Relatório de Crise - 20250417_190707

Relatório de Crise: Ataque Cibernetico

Resumo do Incidente

Um ataque cibernetico externo utilizando DDoS (Distributed Denial of Service) foi detectado e confirmado no sistema de autenticação ("servidor_auth"). O ataque resultou em uma perda de disponibilidade do serviço, afetando a capacidade dos usuários de fazer login.

Detalhes do Incidente

* **Origem:** Externa
* **Tipo de Ataque:** DDoS (Distributed Denial of Service)
* **Sistema Afetado:** Servidor Auth
* **Erro Observado:** Não é possível acessar o servidor.
* **Impacto Observado:** Usuários não conseguem fazer login.

Resposta Reativa

Uma resposta reativa imediata foi implementada para minimizar os danos:

* Ataque detectado! Acionamento do time de segurança e bloqueio de tráfego suspeito.

Plano de Ação

Para resolver o problema, a equipe de segurança implementou os seguintes passos:

1. **Isolar sistemas afetados:** Isolare os sistemas afetados para prevenir a propagação do ataque.
2. **Analisar logs:** Análise dos logs para identificar as origens e métodos utilizados pelo ataque.
3. **Comunicar stakeholders:** Comunicação com os stakeholders envolvidos, incluindo administradores de sistema, usuários afetados e autoridades competentes.

Prioridade do Incidente

O incidente foi classificado como **CRÍTICO**, pois resultou em uma perda significativa de disponibilidade do serviço e impactou a capacidade dos usuários de realizar suas atividades normais.

Evolução do Incidente

A situação está sob controle, mas é importante monitorar os logs para detectar possíveis tentativas futuras de ataque. A equipe de segurança irá continuar a trabalhar no resolução do incidente e implementar medidas preventivas para evitar futuros ataques ciberneticos.

Conclusão

O ataque cibernetico foi detectado e respondido rapidamente, minimizando os danos e protegendo os dados sensíveis. A equipe de segurança continuará a monitorar os sistemas e tomar medidas preventivas para evitar futuras ameaças.