TRY HACK ME

Exemplo prático de segurança defensiva

Um exemplo prático de segurança defensiva pode ser observado no uso de **firewalls e sistemas de detecção e prevenção de intrusões (IDS/IPS)** para proteger a rede de uma empresa contra acessos não autorizados e atividades maliciosas.

Cenário: Proteção de uma Rede Empresarial

Uma empresa que armazena dados sensíveis de clientes e transações financeiras decide implementar um conjunto de medidas de segurança defensiva para proteger suas operações contra ataques cibernéticos, como ransomware ou vazamento de dados.

Soluções Adotadas

1. Firewall

- **Configuração:** Um firewall é configurado na borda da rede para filtrar todo o tráfego de entrada e saída. Ele bloqueia conexões não autorizadas e permite apenas tráfego legítimo com base em regras específicas.
    - Exemplo: Bloquear portas usadas para tráfego de comandos maliciosos (como a porta 445 para ataques de worms).

2. IDS/IPS

- **Implementação:** Um sistema IDS/IPS é integrado ao ambiente para monitorar e reagir a tráfego suspeito em tempo real.
    - **IDS (Sistema de Detecção de Intrusão):** Detecta atividades incomuns, como tentativas de acesso por força bruta.
    - **IPS (Sistema de Prevenção de Intrusão):** Responde automaticamente, bloqueando IPs suspeitos ou encerrando sessões não autorizadas.

3. Criptografia

- **Proteção de Dados:** A empresa criptografa todas as comunicações internas e externas usando TLS (Transport Layer Security), garantindo que dados interceptados sejam ilegíveis para atacantes.

4. Gerenciamento de Acessos

- **MFA (Autenticação Multifator):** Implementa autenticação em dois fatores para todos os funcionários, exigindo uma senha e uma confirmação adicional (como um código enviado por SMS).
- **Privilégios Limitados:** Apenas usuários específicos têm permissão para acessar dados sensíveis.

5. Monitoramento Contínuo

- **SIEM (Security Information and Event Management):** Soluções de SIEM são implementadas para coletar, correlacionar e analisar logs de eventos, identificando padrões que possam indicar um ataque.
    - Exemplo: Um alerta é gerado quando múltiplas tentativas de login falham em um curto período.

6. Plano de Resposta a Incidentes

- **Simulação de Ataques:** A equipe realiza exercícios simulados de ataques de ransomware para treinar sua resposta.
- **Plano de Backup:** Backups automatizados são configurados para garantir a recuperação rápida em caso de ataques ou falhas.

Exemplo em Ação

1. Um atacante tenta acessar a rede usando um exploit conhecido na porta 3389 (RDP).
    - O **firewall** bloqueia o tráfego imediatamente com base nas regras configuradas.
    - O **IPS** identifica o comportamento como malicioso e registra o evento.
2. A equipe de segurança recebe uma notificação do **SIEM**, detalhando a tentativa e bloqueando automaticamente o IP do atacante.
3. Enquanto isso, os dados sensíveis da empresa permanecem protegidos pela **criptografia** e acessíveis apenas por funcionários autorizados via **MFA**.

Resultados

Essa abordagem defensiva proativa evita que o atacante obtenha acesso à rede, minimiza o impacto potencial e mantém a integridade, a confidencialidade e a disponibilidade dos dados e sistemas.