Prime

CCS-A

Explorando Vulnerabilidades

Porque existe Vulnerabilidade?

Sistemas corporativos são compostos por diversas partes.

Vários elementos podem ser menos que perfeitos.

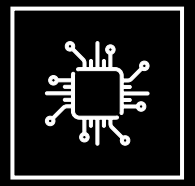
Quase tudo terá fraquezas ou vulnerabilidades.

Compreender onde existem essas fraquezas e vulnerabilidades é fundamental.

Razões para Vulnerabilidades

Sistemas em fim de vida útil:

Um sistema EOL atingiu o fim de sua utilidade ou lucratividade.



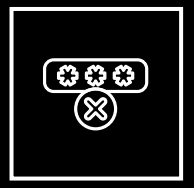
Sistemas embarcados:

Pequeno sistema com hardware mínimo e é incorporado em um dispositivo ou sistema maior para executar funções específicas.

Falta de suporte do fornecedor:

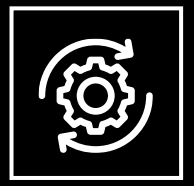
Usar um produto que o fornecedor não oferece mais suporte. Vulnerabilidades que não estão mais sendo corrigidas.

Tipos de Vulnerabilidades



Manipulação de entrada inadequada;

Configuração incorreta/configuração fraca;



Configuração padrão;

Use o OSINT para descobrir as vulnerabilidades conhecidas em produtos.

Vulnerabilidades Baseadas em Nuvem vs. Locais

- Vulnerabilidades existem independente se local ou na nuvem.

Se local, a empresa tem acesso irrestrito à sua infraestrutura.

Se na nuvem, não há visibilidade das vulnerabilidades por parte do cliente.

- A equação “fecha”, pois enxergam-se vantagens na nuvem, como escalabilidade e custos.
- Não importa onde os dados sejam armazenados: sempre haverá vulnerabilidades em potencial.

Dia Zero

Termo usado para vulnerabilidades recém-descobertas e ainda não tratadas.

Da descoberta até a correção ou patch, a vulnerabilidade recebe o nome de **dia zero.**

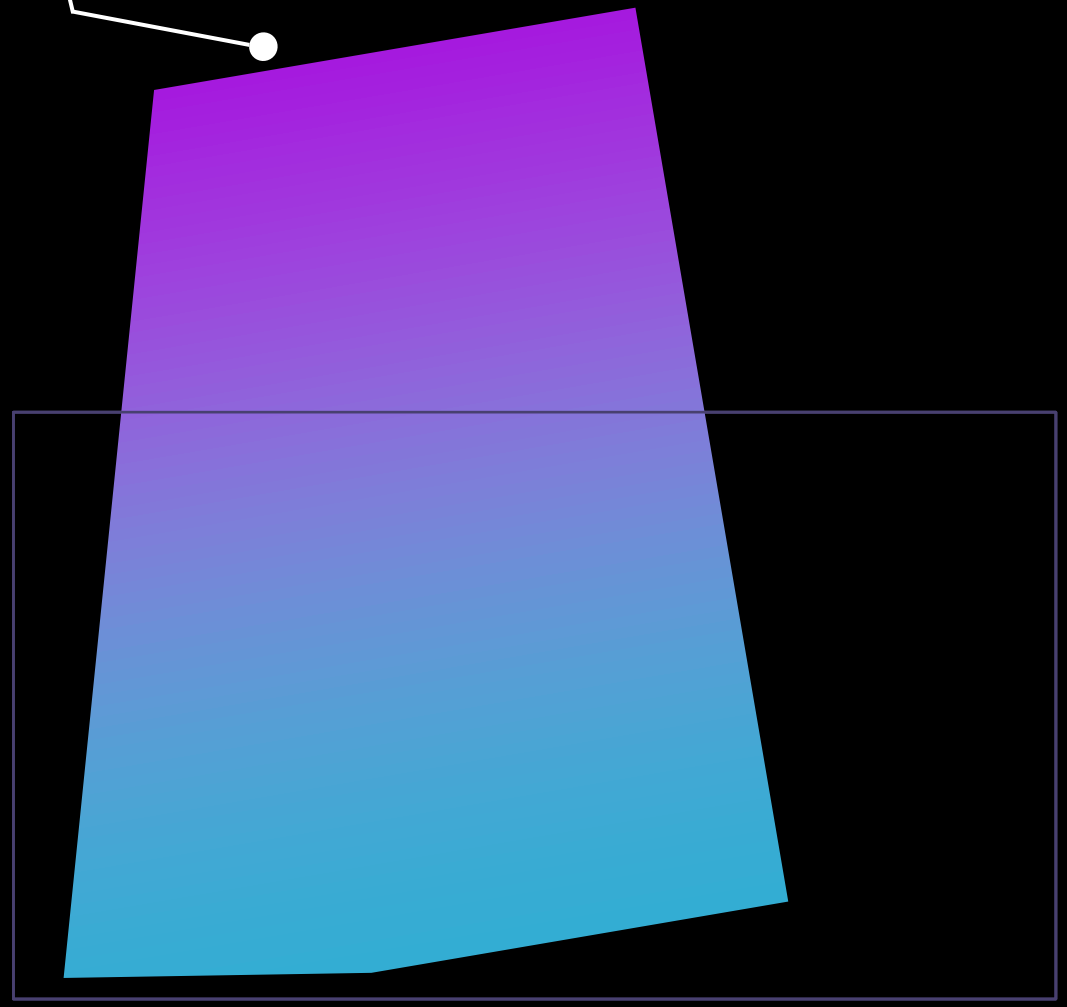
Pesquisadores e desenvolvedores precisam compartilhar informações.

Vulnerabilidades desconhecida pelo fabricante que criou o software.

Configurações Fracas

Um sistema com configuração fraca sofre com problemas de segurança ou desempenho.

- Meio para um invasor obter acesso ou avançar seu nível de privilégio.
- Exemplos:
  - Permissões Abertas;
  - Contas Root Não Seguras;
  - Erros;
  - Criptografia Fraca;
  - Protocolos Não Seguros;
  - Portas e Serviços Abertos.



Permissões Abertas

Permissão: Atividades permitidas em um objeto por um ator em um sistema.

- Deixa o sistema aberto para invasores.
- Como contas convidadas tendo acesso de gravação aos dados.
- Algumas dicas:

Configurar corretamente as permissões é uma defesa;

Quando não configuradas é como não ter nenhum controle sobre nenhum item.

Contas Root Não Seguras

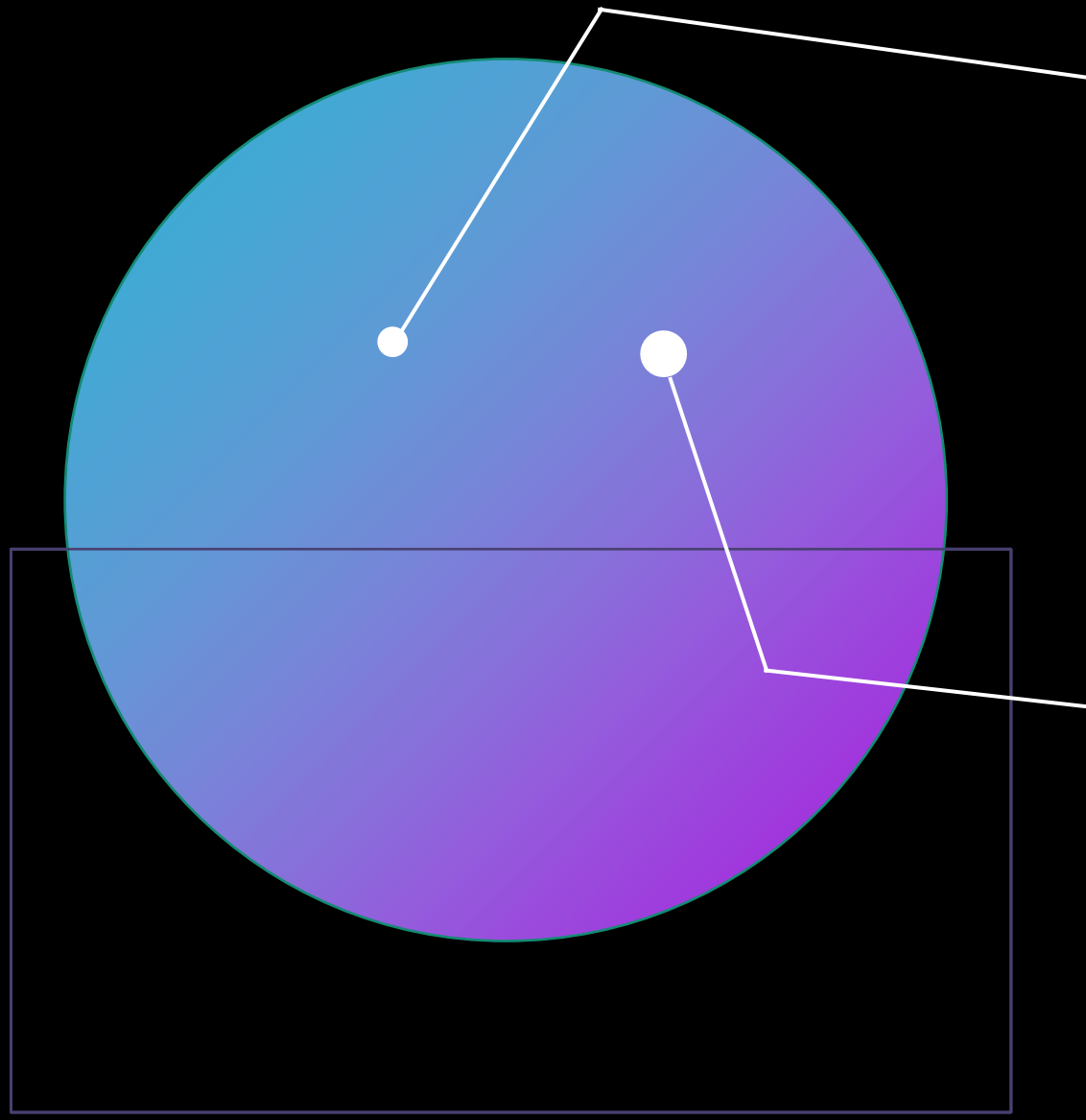
- As contas root têm acesso a tudo e a capacidade de realizar quase toda atividade em uma rede.
  - Devem ser monitoradas e verificar se todos os acessos estão corretos.
- Práticas:
  - Renomear a conta padrão;
  - Definir uma senha forte na conta;
  - Limitar a criação de novas contas de nível root.
- As configurações fortes incluem:

Conta root (Linux);

Contas de administrador (Windows).

Erros

- Todo sistema apresentará **erros**, e é preciso estabelecer a sua captura e as respostas.
- Erro cometido na configuração também pode deixar um sistema vulnerável aos ataques.
- Método de defesa: Gerenciamento de erros e bugs.
- Validações de entrada inadequadas são exploradas por invasores.
- Como tratar erros:
  - Devem ser capturados pelo programa;
  - Arquivos de log apropriados precisam ser gerados.



Criptografia Fraca

Um erro típico para **criptografia fraca** é desenvolver seu próprio algoritmo criptográfico.

- Causas:
  -  Algoritmos criptográficos tornam-se confiáveis somente após anos repelindo ataques.
  -  Erros nas implementações do algorítimo;
  -  Algoritmos obsoletos ou fracos como DES e 3DES;
- Qualquer proteção fornecida não existe se as falhas criptográficas existem.

Protocolos Não Seguros

- Adicione TLS ao HTTP, usando HTTPS.
- Evite FTP, Telnet e SNMPv1.
- O que contribui com acesso não autorizado:
  - Protocolos e serviços de comunicação protegidos de forma inadequada;
  - Credenciais não seguras, como no SFTP.
- Podem provocar acesso indevido:


Roteadores;


Switches;


Pontos de acesso;


Gateways;

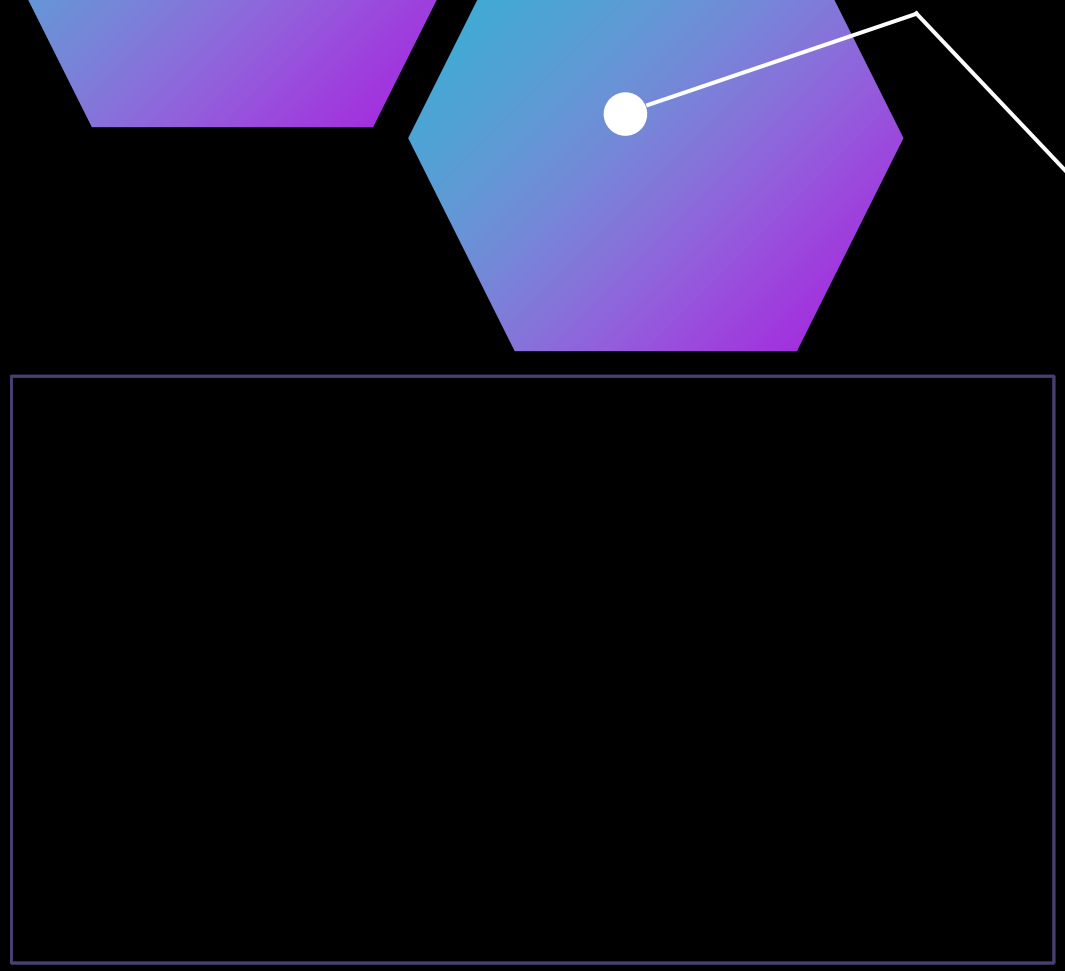

Proxies;


Firewalls.

Configurações Padrão

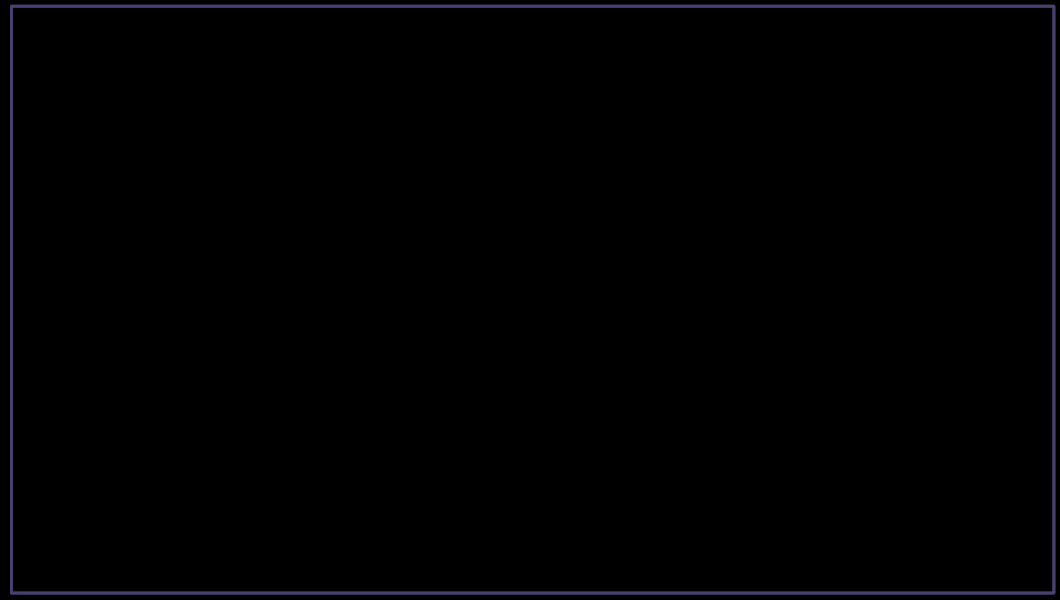
Configurações padrão podem ser um risco de segurança.

- Exemplo: Sistemas Operacionais mais antigos.
- A maioria dos fornecedores define valores padrão com a segurança.
- Exemplo clássico:
  - Windows Server que vinha com o software de servidor web da Microsoft instalado por padrão.



Portas e Serviços Abertos

- Para que um serviço responda a uma solicitação, sua porta deve estar **aberta** para comunicação.
- Recomendações:
  - Não manter serviços abertos em excesso;
  - Desabilitar serviços;
  - Fechar portas;
  - Usar firewalls para evitar comunicações.
- É preciso habilitar somente aquilo que é necessário.
- Configurações fracas aumentam a probabilidade de ataques. Faça auditoria regularmente.



Riscos de Terceiros

- O ambiente de computação empresarial está repleto de **terceiros**, que traz riscos:

Desenvolvimento de código terceirizado;

Manutenção de sistemas;

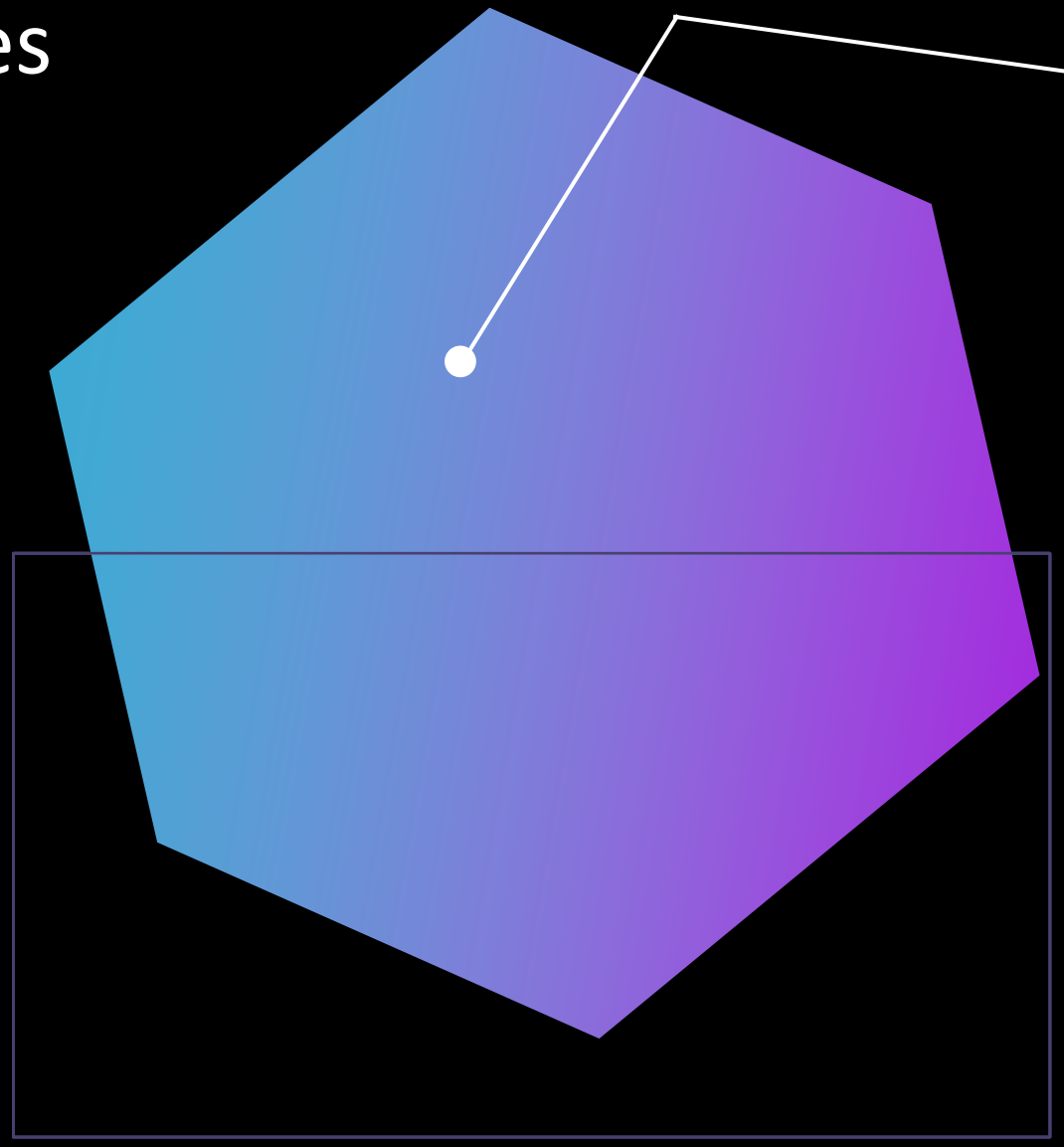
Armazenamento de dados no computador de outra parte.

Cuidados com Terceiros

- Sobre o software de terceiros, é importante ter um inventário sobre:
  - O que é;
  - Onde é usado;
  - Qual a versão do software.
- Preocupações com terceiros envolvem:
  - Cadeia de suprimentos;
  - Falta de suporte do fornecedor.

Gerenciamento de Fornecedores

- Fornecedor é qualquer empresa que tem um relacionamento comercial com sua empresa.
- Como este fornecedor gerencia seus produtos e tem acesso ao seu ambiente?
- No gerenciamento de fornecedores:
  - Determine as próprias necessidades;
  - Encontre fornecedores que ofereçam a melhor proposta.
- Valor de longo prazo envolve:
  - Questões de suporte;
  - Vida útil do sistema;
  - Manutenção.



Integração de Sistemas

- Empresas de Integração são compostas por muitos componentes.

  Diferentes componentes servem a diferentes funções mas precisam trabalhar juntos.

- A integração de sistemas é uma área onde podem existir vulnerabilidades:

  Peças podem apresentar lacunas em sua integração;

  Capacidades que não estão de acordo com o que é desejado.

Falta de Suporte do Fornecedor

- Vulnerabilidades que envolvem falta de suporte:

Fabricante original do item não oferece mais suporte (EOL);

Falta de atualização de patches e correções;

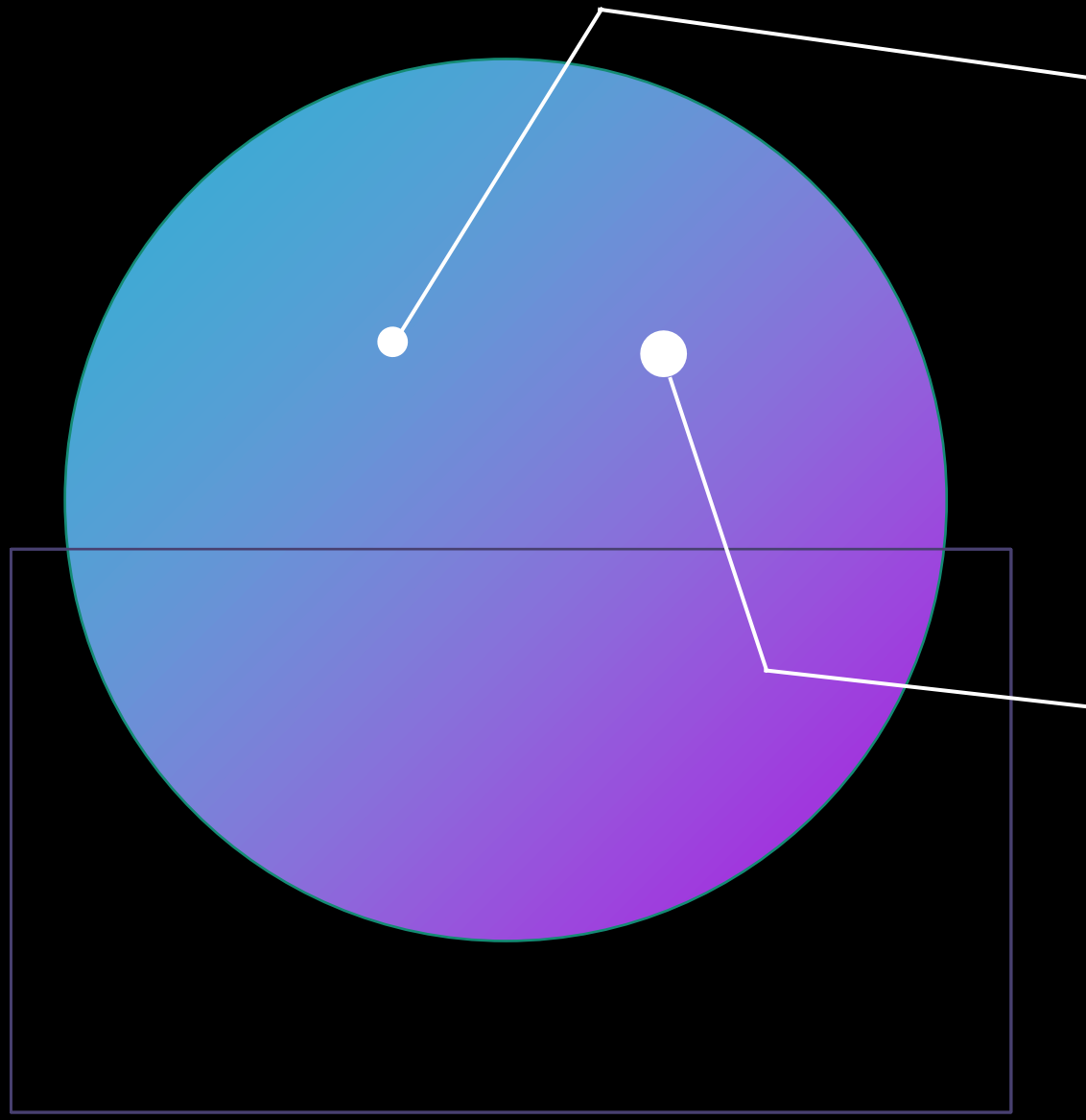
Implementação de sistema por um fornecedor que posteriormente sai do mercado.

Falta de habilidade com testes de regressão.

Relacionadas a idade do produto/sistema (peças antigas ou sistema embarcado).

Cadeia de Suprimentos

- O risco de cadeia de suprimentos é causado por vulnerabilidades na própria cadeia. Alguns riscos incluem:
  - Eventos externos;
  - Atrasos no lançamento de produtos;
  - Atraso em atualizações;
  - Falta de entrega de elementos do software.
- Geralmente acontece no elo de segurança mais fraco da cadeia.



Desenvolvimento de Código Terceirizado

- O código pode ser uma fonte de vulnerabilidade. Os motivos são:
  - Envolvimento em vários aspectos do negócio;
  - Terceirização e dificuldade do gerenciamento.
- É importante:
  - Estabelecer condições nos contratos em desenvolvimento terceirizado.
  - Garantir que desenvolvedores terceirizados tenham práticas de programação segura.

Armazenamento de Dados

Armazenamento de dados é um aspecto importante de todas as empresas.

- Garanta que somente a sua empresa possa descriptografar os dados.
- À medida que distribuímos o armazenamento de dados, o gerenciamento se torna mais difícil.
- Para gerenciar, é preciso:

Garantir controles de acesso e proteções de segurança corretos (e.g. backups).

Garantir uma política de armazenamento;

Uma lista de verificação (checklist).

OBRIGADO!

EXPLORANDO
VULNERABILIDADES