Análise das consequências das vulnerabilidades em redes de dados e desenvolvimento de estratégias de mitigação: estudo de caso

Analysis of the consequences of vulnerabilities in data networks and development of mitigation strategies: case study

Pedro Mbala Diekutumena*

dm211625@aluno.ugs.ed.ao

*Universidade Gregório Semedo (Angola)

Recibido: 25/10/2024-Aceptado: 30/12/2024.
Correspondencia: dm211625@aluno.ugs.ed.ao

Resumo

O estudo proposto tem como foco principal a análise das consequências das vulnerabilidades em redes de dados, com ênfase no contexto específico do ISPM, e o desenvolvimento de estratégias eficazes de mitigação. A segurança da informação é um aspecto fundamental em ambientes académicos e institucionais, onde a integridade, confidencialidade e disponibilidade dos dados são essenciais. A pesquisa abordará as principais vulnerabilidades identificadas nas redes de dados do ISPM, os potenciais impactos negativos decorrentes dessas vulnerabilidades e as estratégias recomendadas para mitigar os riscos associados. Serão consideradas as melhores práticas de segurança cibernética, políticas de acesso e controle de dados, bem como medidas preventivas e correctivas para fortalecer a segurança da informação no ISPM. O estudo visa contribuir significativamente para a protecção dos dados institucionais, promovendo a conscientização sobre a importância da segurança cibernética e fornecendo orientações práticas para a implementação de medidas de protecção eficazes. Espera-se que os resultados desta pesquisa sirvam como base sólida para a melhoria contínua da segurança da informação no ISPM e possam ser aplicados em outros contextos similares.

Palavras-chave: Vulnerabilidades em redes de dados, Segurança da informação, Análise de riscos; Estratégias de mitigação e ISPM.

Abstract

The proposed study focuses primarily on analyzing the consequences of vulnerabilities in data networks, with an emphasis on the specific context of ISPM, and developing effective mitigation strategies. Information security is a fundamental aspect in academic and institutional environments, where data integrity, confidentiality, and availability are essential. The research will address the main vulnerabilities identified in ISPM data networks, the potential negative impacts arising from these vulnerabilities, and the recommended strategies to mitigate the associated risks. Cybersecurity best practices, data access and control policies, as well as preventive and corrective measures to strengthen information security in ISPM will be considered. The study aims to contribute significantly to the protection of institutional data by promoting awareness of the importance of cybersecurity and providing practical guidance for the implementation of effective protection measures. It is expected that the results of this research will serve as a solid basis for the continuous improvement of information security in ISPM and can be applied in other similar contexts.

Keywords*: Vulnerabilities in data networks, Information security, Risk analysis; Mitigation strategies and ISPM*

Cómo citar
Mbala Diekutumena, P. (2025). Análise das consequências das vulnerabilidades em redes de dados e desenvolvimento de estratégias de mitigação: estudo de caso. *GADE: Revista Científica*, *4*(7), 124-138. Recuperado a partir de https://revista.redgade.com/index.php/Gade/article/view/549

INTRODUÇÃO

A dependência das redes de computadores, da Internet e à inclusão digital, está cada vez mais notável para o funcionamento e vida das instituições em todas as áreas de actuação tornando

Entretanto, segurança deve ser baseada em testes regulares que identifiquem e solucionem vulnerabilidades, tornando os sistemas mais robustos e confiáveis. Nesse cenário, os pentests (testes de penetração) se destacam como um método crucial de avaliação de vulnerabilidades, sendo o foco principal deste trabalho.

No Instituto Superior Politécnico Maravilha (ISPM), a segurança das redes de dados tornou-se uma prioridade vital para proteger informações sensíveis, garantir a continuidade dos serviços e manter a confiança no sistema de informação.

Este estudo tem como objetivo analisar as consequências das vulnerabilidades em redes de dados e desenvolver estratégias de mitigação, com especial atenção ao ambiente do ISPM.

Propõe-se uma abordagem metodológica focada na Avaliação de Vulnerabilidades e Testes de Penetração (VAPT) para avaliar as vulnerabilidades nas redes do ISPM. A análise detalhada permitirá identificar as principais fraquezas da infraestrutura de rede e propor soluções para mitigar os riscos encontrados.

Com este estudo de caso, busca-se contribuir para o fortalecimento da segurança cibernética no ISPM e oferecer uma visão valiosos para a comunidade acadêmica e profissional sobre a gestão de vulnerabilidades em redes de dados.

Justificativa

A análise das consequências potenciais das vulnerabilidades em redes de dados no ISPM abrange desde a interrupção de serviços essenciais até o comprometimento da integridade e confidencialidade dos dados institucionais. Compreender esses impactos é fundamental para desenvolver estratégias de mitigação que não apenas protejam a infra-estrutura digital da instituição, mas também promovam um ambiente seguro e confiável para todos os usuários.

Ao realizar um estudo de caso específico no ISPM, este trabalho não só identificará as vulnerabilidades existentes e potenciais, mas também

analisará as práticas de segurança actualmente implementadas. A partir dessa análise, serão propostas estratégias personalizadas de mitigação que considerem as necessidades e características específicas da instituição

Formulação de problema

Como as vulnerabilidades da Rede de Dados Impactam o sistema de segurança de Informação do Instituto Superior Politécnico Maravilha de Benguela?

Objectivo Geral

Analisar as principais consequências de vulnerabilidades presentes da Rede de Dados do Instituto Superior Politécnico Maravilha de Benguela.

Objectivos Específicos

1. Conhecer o estado actual da seguraça de Informação da Rede de Dados do ISPM.
2. Revisar literaturas sobre segurança e vulnerabilidade em rede de dados e estratégias de mitigação das mesmas
3. Identificar as principais vulnerabilidades presentes na rede de dados do Instituto Superior Politécnico Maravilha (ISPM)-Benguela
4. Avaliar o impacto das vulnerabilidades identificadas na rede de dados do ISPM-Benguela.
5. Desenvolver estratégias de mitigação das vulnerabilidades identificadas na rede de dados do Instituto Superior Politécnico Maravilha (ISPM)-Benguela

Hipóteses

A implementação de estratégia de mitigação adequadas pode reduzir significativamente os riscos associados às vulnerabilidades da rede de dados do Instituto Superior Politécnico Maravilha de Benguela

Segurança da Informação

A segurança da informação, é a proteção de informações importantes de uma organização, arquivos e dados digitais, documentos em papel, mídia física, até mesmo a fala humana contra acessos, divulgações, alterações ou usos não autorizados. (IBM, 2024)

Importância da Segurança da Informação

A segurança da informação é vital para garantir a confidencialidade, integridade e disponibilidade dos dados (Ciszek & Pfleeger, 2015). Esses três pilares são conhecidos como a tríade CIA (Confidentiality, Integrity, Availability).

Segurança de rede de dados

As redes de dados são o alicerce das comunicações modernas, permitindo a transferência de informações entre computadores, dispositivos móveis e outros sistemas. A segurança de rede visa proteger esses dados em trânsito contra interceptações e ataques (Stallings, 2017).

Principais Ameaças às Redes de Dados

As redes de dados estão sujeitas a diversas ameaças, que incluem desde malware e ransomware até ataques de negação de serviço (DDoS) e interceptação de dados. Ataques de engenharia social, como phishing, também são comuns e podem comprometer a segurança das redes ao explorar vulnerabilidades humanas (Symantec, 2019).

Políticas de Segurança de Rede

A implementação de políticas de segurança da informação é fundamental para a protecção dos dados. Essas políticas definem regras e directrizes sobre como as informações devem ser gerenciadas e protegidas (ISO/IEC 27002, 2013

Pentest

Pentest vem da abreviação de Penetration Test (Literal, Teste de Penetração) mas também é conhecido como Teste de Intrusão, para fazer a detecção minuciosa com técnicas utilizadas por hackers éticos. Esses testes de intrusão visam encontrar possíveis vulnerabilidades em um sistema, servidor ou em uma estrutura de rede. Além disso, o PENtest usa ferramentas específicas para realizar a intrusão que mostram quais dados e informações corporativas podem ser roubadas por meio de tal ação (OSTEC, 2023).

Firewall

Firewall é uma ferramenta essencial para proteger a rede contra acessos não autorizados e ataques. Ele monitora o tráfego de entrada e saída da rede e aplica regras de segurança para bloquear ou permitir o acesso a determinados recursos. (Pfsense, 2024)

Vulnerabilidades

A vulnerabilidade em uma rede de dados é uma falha de segurança que pode ser explorada por hackers ou cibercriminosos para acessar informações confidenciais, interromper o funcionamento da rede ou causar danos aos dispositivos conectados. Essas vulnerabilidades podem surgir devido a configurações inadequadas, falta de atualizações de segurança, falhas de software ou hardware, entre outros

fatores. (Stallings, 2021).

Para o Stallings, 2021, entre várias vulnerabilidades em redes de dados destacam-se:

- Vulnerabilidades de Redes;
- Vulnerabilidades de Processos;
- Vulnerabilidades de Sistemas;
- Vulnerabilidades humanas.

Tipos de ataques a Cibernéticos

De acordo a Kaspersky, 2023, os principais tipos de ataques cibernéticos são: Ransomware, Ataque por engenharia social, Data Modification, Keylogging, Malware, Ping of Death, Phishing, Quebra de senhas e outros.

segurança que evidenciem vulnerabilidades que possam ser exploradas por ameaças, provocando impacto nos negócios da organização, uma atividade de análise que pretende identificar os riscos aos quais os ativos se encontram expostos.

Descrição da infraestrutura da instituição

O ISPM-LAN é uma rede local com diferentes sectores, como biblioteca, coordenação, laboratório, etc. Cada sector possui seu próprio switch, com um switch central, SD-CORE-01, conectando todos os sectores.

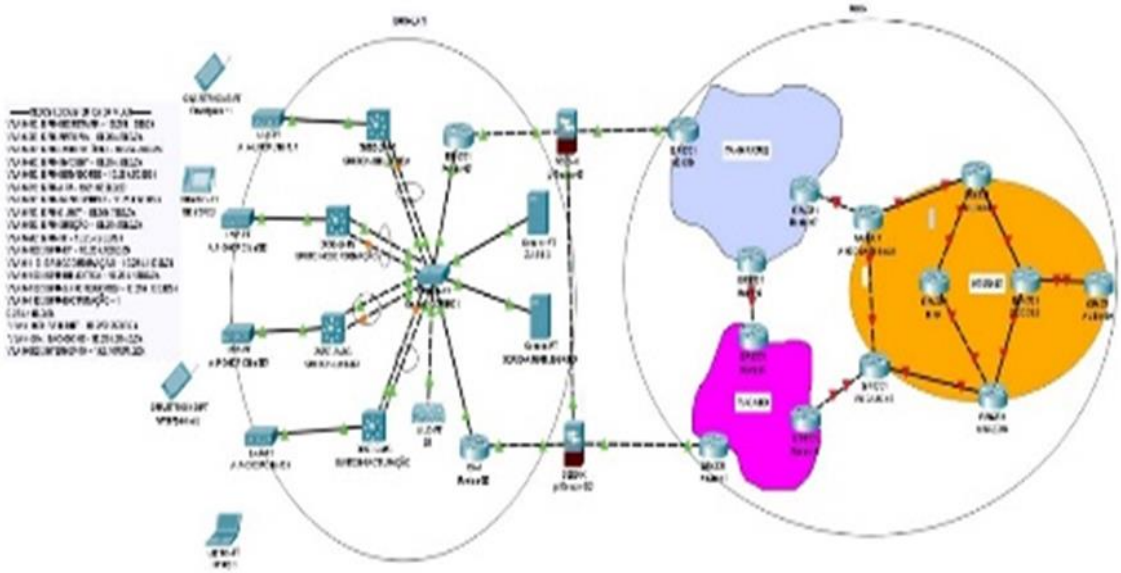

Figura 1: Topologia da lógica da rede de Fuente. dados do ISPM

Análise de Riscos

De acordo o TIVIT (2023) a análise de riscos é uma actividade voltada para a identificação de falhas de

A área WAN é a rede de longa distância, que conecta a ISPM-LAN a diferentes provedores de internet, como o ITA-PARATUS e a TVCABO. A conexão é feita por meio de roteadores (ISR4331) que conectam a ISPM-LAN à WAN. A rede inclui também um

firewall (5506-X) para proteger a rede interna de ataques externos.

MÉTODO

Objetivos

Para alcançar os objectivos Como qualquer outra investigação para ser bem-sucedida foi necessário necessariamente recorrer em métodos de investigação, nesta conformidade para a elaboração da presente dissertação, foi preciso recorrer às práticas de metodologias de investigação de pesquisas, sob forma estudar os padrões de metodologia de avaliação de vulnerabilidades num conhecimento científico (LakatosS & Mrconi, 2010).

Delimitação do tema

Como já se fez a referência do respectivo tema: Análise das Consequências das Vulnerabilidades Em Redes de Dados e Desenvolvimento de Estratégias de Mitigação: Estudo de Caso do Instituto Superior Politécnico Maravilha (ISPM) - Benguela

A Pesquisa foi delimitada no tempo e no espaço. No tempo no período de novembro a julho de ano 2022-2024, e no espaço geográfico situado na província de Benguela, no ISPM.

Tipo de Pesquisa: Para o desenvolvimento do presente trabalho adoptou-se a pesquisa Exploratório-Descritiva: Esta pesquisa explorou e descreveu as vulnerabilidades existentes nas redes de dados do ISPM, as consequências dessas vulnerabilidades e as estratégias de mitigação possíveis. A natureza exploratória permitiu identificar áreas menos conhecidas e descrever fenómenos específicos, enquanto a natureza descritiva ajudou a detalhar as vulnerabilidades e suas implicações (Kothari, 2004).

Métodos de Pesquisa: Tal como diz Kothari (2004), um método de pesquisa é um plano ou uma estrutura que orienta a colecta e análise de dados. Ele especifica os componentes principais da investigação, incluindo as perguntas de pesquisa, as hipóteses, as variáveis, os instrumentos de colecta de dados e as técnicas de análise de dados.

Estudo de campo – Segundo Severino (2007), o objecto ou fonte é abordado em seu meio ambiente próprio. A colecta de dados é feita nas condições naturais em que os fenómenos ocorrem, sendo assim, directamente observados, sem intervenção e manuseio por parte do pesquisador.

Por esta visão tomaram-se como métodos:

Revisão Bibliográfica: Este método permitiu revisar a literatura

existente sobre vulnerabilidades em redes de dados, suas consequências e estratégias de mitigação.

A Pesquisa foi efectuada por meio de bases de dados científicas, livros, artigos académicos, e publicações técnicas relevantes. Identificação de teorias e modelos existentes relacionados ao tema (Creswell, 2014).

Estudo de Caso: Este método objectivou analisar especificamente as vulnerabilidades das redes de dados do ISPM, suas consequências e as estratégias de mitigação que podem ser implementadas.

Procedimentos

Adoptou-se também a análise documental cujo propósito é a colecta e análise de documentos internos do ISPM relacionados à segurança da informação, como políticas de segurança, relatórios de auditoria, incidentes de segurança registados, etc.(Yin, 2018).

Pesquisa Qualitativa

A Pesquisa Qualitativa ou ainda denominados por dados qualitativos, colecta informações que não buscam apenas medir um tema, mas descrevê-lo, usando impressões, opiniões e pontos de vista. A pesquisa qualitativa é menos estruturada e busca se aprofundar em um tema para obter informações sobre as motivações, as ideias e as atitudes. Embora proporcione uma compreensão mais detalhada das perguntas da pesquisa, ao mesmo tempo, dificulta a análise dos resultados (Survey, 2023).

Análise de Logs e Dados Técnicos

Selecionaram -se como Fontes de Dados, os Logs de servidores, dispositivos de rede, sistemas de segurança (e.g., firewalls, IDS/IPS), como ferramentas de análise de logs (e.g., Splunk, ELK Stack), software de análise estatística (e.g., SPSS, R) (Anderson, 2008).

Fez-se a colecta de logs e dados técnicos, processamento e análise para identificar padrões e tendências de vulnerabilidades (Chandramouli, 2001).

Análise de Dados

Para a Análise Qualitativa utilizaram-se técnicas de análise de conteúdo para entrevistas e observações, categorização e identificação de temas recorrentes (Elo & Kyngäs, 2008).

Validação dos Dados

Preferencialmente houve um Feedback dos Participantes em que se fez a apresentação preliminar dos resultados aos participantes chave para verificar a

ISSN: 2745-2891

precisão das interpretações(Lincoln & Guba, 1985).

Instrumentos

Ferramentas utilizadas foram: **VirtualBox:** Esta ferramenta foi utilizada para criação de um servidor de teste.

Kali Linux: foi utilizado como um servidor de teste que permitiu realizar várias actividades, como scanear ou varredura de portas, teste de penetração com recursos a nmap e Wireshark para verificar a existência de portas abertas que podem ser vulnerável da rede e do servidor local e explorados para terceiros

Pentest-tools: A ferramenta Pentest-tools nos foi útil para a realização de teste de penetração em diferentes alvos entre hosts e sistemas.

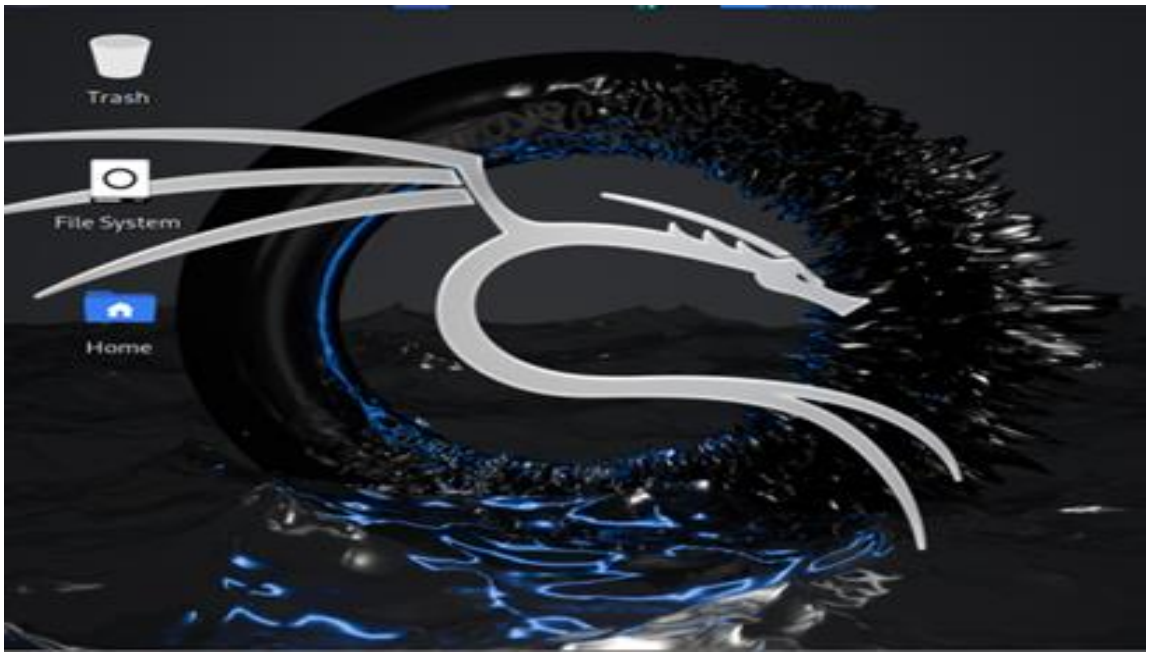

Figura 2: Servidor de teste

Nessus: foi utilizado nesta pesquisa para realizar várias varreduras para detectar possível falha existente na rede de dados da instituição esma.

Advanced IP Scanner: Esta ferramenta foi utilizada para permitir fazer Scanner para identificar endereços IPs de dispositivos ativos em redes que foram utilizados como alvos como mostra a figurara nº3.

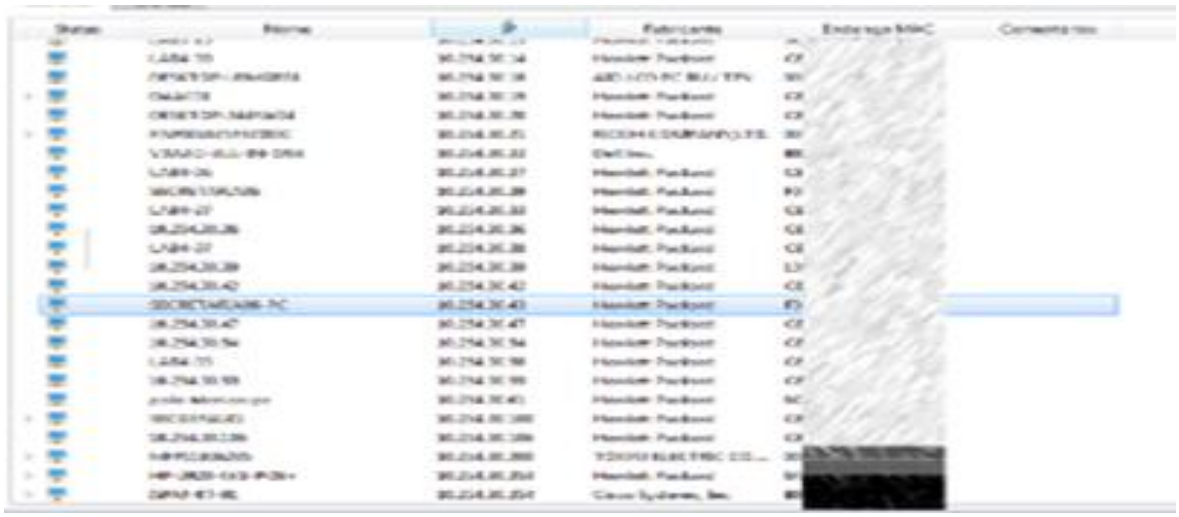

Figura 3: Scanner de IPs da rede local do ISPM.

Nmap: Ele foi usado para escancear redes, e detectar falhas de portas vulneráveis que podem ser exploradas por pessoas mal-intencionados.

Keyloggers: Foi utilizada para captura de registos de senha utilizado num dos computadores alvo do gabinete de termos, onde são realizadas a gestão de pautas no a fim de saber o tipo de criptografia e a qualidade de senhas de usuários.

Figura 4: Dados capturados pelo Keyloggers na estação de trabalho alvo 10.254.30.3

Spyware: Esta ferramenta foi utilizada para espionar actividades exercidas na área da tesouraria para comprovar o comportamento de usuários de áreas sensíveis e recolher dados para análise sobre o tipo de criptografia e autenticação de usuários usada na instituição.

Wireshark : Nesta pesquisa, a ferramenta Wireshark possibilitou-nos a fazer análise de tráfego e pacotes na rede local da instituição a partir do servidor central.

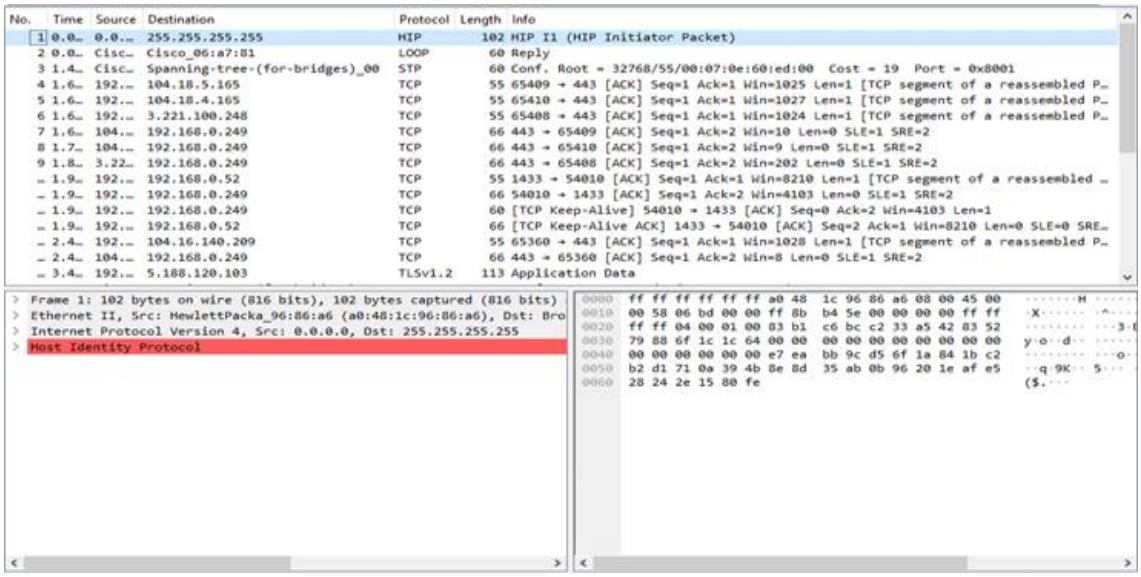

Figura 5: Wireshark para análise de pacotes

Procedimento de recolha e análises dos dados

A Entrevistas Semiestruturadas foi aplicada com profissionais de TI, segurança da informação e gestores do ISPM para obter ideias detalhadas sobre as práticas actuais de segurança e as vulnerabilidades identificadas (Patton, 2002). Para assegurar a visão sobre as boas práticas dos utilizadores do sistema e não só, aplicou-se a Observação Directa: e garantiu a observação das práticas de segurança em vigor no ISPM e identificação de possíveis falhas (Bryman, 2016). Para a análise de resultados usou s ferramenta Nessus que apresentou o impacto e criticidade da segurança da rede e das informações da instituição.

RESULTADOS

Foi realizada uma análise minuciosa das das vulnerabilidades e principais consequências dessas vulnerabilidades e seu impacto no negócio, propondo-se estratégias de mitigação para garantir o cumprimento dos objectivos propostos no início do trabalho.

Vulnerabilidades identificadas

Foram identificadas quatros (4), vulnerabilidades durante a pesquisa que são: Vulnerabilidades humanas, Vulnerabilidades de processos, Vulnerabilidades de sistema e Vulnerabilidades de rede.

Estratégia de mitigação

Tabela 1:

Principais estratégias de Mitigação.

Vulnerabilidade humano	vulnerabilidades com processos	Vulnerabilidades de sistemas	Vulnerabilidades de rede
• Desenvolver políticas claras • Fornecer treinamento regular • Implementar políticas de complexidade de senha e autenticação	• Implementar controles de acesso baseados em níveis de autorização • Auditar regularmente os acessos para identificar potenciais anomalias	• Implementar uso de sistemas de detecção de intrusos (IDS • Realizar avaliações de vulnerabilidades periodicamente para identificar possíveis falhas de segurança)	• Realizar auditorias regulares na configuração da rede para identificar e corrigir possíveis falhas • implementar o uso de protocolos de criptografia segura, como SSL/TLS

Tabela 2:

Escala de impacto de avaliação de risco e suas consequências.

Impacto	Escala	Avaliação de Risco e Consequências
ACEITÁVEL	2	Impacto mínimo. Pode ser tolerado sem causar grandes interrupções nas operações ou grande perda de dados ou recursos.
BAIXO	4	Impacto relativamente baixo. Pode resultar em algumas interrupções ou perda de dados que podem ser recuperadas com facilidade e não afetar significativamente as operações, mas que as soluções envolvem custos financeiros.
MÉDIO	6	Impacto moderado no negócio. Pode resultar em interrupções temporárias nas operações ou perda de dados significativa que exigem esforço para recuperar, mas não causam danos graves ou permanentes, mas as soluções envolvem custos financeiros.
ALTO	8	Impacto substancial. Pode resultar em **interrupções significativas nas operações, perda de dados críticos ou recursos importantes, requerendo ação imediata para mitigar os danos e minimizar as perdas,** mas as soluções envolvem muitos custos financeiros.
CRÍTICO	10	Impacto crítico. Pode resultar em **danos graves e irreparáveis à reputação da empresa, perda de dados sensíveis ou confidenciais, interrupções prolongadas nas operações ou até mesmo ameaçar a sobrevivência da organização, as soluções** envolvem elevados custos financeiros.

ISSN: 2745-2891

Figura 6: Análise dos resultados de sanear da rede.

CONCLUSÕES

Ao longo deste estudo, analisaram-se detalhadamente as consequências das vulnerabilidades em redes de dados no contexto do Instituto Superior Politécnico Maravilha (ISPM)-Benguela. Este estudo visou responder à questão científica central: Como as vulnerabilidades da Rede de Dados Impactam o sistema de segurança de Informação do Instituto Superior Politécnico Maravilha de Benguela

Durante o estudo, foram identificados quatro (4) principais tipos de vulnerabilidade, designadamente: as humanas que são resultantes de erros humanos no uso de sistemas, engenharia social, fraude interna, falta de treinamento e uso de senhas fracas, segue-se também a vulnerabilidade com processos que resulta de falta de políticas de segurança, falta de controle de acesso e falta de actualização de softwares.

Na mesma senda identificou-se a vulnerabilidade de sistemas causada pelas falhas com Software, falta de criptografia, configuração inadequada de dispositivos, ataques de malware, ataque de força bruta e ataque de phishing,e finalmente a vulnerabilidade de rede resultante de falhas de configuração, ataques de negação de serviço e Intercetação de dados.

Constatou-se, através do estudo, que tais vulnerabilidades podem resultar no acesso não-autorizado, modificação ou destruição de dados e interrupções nos serviços críticos da instituição. Estes problemas, não apenas ameaçam a segurança dos dados, como também,

podem comprometer a segurança e a operação contínua de actividades do ISPM.

Analisando estas vulnerabilidades, notou-se que estas podem ter um impacto médio de escala 6. Considerado um impacto moderado no negócio que pode resultar em interrupções temporárias nas operações ou perda de dados significativa que exigem esforço para recuperar.

As vulnerabilidades detetadas apresentam um impacto negativo porquanto, em termos de Confidencialidade, elas podem resultar em acesso não autorizado à informações confidenciais ou sensíveis.

Quanto à Integridade, elas podem comprometer a integridade dos dados (modificação ou corrupção). E em termos de Disponibilidade, elas podem causar interrupções nos serviços ou na rede (ataques de negação de serviço, por exemplo).

Para resolver este problema, foram desenvolvidas algumas estratégias de mitigação, baseadas em uma combinação de metodologias, destacando o desenvolvimento de políticas de segurança de informação claras, a educação de uma equipe e de estudantes sobre as táticas comuns de engenharia social, a implementação de um processo de gestão de vulnerabilidades, do uso de protocolos de criptografia sofisticados para proteger a integridade e confidencialidade dos dados em trânsito e em repouso, realizar auditorias regulares na configuração da rede para identificar e corrigir possíveis falhas de segurança.

Estas estratégias incluem a implementação de um sistema de gestão de segurança da informação (SGSI) alinhado às normas internacionais, como a ISO/IEC 27001, que estabelece políticas e procedimentos claros para proteger os activos de informação e especial das redes de dados como no caso do ISPM. A sua implementação efectiva contribui de forma sustentável para a segurança do sistema de redes de dados do ISPM.

REFERÊNCIAS

Advanced, I. (2024, July 6). Advanced-ip-scanner.com. Acesso em 6 de Julho de 2024, em https://www.advanced-ip-scanner.com/br/

IBM. (1 de Setembro de 2024). IBM.com/br. Acesso em 1 de Setembro de 2024, from https://www.ibm.com/br-pt/topics/information-security

ISO/IEC-27033-1. (5 de Janeiro de 2015). Lead Network Security Manager. ISO/IEC 27033 Lead Network Security Manager.

ISO-27001. (13 de Fevereiro de 2013). Implementação de um sistema de gerenciamento de segurança da informação. Os principais pontos da certificação de Cibersegurança.

Kali, O. (12 de Julho de 2024). Kali.org. Acesso em 12 de Julho de 2024, em https://www.kali.org/

Kaspersky. (20 de Abril de 2023). Kaspersky.com.br. Acesso em 20 de Abril de, 2023, em https://www.kaspersky.com.br/resource-center/definitions/what-is-social-engineering

Lakatos, M. d. (2017). Metodologia do trabalho científico. São Paulo: Atlas.

Lakatos, E. M., & Mrconi, M. d. (2010). Fundamentos de metodologia

Nmap. (20 de Agosto de 2023). Acesso em 20 de Agosto de 2023, em https://nmap.org/

Nmap. (12 de Julho de 2024). Nmap.org. Acesso em 12 de Julho de 2024, em https://nmap.org/

Oracle. (13 de Julho de 2024, July 13). Oracle.com. Acesso em 13 de Julho de 2024, em https://www.oracle.com/br/virtualization/virtualbox/

OSTEC. (7 de Maio de 2023). OSTEC. Acesso em 7 de Julho de 2023, em https://ostec.blog/geral/

Pentest. (9 de Julho de 2024). Pentest-tools.com. Acesso em 9 de Julho de 2024, em https://pentest-tools.com

Stallings, W. (2021). Network security essentials: Applications and standards - William Stallings. America: Pearson.

Tanenbaum, S., & Wetherall, J. (2017). Redes de computadores. USE: Pearson.

Tarapanoff, K. (8 de Agosto de 20016). Inteligencia, informação e conhecimento. Brasília, Brasil: IBICT & UNESCO.

Tenable. (24 de Maio de 2024). Tenable.com. Acesso em 24 de Maio de 2024, em https://pt-br.tenable.com/products/nessus/nessus-professional

TIVIT. (7 de Maio de 2023). Análise de vulnerabilidade: O guia definitivo sobre o assunto. Acesso em 7 de Maio de 2023, em https://blog.tivit.com/analise-de-vulnerabilidade

Wireshark. (2 de JUnho de 2024). Wireshark.org. Acesso em 2 de Junho de 2024, em https://www.wireshark.org/about.html