TRABALHO / RESOLUÇÃO:

Introdução:

O presente relatório tem como objetivo analisar a arquitetura de rede de uma organização de média dimensão, identificando vulnerabilidades de segurança e propondo controlos adequados para mitigar os riscos identificados. Pretende-se assim propor medidas que reforcem a confidencialidade, integridade e disponibilidade dos dados, concluindo com a demonstração de uma solução criptográfica básica.

Relatório dividido em cinco partes:

- Primeira parte: Análise do sistema de rede e verificação de possíveis pontos de segurança a melhorar.
- Segunda parte: Listagem de ameaças, categorização e listagem de possíveis ataques que possam ser efetuados. Elaboração de dois exemplos de diagramas de árvores de ataque.
- Terceira parte: Proposta de reforço de segurança da rede e explicação do seu relacionamento com as falhas encontradas.
- Quarta parte: Explicação da importância da encriptação de dados para a segurança da rede e implementação com breve explicação de uma possível solução baseada em AES (encriptação simétrica) e RSA (encriptação assimétrica).
- Quinta parte: Explicação da resolução das falhas de segurança identificadas e discussão da importância da manutenção da segurança no presente e futuro.

1. - Análise de Rede

A análise da arquitetura de rede revela uma infraestrutura com dois meios de ligação: LAN (rede com fios) e WLAN (rede sem fios). Os dispositivos móveis como portáteis, smartphones e tablets conectam-se através de Wi-Fi (WLAN), enquanto os dispositivos fixos como desktops e impressoras utilizam ligações por cabo (LAN). A WLAN funciona como extensão da LAN, oferecendo mobilidade aos utilizadores. A análise da superfície de ataque identifica múltiplos pontos de exposição que aumentam significativamente o risco de comprometimento da rede.

Vulnerabilidade nº1 - Falta de Segmentação entre WLAN e LAN:

Verifica-se que não existe segmentação entre as duas redes, criando uma vulnerabilidade crítica. As redes WLAN são inerentemente menos seguras devido à facilidade de comprometimento de dispositivos móveis, permitindo que um atacante execute movimentos laterais da WLAN para a LAN, acedendo a recursos sensíveis da rede interna.

Vulnerabilidade nº2 - Posicionamento incorreto do IDS/IPS:

Ambas as redes conectam-se a um Switch com duas saídas: uma para o IDS/IPS (sistema de deteção/prevenção de intrusões) e outra para a DMZ (zona desmilitarizada). Identifica-se uma falha crítica nesta arquitetura, pois o IDS/IPS está posicionado de modo paralelo ao tráfego de rede, funcionando como dispositivo terminal, quando deveria estar posicionado "in-line" entre a Firewall e o Switch. Desta forma, o IDS/IPS não monitoriza o tráfego que entra na rede, permitindo a entrada de tráfego malicioso que compromete a segurança do sistema.

Vulnerabilidade nº3 - Database Server na DMZ:

Aqui existe outro comprometimento grave, o Database Server está localizado na DMZ, exposto juntamente com o WebServer e o Email Server. Como a DMZ é a zona mais exposta a ataques externos, colocar o Database Server (que contém dados sensíveis) nesta área viola o princípio da Defesa em Profundidade. Um atacante que comprometa o WebServer pode aceder diretamente ao Database Server sem atravessar camadas adicionais de segurança. O Database Server deveria situar-se na rede LAN interna, protegido por Firewall.

Vulnerabilidade nº4 - Exposição do WebServer e Email Server:

O WebServer e o Email Server, localizados na DMZ, ficam adicionalmente comprometidos devido ao mau posicionamento do IDS/IPS, que não efetua a filtragem adequada dos dados que entram na rede, aumentando a possibilidade de acessos ilegítimos.

Vulnerabilidade nº5 - Ponto Único de Falha (Firewall Única):

O Switch está ligado a uma única Firewall, responsável por toda a defesa do perímetro da rede. Esta configuração cria um ponto único de falha: se a Firewall for mal configurada, comprometida ou sofrer uma avaria de hardware, toda a rede fica exposta.

2. - Listagem de Ameaças por Categorias

Componentes	Tipo de Impacto (CIA)	Ameaça	Nível de Risco
Falta de Segmentação na LAN e WLAN	Confidencialidade Integridade Disponibilidade	Infeção por ransomware na rede interna Sniffing (espionagem de rede)	Médio
Database Server	Confidencialidade Integridade	Roubo de informação sensível Destruição de dados Escalada de privilégios	Alto
WebServer e EmailServer Expostos	Integridade Disponibilidade	Ataque de DoS/SQL Injection Servidores usados para spam ou phishing	Médio
Posicionamento incorreto do IDS/IPS	Integridade Disponibilidade	Ataques de DoS Infeção por malwares e SQL Injection	Alto
Firewall única	Disponibilidade	Ataque DoS ou falha de hardware	Médio

Diagrama de Árvore de Ataque 1:

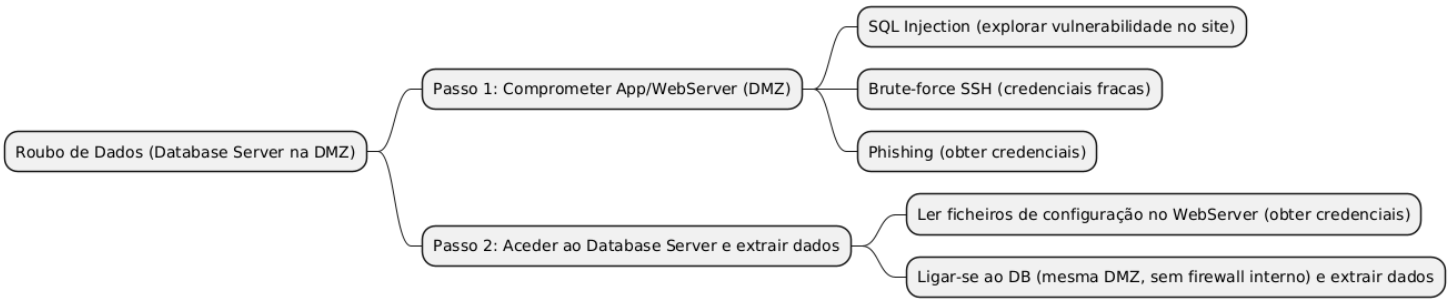

Diagrama de Árvore de Ataque — Objetivo: Roubo de Dados (Database Server na DMZ):

Raiz — Roubo de Dados (Database Server)

- Passo 1 — Comprometer App/WebServer (DMZ)
  - Vetor 1: Explorar vulnerabilidade no site → SQL Injection.
  - Vetor 2: Acesso por SSH via brute-force com credenciais fracas.
  - Vetor 3: Credenciais obtidas por phishing.
- Passo 2 — Aceder à Database Server e extrair dados
  - Vetor 1: Ler ficheiros de configuração no WebServer (obter credenciais).

- Vetor 2: Ligar-se ao Database Server (mesma DMZ, ausência de firewall interno) e extrair informação.

Diagrama de Árvore de Ataque 2:

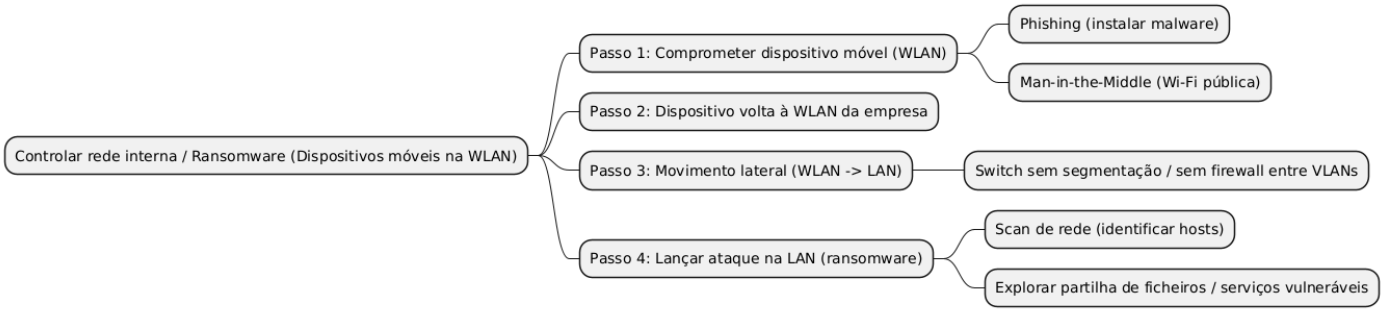

Diagrama de Árvore de Ataque — Objetivo: Controlar a rede interna / Execução de ransomware (origem: dispositivos móveis na WLAN)

Raiz — Controlar rede interna / Executar ransomware

- Passo 1 — Comprometer dispositivo móvel (WLAN)
  - Vetor 1: Phishing (clique em link malicioso, seguido de instalação de malware).
  - Vetor 2: Man-in-the-Middle (vítima em Wi-Fi pública, seguido de injecção de payload).
- Passo 2 — Aguardar a ligação do dispositivo comprometido à WLAN da empresa.
- Passo 3 — Movimento lateral WLAN para LAN
  - Possível devido à falta de firewall entre VLANs.
- Passo 4 — Lançar ataque contra a LAN
  - Vetor 1: Scan de rede para identificar hosts e servidores internos.
  - Vetor 2: Explorar vulnerabilidades de partilha de ficheiros / serviços expostos - propagar do ransomware.

3. – Proposta de controlo de segurança:

- **Controlo proposto nº 1 – Segmentação e isolamento interno**:

Vulnerabilidades:

- Comunicação direta entre LAN e WLAN sem firewall interna.
- Falta de filtragem e isolamento de tráfego interno.

Controlos aplicados:

- Criação de VLANs para segmentar redes internas (LAN/WLAN) e definir controlos de confiança.
- Implementação da firewall interna com regras ACL entre segmentos.

Justificação:

- Cria separação lógica entre utilizadores e servidores críticos, impedindo movimento lateral de ataques.
- Reduz impacto de infeções ou acessos indevidos dentro da organização.
- Reforça Confidencialidade e Integridade, aplicando o princípio da Defesa em Profundidade.

- **Controlo proposto nº 2 – Monitorização contínua e proteção do perímetro da rede**:

Vulnerabilidades:

- Ausência de inspeção adequada do tráfego na DMZ.
- Falta de deteção precoce de ameaças externas.

Controlos aplicados:

- Instalação de um WAF (Web Application Firewall) para filtrar tráfego HTTP/S e bloquear SQL Injections.
- Colocação do IDS/IPS em modo in-line e atualizações regulares dos sistemas.

Justificação:

- Garante monitorização ativa e bloqueio de tráfego malicioso na fronteira da rede.
- Melhora a capacidade de resposta a incidentes e reduz o tempo de exposição.
- Reforça Confidencialidade e Integridade dos sistemas na DMZ.

- **Controlo proposto nº 3 – Autenticação Forte e Defesa Ativa:**

Vulnerabilidades:

- Acesso indevido por credenciais comprometidas.
- Indisponibilidade devido a falha humana ou elétrica.

Controlos aplicados:

- Implementação de MFA (autenticação multifator) para acessos administrativos e VPN.
- Formação de sensibilização em cibersegurança e instalação de UPS para redundância elétrica.

Justificação:

- MFA reduz o risco de phishing e acesso não autorizado.
- Formação tenta garantir a utilização segura dos sistemas e reação adequada a incidentes.
- UPS assegura continuidade e disponibilidade em caso de falha de energia.

Controlos Complementares Recomendados:

- Gestão de Credenciais: Implementação de política de passwords fortes (mínimo 12 caracteres misto com complexidade) e renovação trimestral.
- Proteção contra Malware: Antivírus com atualização automática e scanning em tempo real.
- Redundância Elétrica: UPS (Uninterruptible Power Supply) para servidores críticos, garantindo 30 minutos de autonomia mínima.
- Atualizações de Segurança: Política de patch management com atualizações críticas aplicadas em 48h e não-críticas mensalmente.
- Controlo de Acesso Físico: Restrição de acesso físico à sala de servidores com cartões de proximidade e registo de acessos.
- Plano de Contingência: Disaster Recovery Plan (DRP) com backups diários incrementais e semanais completos, armazenados off-site.

4. – Implementação de solução criptográfica:

Para proteger os dados da empresa passam pela Internet vai ser necessário combinar velocidade com segurança. Ou seja, o sistema de proteção não pode ser lento e tem de ser seguro pois lida com dados sensíveis. Como obter a proteção perfeita é impossível, é ideal escolher algo híbrido, juntando a velocidade à segurança.

4.1 - A encriptação simétrica (AES) é mais rápida, porém como apenas existe uma única chave de encriptação, pode ser acessível a possíveis intrusos ficando eles com o poder de aceder a informação sensível.

 # Código em Python - AES-GCM (simétrico)

```
from cryptography.hazmat.primitives.ciphers.aead import AESGCM
import os

key = AESGCM.generate_key(bit_length=256)

aes = AESGCM(key)

nonce = os.urandom(12)

ct = aes.encrypt(nonce, b"dados confidenciais", b"metadados")

pt = aes.decrypt(nonce, ct, b"metadados")
```

Vantagens:

- Velocidade: Computacionalmente muito rápida e com baixo impacto na performance.
- Segurança: Chaves mais curtas, para o mesmo tipo de segurança que na encriptação assimétrica.
- Eficiência: Simplicidade do algoritmo de implementação.

Desvantagens:

- Gestão de Chaves: Não é totalmente segura a forma de compartilhar as chaves.
- Sistema: Requer um canal seguro para a troca de chaves sem comprometer a segurança.

4.2 - A encriptação assimétrica (RSA) é mais segura, porém com a segurança peca-se na velocidade. Sendo esta encriptação feita através de uma chave privada e uma chave pública.

 # Código em Python - RSA-OAEP (assimétrico):

```
from cryptography.hazmat.primitives.asymmetric import rsa, padding

from cryptography.hazmat.primitives import hashes

priv = rsa.generate_private_key(public_exponent=65537, key_size=2048)

pub = priv.public_key()

msg = b"chave AES"

ct = pub.encrypt(msg, padding.OAEP(mgf=padding.MGF1(hashes.SHA256()),
algorithm=hashes.SHA256(), label=None))
```

pt = priv.decrypt(ct, padding.OAEP(mgf=padding.MGF1(hashes.SHA256()), algorithm=hashes.SHA256(), label=None))

Vantagens:

- Gestão de Chaves: Resolve o problema da encriptação AES, sendo que o Cliente só precisa da chave pública para enviar os dados ao servidor.
- Autenticação: Permite comprovar dados e passwords.

Desvantagens:

- Velocidade: É bastante lento, especialmente para tráfego volumoso.

4.3 - A solução híbrida usa a encriptação assimétrica (RSA) para resolver o problema da partilha de chaves da encriptação simétrica (AES). O que acontece na prática é que são geradas as chaves pública e privadas pela encriptação RSA e após isso passa-se à encriptação AES para encriptar e desincriptar dados da mensagem. Sucintamente, a encriptação AES é usada pela rapidez e a encriptação RSA protege a chave AES.

 # Código em Python - Esquema híbrido (AES + RSA):

```
from cryptography.hazmat.primitives.ciphers.aead import AESGCM
from cryptography.hazmat.primitives.asymmetric import rsa, padding
from cryptography.hazmat.primitives import hashes

import os

# Gerar chaves

priv = rsa.generate_private_key(public_exponent=65537, key_size=2048)

pub = priv.public_key()

session_key = AESGCM.generate_key(bit_length=256)

# Encriptar dados e chave

aes = AESGCM(session_key)

nonce = os.urandom(12)

ct = aes.encrypt(nonce, b"mensagem", None)

enc_key = pub.encrypt(session_key,
padding.OAEP(mgf=padding.MGF1(hashes.SHA256()), algorithm=hashes.SHA256(),
label=None))

# Servidor: decifra chave e dados
```

```
dec_key = priv.decrypt(enc_key, padding.OAEP(mgf=padding.MGF1(hashes.SHA256()),
algorithm=hashes.SHA256(), label=None))

pt = AESGCM(dec_key).decrypt(nonce, ct, None)
```

5. - Reflexão sobre a estratégia de segurança:

Resumo das Vulnerabilidades Resolvidas:

A análise identificou cinco vulnerabilidades críticas que foram apontadas: 1 - Falta de segmentação WLAN/LAN, resolvida com VLANs; 2 - Database Server exposto na DMZ, movido para a LAN interna; 3 - IDS/IPS mal posicionado, reconfigurado em modo in-line; 4 - servidores públicos sem proteções específicas, protegidos com WAF e Gateway Anti-Spam; 5 - Firewall única, complementada com Firewall interna adicional.

Eficácia da Estratégia:

A estratégia reduz significativamente os riscos, aplicando sistematicamente os princípios de Defesa em Profundidade, Privilégio Mínimo e Separação de Privilégios. A segmentação de rede impede movimentos laterais, enquanto a proteção do Database Server elimina a vulnerabilidade mais crítica. A solução criptográfica híbrida (AES+RSA) protege o tráfego de dados, garantindo confidencialidade e integridade das comunicações.

Preocupações Remanescentes:

Permanecem riscos não completamente endereçados: ameaças internas (insider threats), engenharia social, phishing, DDoS de grande escala e falta de políticas formais de backup. A eficácia das medidas depende criticamente da configuração correta e manutenção contínua.

Recomendações Futuras:

- Curto prazo: implementar autenticação multifator (MFA), formação em cibersegurança para colaboradores, e backups automáticos off-site.
- Médio prazo: Testes de penetração periódicos.
- Longo prazo: Evolução para arquitetura Zero Trust.

Conclusão:

A estratégia proposta transforma uma arquitetura vulnerável numa infraestrutura defensível, estabelecendo uma base sólida que, combinada com as melhorias recomendadas e cultura de segurança organizacional, permitirá proteger eficazmente os ativos digitais da

organização no contexto de ameaças em constante evolução, sendo que as medidas tomadas consolidam uma cultura de segurança e demonstram a aplicação prática dos princípios CIA.

Referências Bibliográficas:

- Stallings, W., Brown, L. (2025). ComputerSecurity: Principles and Practice (5th Edition).Pearson.
- OWASP Foundation (2025). OWASP Top Ten Web Application Security Risks: https://owasp.org/www-project-top-ten/
- Shostack, A. (2014). Threat Modeling: Designing for Security. Wiley.
- NCSC (2025). Using Attack Trees to Understand Cyber Security Risk. National Cyber Security Centre: https://www.ncsc.gov.uk/collection/risk-management/
- Practical DevSecOps (2025). Threat Modeling Using Attack Trees: https://www.practical-devsecops.com/threat-modeling- using-attack-trees/
- Python Cryptography Documentation (2024). Hazmat Primitives: https://cryptography.io/en/latest/
- GeeksforGeeks (2025). RSAAlgorithm in Cryptography: https://www.geeksforgeeks.org/rsa-algorithm-cryptography/
- Real Python (2025). Python Cryptography: Encrypt Data with AES https://realpython.com/python-cryptography/
- Stack Overflow (2025): https://stackoverflow.com/questions/12524994/
- Mamede, H. S. (2025). Instruções de realização do efolio A - Segurança em Redes e Computadores, Universidade Aberta.
- Materiais da UC: Slides PDF e fórum da UC: Segurança em Redes e Computadores (21181).
- Claude 3.5 Sonnet. Consultado em Novembro de 2025 para esclarecimento de conceitos de segurança de redes e revisão de código Python.