Projeto rede Wi-Fi - SecurityPro
(Políticas de Segurança)

Políticas de segurança:

Objetivo:

O objetivo desta política é garantir a segurança da rede Wi-Fi da Empresa SecurityPro, protegendo os dados confidenciais da empresa e garantindo o funcionamento e tráfego seguro dos dispositivos conectados à rede.

Escopo:

Esta política se aplica a todos os dispositivos e usuários que acessam a rede Wi-Fi da Empresa SecurityPro, e a todas as equipes técnicas envolvidas na implementação da rede, incluindo colaboradores, prestadores de serviços/fornecedores e visitantes.

1. **Responsabilidades:**

   A equipe de TI da Empresa SecurityPro é responsável por implementar e fazer cumprir esta política de segurança, bem como todos envolvidos;

   Todos os usuários são responsáveis por aderir a esta política e tomar medidas para proteger a segurança da rede.

2. **Autenticação e Criptografia**

   O ponto de acesso corporativo deve ser configurados com WPA2 Enterprise com autenticação EAP-TLS para garantir uma autenticação forte dos usuários com dispositivos da empresa;

   E os pontos de acesso: Dispositivos-Pessoais e Convidados, devem ser configurados para garantir a autenticação forte com WPA2-PSK para todos os usuários;

   A PSK para os APs da política anterior, será disponibilizada pela gerência de TI, que deverá registrar a liberação da senha para cada usuário que necessitar conectar na rede;

   A criptografia AES será utilizada para proteger o tráfego de dados entre os dispositivos e os pontos de acesso Wi-Fi.

3. **Senha**

   Deverá ser configurado senha forte contendo letras, números e caracteres especiais, para cada Ponto de Acesso e para acesso ao servidor AAA.

As senhas deverão ser alteradas seguindo o mesmo padrão de segurança da política anterior, a cada revisão das Políticas de Segurança.

4. **Controle de Acesso:**

O controle de acesso será feito através de configuração do SSID que será oculto para evitar a fácil identificação da rede, que será informado pela gerência de TI;

O SSID será oculto e deverá ser preenchido quando algum colaborador novo e autorizado precisar acessar a rede Wi-Fi;

5. **Controle de Acesso à Recursos Específicos:**

Será configurado ACls no roteador para controlar o tráfego entre as Vlans, permitindo apenas o tráfego necessário e bloqueando tráfego não autorizado como ICMP, TCP e outros;

Também será utilizado as ACLs para controle de recursos sensíveis na rede, como o acesso ao servidor de autenticação EAP.

Desativar todas as portas no switches que não serão utilizadas;

Desabilitar conexão remota nos roteadores e Pontos de Acesso.

6. **Segregação de redes:**

A rede Wi-Fi será segmentada em três VLANs: uma vlan100 para os dispositivos corporativos. vlan200 para os dispositivos pessoais dos funcionários e a vlan300 para convidados;

Será bloqueado todo o tráfego entre VLANs.

7. **Redundância**

Utilizar o modelo de redundância com uso de 3 switches para garantir a qualidade de serviço e evitar a interrupção na rede.

Utiliza-se o STP Spanning Tree Protocol que indicará o melhor caminho para o tráfego da rede.

8. **Configuração de Firewall:**

No momento a rede será inicializada sem um firewall configurado, porém a equipe de TI deverá realizar analisar a possibilidade de implementação na próxima revisão dessa política de segurança;

Um plano de resposta a incidentes será estabelecido para lidar com qualquer violação de segurança de forma rápida e eficaz.

9. **Frequência de banda:**

Será configurado os canais de acordo com o posicionamento físico da rede, e será utilizada a frequência de 2,4 GHz no padrão 802.11n para garantir que todos os dispositivos tenha suporte para acessar a rede Wi-Fi;

Deverá ser configurado canais diferentes e em frequências alternadas em cada Ponto de Acesso, para evitar interferência de sinal;

Deverá ser configurado:

AP-Corporativo: canal e frequência 6 - 2.437GHz,

AP-Dispositivos-Pessoais: 5 - 2.432GHz

AP-Convidados: 1 - 2.412GHz.

10. Conscientização e Treinamento:

Todos os usuários serão treinados regularmente sobre as práticas recomendadas de segurança da rede e a importância da proteção de dados;

A conscientização sobre segurança será promovida por meio de campanhas educacionais e materiais de treinamento.

11. Respostas a incidentes

A equipe de TI juntamente com a equipe de segurança da informação deverá ter um plano de resposta a incidentes antes da rede entrar em funcionamento;

Deverá haver um contato bem alinhado entre as equipes de TI, infra, segurança;

As tarefas a serem executadas pelas equipes na resposta à incidentes são: verificar o status da rede, identificar a causa do problema e restaurar a conectividade.

Deverá ser realizado testes regulares para monitorar e verificar o bom funcionamento da rede.

Deverá ser analisado os logs de tráfego na rede.

12. Atualizações e Manutenção:

Todos os dispositivos corporativos de rede serão mantidos atualizados com os patches de segurança mais recentes e as configurações de segurança adequadas.

Os dispositivos pessoais dos colaboradores deverão também seguir os processos de atualização dos patches de segurança.

As políticas de segurança serão revisadas periodicamente a cada 6 meses para garantir sua eficácia e atualizadas conforme necessário.