# A Invasão Oculta: Ransomware e Resiliência Cibernética

Desvendando um Caso Fictício de Ataque Cibernético em uma Empresa Europeia.

# Agenda

01

## Introdução ao Cenário

O contexto da empresa e as vulnerabilidades pré-existentes.

02

## A Linha do Tempo do Ataque e Motivação

Detalhes das etapas e técnicas empregadas pelos invasores.

03

## As Falhas Críticas

Análise das brechas que permitem a invasão.

04

## Lições Aprendidas

Recomendações e estratégias para fortalecer a segurança.

# Cenário da Vítima: Vulnerabilidades Expostas

A empresa europeia, de porte médio, operava com uma infraestrutura de TI que, embora funcional, possuía pontos cegos críticos. A cultura de segurança interna era incipiente, priorizando a conveniência sobre a proteção.

- **Exposição de informações de funcionários em redes sociais.**
- **Acesso a sites externos não confiáveis.**
- **Falta de segmentação de rede.**
- **Dispositivos IoT inseguros, como termostatos conectados.**

# Fase 1: Reconhecimento e Acesso Inicial

### OSINT: Coleta de Dados

O atacante iniciou com OSINT, utilizando informações de funcionários e da empresa disponíveis publicamente para traçar perfis e identificar alvos vulneráveis. Dados de redes sociais foram cruciais.

### Injeção de I-frame Malicioso

Um site legítimo, mas com falhas de segurança, foi comprometido com a injeção de um i-frame malicioso. Este serviu como vetor para a próxima fase do ataque.

### Infecção de Funcionário

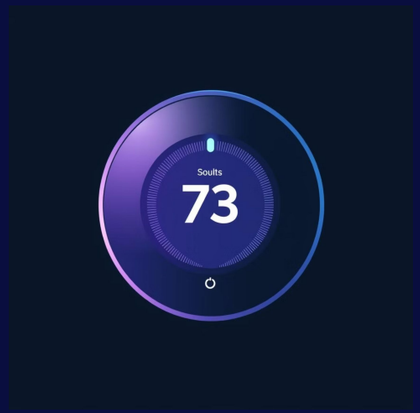
Um funcionário, ao acessar o site comprometido, teve seu computador infectado. Esta foi a porta de entrada inicial para a rede corporativa.

# Fase 2: Movimento Lateral e Persistência

## Exploração da Rede Interna

Com acesso ao computador do funcionário, o atacante explorou a falta de segmentação da rede, movendo-se lateralmente entre os sistemas. O objetivo era mapear a infraestrutura e escalar privilégios.

## A Surpresa: IoT como Esconderijo




Para garantir persistência, o invasor utilizou um termostato conectado (IoT) como um ponto de acesso usando a senha padrão . Dispositivos IoT, frequentemente esquecidos na estratégia de segurança, provaram ser um elo fraco e um excelente local para ocultar-se.

## Motivação

A motivação principal do ataque foi a ganância dos invasores, que buscavam explorar vulnerabilidades para obter lucro

# Fase 3: O Ataque Final – Ransomware

### Criptografia Massiva

Uma vez com controle suficiente e persistência garantida, o ransomware foi ativado. Ele criptografou dados críticos em toda a rede da empresa, paralisando as operações.

### Exclusão de Backups

Para intensificar a pressão e dificultar a recuperação, o invasor também buscou e excluiu os backups online e de rede, comprometendo a capacidade de restauração da empresa.

### A Exigência do Resgate

A tela dos computadores exibia uma mensagem: 75 Bitcoins, equivalente a milhões de Euros, para a descriptografia dos dados. A motivação era puramente financeira.

# As Falhas Críticas que Possibilitaram a Invasão

### Gestão de Vulnerabilidades Ineficaz

Falta de escaneamento regular e correção de brechas, tanto em sistemas tradicionais quanto em dispositivos IoT.

### Conscientização de Segurança Baixa

Funcionários não treinados para identificar e reportar ameaças como phishing ou sites comprometidos.

### Arquitetura de Rede Fragilizada

Ausência de segmentação de rede permitiu o movimento lateral irrestrito após o acesso inicial.

### Estratégia de Backup Deficiente

Backups não isolados ou imutáveis, tornando-os vulneráveis à exclusão pelos atacantes.

# Lições Aprendidas: Fortalecendo a Resiliência Cibernética

**Segurança 360°**

Implementar uma estratégia de segurança holística, que contemple desde a educação do usuário até a proteção de dispositivos IoT e segmentação de rede.

**Treinamento Continuo**

Capacitar funcionários para serem a primeira linha de defesa, reconhecendo e evitando ameaças comuns como engenharia social.

**Testes de Penetração e Varreduras**

Realizar pentests e varreduras de vulnerabilidades regularmente para identificar e corrigir falhas antes dos atacantes.

# Lições Aprendidas: Fortalecendo a Resiliência Cibernética

### Segmentação de Rede

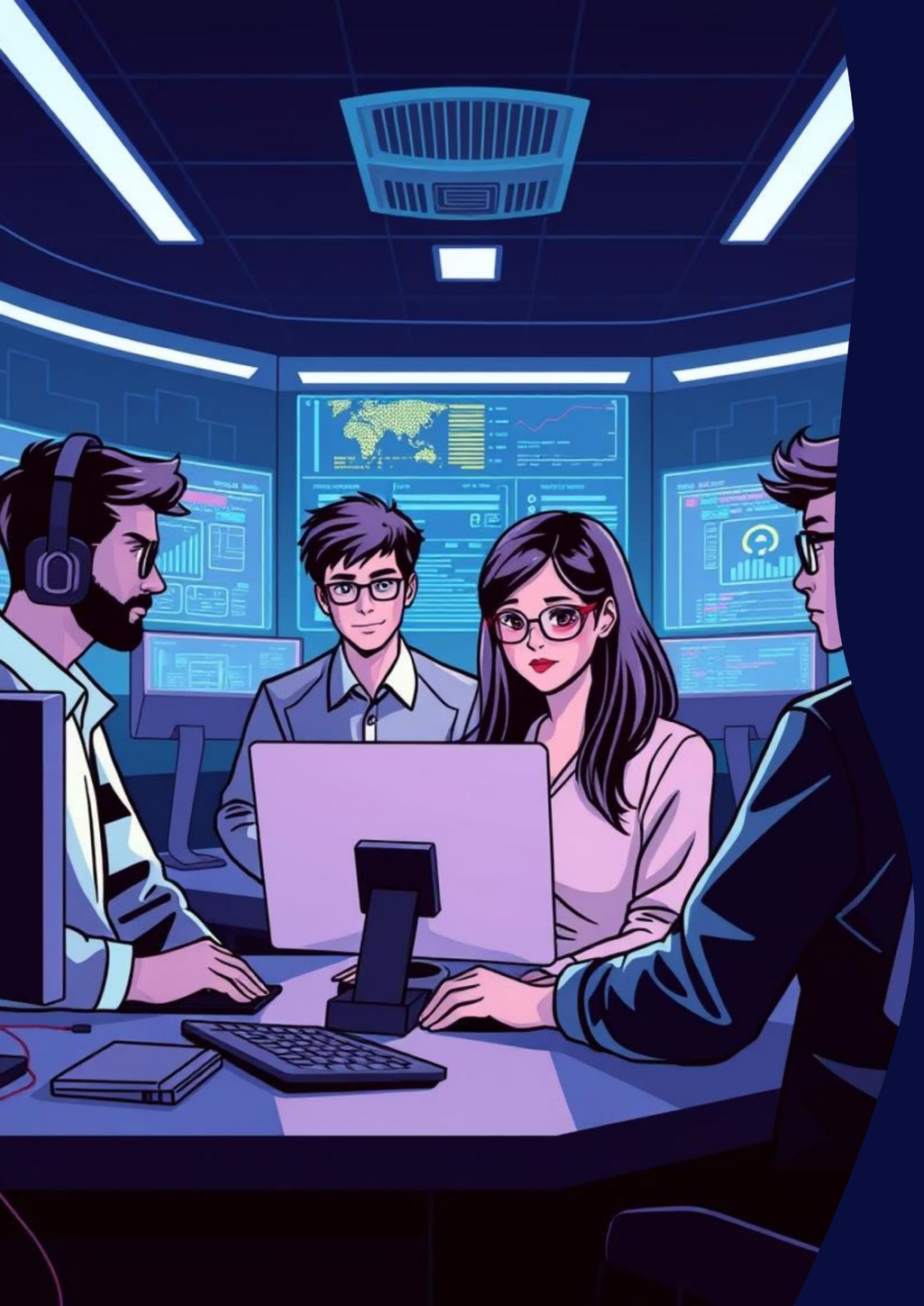
Dividir a rede em zonas isoladas minimiza o impacto de um acesso inicial, contendo o movimento lateral dos atacantes.

### Backups Imutáveis e Off-site

Garantir que os backups sejam protegidos contra exclusão e mantidos em locais seguros e desconectados da rede principal.

### Plano de Resposta a Incidentes

Ter um plano claro e testado para reagir rapidamente a incidentes, minimizando danos e acelerando a recuperação.



Bruno de Oliveira Santos - 8232235123

Guilherme Dourado Nascimento - 825116419

Felipe Pereira do Nascimento - 825126069

Kauane Sandes Brandão - 825113309

Stephanny Ramos Rodrigues -825123391

Pedro Miranda Rabelo - 825243591