Prime

CCS-A

Mais sobre Vulnerabilidades

Gerenciamento de Patches
Fraco ou Inadequado

- **Patches**
  - Hackers podem fazer engenharia reversa.
- **Gerenciamento de Patches:**
  - Programa forte que abranja todos os sistemas e softwares.
- **Gerenciamento de Patches fraco**
  - Convite aberto para explorar vulnerabilidades.
  - É preciso controlar os processos.
  - É preciso definir a periodicidade da instalação dos patches.
  - É preciso determinar a necessidade de cada patch.

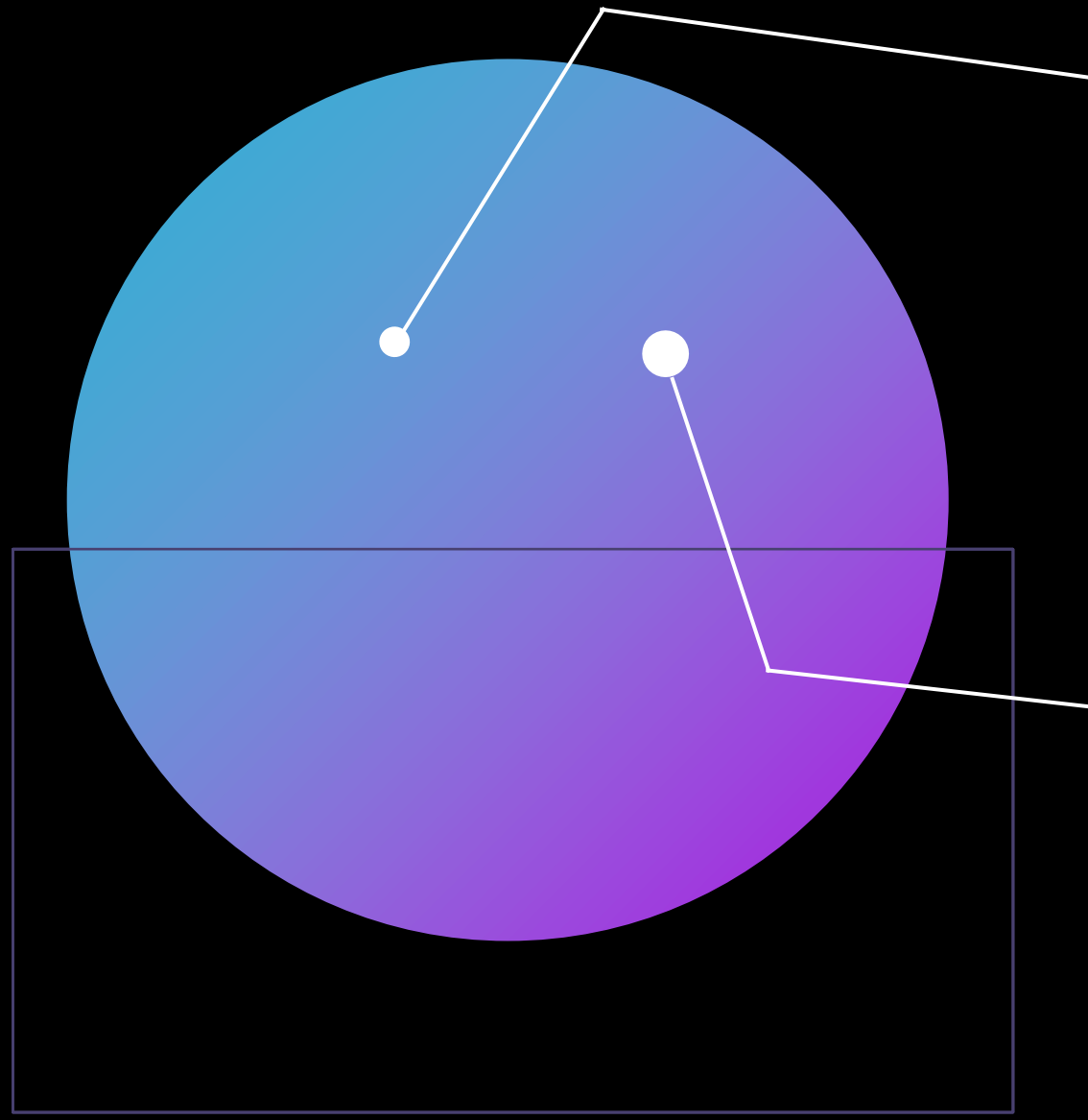
MAIS SOBRE VULNERABILIDADES

Firmware

- Outra forma de software.
  - Armazenado em hardware;
  - Possui as vulnerabilidades de um software.
- Sobre o firmware, é importante se perguntar sobre:
  - Como é atualizado?
  - Qual frequência da atualização?
  - Como a distribuição das atualizações?

Responsável:

Sua organização! Mesmo para servidores, roteadores, switch etc.



MAIS SOBRE VULNERABILIDADES

Sistema Operacional (SO)

- Antigamente era uma tarefa difícil.

Exigia intervenção manual.

- Passos importantes:
  - Política eficiente de gerenciamento de patches;
  - Correção de tudo através da política;
  - Rastreamento dos patches;
  - Acompanhamento da política.
- O hacker vai te fazer um “favor” verificando a aplicação do patch e testar a correção do seu SO.

Aplicativos

- Demonstram como uma empresa “funciona”.
  - Aplicativos nos servidores web;
  - Aplicativos nos servidores de banco de dados;
  - Aplicativos nos desktops.

Desafio:
Rastrear todos os aplicativos usados.

- Responsabilidades do profissional de segurança:
  - Acompanhamento das CVEs;
  - Atualização e correção de sistemas, além do firmware, SO, virtual machine, dispositivos etc.

Sistemas Legados

- Termo usado para descrever sistemas que não são mais suportados ou comercializados.

Considerados antigos;

Representam um problema caso sejam descobertos;

Não podem ser corrigidos.

- Ação para correção parcial:
  - Controles de compensação (extintores);
  - Separar física e logicamente a rede.

MAIS SOBRE VULNERABILIDADES

Consequências da Vulnerabilidade

- Perda de dados;
- Violação de dados;
- Exfiltração de dados;
- Roubo de Identidade;
- Perda financeira;
- Perda de reputação;
- Perda de disponibilidade.

MAIS SOBRE VULNERABILIDADES

Perda de Dados

- Perda de dados = perda de informações.
- Arquivos podem ser:
  -  Excluídos;
  -  Substituídos;
  -  Extraviados.
- Forma mais perigosa: Ransomware.

Violações de Dados

- Obter acesso não autorizado a dados confidenciais;
- Invasores se infiltram em um sistema para roubar:
  - Informações de identificação pessoal (PII);
  - Dados financeiros;
  - Dados corporativos;
  - Propriedade intelectual.
- Como diminuir o impacto:
  - Controle de acesso;
  - Criptografia;
  - Prevenção contra perda de dados (DLP).

MAIS SOBRE VULNERABILIDADES

Exfiltração de Dados

- O que é exfiltração?

Exportar dados roubados de um dispositivo para outro.
(Extrusão, exportação ou roubo de dados).
É uma forma de violação de segurança quando há cópia.

O termo exfiltração é único, pois em um roubo (cópia), os dados originais não são afetados.

Desafio:
O verdadeiro roubo só ocorre quando os invasores escapam com o item.

- Possíveis perdas:

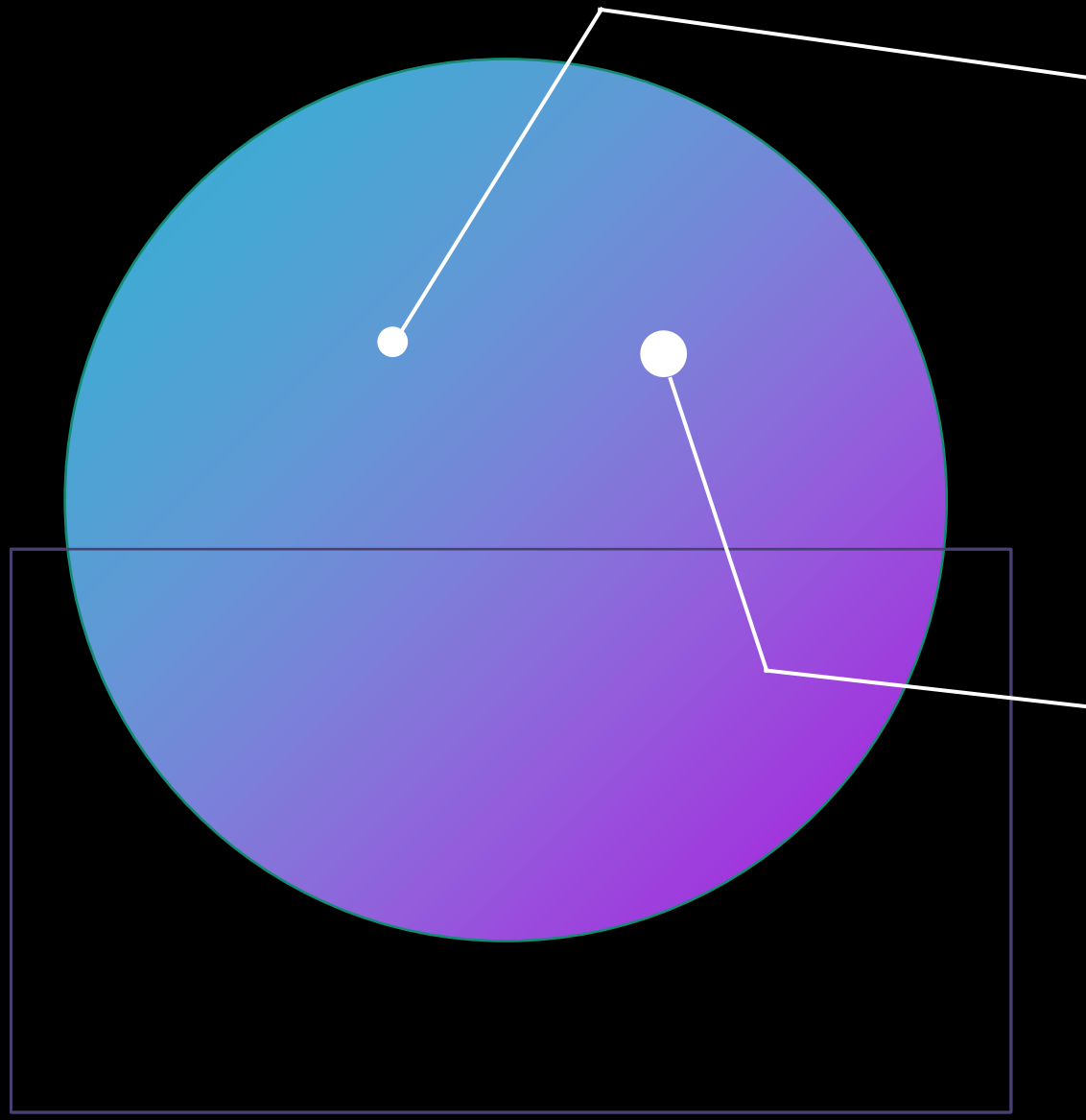
Propriedade intelectual;

Perda de dados.

MAIS SOBRE VULNERABILIDADES

Roubo de Identidade

- Crime em que alguém usa informações para se passar por outra pessoa.
- Impactos:
  - Perda de dinheiro;
  - Perda de propriedade;
  - Perda de tempo.
  - Exfiltração de dados que inclui informações de identificação pessoal.
- Problema maior para empresas menores.



MAIS SOBRE VULNERABILIDADES

Financeiro

- O risco é medido em termos de perdas financeiras para reparo.
- Itens que contribuem para os custos de um ataque:

Investigação e correção dos sistemas;

Tempo de inatividade do sistema;

Descumprimento regulatório das leis de privacidade;

Pagamento de advogados;

Pagamentos de resgate;

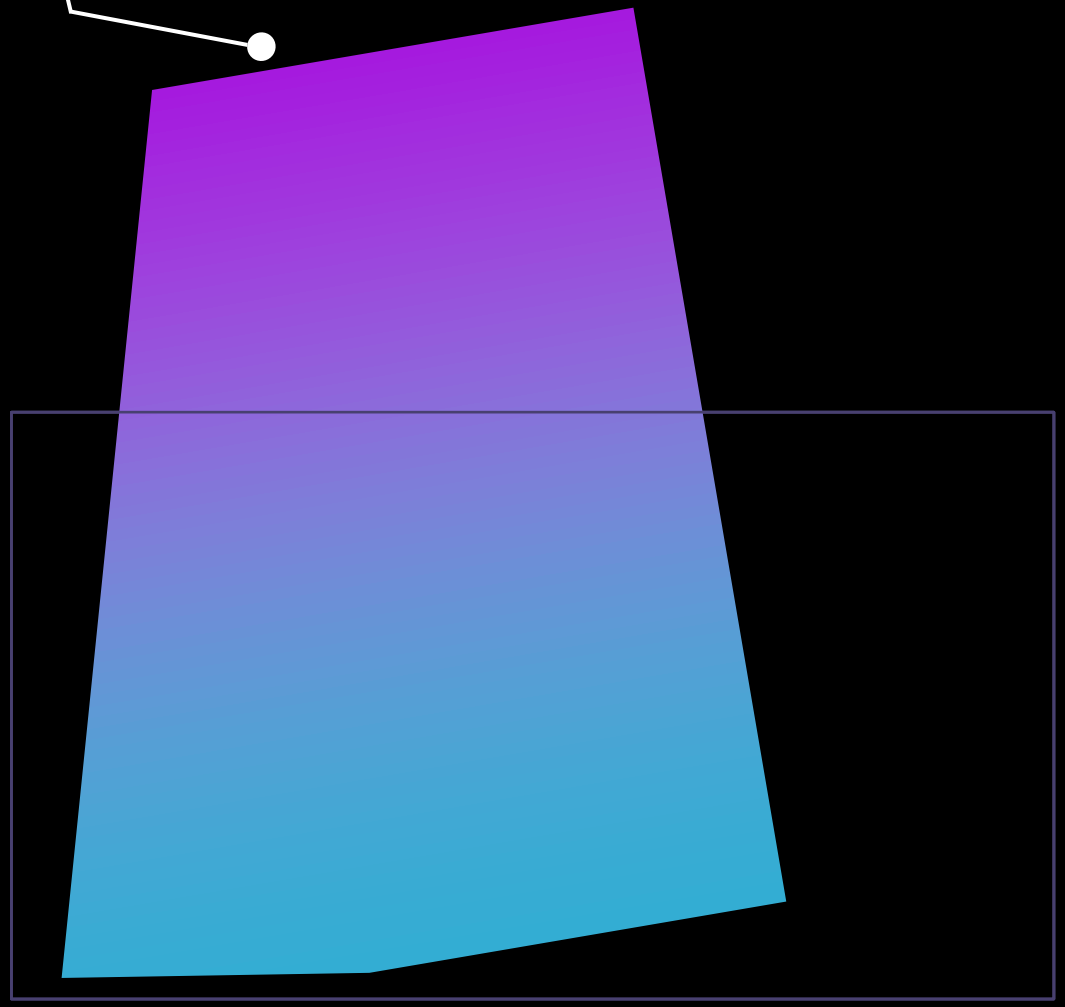
Perdas por conta da propriedade intelectual que foi roubada;

Queda de ações.

MAIS SOBRE VULNERABILIDADES

Reputação

- Impacto na reputação:
  - Perda de confiança do cliente;
  - Perda competitiva de funcionários;
  - Clientes podem procurar outra empresa.
- É preciso pensar nesses impactos para não perder mão-de-obra qualificada.



Perda de Disponibilidade

- Tríade C-I-D:

- Tempo de inatividade = Queda de receita.
  - Os investimentos em recursos são para que o sistema funcione não para consertá-los.

MAIS SOBRE VULNERABILIDADES

OBRIGADO!

MAIS SOBRE
VULNERABILIDADES