Universidade de Itaúna		**Curso:** Ciência da Computação	**Disciplina:** Redes de Computadores II
Professor (a): Adriano Benigno			Ano: 2023
7º Período	Turno: Noite	**CIU:** 82148	Atividade relativa à 3ª Avaliação
Nome: Davi Ventura Cardoso Perdigão			

Projeto de Segurança para Empresa com Setor Financeiro

Objetivo: Implementar estratégias práticas e utilizar tecnologias eficazes para proteger as informações sensíveis em uma empresa com 20 pessoas distribuídas em diferentes setores, relacionados inclusive a pagamentos e recebimentos de valores.

- **Segmentação de Rede:** Implementar servidores dedicados para o setor financeiro, separados dos demais departamentos. Esses servidores podem incluir o servidor de banco de dados financeiro, o servidor de aplicativos financeiros e outros sistemas específicos para a gestão da empresa.

  Uma opção também é utilizar VLANs para criar segmentos lógicos na rede, isolando o setor financeiro dos outros departamentos. Isso pode ser feito por meio de switches gerenciáveis que suportem a criação de VLANs e configuração de regras de tráfego entre elas. Cada VLAN seria designada para um departamento específico.

  Outra abordagem é utilizar redes físicas separadas, com switches dedicados para cada departamento. Nesse caso, o setor financeiro teria seu próprio switch físico e cabos de rede, garantindo a separação física dos outros departamentos.

Para fornecer acesso Wi-Fi para os funcionários, é importante implementar medidas de segurança adequadas. Recomenda-se a criação de uma VLAN separada para a rede Wi-Fi, com autenticação individual para cada usuário. Isso impedirá que dispositivos conectados ao Wi-Fi tenham acesso direto à rede interna, incluindo o setor financeiro. Além disso, é fundamental configurar o Wi-Fi com criptografia forte (como WPA2 ou WPA3) e uma senha robusta. Restringir o acesso apenas a dispositivos autorizados e periodicamente revisar as configurações de segurança do Wi-Fi são práticas recomendadas para garantir a segurança da rede sem fio.

- **Firewall de Próxima Geração:** Implementar um firewall de próxima geração que combine recursos de firewall tradicional com recursos avançados de segurança. Esse firewall deve ser capaz de inspecionar o tráfego em camadas mais profundas, como análise de conteúdo, aplicação e comportamento do tráfego, para identificar ameaças avançadas.

- **Política de Backup:** Implementar uma política de backup prática que envolva realizar backups diários completos dos dados (principalmente os financeiros) e armazená-los em dispositivos externos, como unidades de disco rígido criptografadas. Além disso, é importante realizar testes regulares de restauração dos backups, implementar uma rotação de mídia para diversificar o armazenamento, considerar o armazenamento em nuvem como uma medida adicional de proteção, definir uma política de retenção de dados e monitorar e manter regularmente os dispositivos de backup. Essa política de backup garante a proteção dos dados sensíveis e possibilita a recuperação eficiente em caso de perda ou corrupção dos dados.

- **Prevenção de Intrusões (IPS):** Utilizar um sistema de prevenção de intrusões para monitorar o tráfego de rede em tempo real e detectar atividades maliciosas. O IPS deve ser configurado para bloquear automaticamente qualquer tráfego suspeito ou malicioso, minimizando o impacto de ataques e reduzindo a necessidade de intervenção humana.

- **Detecção de Intrusões (IDS):** Implementar um sistema de detecção de intrusões para complementar as defesas de segurança. O IDS analisa o tráfego de rede em busca de padrões de comportamento e assinaturas conhecidas de ataques. Ele emitirá alertas em tempo real para que a equipe de segurança possa investigar e responder a incidentes de forma rápida.

- **Autenticação:** Adotar a autenticação multifator para garantir que apenas usuários autorizados tenham acesso aos sistemas financeiros. Isso envolve o uso de senha, token ou dispositivo móvel, e até biometria. Isso reduz significativamente o risco de acesso não autorizado.

- **Monitoramento de Log e Eventos:** Implementar um sistema de monitoramento centralizado que registre e analise os logs de eventos de segurança em tempo real. Isso permitirá a detecção precoce de atividades suspeitas e ajudará na investigação de incidentes.

- **Conscientização e Treinamento em Segurança:** Promover treinamentos regulares de conscientização em segurança da informação para todos os funcionários, com foco especial para o setor financeiro. Isso inclui ensinar boas práticas de segurança, como não abrir e-mails suspeitos, criar senhas fortes e atualizá-las regularmente, além de fornecer orientações sobre a proteção adequada de informações confidenciais.

- **Atualizações e Patches:** Manter todos os sistemas e softwares atualizados com as últimas atualizações e patches de segurança. Isso é fundamental para corrigir vulnerabilidades conhecidas e garantir que as soluções de segurança estejam efetivamente protegendo a rede e os dados financeiros.