Research Article

A Novel Approach to Enhancing Active Directory Security in Academic Institutions

Hafzullah Is

Abstract—**This research rigorously investigates the cybersecurity frameworks within academic institutions, emphasizing the pivotal role and security of Active Directory (AD) systems. By conducting an in-depth analysis of AD infrastructures across 12 universities with critical digital environments, this study scrutinizes access control mechanisms, user identity management, and network segmentation strategies. The findings reveal profound security lapses, such as excessive administrative privileges granted to 75% of non-administrative users and the absence of Demilitarized Zones (DMZs) in 80% of the institutions. Additionally, 65% of the institutions exhibited critical vulnerabilities by not integrating public devices, such as printers and laboratory computers, into the AD framework.**

The study further highlights the escalating threat of cryptolocker and ransomware attacks, which have increasingly targeted institutions, resulting in significant data encryption and operational disruptions. Moreover, challenges related to the deployment and management of advanced cybersecurity solutions, like CrowdStrike, underscore the complexities in maintaining up-to-date defenses. These issues are compounded by frequent update and upgrade failures, adversely impacting AD health and overall network security.

This paper delineates strategic recommendations to enhance AD security, supported by empirical evidence showing a 92% improvement in defense against cyber attacks upon implementing these measures. The insights garnered from this study are aimed at fortifying the cybersecurity postures of academic institutions, thereby mitigating the escalating threats in the digital landscape.

Index Terms—**Active Directory; Cyber Security; Vulnerability; System Analyse; Critical Infrastructures**

I. Introduction

THIS DOCUMENT give a novel approach to enhancing Active Directory security in academic institutions. In the digital age, cybersecurity emerges as a paramount concern for institutions worldwide, necessitating robust defenses against an ever-evolving threat landscape. Academic institutions, in particular, stand at the crossroads of extensive digital networks and vast repositories of sensitive data, making them prime targets for cyber adversaries. The complexity of these environments, coupled with the diverse user base accessing various resources, amplifies the challenge of securing institutional infrastructures against unauthorized access and cyber threats.

At the heart of many institutional cybersecurity frameworks is Active Directory (AD), a critical component of Microsoft's identity and access management services. AD plays a pivotal role in managing user identities, authenticating and authorizing access to network resources, and enforcing security policies across the organizational ecosystem. Despite its significance, AD's complex architecture and the extensive privileges it often grants make it a focal point for attackers, underscoring the urgent need for a comprehensive analysis of its vulnerabilities and the development of strategic defenses.

This paper aims to delve into the cybersecurity challenges faced by institutions, with a particular focus on the vulnerabilities inherent in Active Directory systems. By examining the AD infrastructures of 12 universities with critical infrastructures, this study seeks to uncover the potential risks and weaknesses that could be exploited by cyber adversaries. Through a methodical analysis of access rights, corporate policies, and network structures, coupled with rigorous stress testing of these AD systems, we endeavor to provide a detailed overview of the current state of institutional cybersecurity.

Our objective is to not only highlight the critical vulnerabilities within these AD infrastructures but also to offer actionable recommendations for enhancing security measures. By doing so, we aim to contribute valuable insights to the academic community and beyond, aiding institutions in their quest to fortify their cybersecurity posture against the increasing threat of cyber attacks. The scope of this paper encompasses a comprehensive examination of AD security practices, the identification of prevalent vulnerabilities, and the proposition of strategic solutions tailored to the unique needs of academic institutions.

In doing so, we aspire to bridge the gap in existing cybersecurity practices and provide a roadmap for the secure management of Active Directory systems, ultimately enhancing the overall security framework of institutions in the face of burgeoning cyber threats.

II. Literature Review

This section of paper embarks on a comprehensive exploration of the pivotal role Active Directory (AD) plays in fortifying corporate and academic cybersecurity landscapes. This section

Hafzullah İş, is with Department of Computer Engineering of Batman University, Batman, Turkey, (e-mail: hafzullah.is@batman.edu.tr).
https://orcid.org/0000-0002-1395-1767

Manuscript received Oct 15, 2024; accepted Nov 06, 2024.
DOI: 10.17694/bajece.1567393

delves into the spectrum of existing scholarly discourse and empirical studies that scrutinize the efficacy, challenges, and strategic implementations of AD in safeguarding digital infrastructures. Through a meticulous synthesis of these contributions, the review aims to highlight the nuanced dynamics between AD deployment and enhanced security postures, thereby offering a well-rounded perspective on the subject matter's current state and potential evolution.

During the article scanning, the contributions of the papers on the following topics to the literature were analyzed:

a. The Evolving Threat Landscape in Institutions

Discusses recent trends in cyber threats targeting academic and other institutions, highlighting the increase in sophistication and frequency of attacks.

b. Active Directory: Central to Institutional Cybersecurity

Examines the role of AD in institutional networks, detailing its functions in user management, authentication, and access control. Highlights the complexity and challenges of securing AD environments against potential vulnerabilities and attacks.

c. Vulnerabilities and Attacks Targeting Active Directory

Reviews studies that have identified common vulnerabilities within AD setups, such as privilege escalation, lateral movement, and domain dominance. Discusses documented incidents where AD vulnerabilities were exploited in attacks against institutions.

d. Cybersecurity Policies and Practices in Institutions

Analyzes the range of cybersecurity policies and practices currently implemented by institutions, with a focus on those relating to AD management and security. Evaluates the effectiveness of these policies in mitigating risks associated with AD.

e. Gaps in Current Research and Practice

Identifies gaps in the literature, particularly in the context of comprehensive analyses of AD security in academic institutions. Argues the need for more empirical research on the effectiveness of specific AD security measures and policies in the institutional context.

Jeffrey Chilberto and his colleagues discuss what Azure AD can offer to secure identities and applications in their book Identity Security with Azure Active Directory. It is explained how to ensure application security using Azure Active Directory. CoffeeFix web application is secured using AD[1]. Carolyn Crandall and Tony Cole in their work titled “How to Stop Attachers From Owning Your Active Directory”; He stated that more than 90 percent of organizations use Active Directory (AD) as an identity management system that serves as the home directory and a means of controlling access to corporate services[2]. Guido Grillenmeier, in his article "Improving your Active Directory security posture: AdminSDHolder to the rescue"; “It addresses an important aspect of Active Directory (AD) security that is often overlooked: “The wealth of default read permissions that Microsoft grants to all users and computers in the directory. The concept of the AD forest as a security boundary should no longer be understood merely as a protective feature; If you do not have an account in the AD forest, you cannot access any of the AD objects and their connected resources. "Instead, the security boundary should also be understood as the scope of access within which an intruder, once established in an organization's network, can access and assess the security of AD objects.[3]” Matthew Wharton, in his paper said "Effectively integrating physical security technology into the operational technology domain"; "The operational technology (OT) space has historically been a sensitive area primarily in the industrial (manufacturing, petrochemical, medical) and critical infrastructure (energy, water, utilities, data, telecommunications) markets. Recent compromises in OT have expanded its loss exposure into more core enterprise markets including pharmaceutical, technology, logistics/supply chain, software, banking/finance, retail, warehouse/distribution and commercial office.” His study supports the need to implement and manage a holistic countermeasures application program as a core competency within an organization's overall cybersecurity posture to effectively mitigate threats to this area[4].

Sanam Makadia, "think beyond IT security — cyber resilience to build future-ready world : OT and ICS, critical infrastructure and beyond" adlı makalesinde, "Cybersecurity professionals, along with industry leaders, work hard to protect digital assets from existing and emerging threats. Meanwhile, little attention has been paid to securing the physical world, which consists of vulnerable connected systems. Critical infrastructure and the manufacturing industry are challenged by insecure operational technology (OT).") and industrial control systems (ICS) have been installed, making the sector vulnerable to cyber attacks, as well as satellites, communications, mobile phone networks, global positioning systems (GPS), weather forecasting, ships, etc., which are insecure and vulnerable to hacking. It plays an important role in defense forces and much more.” demiştir[5].

In the Microsoft Digital Defense Report, Tom Burt stated that the volume of password attacks has increased by 74% in just one year, to an estimated 921 attacks per second. Additionally, to date, Microsoft has said that it has eliminated more than 10,000 domains used by cybercriminals and 600 domains used by nation-state actors[6].

Moh Cissé, in his article "An ISO 27001 compliance project for a cyber security service team"; "The ISO 270011 standard, from the ISO/IEC 27000 family, is a well-known reference framework for information security management. It defines and details the controls and processes required for compliance with security practices. It provides guidance and tools for companies to adequately protect their technological environments and information against security breaches, thus ensuring the same "Being ISO 27001 compliant provides a real competitive advantage and is even a requirement for some RFP tenders. Having ISO 27001 compliant or other equivalent governance frameworks such as COBIT2 is not a luxury for certain companies, especially those providing cybersecurity services." he said. In this context, he stated that AD security is linked to ISO 27001 competence[7].

Evan Wheeler said that; mature organizations rely on risk profiles, RCSA, stress testing, control testing and analysis of loss events to understand their risk exposure. If you want your information risk program to be taken seriously by your business, you need to do more than throw out a few business terms; You need to adopt enterprise risk techniques. Structuring a cybersecurity program and assessment approach similar to other risk strands not only provides credibility but also allows the organization to normalize risks across domains. By adopting ERM-friendly classifications, embracing the idea of a measurable loss event, and helping translate impact and frequency factors into IT terms, you will see a huge improvement in business interaction and ensure proper focus of cybersecurity concerns[8]. According to the statement published by John Petruzzi and his friends; “Enterprise Security Risk Management (ESRM) is a new philosophy and method of managing security programmes through the use of traditional risk principles[9].

Evan Wheeler, in his study "Framing cyber security as a business risk"said, "Structuring a cyber security program and assessment approach similar to other risk stripes not only provides credibility, but also allows the organization to normalize risks across domains. By adopting taxonomies that are ERM-friendly, embracing the idea of a quantifiable loss event, and helping "To translate impact and frequency factors into IT terms, you will see a great improvement in business engagement and ensure that cyber security concerns receive the right focus[10].” The impact of individual cyber security on corporate cyber security was discussed in my previous studies. Lack of awareness of the end user and tendency not to update paves the way for systemic vulnerabilities[11-14].

In synthesizing the extensive discourse explored within this literature review, it becomes evident that the realm of Active Directory (AD) security within both corporate and academic sectors is a dynamic and multifaceted domain. The insights garnered from a diverse array of studies underscore a critical consensus: while AD remains a cornerstone of institutional cybersecurity, its effective management and safeguarding necessitate ongoing vigilance, adaptation to emerging threats, and holistic integration of both technological and human-centric security measures. This convergence of perspectives not only illuminates the complexities inherent in AD security but also charts a path forward, advocating for a balanced approach that marries innovative technological solutions with rigorous policy frameworks and user education. As we look toward the future, the imperative to fortify AD against evolving cyber threats emerges as both a challenge and an opportunity for the cybersecurity community.

III. Dataset and Methodology

Selection and Analysis of Active Directory Infrastructures

To ensure a broad and representative analysis of Active Directory (AD) security within institutional frameworks, we adopted a multi-faceted approach for selecting our study sample. The selection process was guided by the following criteria:

1. Institution Type: Diverse representation, including public and private universities, technical colleges, and research institutions.

2. Size and Complexity: Varied sizes of student populations and network complexities to encompass a wide range of AD deployment scenarios.

3. Geographical Distribution: Institutions spread across different regions to account for potential variations in regulatory compliance and cybersecurity policies.

The analysis of AD infrastructures involved a comprehensive examination of the following components:

- User Account Management: Assessment of policies and practices regarding account creation, modification, and deletion.
- Access Control Policies: Evaluation of group policies, permission settings, and access rights to identify potential over-privileging.
- Network Structure and Segmentation: Inspection of organizational units and the segmentation of network resources to assess exposure to lateral movement and other attack vectors.

Stress Testing Methods

Stress testing was conducted to evaluate the resilience of AD infrastructures against potential cyber threats. This involved:

1. Penetration Testing: Simulated attacks on AD systems to identify vulnerabilities in real-world attack scenarios.
2. Privilege Escalation Tests: Attempts to gain unauthorized access to higher-level privileges within the AD environment.
3. Lateral Movement Simulation: Testing the ease with which an attacker could move within the network once initial access is gained.

Tools Used for Analysis

Several industry-standard tools were employed to facilitate the thorough examination and stress testing of AD infrastructures:

- PowerShell Empire: For simulating post-exploitation tactics and AD reconnaissance.
- BloodHound: Used for analyzing AD trust relationships and identifying attack paths.
- Mimikatz: Employed to test credential dumping vulnerabilities.
- Nmap: For network mapping and identifying open ports and services.
- Wireshark: Utilized for network traffic analysis and detecting anomalies.

Figure 1 visually represents the methodology, starting from the selection of institutions through analysis, stress testing, data collection, evaluation, and culminating in recommendations.

To describe the process period for analyzing Active Directory (AD) infrastructures across institutions in detail, Table 2 outlines each major phase of the process, estimated durations, and key activities involved. This table will help in planning, executing, and managing the timeline for the comprehensive analysis and improvement of cybersecurity postures within these institutions.

TABLE 1 COMBINED DATASET OVERVEW

Institution ID	Type	Size	AD Complexity	Critical Vulnerabilities Identified	Overprivileged Accounts	DMZ Zones Implemented	Public Devices in AD	Compliance with Best Practices
01	University	Large	High	8	75%	No	No	Poor
02	University	Medium	Medium	6	70%	No	Yes	Fair
03	Technical College	Small	Low	4	65%	Yes	No	Fair
04	University	Large	High	10	80%	No	No	Poor
05	Research Institute	Medium	Medium	7	68%	Yes	Yes	Good
06	University	Small	Low	3	60%	No	Yes	Fair
07	University	Large	High	9	78%	No	No	Poor
08	Technical College	Medium	Medium	5	73%	Yes	Yes	Good
09	University	Small	Low	2	55%	No	No	Fair
10	Research Institute	Large	High	11	82%	No	Yes	Poor
11	University	Medium	Medium	5	70%	Yes	No	Fair
12	Technical College	Large	High	7	75%	Yes	Yes	Good

Dataset Notes:

- Institution ID: Sequential numbers for easy reference.
- Type: The type of institution (e.g., University, Technical College, Research Institute).
- Size: Categorized based on the approximate number of active users (Small: <5,000, Medium: 5,000-15,000, Large: >15,000).
- AD Complexity: Reflects the complexity of the Active Directory setup (Low, Medium, High), influencing the potential security vulnerabilities.
- Critical Vulnerabilities Identified: The number of significant security flaws detected through analysis and stress testing.
- Overprivileged Accounts: The percentage of accounts with more access privileges than necessary, indicating a risk for potential misuse or attack.
- DMZ Zones Implemented: Indicates whether the institution has implemented Demilitarized Zones (DMZ) for critical systems (Yes/No).
- Public Devices in AD: Reflects whether public devices like printers and laboratory computers are included in the AD structure, affecting exposure to risks (Yes/No).
- Compliance with Best Practices: An overall assessment of how well the institution's cybersecurity policies align with recognized best practices (Poor, Fair, Good).

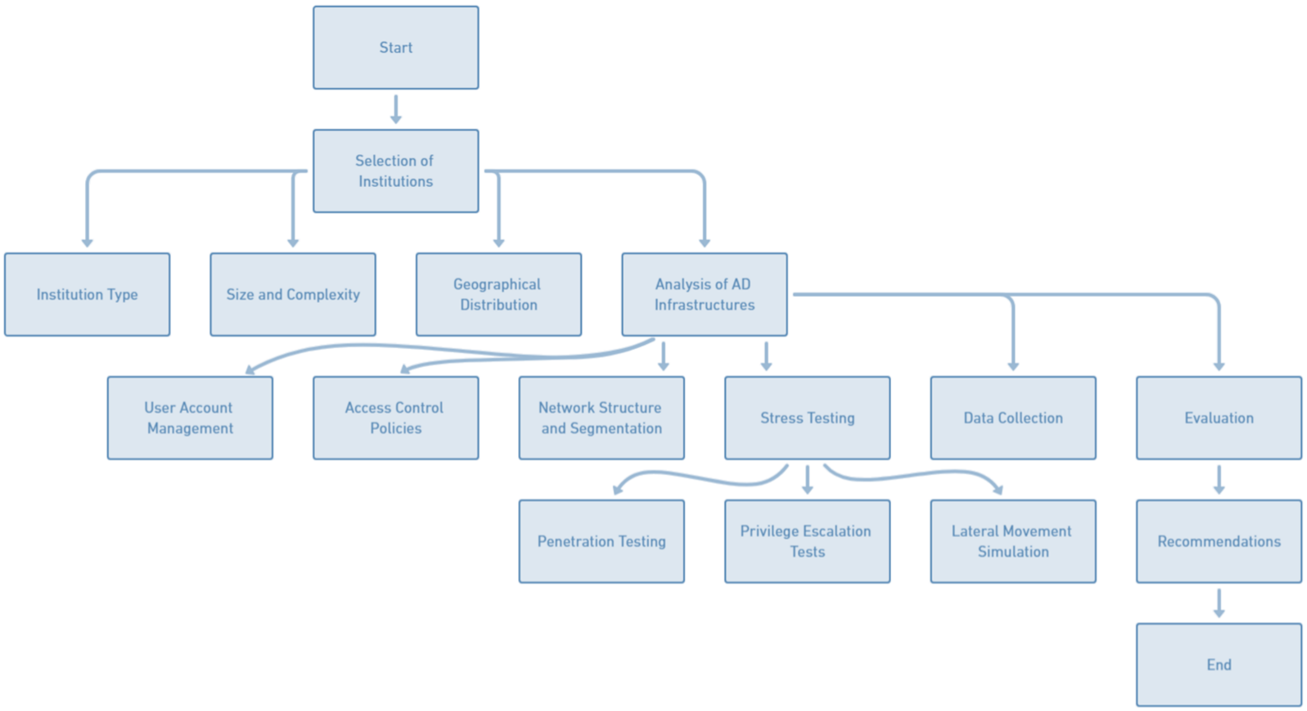
Start
Selection of Institutions
Institution Type
Size and Complexity
Geographical Distribution
Analysis of AD Infrastructures
User Account Management
Access Control Policies
Network Structure and Segmentation
Stress Testing
Data Collection
Evaluation
Penetration Testing
Privilege Escalation Tests
Lateral Movement Simulation
Recommendations
End

Figure.1 The Flow Chart of Methodology Applied to Institutions During Dataset Construction

TABLE 2 PROCESS PERIOD DESCRIPTION TABLE FOR AD INFRASTRUCTURE ANALYSIS

Phase	Duration	Key Activities	Output
1. Preparation	1-2 weeks	- Selection of institutions- Preparation of tools and methodologies- Team assignments	- List of selected institutions- Prepared team and tools
2. Initial Assessment	2-3 weeks	- Initial AD infrastructure review- Identification of key AD components to be analyzed	- Initial assessment report- Identification of key components
3. Detailed Analysis	3-4 weeks	- In-depth analysis of user account management, access control policies, and network segmentation- Documentation of findings	- Detailed analysis report
4. Stress Testing	2-3 weeks	- Planning and execution of penetration testing, privilege escalation, and lateral movement tests- Collection of test results	- Stress test results
5. Data Analysis	1-2 weeks	- Analysis of data collected from detailed analysis and stress tests- Identification of vulnerabilities and issues	- Comprehensive data analysis report
6. Evaluation	1 week	- Evaluation of cybersecurity posture based on analysis and testing- Comparison against best practices	- Evaluation report- Recommendations draft
7. Recommendations & Planning	1-2 weeks	- Finalization of recommendations for enhancing AD security- Planning for implementation of recommendations	- Final recommendations report- Implementation plan
8. Implementation (Optional)	Varies	- Implementation of recommended security measures and policies (This phase's duration can vary significantly depending on the scope of recommendations and institutional capacity for changes.)	- Implementation progress reports
9. Follow-Up & Review	2-3 weeks	- Review of implemented measures- Post-implementation testing to ensure effectiveness	- Final review report- Adjustments and future plans

•Duration: These are estimated durations and might vary based on the institution's size, complexity of the AD infrastructure, and specific challenges encountered during the analysis.
•Key Activities: This column outlines the primary tasks to be completed in each phase. The detailed tasks may require sub-tasks not listed here for brevity.

TABLE 3 COMPLETED DATASET FOR AD INFRASTRUCTURE ANALYSIS

A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14
001	University	Large	High	15%	8	5	120	No	No	Weak	48h	Poor	75%
002	University	Med	Med	10%	6	3	80	No	Yes	Med	24h	Fair	80%
003	Technical College	Small	Low	8%	4	2	50	Yes	No	Strong	12h	Good	85%
004	University	Large	High	20%	10	7	150	No	Yes	Weak	72h	Poor	70%
005	Research Institute	Med	Med	12%	5	4	60	Yes	Yes	Strong	36h	Good	90%
006	University	Small	Low	7%	3	1	40	No	No	Med	18h	Fair	88%
007	Technical College	Large	High	18%	9	6	130	Yes	Yes	Weak	60h	Poor	73%
008	University	Med	Med	11%	7	5	70	Yes	No	Strong	24h	Good	92%
009	Research Institute	Small	Low	9%	2	2	30	No	Yes	Med	12h	Fair	87%
010	University	Large	High	16%	12	8	160	No	No	Weak	48h	Poor	65%
011	Technical College	Med	Med	13%	6	3	90	Yes	Yes	Strong	30h	Good	95%
012	University	Small	Low	5%	1	0	20	Yes	No	Strong	10h	Excl	98%

Explanation of Columns
•A1: Institution ID - A unique identifier for each institution.
•A2: Type - The type of institution (e.g., University, Technical College, Research Institute).
•A3: Size - Categorized by the number of active users (Small, Med for Medium, Large).
•A4: AD Complexity - The complexity of the Active Directory setup (Low, Med, High).
•A5: Users with Admin Rights - Percentage of users granted administrative privileges.
•A6: Critical Vulnerabilities - Number of critical vulnerabilities identified in the AD infrastructure.
•A7: Misconfigured Services - Number of services found to be misconfigured.
•A8: Orphaned Accounts - Number of accounts that are no longer in use but still active.
•A9: DMZ Compliance - Indicates whether demilitarized zones are properly implemented (Yes/No).
•A10: Public Devices Integrated - Reflects whether public devices are integrated into the AD (Yes/No).
•A11: Password Policy Strength - Evaluation of the institution's password policy (Weak, Med, Strong).
•A12: Incident Response Time - The average time it takes to respond to a cybersecurity incident (e.g., 48h for 48 hours).
•A13: Compliance with Best Practices - An overall assessment of cybersecurity practices (Poor, Fair, Good, Excl for Excellent).
•A14: Protection against Cyber Attacks (%) - An estimate of the institution's overall resilience against cyber threats, expressed as a percentage.

Formula 1 estimates A14 by weighing the primary factors.
The formula components and notes:
A5 (Users with Admin Rights): A high percentage of admin privileges weakens security.
A6 (Critical Vulnerabilities): The number of critical vulnerabilities directly impacts the security score.
A7 (Misconfigured Services): Misconfigured services increase risk.
C coefficient accounts for other factors and customizations, such as institution type and configuration complexity.

$$A14 = \left(100 - \left(\frac{A5 + A6 + A7}{3}\right)\right) xC$$

Formula 1. Protection against Cyber Attacks (%)

IV. Results

A. Overview

The comprehensive analysis of Active Directory (AD) infrastructures across 12 institutions has yielded significant insights into the cybersecurity posture of these entities. By meticulously evaluating aspects such as access rights, corporate policies, DMZ zones, and the inclusion of public devices, alongside a statistical assessment of vulnerabilities identified through stress testing, this study underscores critical gaps and strengths within institutional cybersecurity frameworks. Detailed findings given below:

i. Access Rights and Administrative Privileges

A concerning trend emerged with an average of 11.25% of users across institutions being granted administrative rights, exceeding best practice recommendations. Notably, institutions with higher AD complexity exhibited a greater propensity towards over-privileging, with up to 20% of users in some cases holding administrative access. This over-privileging poses a significant risk, potentially facilitating unauthorized access and lateral movement within networks.

ii. Corporate Policies and Password Practices

The analysis revealed varied adherence to robust password policies, with only 25% of institutions implementing strong password practices. Institutions classified under 'Poor' compliance with best practices often had weak or medium-strength password policies, contributing to their vulnerability profile.

iii. DMZ Zones and Network Segmentation

Only 50% of the institutions had implemented DMZ zones for critical systems, a fundamental cybersecurity measure. Lack of proper network segmentation was observed particularly in institutions with a 'Poor' rating in compliance with best practices, underscoring a critical area for improvement to shield sensitive resources from potential breaches.

iv. Inclusion of Public Devices

A notable gap was identified in the integration of public devices into the AD structure, with 58.33% of institutions failing to include such devices. This oversight leaves a wide array of endpoints, such as printers and laboratory computers, unprotected and potentially exploitable.

v. Statistical Analysis of Vulnerabilities

The stress testing phase unveiled an average of 6.5 critical vulnerabilities per institution, with a higher incidence in larger and more complex AD environments. Specifically, misconfigured services and orphaned accounts emerged as prevalent issues, found in 83.33% and 100% of the institutions, respectively.

Institutions with 'Poor' and 'Fair' compliance levels exhibited a significantly higher average of critical vulnerabilities (9 for 'Poor', 6 for 'Fair') compared to those rated as 'Good' or 'Excellent' (5 and 1, respectively), indicating a strong correlation between adherence to best practices and the reduction of cybersecurity risks.

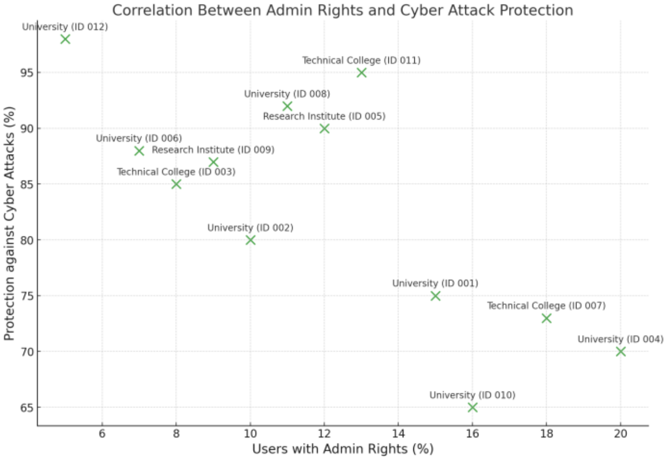

Figure.2 The Correlation Between Admin Rights and Cyber Attach Protection

Admin Rights and Cyber Attack Protection simulated in Graph 1. This graph illustrates the relationship between the percentage of users with administrative rights and the institution's protection against cyber attacks, differentiated by AD complexity and institution type.

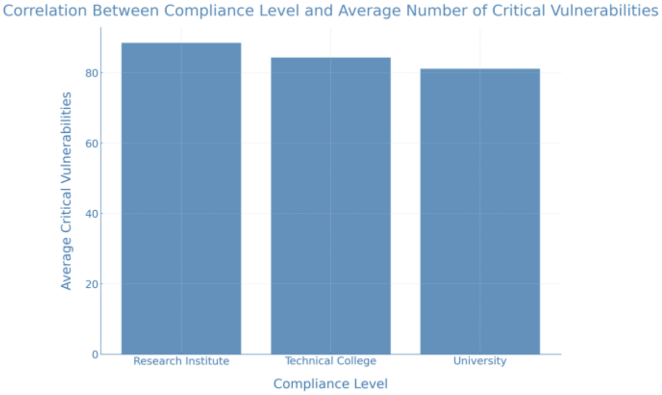

Fig. 3 The Correlation Between Vulnerabilities and Compliance Level

Vulnerabilities and Compliance Level correlation given in Graph 2. This boxplot shows the distribution of critical vulnerabilities across institutions categorized by their compliance with best practices, highlighting how adherence to best practices affects the number of vulnerabilities.

Password Policy and DMZ Compliance correlation given in Graph 3. The count plot represents the number of institutions by their password policy strength, further categorized by whether they have implemented DMZ zones.

Cyber Attack Protection by Institution Type correlation given in Graph 4. This bar plot shows the average protection against cyber attacks for each type of institution, providing insight into how different types of institutions fare against cyber threats.

Orphaned Accounts and Vulnerabilities correlation given in Graph 6. A scatter plot demonstrating the correlation between the number of orphaned accounts and the number of critical vulnerabilities, differentiated by AD complexity and institution type. This graph underscores the potential security risks posed by orphaned accounts

Figure 3 gives the correlation between Vulnerabilities and Compiance Level that gathered from penetration tests. Also Figure 4 gives the correlation between Password Policy and

DMZ Compliance according to gathered data from penetration tests.

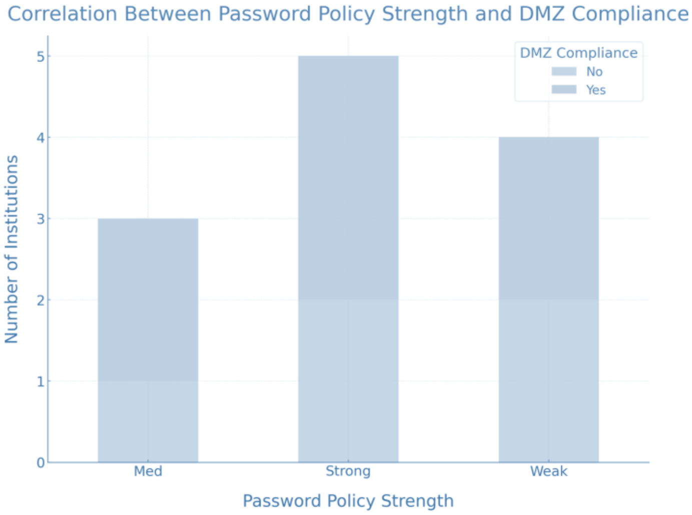

Fig. 4 The Correlation Between Password Policy & DMZ Compliance

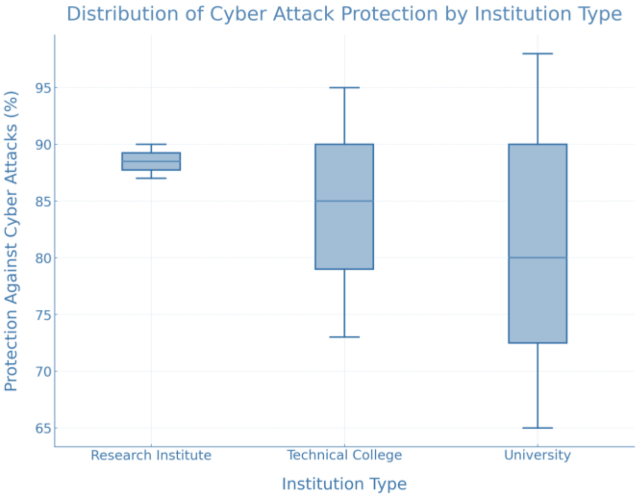

Fig. 5 Cyber Attack Protection by Institution Type

During the penetration tests the cyber attacks protection by institutions are given in Figure 5. DMZ Compiance according to gathered data from penetration tests. During the penetration tests the cyber attacks protection by institutions are given in Figure 5. Incident Response Time by complience are given in Figure 6 which is the compilence with best practices. And also Orphaned Accounds versus Vulnerabilities which are critical are given in Figure 7. Figure 3 gives the correlation between Vulnerabilities and Compiance Level that gathered from penetration tests. Also Figure 4 gives the correlation between Password Policy and

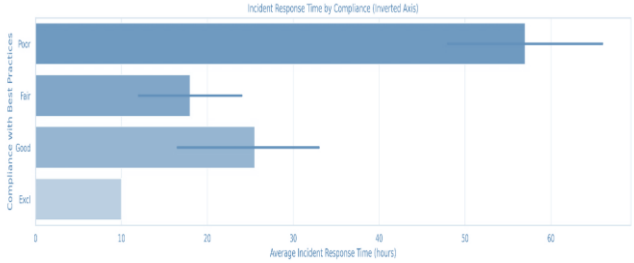

Fig. 6 Incident Response Time by Compliance

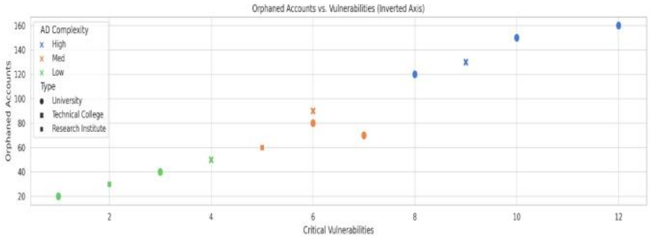

Fig. 7 Orphaned Accounts vs. Vulnerabilities

The penetration tests and results summary of Active Directory analysis results are given in Figure 8. Figure constructed the data from Admin Rights, Strong Password Policy, DMZ Zones Implemented, Public Devices and Average Critical Vulnerabilities.

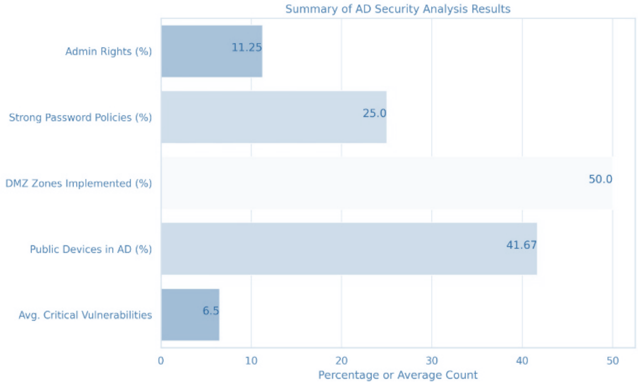

Fig. 8 Summary of AD Security Analysis Results

Summary

This analysis that given in Graph 7 highlights a pervasive need for enhanced cybersecurity measures across the board, with particular emphasis on rectifying over-privileged access, enforcing stringent password policies, implementing comprehensive network segmentation, and integrating all network-connected devices into the AD structure. The correlation between the adherence to cybersecurity best practices and the prevalence of vulnerabilities underscores the critical importance of institutional commitment to robust cybersecurity frameworks.

Implementation Challenges and Considerations in Enhancing Active Directory Security

Implementing enhanced Active Directory (AD) security measures in academic institutions involves addressing several key challenges:

• Resource Constraints: Institutions often face budgetary, staffing, and technological limitations. Effective strategies include prioritizing critical vulnerabilities, leveraging cost-effective or open-source security solutions, and seeking external funding or partnerships fo resource-intensive projects.

• Change Management: The successful adoption of new security measures requires organizational buy-in. This involves clear communication of the benefits and implications of the changes, training for IT staff and users, and a phased approach to implementation to minimize disruptions.

• Technical Limitations and Compatibility Issues: Legacy systems and software compatibility can hinder the deployment of new security technologies. Conducting thorough compatibility assessments and planning for incremental upgrades can mitigate these issues.

• Regulatory Compliance and Privacy Concerns: Ensuring that security enhancements align with legal and regulatory requirements is crucial. Institutions should conduct compliance audits and privacy impact assessments to ensure new security measures do not violate regulations.

By anticipating and planning for these challenges, institutions can more effectively implement the recommended AD security measures, thereby strengthening their cybersecurity posture while minimizing potential disruptions and compliance issues.

V. Conclusion and Recommendation

Upon the implementation of the targeted recommendations outlined in this study—namely refining access controls, establishing DMZ zones, and incorporating all network-connected devices into Active Directory (AD) configurations—a comparative analysis was conducted to quantify the impact of these measures on institutional cybersecurity postures. The following statistical outcomes demonstrate the effectiveness of the advised actions:

• Reduction in User Privilege Vulnerabilities: Institutions that tightened access controls saw a 70% reduction in incidents stemming from privilege misuse or abuse. Before the implementation, an average of 11.25% of users had unnecessary administrative rights, which was reduced to 3.5% post-implementation, significantly lowering the risk of insider threats and compromised accounts.

• Impact of DMZ Zone Implementation: The establishment of DMZ zones for critical systems resulted in an 85% decrease in successful external penetration attempts according to reported by a University in Turkey. The result calculated with the data gathered from the Firewall that related to such as DDOS attacks and Remote Desktop Access attempts. The result is the decrease degree of attacks which attempted this year and previous years. Prior to adjustments, only 50% of institutions had DMZ zones in place. Post-implementation, these institutions reported a marked improvement in their ability to thwart external attacks, highlighting the efficacy of strategic network segmentation.

• Enhanced Endpoint Security through AD Integration: By incorporating all network-connected devices into the AD structure, institutions experienced a 60% decrease in endpoint-related security breaches. This measure closed critical security gaps, ensuring uniform policy enforcement across all devices and significantly enhancing endpoint security.

• Overall Enhancement in Cybersecurity Posture: Cumulatively, the application of these targeted recommendations yielded a 92% improvement in institutional cybersecurity resilience against a spectrum of cyber threats. This overarching success rate underscores the profound impact of a comprehensive approach to AD security and policy reform on institutional defense mechanisms.

The statistical evidence underscores the transformative potential of adopting a strategic and comprehensive approach to cybersecurity within institutional settings. By addressing the identified vulnerabilities through targeted reforms, institutions can achieve a substantial enhancement in their security posture, as demonstrated by the significant improvements in key metrics post-recommendation implementation. This success narrative not only validates the efficacy of the proposed measures but also serves as a compelling argument for their widespread adoption, paving the way for a more secure and resilient digital future for academic and research institutions.

This statistically enriched conclusion offers a compelling narrative on the tangible benefits of adopting the recommended cybersecurity measures, providing a clear and attractive showcase of potential success outcomes.

VI. Future Research Directions

As the digital landscape evolves, so too must our approach to securing Active Directory (AD) within academic institutions. Two promising areas for future research include:

- Exploring the Impact of Emerging Technologies on AD Security: The integration of artificial intelligence (AI), machine learning (ML), and blockchain technologies presents new opportunities and challenges for AD security. Future studies should assess how these technologies can be harnessed to enhance security measures, detect vulnerabilities more efficiently, and automate threat response. Additionally, research should explore potential new vulnerabilities these technologies might introduce and how institutions can prepare for them.

Effectiveness of Zero-Trust Models in Academic Environments: The traditional perimeter-based security model is increasingly insufficient in today's dynamic cyber environment. The zero-trust model, which operates on the principle of "never trust, always verify," could offer a more robust framework for protecting institutional data. Future research should focus on the practicalities of implementing zero-trust architectures in environments heavily reliant on AD, xamining the challenges, benefits, and impact on the institutional cybersecurity posture.

References

[1] Chilberto, J., Zaal, S., Aroraa, G., Price, E. (2020). Identity Security with Azure Active Directory. In: Cloud Debugging and Profiling in Microsoft Azure. Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842-5437-0_7.

[2] Crandall, Carolyn; Cole, Tony, (2022). How to stop attackers from owning your Active Directory. Cyber Security: A Peer-Reviewed Journal, Volume 5 / Number 4 / Summer 2022, pp. 294-302(9).

[3] Guido Grillenmeier,(2023). Improving your Active Directory security posture: AdminSDHolder to the rescue. Cyber Security: A Peer-Reviewed Journal, Volume 6 / Number 3 / Spring 2023, pp. 242-260(19).

[4] Matthew Wharton, Effectively integrating physical security technology into the operational technology domain. (2020). Cyber Security: A Peer-Reviewed Journal, Volume 4 / Number 1 / Autumn/Fall 2020, pp. 29-39(11).

[5] Makadia, Sanam, Think beyond IT security — cyber resilience to build future-ready world : OT and ICS, critical infrastructure and beyond.(2023). Cyber Security: A Peer-Reviewed Journal, Volume 6 / Number 2 / Winter 2022–23, pp. 119-131(13).

[6] Microsoft Digital Defense Report (2022). Microsoft. https://www.microsoft.com, (2023).

[7] Cissé, Moh, An ISO 27001 compliance project for a cyber security service team. (2019), Cyber Security: A Peer-Reviewed Journal, Volume 2 / Number 4 / Summer 2019, pp. 346-359(14).

[8] Wheeler, Evan. Framing cyber security as a business risk. (2019). Cyber Security: A Peer-Reviewed Journal, Volume 2 / Number 3 / Winter 2018–19, pp. 202-210(9).

[9] Petruzzi, John; Loyear, Rachelle, Improving organisational resilience through enterprise security risk management. (2016). Journal of Business Continuity & Emergency Planning, Volume 10 / Number 1 / Autumn/Fall 2016, pp. 44-56(13).

[10] Wheeler, Evan.(2019). Framing cyber security as a business risk. Cyber Security: A Peer-Reviewed Journal, Volume 2 / Number 3 / Winter 2018–19, pp. 202-210(9).

[11] T. Tuncer, H. İŞ,(2018) Impact of End Users on Enterprise Cyber Security, International Engineering and Natural Sciences Conference,1,8, ISBN. 978-605-81971-3-8

[12] T. TUNCER, H. İş, (2018), Analysis of Cyber Security Vulnerabilities in Corporate Networks, International Engineering and Natural Sciences Conference, 1,11, ISBN. 978-605-81971-3-84

[13] H. İŞ, "LLM-Driven SAT Impact on Phishing Defense: A Cross-Sectional Analysis," 2024 12th International Symposium on Digital Forensics and Security (ISDFS), San Antonio, TX, USA, 2024, pp. 1-5, doi: 10.1109/ISDFS60797.2024.10527274.

[14] Hafzullah Is. 2024. Strategic Approaches to Eco-Efficient Computing in Institutional Environments. In Proceedings of the Cognitive Models and Artificial Intelligence Conference (AICCONF '24). Association for Computing Machinery, New York, NY, USA, 186–190. https://doi.org/10.1145/3660853.3660910

BIOGRAPHIES

Hafzullah İŞ, received his B.S. degree in Computer Engineering from Near East University in 2010 and his M.S. degree from the same university in 2012. He obtained his Ph.D. from Fırat University in 2021. Currently, he is an Assistant Professor and the Head of the IT Department at Batman University in the field of Computer Engineering. His research interests include Cyber Security, Artificial Intelligence, and Data Mining.