Segurança da Informação - Implementação de Medidas de Segurança

1. **Implementação de Políticas de Controle de Acesso aos Sistemas e Dados**
   Para mitigar os riscos identificados e garantir a segurança da informação, é fundamental implementar políticas robustas de controle de acesso. Estas políticas devem ser desenvolvidas com base nos riscos identificados e na estrutura organizacional da HealthTech Balderi Solutions.

   Políticas de Controle de Acesso:
   1. Autenticação Multifator (MFA) : Todos os usuários devem usar autenticação multifator para acessar sistemas críticos e dados sensíveis.
   2. Princípio do Menor Privilégio : Os usuários só devem ter acesso aos dados e sistemas necessários para realizar suas funções.
   3. Gestão de Identidade e Acesso (IAM) : Implementar um sistema IAM para gerenciar identidades de usuários e controlar o acesso a recursos com base em funções e responsabilidades.
   4. Revisão Regular de Acessos : Realizar revisões periódicas das permissões de acesso dos usuários para garantir que estejam atualizadas e adequadas.
   5. Senhas Fortes e Política de Senhas : Exigir que todas as senhas sejam fortes e trocadas regularmente. Políticas devem incluir requisitos mínimos de comprimento, complexidade e periodicidade de troca.
   6. Acesso Baseado em Funções (RBAC) : Implementar controles de acesso baseados em funções, onde as permissões são atribuídas com base na função do usuário dentro da organização.
   7. Controle de Acesso Físico : Limitar o acesso físico a servidores, centros de dados e áreas sensíveis a pessoal autorizado mediante identificação e autenticação.
   8. Logs de Acesso e Auditoria : Manter registros detalhados de todas as tentativas de acesso e atividades dos usuários, com auditorias regulares para detectar e responder a atividades suspeitas.
   9. Treinamento e Conscientização de Segurança :Treinar regularmente os funcionários sobre práticas seguras de acesso e conscientização sobre phishing, engenharia social e outras ameaças.
   10. Política de Desligamento Automático : Configurar sistemas para desligar automaticamente sessões inativas após um período determinado para prevenir acessos não autorizados.

Exemplo de Política de Controle de Acesso:
Título: Política de Acesso Baseado em Funções (RBAC)
Objetivo: Assegurar que os usuários tenham apenas os acessos necessários para desempenhar suas funções, minimizando os riscos de acesso não autorizado.
Escopo: Todos os funcionários, contratados e terceiros que necessitam acessar os sistemas e dados da HealthTech Balderi Solutions.

Política:
1. Definição de Funções: Todas as funções dentro da organização serão definidas e categorizadas com base nas necessidades de acesso a sistemas e dados.
2. Atribuição de Permissões: Permissões serão atribuídas a funções, e não a usuários individuais, para facilitar a gestão e garantir a conformidade.
3. Revisão de Acessos: As permissões de acesso serão revisadas trimestralmente para assegurar que os usuários mantenham apenas os acessos necessários.
4. Modificação de Acessos: Quaisquer mudanças nas funções dos funcionários (promoções, transferências, demissões) devem resultar em revisão e ajuste imediato das permissões de acesso.
5. Acesso Temporário: Acessos temporários, se necessários, devem ser concedidos com base em justificativas documentadas e com uma data de expiração claramente definida.

Procedimentos:
1.1 Solicitação de Acesso: Todas as solicitações de acesso devem ser submetidas por meio do sistema de gestão de identidades (IAM) e aprovadas pelo supervisor imediato do funcionário.
1.2 Auditoria e Monitoramento: Auditorias regulares serão conduzidas para revisar logs de acesso e detectar anomalias. Responsabilidades:
1.3 Gestores de TI: Implementar e manter o sistema IAM, assegurar a conformidade com a política de RBAC.
1.4 Supervisores: Aprovar solicitações de acesso e garantir que as permissões estejam alinhadas com as responsabilidades dos funcionários.
1.5 Funcionários: Seguir as políticas de acesso e reportar quaisquer incidentes ou suspeitas de acesso não autorizado imediatamente.

Configuração de Sistemas de Detecção de Intrusão e Prevenção de Ataques

Configuração de Sistemas de Detecção de Intrusão e Prevenção de Ataques

Para fortalecer a segurança dos sistemas da HealthTech Balderi Solutions, é essencial implantar e configurar sistemas eficazes de detecção de intrusão e prevenção de ataques. Abaixo estão 10 medidas de detecção e prevenção de ataques recomendadas para proteger os ativos de informação da empresa.

Medidas de Detecção e Prevenção de Ataques:

1. Firewalls de Rede : Configurar firewalls de rede para filtrar e monitorar o tráfego de rede, bloqueando tráfego malicioso e permitindo apenas comunicações autorizadas.
2. Sistemas de Detecção de Intrusão (IDS) : Implementar IDS para monitorar o tráfego de rede em busca de atividades suspeitas ou padrões de comportamento maliciosos que possam indicar uma intrusão.
3. Sistemas de Prevenção de Intrusão (IPS) : Complementar os IDS com sistemas de IPS, que podem responder automaticamente a atividades maliciosas, bloqueando pacotes de rede suspeitos ou aplicando políticas de segurança.
4. Monitoramento de Logs : Configurar sistemas de monitoramento de logs para registrar e analisar atividades de sistemas e rede, facilitando a detecção de comportamentos anômalos e eventos de segurança.
5. Análise de Tráfego SSL/TLS •:Realizar inspeção SSL/TLS para detectar e bloquear tráfego malicioso criptografado, garantindo que todo o tráfego seja visível e passível de inspeção.
6. Sistemas de Detecção de Malware : Implementar sistemas de detecção de malware para identificar e bloquear arquivos maliciosos antes que possam causar danos aos sistemas da empresa.
7. Controle de Acesso Baseado em Comportamento (BAC) : Utilizar sistemas de BAC para monitorar o comportamento dos usuários e detectar atividades anômalas que possam indicar comprometimento de contas ou credenciais.
8. Atualizações de Segurança Automáticas : Configurar sistemas para receber e aplicar automaticamente atualizações de segurança, garantindo que os sistemas estejam protegidos contra vulnerabilidades conhecidas.
9. Bloqueio de Portas Não Utilizadas : Desativar e bloquear portas de rede não utilizadas nos sistemas da empresa para reduzir a superfície de ataque e limitar pontos de entrada para potenciais invasores.

10. Autenticação Forte : Implementar autenticação forte para acessar sistemas críticos, como autenticação de dois fatores (2FA) ou autenticação baseada em certificados.

Exemplo de Configuração:
Medida: Configuração de IDS/IPS
Descrição: Implementar um sistema de IDS/IPS para monitorar o tráfego de rede em tempo real, detectando e bloqueando atividades maliciosas.
Configuração:

1.1 Instalar e configurar um IDS/IPS em um ponto estratégico da rede, como na borda da rede.

1.2 Definir políticas de detecção para identificar padrões de tráfego malicioso, como ataques de negação de serviço (DDoS), explorações de vulnerabilidades conhecidas e tentativas de acesso não autorizado.

1.3 Configurar ações de resposta automáticas para atividades suspeitas, como bloquear endereços IP, desativar portas ou enviar alertas para a equipe de segurança.

1.4 Realizar regularmente atualizações de assinaturas e regras de detecção para garantir a eficácia contínua do IDS/IPS contra ameaças emergentes