Cibersegurança aplicado a Industria 4.0

12/08/2024

INDT - Instituto de Desenvolvimento Tecnológico

Apresentação

Wanderlyn Raposo

- **Especialista em Redes no INDT**
- Formado em **Tecnólogo de Redes de Computadores**,
- Pós-graduado em **Gestão do ensino Médio, técnico e Superior.**
- Certificações **MTCRE**, **CCNP R&S** é **CCNA Security**, **CCNA Cyber Ops, Instrutor da academia CISCO**
- Mais de 15 anos de experiência na área de telecomunicação e datacenter.

O que é Indústria 4.0

- **Automatização Inteligente:** A Indústria 4.0 representa a automação avançada, com máquinas e sistemas que podem tomar decisões e se adaptar de forma autônoma.

- **Conectividade Total:** A interconexão de dispositivos e sistemas, juntamente com o uso de Internet das Coisas (IoT), permite o compartilhamento de dados em tempo real em toda a cadeia de produção.

- **Transformação Digital:** A Indústria 4.0 impulsiona a transformação digital, otimizando processos, reduzindo custos e melhorando a eficiência em setores industriais.

Internet das Coisas

- **Conexão Onipresente:** O IoT é uma rede de dispositivos interconectados que coletam e compartilham dados pela internet, permitindo uma ampla gama de aplicações em tempo real.

- **Sensores e Dispositivos Inteligentes:** Sensores e dispositivos inteligentes coletam informações do ambiente físico, como temperatura, umidade, localização e muito mais, tornando-o acessível e controlável remotamente.

- **Impacto nas Indústrias:** O IoT está transformando setores como saúde, agricultura, manufatura e logística, oferecendo insights avançados, automação e eficiência operacional.

Ataques em ambientes IoT

Ataque Stuxnet (2010):

- **Tipo**: Ataque de computador altamente sofisticado.
- **Alvo**: Usinas nucleares no Irã, em particular a usina de Natanz.
- **Detalhes**: Stuxnet foi um worm de computador que visava sistemas de controle industrial (SCADA) e foi projetado para sabotar as centrífugas de enriquecimento de urânio. Foi o primeiro ataque cibernético conhecido que causou danos físicos a instalações industriais.

Ataque WannaCry (2017):

- **Tipo:** Ransomware.
- **Alvo:** Empresas e organizações em todo o mundo, incluindo hospitais e sistemas de saúde.
- **Detalhes:** WannaCry se espalhou rapidamente por meio de vulnerabilidades em sistemas Windows desatualizados. Afetou serviços críticos, incluindo hospitais, devido à sua capacidade de criptografar dados e exigir resgates em troca da chave de descriptografia

Ataques em ambientes IoT

Ataque Mirai (2016):

- **Tipo:** Botnet IoT.
- **Alvo:** Dispositivos de Internet das Coisas (IoT), como câmeras IP e roteadores.
- **Detalhes:** O ataque Mirai usou dispositivos IoT comprometidos para criar uma botnet massiva que realizava ataques de negação de serviço distribuídos (DDoS). Esses ataques congestionaram sites e serviços populares, causando interrupções em larga escala.

Segurança da Informação

- **Conjunto** de **práticas** com o objetivo de **garantir** a **Segurança** dos dados corporativos

- Segurança da Informação **também** pode ser **aplicada** a **dados individuais**

Pilares


SEGURANÇA
DA
INFORMAÇÃO
CONFIDENCIALIDADE
INTEGRIDADE
DISPONIBILIDADE

Vulnerabilidades em SI

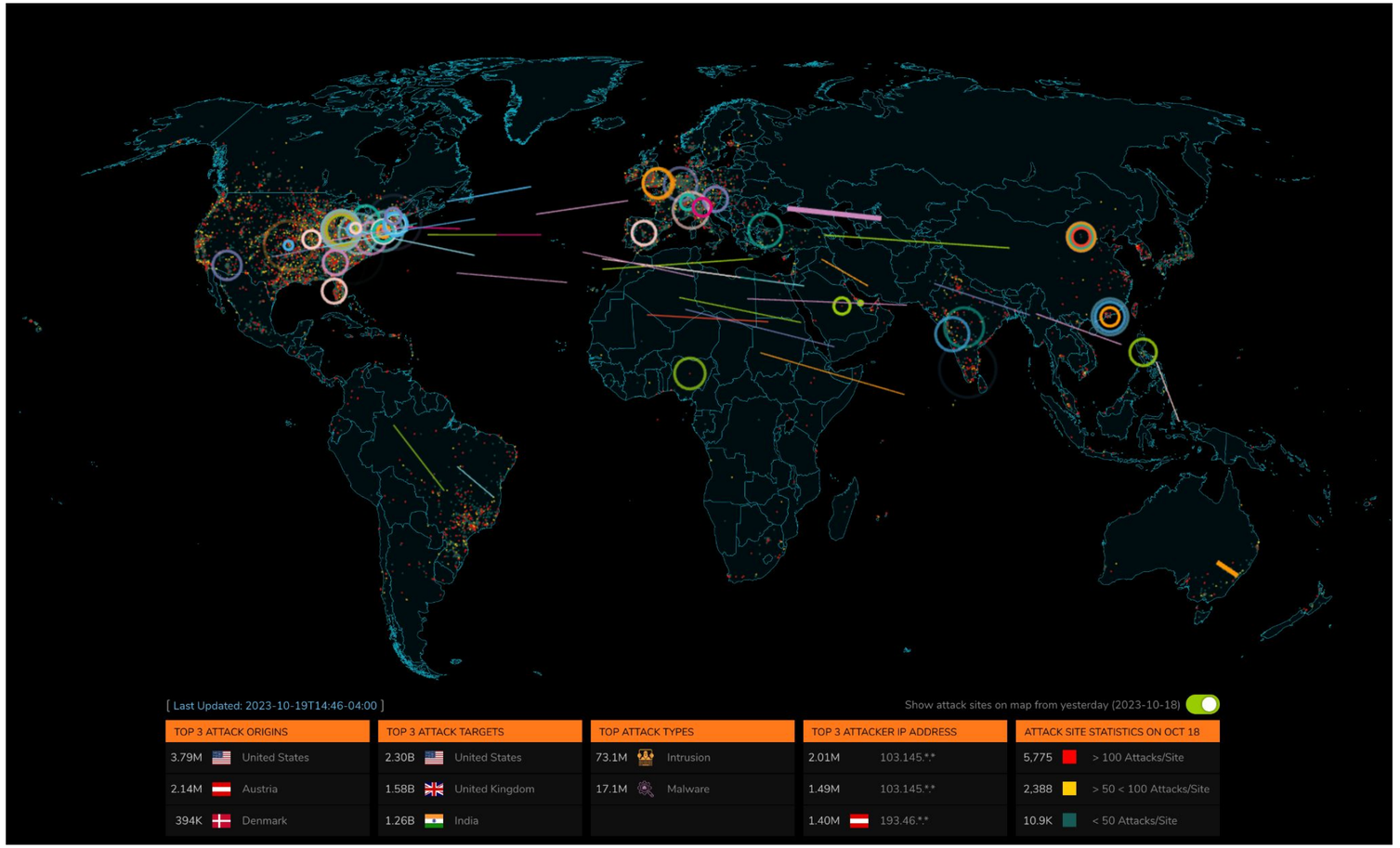
- **Fraqueza** ou **falha** que pode ser **explorada** por um atacante, comprometendo a **disponibilidade**, **integridade** e **confidencialidade** dos dados

- **Vulnerabilidades** podem ser geradas de forma **intencional** ou **não intencional**

Ataque cibernético

- **Ação** que visa **afetar** algum dos **pilares** da **segurança** da informação

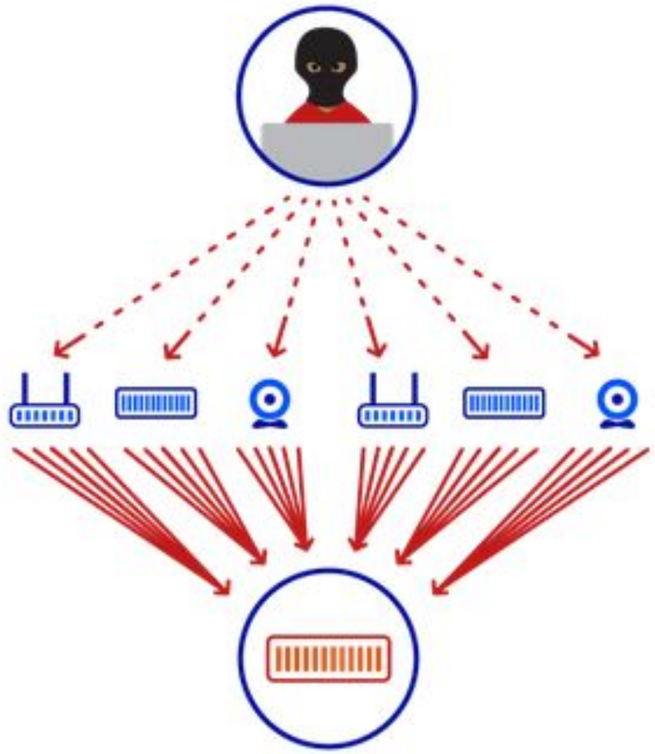
- Pode ter origem **criminosa** ou **não criminosa**



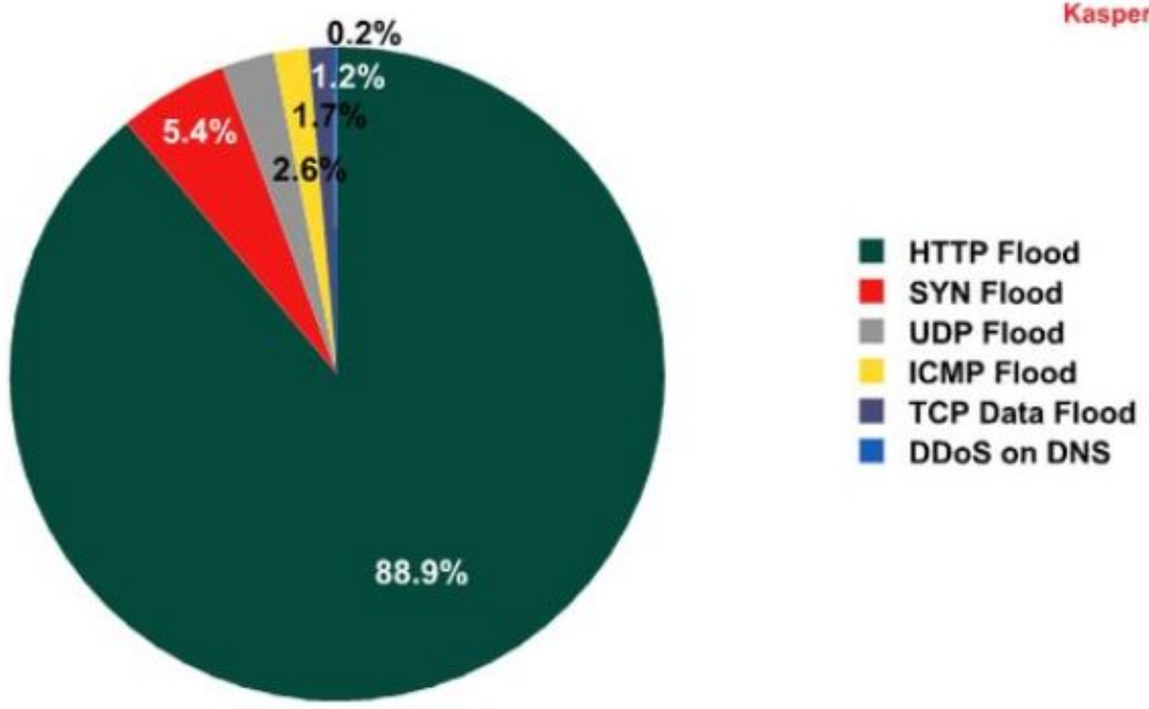
Fonte: Mapa ciberataques (SonicWall)

Negação de serviço distribuído (DDoS)

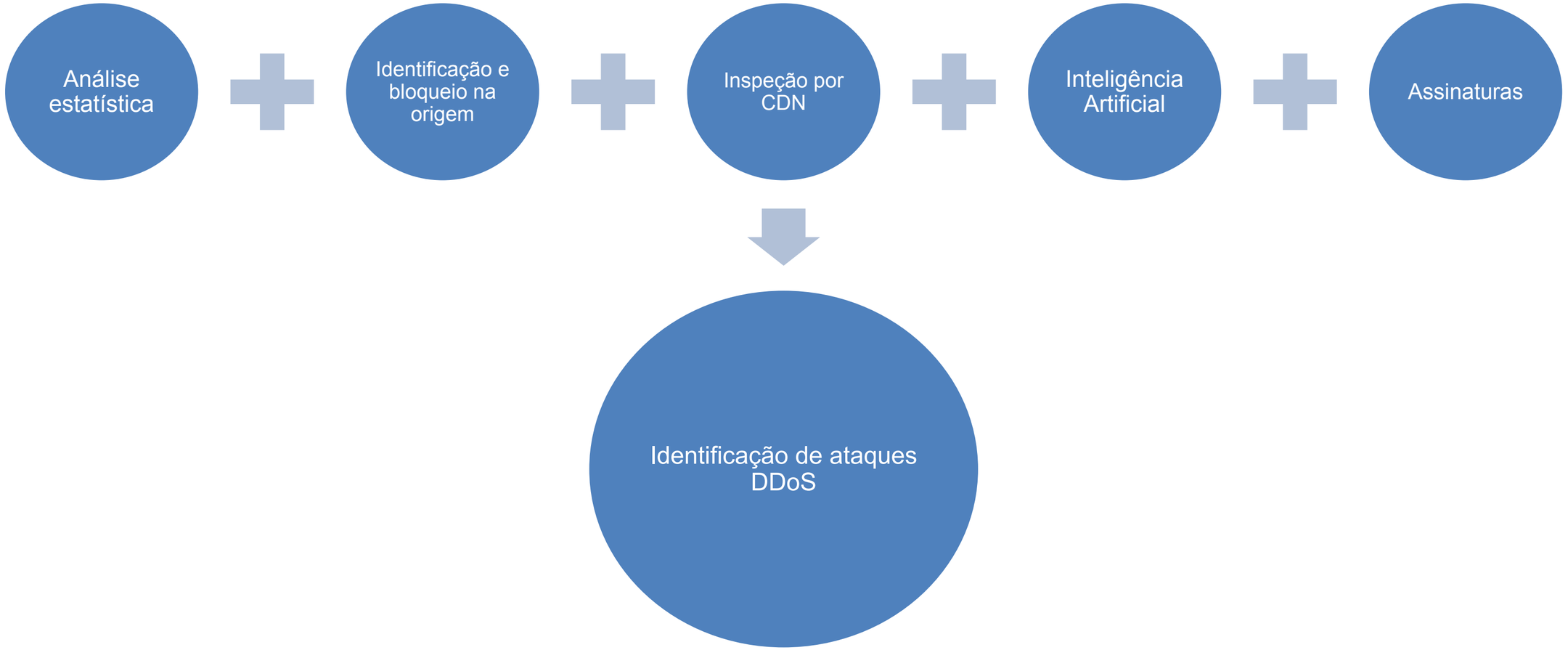
- **DDoS** ocorre com o uso de **dispositivos** finais e elementos de Infraestrutura **infectados** disparam pacotes ou abrem conexões **simultâneas** para **esgotar** a **capacidade** do site.



Tipos de ataques DDoS



Como mitigar ataques DDoS

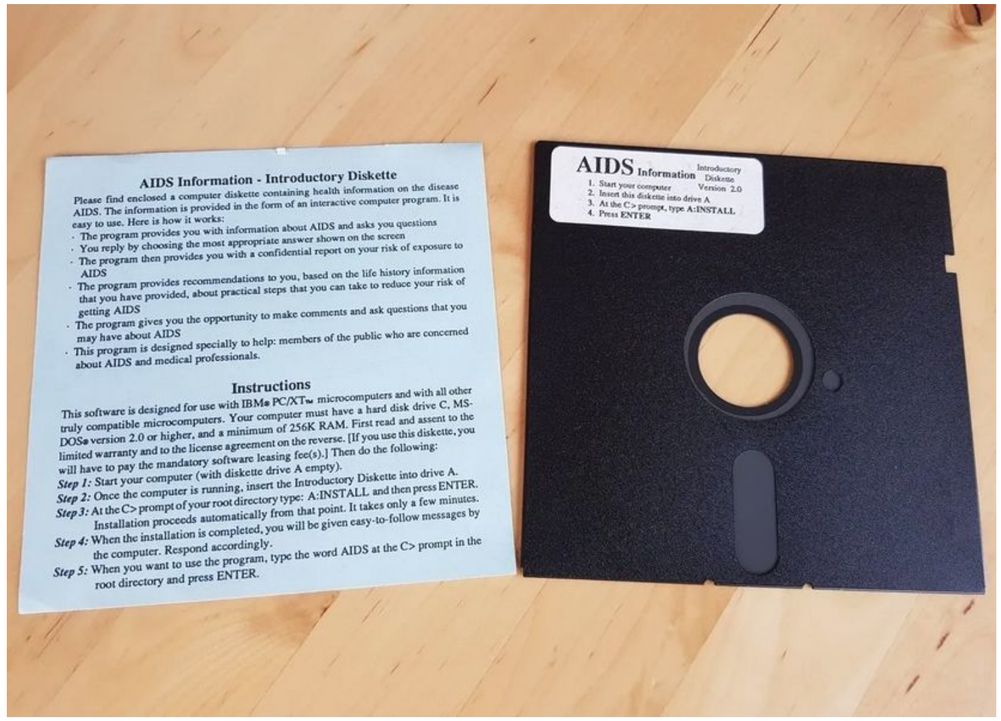


Ransomware

- **Ataque** que **promove** o **sequestro** de **dados** de pessoas ou grandes corporações.
- Atacante **invade** computadores locais, geralmente após **erros** de **usuários**, procurando **servidores** para **Infectar**.

Primeiro Ransomware

- Feito por **Joseph Popp**, PHD em Biologia
- Foram enviados **2000 disquetes infectados** para pesquisadores no **mundo** todo
- O **ransomware** modificar o nome de pastas, **impedindo** a **inicialização**

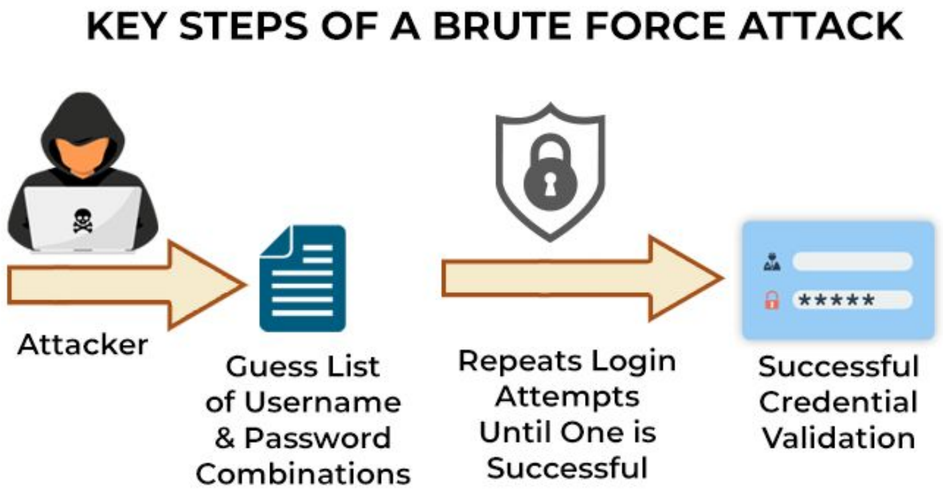


Contra medidas

- Faça **backup** regularmente
- **Restringir** direitos de administrador
- **Filtre** o tráfego da **web**
- **Eduque**-se e sua **equipe**
- Atualize políticas de senha
- Tenha um **plano** de resposta a incidentes
- Uso de Antivirus

Ataques de força Bruta

- **Scripts** realizam a descoberta de senhas por **tentativa** e **erro**
- Ocorre pelo uso de **senhas fáceis**
- Ferramentas de **inteligência artificial** estão sendo utilizadas para facilitar a **quebra de senhas**
- PassGAN quebra senhas fáceis em até 1 minuto



https://github.com/brannondorsey/PassGAN

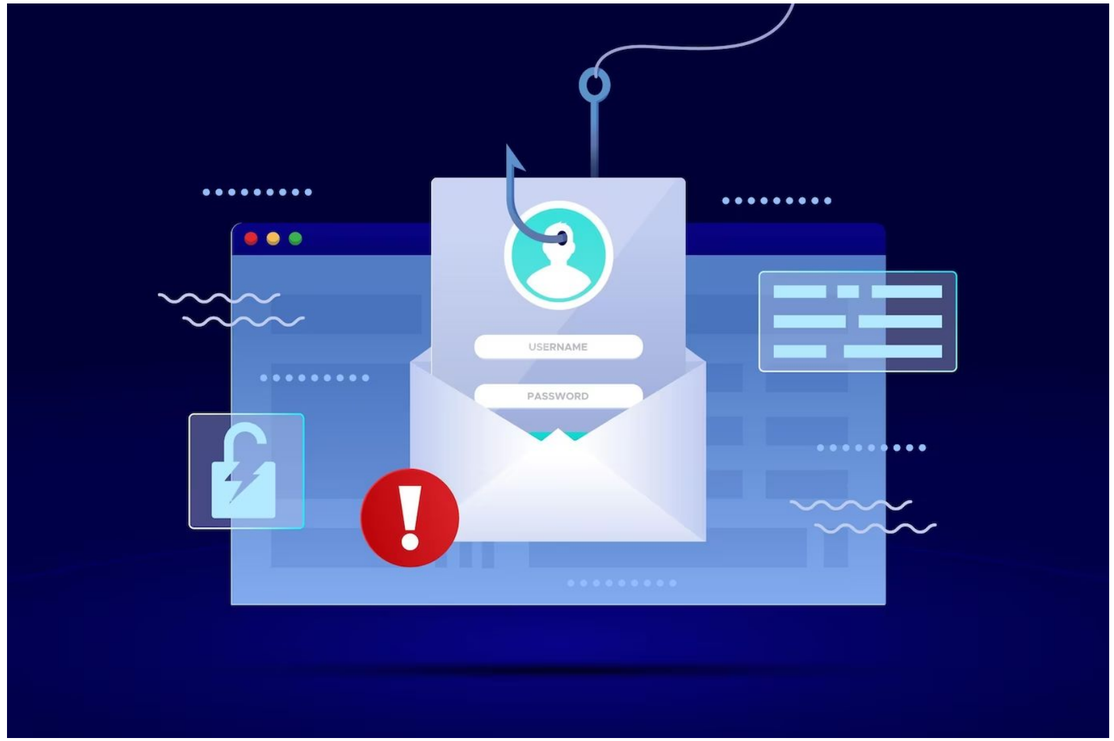
Fonte: SpiceWorks

Contra medidas

- Uso de **senhas fortes**, com caracteres especiais
- Sistemas com **captcha**
- Plataformas com número reduzido de tentativas de login por segundo

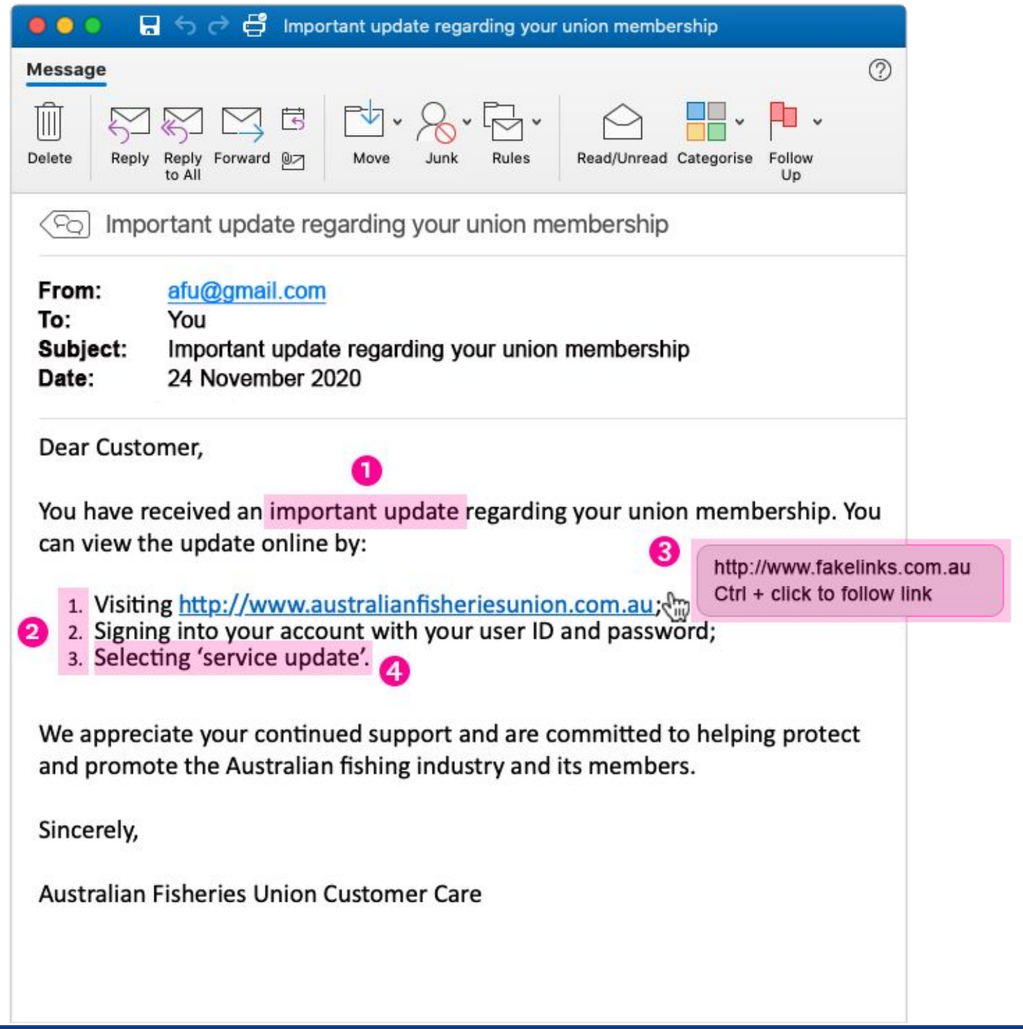
Ataque de Phishing

- Ocorre quando um **invasor** entra em **contato** com você **fingindo** ser alguém que **você conhece** ou uma **organização** que você **confia** e tenta fazer você **fornecer informações** pessoais ou **abrir** um **site** ou **arquivo mal-intencionado**.



Ataque de Phishing

- Um dos **principais vetores** de **ameaça** a Segurança
- **62%** das **ameaças** de Segurança tiveram **êxito** através de phishings bem sucedidos (Verizon)
- **Brasil** foi o país que **mais** recebeu **ataques** de **phishing** em 2022 (starista)



Tipos de Phishing

Como se proteger

- Uso de **antivírus** em PCs
- Uso de proxys **monitorando** conexões realizadas;
- **Treinamento** frequente para **funcionários** identificarem estes **ataques**
- **Utilização** de sistemas de **Spam**;

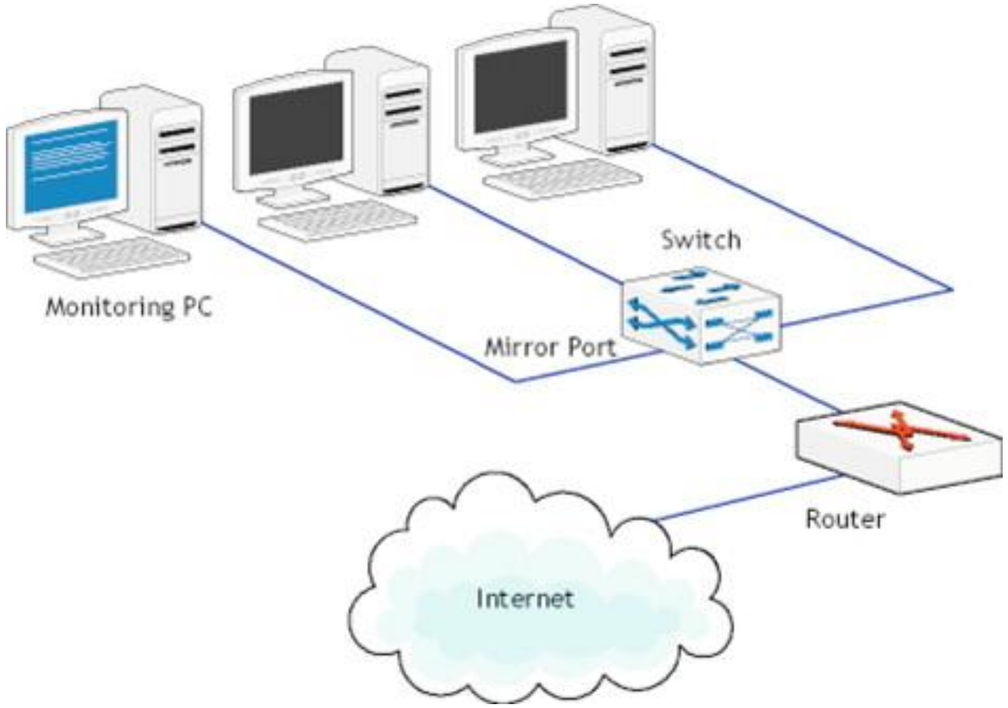
Vulnerabilidades - PortScan

- Nmap (**Scripts**) e OpenVas
- Mitre
- Common Vulnerabilities and Exposures (**CVE**)
- Serviços com software **desatualizado** podem ser **porta de entrada** para **atacantes**
- **Software** configurado **incorretamente** pode ser alvo de **ataques**

```
25/tcp   open  smtp         Microsoft ESMTP 5.0.2195.7035
80/tcp   open  http         Microsoft IIS httpd 5.0
|_http-server-header: Microsoft-IIS/5.0
| vulners:
|   cpe:/a:microsoft:iis:5.0:
|       CVE-2009-3023   9.3     https://vulners.com/cve/CVE-2009-3023
|       CVE-2008-1446   9.0     https://vulners.com/cve/CVE-2008-1446
|       CVE-2009-1535   7.6     https://vulners.com/cve/CVE-2009-1535
|       CVE-2009-1122   7.6     https://vulners.com/cve/CVE-2009-1122
|       CVE-2011-5279   6.4     https://vulners.com/cve/CVE-2011-5279
|       CVE-2009-4444   6.0     https://vulners.com/cve/CVE-2009-4444
|_      CVE-2009-2521   2.6     https://vulners.com/cve/CVE-2009-2521
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn  Microsoft Windows netbios-ssn
443/tcp  open  https?
445/tcp  open  microsoft-ds Microsoft Windows XP microsoft-ds
515/tcp  open  printer      Microsoft lpd
```

Vulnerabilidades - Sniffing

- **Tráfego** de usuários é **espelhado** para porta de um **atacante**.
- Tráfego **não criptografado** é varrido a **procura** de **senhas** e outras i**nformações valiosas**.
- **Atacante** pode obter o **fingerprint** do usuário a partir dos **metadados** de **navegação**.



Como se proteger

- Atenção aos **softwares** instalados
- Uso de **senhas fortes**
- **Atualizações** frequentes do Sistema operacional
- Proteção física do equipamento
- **Firewalls** e camadas de comunicações bem **configurados**

SOC

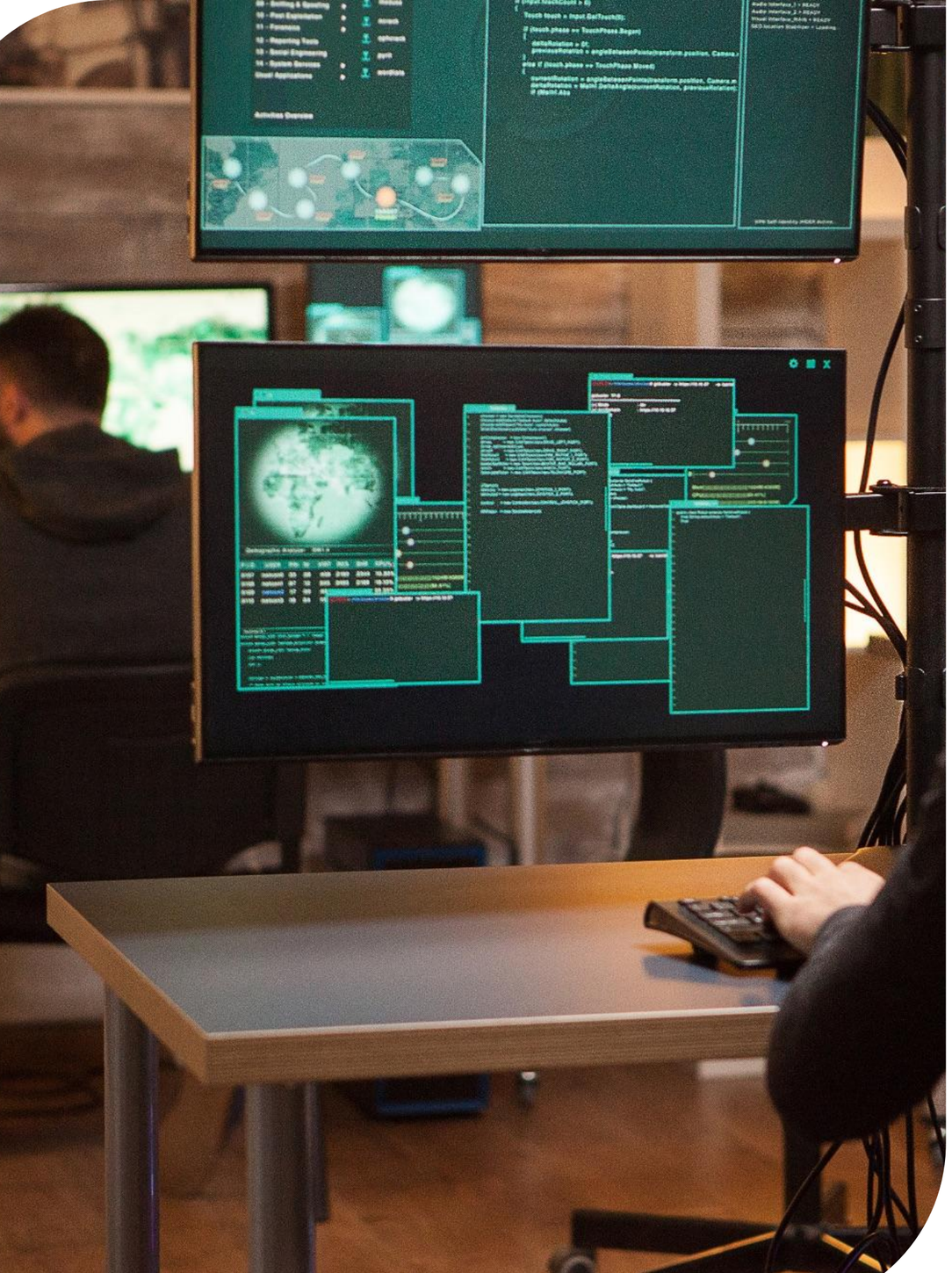
Laboratório de Segurança Cibernética

Cenário Atual INDT

NOC – Monitoramento de rede e serviços alocados no INDT.

Data Center moderno com a tecnologia de hiper convergência, adequado para desenvolvimento de projetos e sistemas preditivos de segurança.

Oferecemos cursos e treinamentos voltados para Pentests e Desenvolvimento Seguro de aplicações (SSDLC)



Serviços

Site Survey - Mapeamento e análise de riscos, construção de plano de segurança cibernética e simulação de ciberataques para empresas e indústrias

Monitoração proativa de elementos de rede, garantindo que os serviços operam em alta disponibilidade e com desempenho dentro de padrões contratados (NOC)

Monitoração proativa de segurança da infraestrutura do cliente, monitorando possíveis ataques e identificando possíveis vulnerabilidades (SNOC)

Serviços

Consultoria e elaboração de projetos para instalação e gerenciamento de dispositivo IoT (assistentes virtuais, câmeras e outros)

Análise de vulnerabilidades em redes identificando falhas de segurança em servidores e equipamentos de redes

Elaboração de projetos para realizar as correções das falhas de segurança

Contato

Wanderlyn Raposo
wanderlyn.raposo@indt.org.br

Mateus Azevedo
matheus.azevedo@indt.org.br

Luana Lobão
luana.lobão@indt.org.br


INDT
INSTITUTO DE DESENVOLVIMENTO
TECNOLÓGICO