# Relatório de avaliação de risco de segurança

|  |
| --- |
| **Parte 1: Selecione até três ferramentas e métodos de proteção para implementar** |
| * **Implementação de Autenticação Multifator (MFA) e Políticas de Senhas Robustas** (com suporte de Ferramentas de Auditoria de Senhas, como o John the Ripper, para verificação da força das senhas * **Configuração e Gestão Eficaz de Firewalls** (utilizando Ferramentas de Gestão de Firewall, como o pfSense, para definir e aplicar regras de filtragem de tráfego. * **Implementação de Varreduras de Vulnerabilidade Regulares** (utilizando Scanners de Vulnerabilidade, como o Nessus, para identificar proativamente configurações incorretas e outras falhas de segurança |
|

|  |
| --- |
| **Parte 2: Explique suas recomendações** |
| **Implementação de Autenticação Multifator (MFA) e Políticas de Senhas Robustas**   * **Por que a técnica de reforço de segurança recomendada é eficaz?**   + A **Autenticação Multifator (MFA)** é uma das formas mais eficazes de prevenir o acesso não autorizado a contas, mesmo que as credenciais de senha sejam comprometidas. Ao exigir uma segunda forma de verificação (além da senha, como um código de uma aplicação, uma impressão digital ou um token físico), a MFA mitiga diretamente o risco associado à **partilha de senhas entre funcionários** e ao facto de a **MFA não ser usada** atualmente. Se uma senha for partilhada ou roubada, o atacante ainda precisaria do segundo fator para obter acesso.   + **Políticas de Senhas Robustas** são cruciais para resolver a vulnerabilidade da **senha de administrador do banco de dados definida como padrão** e para desencorajar a **partilha de senhas**. Estas políticas devem incluir:     - A alteração imediata de todas as senhas padrão para senhas únicas e complexas.     - Requisitos de complexidade (combinação de letras maiúsculas e minúsculas, números e símbolos) e comprimento mínimo.     - Proibição explícita da partilha de senhas, complementada por formação de consciencialização.     - Implementação de um gestor de senhas corporativo para ajudar os funcionários a gerir senhas únicas e complexas sem as partilhar.   + O uso de **Ferramentas de Auditoria de Senhas** como o "John the Ripper" pode ajudar a organização a "detetar senhas fracas" que não cumprem as novas políticas, permitindo uma correção proativa. * **Com que frequência a técnica de reforço precisa ser implementada?**   + **MFA:** Deve ser implementada e tornada obrigatória para todos os funcionários, especialmente para acesso a sistemas críticos e dados sensíveis (como o banco de dados de clientes), o mais rapidamente possível. Uma vez implementada, a MFA é uma medida de segurança contínua. As configurações e políticas de MFA devem ser revistas anualmente.   + **Políticas de Senhas Robustas:** Devem ser definidas, comunicadas e tecnicamente aplicadas (sempre que possível) imediatamente. A formação sobre estas políticas deve ser incluída no processo de integração de novos funcionários e realizada anualmente para todos os funcionários. As próprias políticas devem ser revistas anualmente.   + **Auditoria de Senhas:** Deve ser realizada regularmente, por exemplo, trimestralmente, para garantir a conformidade e identificar senhas que não cumprem as políticas.   **2. Configuração e Gestão Eficaz de Firewalls**   * **Por que a técnica de reforço de segurança recomendada é eficaz?**   + Firewalls são a primeira linha de defesa para uma rede. A vulnerabilidade de **firewalls não terem regras implementadas para filtrar o tráfego** significa que a rede está aberta a uma vasta gama de ataques e acessos não autorizados. Ao implementar regras de firewall baseadas no princípio do menor privilégio (permitir apenas o tráfego explicitamente necessário para as operações de negócio e bloquear todo o resto), a organização pode reduzir drasticamente a sua superfície de ataque.   + **Ferramentas de Gestão de Firewall** como o "pfSense" "fornecem um conjunto abrangente de capacidades de firewall, encaminhamento e VPN". Estas ferramentas permitem a criação, gestão e monitorização de regras de firewall de forma eficaz, ajudando a "proteger perímetros de rede" e "segmentar redes", o que é crucial para proteger o banco de dados de clientes e outros ativos internos. As regras devem ser configuradas para filtrar tanto o tráfego de entrada (ingress) como o de saída (egress). * **Com que frequência a técnica de reforço precisa ser implementada?**   + A configuração inicial das regras de firewall deve ser realizada imediatamente.   + As regras de firewall devem ser revistas e auditadas regularmente, no mínimo trimestralmente, ou sempre que houver mudanças significativas na infraestrutura de rede, aplicações ou requisitos de negócio.   + Os logs do firewall devem ser monitorizados continuamente (idealmente integrados com uma solução de Gestão de Logs & SIEM como o "Splunk") para detetar atividades suspeitas e garantir que as regras estão a funcionar como esperado.   **3. Implementação de Varreduras de Vulnerabilidade Regulares**   * **Por que a técnica de reforço de segurança recomendada é eficaz?**   + Mesmo com firewalls e senhas fortes, novas vulnerabilidades podem surgir em software, configurações ou através de erro humano. **Scanners de Vulnerabilidade** como o "Nessus" são ferramentas que "identificam vulnerabilidades em dispositivos de rede, aplicações e sistemas operativos". Realizar varreduras regulares permite à organização identificar proativamente estas fraquezas, incluindo configurações incorretas como senhas padrão que possam ter sido negligenciadas, antes que sejam exploradas por atacantes. Isto é essencial para manter uma postura de segurança robusta e prevenir futuras violações. O Nessus é útil para "auditorias de segurança regulares" e "verificações de conformidade". * **Com que frequência a técnica de reforço precisa ser implementada?**   + As varreduras de vulnerabilidade devem ser realizadas com frequência. Recomenda-se:     - Varreduras semanais ou quinzenais para sistemas críticos e expostos à internet.     - Varreduras mensais para a rede interna.     - Varreduras completas e autenticadas (com credenciais) devem ser agendadas pelo menos trimestralmente.   + Os resultados das varreduras devem ser analisados prontamente, e um processo de gestão de vulnerabilidades deve ser implementado para priorizar e corrigir as falhas identificadas. |