Proposta Técnica: Projeto de Rede Segura para "Advocacia Segura & Associados"

Autor: Flaviano Kiffer Teodoro

Data: 28/07/2025

Sumário Executivo

Este documento apresenta a proposta técnica para a reestruturação da rede corporativa da "Advocacia Segura & Associados". O objetivo principal é proteger a confidencialidade e integridade das informações dos clientes e dos dados processuais, que são o ativo mais crítico da organização. A solução proposta baseia-se numa arquitetura de defesa em profundidade, implementando uma segmentação rigorosa da rede através de VLANs para isolar departamentos, sistemas de prevenção contra fugas de dados (DLP) e acesso remoto seguro via VPN com autenticação multifator (MFA). O plano de ação foca-se em medidas de alto impacto para mitigar os riscos de acessos não autorizados e garantir a conformidade com os regulamentos de proteção de dados.

1. Objetivo

Projetar e implementar uma infraestrutura de rede que garanta a máxima segurança para as informações sigilosas dos clientes, assegurando o sigilo profissional advogado-cliente e a continuidade das operações do escritório.

2. Escopo

A análise e a proposta abrangem a rede da matriz, que comporta 75 utilizadores, divididos nos seguintes setores: Sócios, Advogados, Estagiários, Administrativo e TI. O escopo inclui a rede local, o acesso à Internet, as políticas de acesso remoto e a segurança dos servidores internos.

3. Metodologia

A arquitetura foi desenhada com base em frameworks de segurança reconhecidos no mercado, visando uma abordagem proativa contra ameaças:

- **Análise de Ameaças:** Utilizamos os modelos Cyber Kill Chain e MITRE ATT&CK para antecipar as táticas, técnicas e procedimentos (TTPs) que poderiam ser utilizados contra um ambiente jurídico.
- **Segmentação de Rede:** O conceito de subnetting será a base para dividir a rede em zonas de segurança, isolando sistemas e utilizadores para conter possíveis incidentes.
- **Mapeamento de Serviços:** A fase inicial consistirá num footprinting ativo para mapear todas as portas e serviços ativos na rede atual, utilizando ferramentas como Nmap e RustScan para identificar a superfície de ataque.

4. Diagrama da Rede Proposta

Descrição do Diagrama:

- **Perímetro:** A ligação à Internet é protegida por uma Firewall, que atua como primeira linha de defesa.
- **VLANs por Nível de Acesso:** A rede interna será segmentada nas seguintes VLANs:
    - **VLAN Sócios:** Acesso irrestrito.
    - **VLAN Advogados:** Acesso amplo aos sistemas de processos e ficheiros de clientes.
    - **VLAN Estagiários:** Acesso limitado aos sistemas necessários para as suas tarefas, com regras de firewall mais restritivas para impedir o acesso a áreas sensíveis.
    - **VLAN Administrativo:** Acesso aos sistemas financeiros e de gestão.
    - **VLAN Servidores:** Zona de alta segurança onde residem os servidores de ficheiros (SMB) e bases de dados, com acesso permitido apenas a partir de VLANs autorizadas e em portas específicas.
- **Controle de Tráfego:** Todo o tráfego entre as VLANs passará obrigatoriamente pela firewall, que aplicará regras de acesso, permitindo apenas a comunicação estritamente necessária.

5. Proposta Técnica (Diagnóstico)

A estratégia foca-se em proteger o ciclo de vida da informação dentro do escritório.

5.1. Prevenção Contra Fuga de Dados (DLP)

Dado o alto grau de sensibilidade dos documentos, será implementada uma solução de DLP. Esta tecnologia monitoriza os dados em trânsito e em repouso, prevenindo que documentos confidenciais (ex: petições, contratos) sejam enviados para fora da rede por e-mail, pen drives ou serviços na nuvem não autorizados.

5.2. Hardening de Serviços Internos

Serviços internos de partilha de ficheiros e gestão de rede são alvos frequentes.

- **SMB (Server Message Block):** As configurações dos servidores de ficheiros serão revistas para eliminar o risco de acesso anónimo (Null Sessions) e garantir que as partilhas (shares) tenham permissões restritivas, evitando o acesso indevido a pastas de casos.
- **SNMP (Simple Network Management Protocol):** As community strings padrão ("public", "private") em switches e routers serão alteradas. A versão 3 do SNMP (SNMPv3), que oferece encriptação, será implementada para evitar a fuga de informações da infraestrutura.

5.3. Gestão de Vulnerabilidades

Será estabelecido um ciclo contínuo de gestão de vulnerabilidades, utilizando um scanner como o OpenVAS. As varreduras automatizadas irão identificar falhas de segurança

(CVEs), que serão classificadas por criticidade (CVSS) e tratadas de forma prioritária, começando sempre pelas mais críticas.

5.4. Análise e Monitorização de Tráfego

Para garantir a visibilidade sobre a rede, implementaremos:

- **Análise de Pacotes:** Uso do **Wireshark** para análise forense e diagnóstico de problemas de rede, permitindo uma investigação profunda do tráfego em caso de atividades suspeitas.
- **Logs Centralizados (SIEM):** Todos os logs de firewall, servidores e sistemas de segurança serão centralizados numa plataforma SIEM para correlação e deteção de padrões anômalos que possam indicar um ataque em andamento.

6. Recomendações

- **Implementar segmentação granular com VLANs:** Isolar os estagiários e o setor administrativo das redes dos advogados e sócios.
- **Adotar uma solução de DLP:** É fundamental para proteger a propriedade intelectual e os dados dos clientes.
- **Exigir MFA para todo o acesso remoto:** O acesso à VPN e ao e-mail corporativo fora do escritório deve ser protegido com MFA.
- **Realizar hardening imediato dos servidores de ficheiros:** Corrigir permissões em pastas partilhadas (SMB) é uma medida de baixo custo e alto impacto.
- **Formação focada:** Conduzir formação de segurança focada no manuseamento seguro de documentos digitais e na identificação de e-mails de *spear phishing*.

7. Plano de Ação (Modelo 80/20)

Ação	Impacto na Segurança	Facilidade de Implementação	Prioridade
Habilitar MFA para VPN e E-mail	**Alto**	Alta	**Alta**
Rever e corrigir permissões dos servidores de ficheiros (SMB)	**Alto**	Média	**Alta**
Implementar VLANs para Sócios, Advogados e Estagiários	Alto	Média	Média

Alterar senhas padrão de todos os equipamentos de rede (SNMP)	Médio	Alta	Média
Implementar a solução de DLP	Alto	Baixa	Baixa

8. Conclusão

A segurança da informação num ambiente jurídico não é um custo, mas um pilar para a confiança do cliente e para a reputação do escritório. A implementação desta arquitetura de rede segura irá mitigar os riscos de forma significativa, transformando a tecnologia numa aliada na proteção do sigilo profissional e na garantia da continuidade dos negócios da "Advocacia Segura & Associados".