Relatório de avaliação de risco de segurança

Parte 1: Selecione até três ferramentas e métodos de endurecimento para implementar
1. Políticas de senha: Implementação de diretrizes rigorosas para a criação e gestão de senhas, visando eliminar o compartilhamento e o uso de credenciais padrão. **2. Autenticação multifator (MFA):** Exigência de múltiplos fatores de verificação para acesso a sistemas e recursos críticos, adicionando uma camada essencial de segurança. **3. Filtragem de portas:** Configuração precisa das regras de firewall para controlar o tráfego de rede, permitindo apenas comunicações autorizadas e bloqueando acessos indesejados.

Parte 2: Explique suas recomendações
1. Políticas de senha: **Eficácia:** As políticas de senha são cruciais para mitigar as vulnerabilidades de senhas compartilhadas e senhas de administrador padrão. Ao implementar políticas que exigem senhas fortes (combinação de caracteres, números e símbolos), proíbem o uso de senhas padrão e incentivam a não reutilização, a organização dificulta significativamente que atacantes adivinhem ou quebrem senhas. Além disso, a conscientização sobre a importância de não compartilhar senhas é reforçada por essas políticas. **Frequência de implementação:** As políticas de senha devem ser implementadas uma vez e revisadas periodicamente (ex: anualmente ou a cada nova ameaça significativa) para garantir que permaneçam robustas e alinhadas com as melhores práticas de segurança (como as recomendações do NIST, que focam em salgar e hashear senhas em vez de trocas frequentes). **2. Autenticação multifator (MFA):** **Eficácia:** A MFA é uma defesa poderosa contra o acesso não autorizado,

especialmente quando senhas são comprometidas ou fracas (como no caso de senhas compartilhadas ou padrão). Ao exigir uma segunda forma de verificação (ex: código enviado para o celular, biometria), mesmo que um atacante obtenha a senha de um funcionário ou a senha padrão do banco de dados, ele não conseguirá acessar o sistema sem o segundo fator. Isso aborda diretamente as vulnerabilidades 1, 2 e 4.
Frequência de implementação: A MFA deve ser configurada uma vez para todos os usuários e sistemas críticos. Sua eficácia é contínua, pois exige verificação a cada tentativa de login. A revisão da configuração e a educação dos usuários sobre seu uso devem ser feitas periodicamente.

3. Filtragem de portas:

Eficácia: A filtragem de portas, uma função essencial do firewall, é fundamental para resolver a vulnerabilidade de firewalls sem regras implementadas. Ao configurar regras específicas para bloquear ou permitir o tráfego em portas determinadas, a organização pode controlar rigorosamente quais comunicações entram e saem da rede. Isso impede que tráfego malicioso ou não autorizado acesse a rede interna, protegendo contra varreduras de portas, ataques de força bruta e exploração de serviços vulneráveis expostos. Isso aborda diretamente a vulnerabilidade 3.
Frequência de implementação: As regras de filtragem de portas devem ser configuradas inicialmente e revisadas regularmente (ex: trimestralmente ou sempre que houver mudanças na infraestrutura de rede ou novas ameaças) para garantir que continuem eficazes e alinhadas com as necessidades de segurança da organização.