Prime

CCS-A

# Arquitetura de Segurança Corporativa – Parte 2

# Controles de Resposta e Recuperação

- Os dados são a força vital de uma organização.
- Dois elementos devem ser projetados:
  - Recuperação de Desastres (DR);
  - Continuidade de Negócios (BC).
- Como resposta, a empresa criar programas de:
  - Controles para respostas a incidentes + BC + DR + backup + etc.
  - Mecanismos, processos e **sequenciamento** de recuperação e restauração.

# Considerações Geográficas

Existem leis e regulamentos além das fronteiras físicas.

- Exemplo: GDPR.

A pandemia trouxe um novo olhar sobre onde os dados devem ser armazenados e transmitidos.

A consideração geográfica impacta os negócios, política, questões ambientais (desastres) etc.

# Resiliência de um Site / Locais de Recuperação

- Consideração dos locais (sites) usados para continuidade das operações.
- Não só do backup, mas das pessoas, serviços, instalações e processos.
- Sites de recuperação - Site onde podemos transportar os nossos dados caso haja algum dano físico.

Hot site;

Cold site;

Warm site.

# Hot Site

Ambiente totalmente configurado com dados atualizados.

O site alternativo parece com o ambiente operacional do site principal.

Opera imediatamente ou em poucas horas.

# Cold Site

Normalmente é apenas um espaço físico com controles ambientais básicos necessários para operar.

Não tem componentes computacionais para processamento, ou seja, hardware e software.

Seu funcionamento pode levar algumas semanas.

# Warm Site



Parcialmente configurado com equipamentos sobressalentes.

Possui alguns periféricos, software e/ou servidor de backup para restauração.

Talvez nem possua os servidores principais, devendo ser recriados.

Projetado para operar em alguns dias.

# Inspeção de Secure Sockets Layer (SSL)/ Transport Layer Security (TLS)

- A criptografia TLS é a sucessora da criptografia SSL.
- TLS fornece proteção aos dados, mas impede que ferramentas inspecionem dados para exfiltração.
- O TLS foi criado para garantir à comunicação:

Confidencialidade;

Integridade.

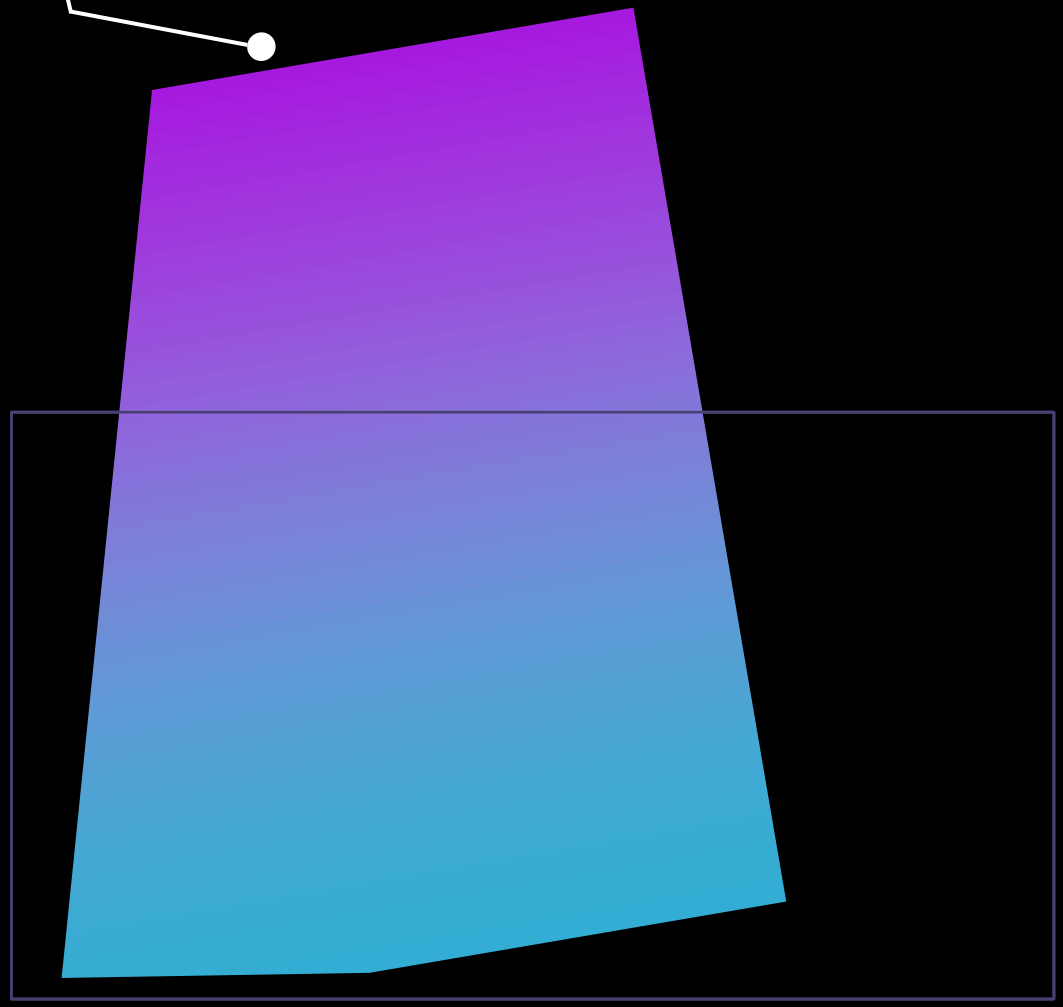
- A inspeção SSL ou TLS permite interceptar o tráfego.
- Você pode querer inspecionar o tráfego criptografado em busca de conteúdo mal-intencionado.
- Porque os hackers usam a criptografia como um método para ocultar o conteúdo mal-intencionado.

# Como Funciona a Inspeção

- Para executar a inspeção o SSL/TLS, é preciso:
  -  Com um conjunto de chaves para a criptografia;
  -  Receber os dados;
  -  Descriptografar os dados;
  -  Realizar sua tarefa de segurança;
  -  Criptografar novamente;
  -  Enviar os dados.
- NGFWs têm a inspeção TLS integrada.

# Hashing

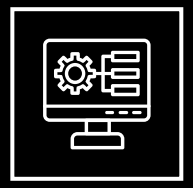
- Tecnologia pela qual a exclusividade de um elemento de dados pode ser representada em uma string.
- Na arquitetura corporativa:
  - É um meio de habilitar a proteção de dados;
  - E ainda sim, usar os dados subjacentes.
- Utiliza criptografia unidirecional.
- Empregada em muitas situações: senha, comparar cópias, garantir integridade etc.



# Considerações Sobre API

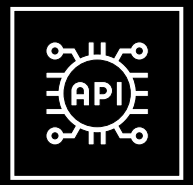


Uma biblioteca de funções que chama seus aplicativos, ou seja, um método de integração.



APIs podem ser inseguras ou mal implementadas.
APIs podem chamar aplicativos inseguros.

Fornecem acesso aos aplicativos e aos dados.
Como se fossem portas e janelas de uma casa.




Para lidar com as APIs, é preciso:

- Um conjunto de protocolos de autenticação;
- Práticas de programação segura;
- Testar componentes de terceiros.

# Deception and Disruption

- Um método de detecção de intrusões.
- Truque para pegar o invasor em flagrante.
- Coleta informações e retardar o ataque.
- A técnica de engano coloca:
  - Ativos de chamariz;
  - Dados falsos;
  - Outros artefatos para atrair até a armadilha.
- A tecnologia falsa não faz parte das configurações da empresa.

# Honeypots

Servidor projetado para atuar como um servidor real localizado na DMZ ou na rede interna.

Atrair o hacker para longe dos sistemas de produção através de uma armadilha.

Enquanto o hacker gasta seu tempo:

- Recebemos notificação da existência dele;
- Registra todas as suas atividades.

Torna-se atraente para hackers, mas cuidado com a “obviedade”.

# Honeynets

- Uma rede inteira projetada para parecer uma rede corporativa.
- O objetivo é atrair o hacker para longe da rede de produção real.
- Coleção de honeypots.
  - Ajuda a identificar a origem do tráfego do invasor e de onde os ataques vêm.
  - Não são visitadas ou usadas por sistemas legítimos.

# Telemetria Falsa

Telemetria falsa gera tráfego falso para fingir ser uma rede "normal“ e não um Honeynet.

Assemelha-se a comunicações reais.

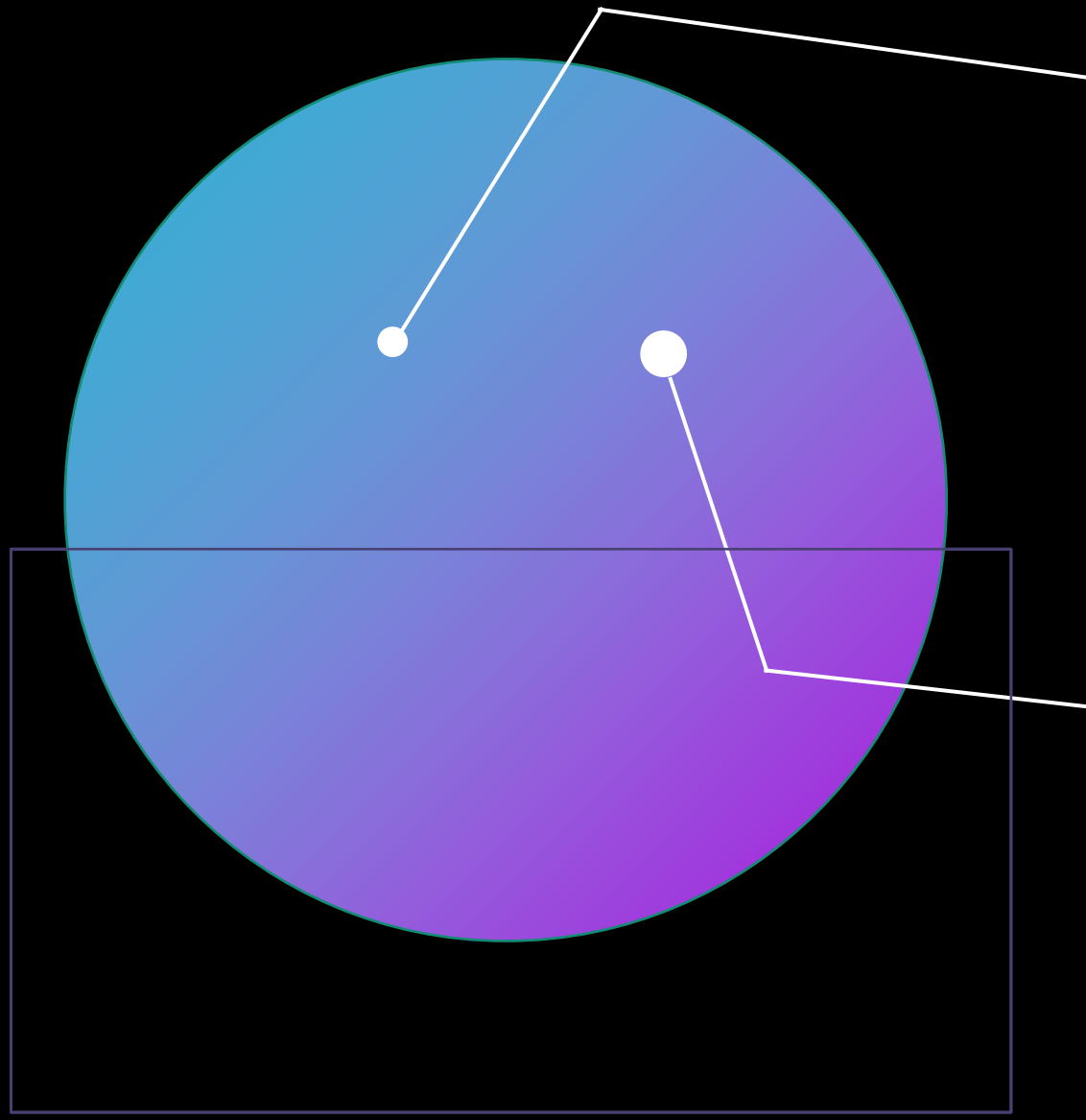
- Fazem honeynets e honeypots parecerem reais.

# Honeyfile

- Arquivo nomeado, por exemplo: senhas.txt.
- Servem como alvos atraentes para invasores.
  -  Podem conter gatilhos para alerta de DLP.
- Variação do honeyfile: honeyrecord em BD
  -  São falsos e nunca são usados.
- Podem ser combinados com arquivos e registros legítimos para tornar a exploração mais provável.

# Sumidouro DNS

- Responde solicitações de IP ou domínio maliciosos.
- Enviando informações falsas para o solicitante.
- Um servidor DNS fornece:
  - Um resultado;
  - Solicitação de resolução.
- Ferramenta útil para:
  - Bloqueio de tráfego malicioso;
  - Combate a bots;
  - Combate a malwares que dependem de respostas de DNS.
- Podem ser usados de maneiras destrutivas e construtivas.



# OBRIGADO!

ARQUITETURA DE SEGURANÇA CORPORATIVA – PARTE 2