Relatório de avaliação de risco de segurança

Parte 1: Selecione até três ferramentas e métodos de hardening para implementar

Para mitigar as vulnerabilidades da organização, recomendo as seguintes ferramentas e métodos de hardening de rede:
 	
1. Autenticação Multifatorial (MFA)
    ○ *Vulnerabilidade abordada*: Funcionários compartilham senhas; MFA não é usada.
    ○ *Justificativa*: O MFA adiciona uma camada extra de segurança, exigindo que os usuários verifiquem sua identidade de múltiplas formas (ex: senha + token ou biometria). Isso reduz drasticamente o risco de acesso não autorizado, mesmo que senhas sejam comprometidas.
2. Configuração e Manutenção de Firewall com Filtragem de Portas
    ○ *Vulnerabilidade abordada*: Firewalls não têm regras implementadas para filtrar tráfego.
    ○ *Justificativa*: A filtragem de portas bloqueia tráfego não essencial e potencialmente malicioso, reduzindo a superfície de ataque. A manutenção regular garante que as regras estejam atualizadas contra ameaças emergentes.
3. Políticas de Senha e Remoção de Credenciais Padrão
    ○ *Vulnerabilidade abordada*: Senha de administrador do banco de dados está definida como padrão; funcionários compartilham senhas.
    ○ *Justificativa*: Políticas de senha (como as recomendações do NIST) incentivam senhas longas e únicas, sem rotatividade desnecessária. A remoção de credenciais padrão elimina pontos de entrada comuns para atacantes.

Parte 2: Explique suas recomendações

1. Autenticação Multifatorial (MFA)

- Por que é eficaz?:
  O MFA impede que invasores acessem sistemas mesmo que obtenham senhas, pois exigirá um segundo fator (ex: código de celular ou impressão digital). Isso protege contra ataques de força bruta e phishing.
- Frequência de implementação:
  Implementado uma vez, mas deve ser mantido e auditado regularmente (ex: semestralmente) para garantir que todos os usuários estejam cadastrados e que os métodos de autenticação estejam atualizados.

2. Configuração e Manutenção de Firewall com Filtragem de Portas

- Por que é eficaz?:
  A filtragem de portas bloqueia comunicações não autorizadas (ex: portas abertas desnecessárias), prevenindo que malware se comunique com servidores externos ou que invasores explorem serviços vulneráveis. A manutenção contínua adapta as regras a novas ameaças.
- Frequência de implementação:
  A configuração inicial deve ser feita imediatamente, com revisões trimestrais das regras. Incidentes de segurança devem disparar atualizações emergenciais.

3. Políticas de Senha e Remoção de Credenciais Padrão

- Por que é eficaz?:
  Políticas baseadas no NIST (ex: senhas longas e fáceis de lembrar, sem rotatividade forçada) reduzem a carga sobre os usuários enquanto mantêm a segurança. A remoção de senhas padrão elimina vulnerabilidades conhecidas (ex: senhas de fábrica).
- Frequência de implementação:
  A remoção de credenciais padrão deve ser feita imediatamente. As políticas de senha devem ser aplicadas continuamente (validação em tempo real) e revisadas anualmente.

Como essas práticas previnem violações futuras?
● O MFA e as políticas de senha tornam o acesso não autorizado significativamente mais difícil. ● A filtragem de portas reduz pontos de entrada para invasores. ● Juntas, essas medidas criam camadas de defesa (defesa em profundidade), tornando a rede mais resiliente. Essas recomendações estão alinhadas com as melhores práticas de segurança e os materiais de apoio fornecidos.