Projeto: Avaliação e Hardening de Rede para Organização de Mídia Social

Descrição do Projeto

Este projeto envolve a análise de uma violação de dados em uma organização de mídia social e a aplicação de práticas recomendadas de hardening de rede para mitigar vulnerabilidades identificadas e prevenir futuros ataques.

Cenário

A organização sofreu uma grande violação de dados que expôs informações pessoais de clientes (nomes, endereços). A análise da rede revelou quatro vulnerabilidades críticas:

- Compartilhamento de senhas entre funcionários.
- Uso de senha padrão para administrador do banco de dados.
- Ausência de regras de filtragem em firewalls.
- Falta de autenticação multifatorial (MFA).

Ferramentas e Métodos Selecionados para Proteção

1. Autenticação Multifatorial (MFA)

Implementação de MFA para todos os acessos críticos, especialmente administradores e acesso remoto, adicionando uma camada extra de proteção mesmo em caso de vazamento de senha.

2. Configuração e Manutenção de Firewall com Filtragem de Portas

Definição rigorosa de regras para controlar o tráfego de entrada e saída, bloqueando portas não utilizadas e filtrando protocolos, limitando o acesso externo e prevenindo movimentos laterais na rede.

3. Políticas Rígidas de Senhas e Gerenciamento de Credenciais

Adoção das recomendações NIST para criação, armazenamento e uso de senhas, eliminando senhas padrão e proibindo o compartilhamento entre funcionários, apoiado pelo uso de gerenciadores de senhas.

Recomendações e Justificativas

Implementação da Autenticação Multifatorial (MFA)

- **Eficácia:** Dificulta o acesso não autorizado mesmo que a senha seja comprometida, protegendo contra ataques de phishing, força bruta e roubo de credenciais.
- **Frequência:** Configuração única por usuário/sistema, com uso contínuo e manutenção periódica para garantir atualizações e compatibilidade.

Manutenção Contínua e Configuração de Firewall com Filtragem de Portas

- **Eficácia:** Controla rigorosamente o tráfego, bloqueando acessos não autorizados e tráfego malicioso, reduzindo a superfície de ataque.
- **Frequência:** Configuração inicial seguida de revisões regulares mensais ou após incidentes para adaptação a novas ameaças.

Resultados Esperados

- Redução significativa no risco de violação de dados e acessos não autorizados.
- Monitoramento ativo e resposta rápida a tentativas de ataque.
- Melhoria na postura geral de segurança da organização, com práticas auditáveis e atualizadas.

Tecnologias e Ferramentas Envolvidas

- Soluções MFA (Google Authenticator, Microsoft Authenticator, etc.)

- Firewalls de próxima geração e sistemas de filtragem de portas
- Gerenciadores de senhas corporativos (ex: Bitwarden, LastPass Enterprise)
- Ferramentas de monitoramento e análise de logs (SIEM)

Links e Contatos

- LinkedIn: https://www.linkedin.com/in/tiago-sants-295a1565
- GitHub: https://github.com/tiagosaants
