988

- Um erro inadvertido em um código de worm projetado para medir o tamanho da Internet resultou no primeiro ataque DoS;
- O erro fez com que o Worm Morris se replicasse incessantemente a ponto de a Internet inicial (Arpanet) ficar entupida e 10% de todos os sistemas conectados travar.

O Departamento de Segurança Interna, 2002

- O Departamento de Segurança Interna dos Estados Unidos, estabelecido pelo presidente George W. Bush em 2002, assumiu a responsabilidade de proteger a infraestrutura de TI crucial dos Estados Unidos;
- Em 2018, Donald Trump sancionou a Lei da Agência de Segurança de Infraestrutura e Segurança Cibernética que deu origem ao Agência de Segurança Cibernética e Infraestrutura (CISA).
- A CISA trabalha com o governo federal na defesa contra ataques cibernéticos;

O nascimento do Anonymous, 2003

- Ele é um coletivo internacional descentralizado que realiza ataques cibernéticos como um meio de chamar a atenção para suas visões políticas e expor alvos de alto perfil;

Operação Aurora, 2009

- A Operação Aurora foi uma série de ataques cibernéticos originados na China e direcionados às informações de propriedade intelectual de mais de trinta empresas do setor privado dos EUA, incluindo Google, Yahoo e Adobe;
- Este incidente trouxe à luz as capacidades das operações cibernéticas como uma ferramenta para realizar espionagem industrial em grande escala;

Stuxnet, 2010

- O Stuxnet era um worm de computador extremamente sofisticado que explorava várias vulnerabilidades zero-day do Windows;
- Supostamente criado por um programa secreto dos EUA-Israel, ele teve como alvo e destruiu centrífugas na instalação de enriquecimento de urânio em Natanz, Irã, causando danos substanciais ao programa nuclear do país;

EternalBlue e ataques ransomware, 2017

- EternalBlue é um exploit que utiliza vulnerabilidades na implementação do Windows do protocolo Server Message Block (SMB);
- Foi divulgado pelo grupo de hackers Shadow Brokers em abril de 2017;
- Dois grandes surtos de ransomware em todo o mundo, WannaCry e NotPetya, usaram esse exploit para afetar computadores sem patch;

Regulamento Geral de Proteção de Dados (GDPR), 2018

- O Regulamento Geral de Proteção de Dados (GDPR) é um regulamento de conformidade que fornece aos cidadãos da União Europeia (UE) maior controle sobre seus dados pessoais;

O hack do Twitter, 2020

- Um dos incidentes de segurança cibernética mais sensacionais deste ano aconteceu quando as contas de vários usuários de alto perfil do Twitter foram hackeadas, incluindo as de Barack Obama, Elon Musk e Bill Gates;
- Os hackers postaram tweets fraudulentos que diziam “Estou retribuindo à comunidade. Todos os Bitcoins enviados para o endereço abaixo serão devolvidos em dobro! Se você enviar $ 1.000, eu irei devolver $ 2.000;
- Só fazendo isso por 30 minutos” e ganharam £ 86.800 em poucas horas.

Trabalho remoto – A nova norma, mais recursos de segurança chegando em 2021

- Na esteira da pandemia COVID-19, a maioria das empresas foi forçada a adotar um modelo de trabalho remoto;
- Embora a transição para muitas organizações tenha sido difícil, as indicações são de que os cenários de trabalho remoto provavelmente permanecerão em vigor mesmo após o fim da pandemia;

Segurança cibernética habilitada para inteligência artificial (IA)

- Com algoritmos de aprendizado de máquina eficientes e integração perfeita de IA em aplicações de segurança cibernética, a detecção de ameaças em tempo real e a resposta automatizada a incidentes são possíveis e estão sendo continuamente aprimoradas;
- Mecanismos de correlação de ameaças eficazes que detectam ataques em seus estágios iniciais se tornarão mais refinados como a defesa da linha de frente para as organizações;

As 3 diretrizes para evolução da liderança de cibersegurança, segundo o Gartner, são:

1º - Manter a análise e a previsão contínua: Os líderes de segurança devem olhar bem além das ameaças imediatas e pensar em um modelo de segurança continuo, com uma estratégia que integre insights de pesquisas relacionadas em recursos internos e ferramentas de terceiros para manter uma abordagem de segurança completa e eficiente.

As 3 diretrizes para evolução da liderança de cibersegurança, segundo o Gartner, são:

2º - Destacar pontos fortes e, como líder, conhecer suas fraquezas: A segurança cibernética empresarial eficiente requer alto conhecimento técnico, comercial e estratégico, mas é improvável que um líder de segurança se destaque nas três áreas simultaneamente.

As 3 diretrizes para evolução da liderança de cibersegurança, segundo o Gartner, são:

3º - Lembra-se de que os ataques nunca acabam: O universo da tecnologia é de mudança contínua, o que significa que novas técnicas de ataque e vetores de ameaças continuarão a surgir, assim como as novas tecnologias vão surgindo.

Ciberameaças: 6 mapas online de ataques cibernéticos

- 1 Mapa Kaspersky Lab;
- 2 Mapa Botnet Deteque;
- 3 Mapa Fortinet;
- 4 Mapa FireEye;
- 5 Mapa SonicWall;
- 6 Mapa Threat Butt;

#1 Mapa Kaspersky Lab

- Com um design elegante e clean, o mapa de ciberataque em tempo real da Kaspersky Lab é uma das ferramentas que se destacam.
- Além de ter excelente apresentação, o mapa garante praticidade e mobilidade aos usuários, já que também funciona muito bem em dispositivos móveis.
- Ao clicar em "*estatísticas*", o usuário pode encontrar facilmente muitos detalhes sobre a origem dos dados e verificar as classificações de ataque do dia.

- **Link: https://cybermap.kaspersky.com/**

#2 Mapa Botnet Deteque

- Entre as ferramentas de mapeamento de ataque hacker em tempo real, outra que se destaca é o mapa de ciberameaças de botnet Deteque. A ferramenta mostra o número total de bots ativos nas últimas 24 horas e apresenta ainda o ranking dos 10 países com maior número de bots ciberataques com botnet.

- **Link: https://www.deteque.com/live-threat-map/**

#3 Mapa Fortinet

- Embora não tenha um projeto visual de destaque, o mapa online de ataques cibernéticos em tempo real da Fortinet possui alguns recursos interessantes que o tornam único.
- O canto inferior esquerdo tem estatísticas de ciberataques fáceis de entender (e dramáticas) e, se você olhar o mapa, verá que um mapa dia / noite está sutilmente sobreposto ao mapa de ciberataques. Assim, você pode ver onde os maus atores gostam de trabalhar à noite.

- **Link: https://threatmap.fortiguard.com/**

#4 Mapa FireEye

- O mapa de ataques cibernéticos em tempo real da FireEye é mais sutil e menos dramático na exibição dos gráficos de ataque. Ao acessar a tela inicial, por exemplo, o usuário precisa desbloquear a visualização do mapa. Além disso, a ferramenta apresenta os números de ataques hackers dos últimos 30 dias em cinco indústrias: financeira, serviços e consultoria, telecomunicações, manufatura e seguros. Aqui está o que o diferencia: é menos dramático com seus gráficos de ataque do que alguns dos outros e também mostra as principais verticais atacadas nos últimos 30 dias.

- Link: https://www.fireeye.com/cyber-map/threat-map.html

#5 Mapa SonicWall

- Mapa SonicWall, esse é um mapa de ameaças cibernéticas ao vivo realmente bonito, dinâmico e completo. Com uma proposta de análise fácil, a parte inferior do mapa mostra quais países são os principais alvos de ataque no momento e o número médio de ataques cibernéticos por site durante o dia, entre outras coisas.

- **Link: https://attackmap.sonicwall.com/live-attack-map/**

#6 Mapa Threat Butt

- O mapa de ataques cibernéticos Threat Butt funciona com a tecnologia patenteada Clown Strike. Ou seja, usa a força bruta do sistema de nuvem privada, híbrida, pública e cumulus para prover inteligência de ameaças de grau Viking para qualquer empresa. Como diferencial, o mapa conta com interface e som "*pew-pew*" dos videogames dos anos 80.

- **Link: https://threatbutt.com/map/**