

UNIVERSIDADE RUY BARBOSA - WYDEN

ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

Gabriella Mizrach Benevides

Desafio: Estudo de Caso

SALVADOR

[2025]

Estudo de Caso: Escritório de Advocacia Mizrach & Associados.

Nome Empresarial: Escritório de Advocacia Mizrach & Associados

Ramo de Atuação: Direito Civil, Empresarial e Processos de Imigração/Cidadania.

Abrangência: Nacional (Sede em Salvador/BA), com atendimento remoto a clientes no exterior.

Estrutura e Porte:

- **Classificação:** Empresa de Pequeno Porte.
- **Quadro de Funcionários (Total 18):**
 - 04 Sócios Advogados (Diretoria).
 - 08 Advogados Associados.
 - 04 Estagiários de Direito (Rotativos).
 - 02 Administrativo/Financeiro.
- **O Cenário (Diagnóstico Inicial):**

1. Avaliação do Cenário Atual :

Ambiente: 8 computadores rodando Windows 10 Home, sem domínio.

Políticas de Senha: Inexistentes. Funcionários usam senhas como "123456" ou o nome da empresa, e nunca as trocam.

Antivírus: Apenas versões gratuitas ou desatualizadas.

Backup: Feito manualmente uma vez por mês em um HD externo que fica conectado o tempo todo no servidor.

Firewall: Padrão, sem regras de bloqueio de portas perigosas.

Fator Humano: Nenhum treinamento. Funcionários clicam em links de e-mails suspeitos e compartilham a senha do Wi-Fi com clientes.

2. Identificação de Vulnerabilidades:

Risco Crítico: Alta probabilidade de infecção por Ransomware devido ao RDP aberto e falta de backup offline.

Vazamento de Dados: Arquivos confidenciais de clientes acessíveis a qualquer estagiário.

Roubo Físico: Se um notebook for roubado, os dados estão legíveis.

Acesso aos computadores ou logins de Usuário: Os usuários utilizam senhas fracas e nunca as alteram, facilitando ataques de força bruta ou adivinhação.

Rede vulnerável: versões gratuitas e desatualizadas. Não há monitoramento centralizado, deixando a rede vulnerável a novas variantes de malware

Falta de conscientização (Treinamento): Os funcionários nunca receberam treinamento sobre segurança. Há histórico de cliques em links suspeitos e compartilhamento de senhas via post-it nos monitores.

- **As Soluções Propostas:**

3. Proposta de Melhorias:

Ação 1: Hardening de Identidade:

Solução: Implementar política obrigatória de 8 caracteres + complexidade.

Impacto: Elimina ataques de força bruta simples.

Ação 2: Segregação de Dados:

Solução: Criar grupos de usuários ("Financeiro", "Jurídico") e aplicar ACLs. O estagiário não acessa mais a pasta do chefe.

Impacto: Implementa o "Princípio do Privilégio Mínimo", garantindo que dados sigilosos e financeiros sejam visíveis apenas aos sócios e gestores autorizados.

Ação 3: Proteção de Dados (BitLocker):

Solução: Ativar Criptografia de Disco em todos os notebooks móveis.

Impacto: Em caso de roubo do equipamento, os dados permanecem inacessíveis.

Ação 4: Backup:

Solução: Automatizar backup diário para nuvem (ex: OneDrive/Azure) e manter uma cópia física desconectada.

Impacto: A cópia em nuvem assegura a continuidade do negócio em caso de desastres físicos (incêndio ou roubo), permitindo restauração rápida de qualquer lugar.

Ação 5: Proteção de Endpoint:

Solução: Padronização do Microsoft Defender em todas as estações, configurando atualização automática diária e bloqueio de execução de scripts desconhecidos.

Impacto: Garante proteção em tempo real e imunidade contra novas ameaças sem depender da memória ou ação do usuário.

Impacto: O bloqueio de scripts desconhecidos impede que malwares silenciosos sejam executados automaticamente ao abrir arquivos ou pendrives infectados.

Ação 6: Fator Humano:

Solução: Realização de workshop semestral sobre Engenharia Social e Phishing.

Impacto: Redução drástica da superfície de ataque via e-mail, diminuindo o risco de sequestro de dados por Ransomware iniciado por cliques indevidos.

- **Conclusão:** O diagnóstico evidencia que o escritório operava em alto risco de perda de dados. A implementação deste plano de ação corrige as vulnerabilidades estruturais e comportamentais, alinhando a empresa aos requisitos mínimos de segurança e confidencialidade exigidos no setor jurídico.