

# Prof. esp. Thalles Canela

- **Graduado:** Sistemas de Informação - Wyden Facimp
- **Pós-graduado:** Segurança em redes de computadores - Wyden Facimp
- **Professor (contratado):**
- **Pós-graduação:** Segurança em redes de computadores - Wyden Facimp
- **Professor (Efetivado):**
- **Graduação:** Todo núcleo de T.I. - Wyden Facimp
- **Tech Lead na Motoca Systems**

## 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](https://www.instagram.com/thalles_canela)
- **Github:** <https://github.com/ThallesCanela>
- **Github:** <https://github.com/aXR6>
- **Twitter:** <https://twitter.com/Axr6S>

A hammerhead shark is shown swimming in deep blue water. The shark is positioned diagonally, with its head towards the upper left and its tail towards the lower right. Its mouth is slightly open, revealing small teeth. The water has a textured, wavy surface. In the bottom right corner, a small group of fish is visible. The text 'AMEAÇAS E VULNERABILIDADES' is centered over the shark in a white, sans-serif font.

# AMEAÇAS E VULNERABILIDADES

# Compreendendo o problema

- **Situação:** empresas de 74 países foram alvos de ataques e seus dados sequestrados. Serão devolvidos mediante pagamento.

# Objetivos

- Conhecer as principais ameaças
- Entender o mecanismo de atuação das ameaças
- Compreender o conceito de vulnerabilidades
- Conhecer os mecanismos básicos de prevenção em segurança da informação

# Ameaças à Informação: Contexto

- Segurança da Informação...
  - É uma preocupação antiga!

# Ameaças à Informação: Contexto

- O mundo mudou muito nas últimas décadas
  - Documentos são digitais
  - Processos são digitais
  - Uso da “nuvem”
  - Dispositivos “sempre online”
  - Todos os dispositivos sempre online...!

# Ameaças à Informação: Contexto

- Os “armários”, hoje em dia, são digitais!

# Ameaças à Informação: Contexto

- Política de Segurança da Informação (PSI)
  - Regulatória x Informativa x Consultiva
  - Procedimentos e obrigações
    - Quem pode/deve o quê
  - Imprescindível!



# Ameaças à Informação: Contexto

- Fontes para uma PSI (ABNT)
  - Princípios, objetivos e necessidades da organização
  - Legislação vigente (Marco Civil e LGPD, p. exemplo)
  - Avaliação de riscos
    - Identificar ameaças e vulnerabilidades

# A MEAÇAS À SEGURANÇA DAS INFORMAÇÕES

# Ameaças à Segurança

- Potencial de violação à segurança
  - Circunstância, ação ou evento
    - quebra da segurança

# Ameaças à Segurança

- Ameaça Organizacional
  - Situações externas
  - Tempo presente ou futuro
  - Podem afetar a empresa negativamente.

# Ameaças à Segurança Organizacional

- Referem-se à perda de:
  - Integridade
    - Informação exposta ao manuseio não autorizado
  - Confidencialidade
    - Informação exposta à visualização não autorizada
  - Disponibilidade
    - Informação deixa de estar acessível no momento necessário às atividades do negócio

# Ameaças à Rede ou Sistemas

- As informações e processos digitais...
  - Dependem do uso de redes e sistemas
- Ameaças podem focar nesses elementos

# Aparte: Hackers x Crackers

- Hackers
  - Muito conhecimento em TIC
  - Conhecimento avançado de programação
  - Conhecimentos de eletrônica, psicologia etc...
  - Ação: dentro da legalidade(?)
  - Motivação: avanço tecnol.(?), causa(?)...
- Crackers
  - Conhecimento como o dos hackers
  - Ação: quebra da legalidade
  - Motivação: notoriedade, vingança, ganhos...

# Aparte: Hackers x Crackers

- Na terminologia hackers
  - Chapéu Branco (White Hat)
  - Chapéu Preto (Black Hat)
  - Chapéu Cinza (Gray Hat)
    - Fins do White Hat
    - Meios do Black Hat



# PRINCIPAIS TIPOS DE AMEAÇAS

# Principais Tipos de Ameaças

- Pessoas mal intencionadas!
  - E seus ataques...
- Golpes diversos (mais na aula que vem)
- Softwares do tipo “malware”
  - Malicious Software
  - Software que se infiltra na máquina de forma ilícita
    - Causa danos, alterações ou roubo de informações

# Principais Tipos de Ameaças

- Softwares do tipo “malware”
  - Como se infiltram?
- Diversos mecanismos:
  - Vulnerabilidades de programas existentes
  - Execução de arquivos infectados
  - Auto-execução de mídias infectadas
  - Acesso a páginas web com navegadores vulneráveis
  - Ação direta de atacantes.

# Principais Tipos de Ameaças

- Principais tipos de malware
  - Vírus
  - Worms
  - Trojans
  - Bots e Botnets
  - Spywares
  - Rootkits

# Malwares - Vírus

- Programas que alteram softwares instalados
- Propagação: execução de arquivos infectados
  - Mídias Removíveis (Disquetes, pen drives...)
  - Comunicação (E-mails, mensagens...)
  - Repositórios
- Tipos
  - Vírus em executável (mais comum em e-mails)
  - Vírus de script (em geral vem por e-mail também)
  - Vírus de macro (em geral em documentos)
  - Vírus de smartphone (mensagens MM ou por BT).

# Malwares - Worms

- Programas que alteram softwares instalados
- Propagação: automática
  - Explorando vulnerabilidades
- Em geral consomem muitos recursos
  - Da rede e dos computadores
- Processo
  - Identifica os computadores alvos
  - Envia cópias
  - Ativação (automática ou por ação do usuário)
  - Volta ao primeiro passo...

# Malwares - Trojan

- Programa “legítimo”, inclui “surpresas”
  - Cartões virtuais, jogos, cracks
- Propagação: ação do usuário
- Tipos de Trojans
  - Downloader/Scareware: baixa/exec. códigos maliciosos
  - Dropper: executa códigos maliciosos embutidos.
- Ações comuns dos Trojans
  - Proxy/Backdoor: age como proxy ou abre backdoor
  - Destructor: apaga coisas, formata discos...
  - Ransomware: criptografa os dados dos usuários
  - Clicker: redireciona a navegação do usuário.
  - Bots, Spyware e Rootkits...

# Malwares - Bots

- Programas que permitem controle da máquina
  - Por meio da rede!
  - Computador vira um “zumbi”
  - Pode-se comandar vários: Botnet
- Propagação
  - Worms ou trojans
  - Explorando vulnerabilidades
- Em geral consomem muitos recursos
  - Da rede e dos computadores... Quando ativos!



# Malwares - Spyware

- Programas que permitem monitorar a máquina
  - Envia informação de interesse para terceiros
- Propagação
  - Worms ou trojans
- Tipos comuns
  - Keylogger: captura as teclas pressionadas
  - Screenlogger: captura a tela da aplicação
  - Banker: obter dados bancários
  - Adware: mostrar propagandas

# Malwares - Rootkits

- Programas que alteram o sistema operacional
  - Abrindo diversas brechas de segurança
- Propagação
  - Worms ou trojans
- Características
  - Comprometem severamente a máquina
    - Permitem que o invasor assuma o papel de “root”
  - Muito difíceis de detectar
  - Muito difíceis de remover

# VULNERABILIDADES

# Vulnerabilidades

- O que são?
  - Pontos fracos existentes nos ativos
  - Quando explorados, afetam
    - Integridade, disponibilidade e confidencialidade.

# Vulnerabilidades

- Não seriam um problema se...
  - Não houvesse ameaças que as explorem
  - Mas as ameaças existem!
  - E com a evolução...
    - As vulnerabilidades tendem a aumentar

# MECANISMOS BÁSICOS DE PROTEÇÃO

# Proteção Básica

- Qual é o mínimo que devo fazer?
  - Antivírus
  - Firewall
  - Configuração Segura da Rede
  - Configuração Segura de Software
  - Rotinas de segurança

# Proteção Básica

- Sempre que possível...
  - Soluções gerenciadas remotamente
    - Limite o acesso às máquinas de gestão de segurança.



# Proteção Básica - Antivírus

- O que tem de importante?
  - Use
  - Use sempre
  - Ative a proteção em tempo real
  - Ative a proteção contra scam/phishing
  - Agende checagens semanais
    - No fim de semana, se máquinas ficam ligadas
    - Segunda no início do expediente, se ficam desligadas.
  - Agente atualizações diárias
    - Do antivírus
    - Das definições de ameaças.

# Proteção Básica - Firewall

- O que tem de importante?
  - Use.
  - Use sempre.
  - Feche absolutamente todas as entradas novas
    - Abra apenas aquelas absolutamente necessárias.
  - As portas que precisem ficar abertas...
    - Se possível, abra apenas para os IPs necessários
      - Pelas interfaces necessárias
    - Se possível, use alternativas (como SSH... 22 para xx)
    - Monitore-as (SSHGuard, por exemplo).
  - Conexões negadas: use DROP ao invés de REJECT

# Proteção Básica - Rede

- Preciso fazer algo?
  - Configure o roteador adequadamente
    - IPv4 e IPv6
    - Use VLANs (LANs virtuais) adequadamente.
  - Roteador: há recursos de filtragem?
    - Use!
    - Compartilhamento de Arquivos e Impressoras?.

# Proteção Básica - Rede

- Preciso fazer algo?
  - Se usar IPv4...
    - Dê preferência para alocar IPs locais para as máquinas
    - Disponibilize publicamente apenas portas necessárias.
  - Se usuários precisarem de acesso remoto: VPN

# Proteção Básica - Software

- Preciso fazer algo?
  - Nunca permita que usuário instale software
    - Se necessário, deve solicitar... E software será avaliado.
  - Sempre mantenha a versão mais atualizada
    - Em especial de softwares que abrem portas na rede.

# Proteção Básica - Software

- Preciso fazer algo?
  - Sempre verifique e configure muito bem
    - A maior parte das “falhas” são configurações ruins.
  - Se possível, use um servidor proxy web (squid etc.)
    - Bloqueie o acesso a sites indesejados
    - Alternativa: liberar apenas os sites “úteis”: cuidado!.

# Proteção Básica - Rotinas

- O que é “rotina de segurança”?
  - Verificação e rotação de logs
    - Sistema, falhas de login, aplicações....
  - Verifique tráfego, CPU, espaço livre etc.
    - Se possível, use um monitor (Zabbix, Nagios...).
  - Cuidar da política de senhas
  - Verificar a execução dos backups
    - Se possível, verificar a restauração dos mesmos.