Journal of Computer Science Advancements, 2(3) - June 2024 176-182

Vulnerabilities and Threats to Ais Security Systems

Dola Ramalinda[1], Agung Raharja[2]
[1,2]Universitas Bandung, Indonesia

Corresponding Author: Dola Ramalinda, E-mail; dolaramalinda@bandunguniversity.ac.id

Article Information:
Received May 24, 2021
Revised June 20, 2021
Accepted June 30, 2021

ABSTRACT

This research explores vulnerabilities and threats to Accounting Information Systems (AIS) and evaluates effective mitigation measures to address these issues. Using both qualitative and quantitative approaches, this research involved literature studies, surveys, expert interviews, and case analysis to identify and analyze the different types of vulnerabilities and threats faced by AIS. The results showed that human error, software flaws, and system integration complexity are the main sources of vulnerabilities in AIS. The most common threats are cyberattacks, insider threats, and Distributed Denial of Service (DDoS) attacks. The impact of these threats includes financial loss, reputational damage, and significant legal implications.Mitigation strategies identified include the development of robust security policies, the use of cutting-edge security technologies, and the conduct of regular audits and monitoring. The findings emphasize the importance of a layered approach to improving AIS security and reliability. This research provides an in-depth insight into how organizations can identify, evaluate and manage vulnerabilities and threats to their AIS, which is essential for maintaining the integrity, confidentiality and availability of accounting data in an increasingly complex digital age.

Keywords: *Cyber Threats, Ddos Attacks, Security Technology*

Journal Homepage https://journal.ypidathu.or.id/index.php/jcsa

How to cite: Ramalinda, D., & Raharja, A. (2024). Vulnerabilities and Threats to Ais Security Systems. *Journal of Computer Science Advancements*, 2(3). 176-182 https://doi.org/10.70177/jsca.v2i3.1055
Published by: Yayasan Pendidikan Islam Daarut Thufulah

INTRODUCTION

Technological developments and developments in the field of software are progressing very rapidly(Raharja, Setiyono, et al., 2024). Accounting Information Systems (AIS) are a vital component in the operation and management of modern businesses(Tuasamu et al., 2023). AIS not only serves as a tool to record financial transactions, but also as a system that provides accurate and relevant data for strategic

decision-making. However, with the increasing reliance on information technology, AIS is becoming increasingly vulnerable to various threats that can damage the integrity, confidentiality, and availability of the data it manages.

This study will analyze and identify risk factors that can influence(Raharja, Pramudianto, et al., 2024) Vulnerabilities in AIS can come from a variety of sources, including human error, software flaws, and cyber threats such as malware and phishing attacks. These threats can result in significant financial losses, damage to a company's reputation, and even legal implications if legally protected data is exposed or misused.

This article will explore the different types of vulnerabilities and threats that can affect AIS, and discuss steps organizations can take to mitigate risks and protect their information systems. A deeper understanding of these threats and their mitigation strategies is essential for companies to ensure the security and reliability of their information systems, and to maintain the trust of stakeholders.

RESEARCH METHODOLOGY

Research methodology is a framework or systematic approach used researchers to plan, conduct, and analyze research(Sutisna et al., 2024) This research uses qualitative and quantitative approaches to identify and analyze vulnerabilities and threats to the Accounting Information System (AIS)(Latifah & Arisyahidin, 2022). The methods used include literature studies, surveys, interviews, and case analysis. The following are details of each method:

Literature Study

Literature Study At this stage the author studies the theories or journals regarding medical records that underlie this research (Raharja, Agung Rachmat, 2024)

Objective: To collect information and findings from previous research on AIS vulnerabilities and threats.

Process:

Identify relevant journals, books, articles and industry reports(Angraini, 2014). Analyze key findings from these sources to get a comprehensive picture of common types of vulnerabilities and threats. Develop a conceptual framework based on the literature findings for use in further research.

Survey

Objective: To collect quantitative data from AIS practitioners on their experiences with vulnerabilities and threats and the mitigation measures they have taken(Muchsam et al., 2023).

Process:

Designed a questionnaire that included questions regarding the types of vulnerabilities experienced, frequency of threats, impact of those threats, and security measures implemented. Distributed the questionnaire to a sample of

accounting and IT professionals in various companies. Used statistical tools to analyze the survey data, such as descriptive and regression analysis.

Interview

Objective: To gain in-depth insights from experts and practitioners on vulnerabilities and threats to AIS and effective mitigation strategies.

Process:

Select interview participants consisting of information security experts, internal auditors, and IT managers with experience in managing AIS. Developed an interview guide with open-ended questions covering topics such as the most common types of threats encountered, actual events related to threats, and mitigation approaches. Conducted interviews face-to-face or via digital communication platforms, recording and transcribing the interviews. Analyzing the interview transcripts to identify common themes and patterns.

RESULT AND DISCUSSION

LITERATURE REVIEW

Research on vulnerabilities and threats to Accounting Information Systems (AIS) has shown that these systems face various types of risks that can affect a company's operations and data security. The following are some of the key findings from the existing literature:

Vulnerabilities in AIS

Human Error

Human error is one of the main sources of vulnerability in AIS. The study by Huber et al. (2013) showed that errors in data entry, mistakes in ntegr configuration, and failure to follow security procedures can lead to significant weaknesses in ntegr.

Software Weaknesses

Weaknesses in software, such as bugs and uninstalled patches, can be exploited by hackers to gain unauthorized access to the AIS. Research by Zviran and Erlich (2006) highlights the importance of proper software maintenance and periodic updates to mitigate this risk.

Complex System Integration

AIS are often integrated with other information systems, which can create new points of vulnerability. According to Xu and Quaddus (2013), the complexity of these integrations can introduce additional security risks if not properly managed. the results, unwarranted speculation, inflating the importance of the findings, tangential issues or over-emphasize the impact of your research.

Threats to AIS

Cyber Attacks

Cyber threats such as malware, ransomware, and phishing are the main threats to AIS. Research by Kshetri (2010) shows that cyberattacks are increasingly sophisticated and often target weaknesses in corporate information security systems.

Insider Threats

Threats from insiders, including disgruntled employees or having malicious motives, are also a significant risk for AIS. Greitzer et al. (2012) identified that these threats are difficult to detect and can cause major damage if not closely monitored.

DDoS Attack

Distributed Denial of Service (DDoS) attacks can disrupt AIS operations by flooding systems with unauthorized internet traffic. According to research by Chang et al. (2016), DDoS attacks can cause significant downtime and large financial losses.

Mitigation Strategies

Development of a strong security policy

Implementation of comprehensive security policies and security training for employees can reduce the risk of human error. Bulgurcu et al. (2010) emphasized the importance of security awareness and education in organizations.

Use Of Cutting-Edge Security Technologies

The use of technologies such as data encryption, firewalls, and intrusion detection systems can help protect AIS from external threats. According to research by Chen et al. (2012), cutting-edge security technology is the key to protecting information systems from cyberattacks.

Regular audits and monitoring

Regular security audits and constant monitoring of system activity can help detect and respond quickly to threats. Research by D'arcy and Hovav (2007) shows that regular audits can identify security weaknesses and ensure compliance with security policies.

This study identifies and analyzes various vulnerabilities and threats to Accounting Information Systems (AIS) and evaluates effective mitigation measures. The results of this study are discussed in several main categories: types of vulnerabilities, types of threats, impacts on organizations, and mitigation strategies.

Types of vulnerability

Human Error

The study found that human error is one of the main causes of vulnerability in AIS. These errors can occur in the form of inaccurate data entry, errors in programming, and omissions in following security procedures. Survey Data show that 45% of respondents have experienced incidents caused by human error.

Software Flaws

Weaknesses in software, such as bugs and patches that are not installed, are a significant source of vulnerability. Analysis of the literature shows that software that is not updated becomes an easy target for hackers. As many as 30% of survey respondents reported having experienced attacks that took advantage of software flaws.

Integration of complex systems

The integration of AIS with other systems often introduces new points of vulnerability. Case studies show that poorly managed integration can lead to data leaks and operational disruptions. About 25% of respondents identified system integration as the main source of vulnerability.For most essays, one well-developed paragraph is sufficient for a conclusion, although in some cases, a two or three paragraph conclusion may be required. The another of important things about this section is (1) do not rewrite the abstract; (2) statements with "investigated" or "studied" are not conclusions; (3) do not introduce new arguments, evidence, new ideas, or information unrelated to the topic; (4)do not include evidence (quotations, statistics, etc.) that should be in the body of the paper.

Types of threats

Cyber Attacks

Cyber attacks, including malware, ransomware, and phishing, are the biggest threat to AIS. Interviews with security experts show that these attacks are increasingly sophisticated and often target sensitive financial data. 60% of respondents reported having experienced a cyberattack in the past two years.

Insider Threats

Threats from insiders, such as disgruntled employees or having malicious motives, are a significant risk. Literature studies and interviews reveal that these threats are difficult to detect because they involve people who have legitimate access to AIS. About 20% of respondents admitted to incidents involving insiders.

DDoS Attack

Distributed Denial of Service (DDoS) attacks can disrupt AIS operations by flooding systems with unauthorized traffic. Case studies show that DDoS attacks can cause significant downtime and financial loss. As many as 15% of respondents have experienced DDoS attacks.

Impact on the organization

The study found that the impact of vulnerabilities and threats to AIS can be very detrimental to organizations. These impacts include:

Financial losses

Cyberattacks and system weaknesses can lead to immediate financial losses, such as costs to restore systems and lost revenue from downtime.

Reputation damage

Security incidents involving data leaks can damage a company's reputation and lower customer confidence.

Legal implications

leakage of legally protected data can result in lawsuits and fines from regulators.

Mitigation Strategies

Strong security policy development

1) Implementation of a comprehensive security policy is the first step in reducing risks. This policy should include protocols for managing access, handling security incidents, and regular training for employees. As many as 70% of respondents who had strong security policies reported lower incident rates.
2) Use Of Cutting-Edge Security Technologies The use of technologies such as data encryption, firewalls, and intrusion detection systems is key to protecting AIS from external threats. Case studies show that companies that invest in advanced security technologies are better able to cope with cyber attacks. About 55% of respondents using this technology reported a significant improvement in the security of their systems.
3) Regular audits and monitoring Regular security audits and constant monitoring of system activity can help detect and respond quickly to threats. Survey Data shows that companies that conduct security audits at least twice a year have a lower incidence rate. As many as 65% of respondents stated that regular audits help identify and fix security flaws before they are exploited.

CONCLUSION

The study reveals that vulnerabilities and threats to AIS are complex and multifaceted issues, requiring layered mitigation approaches. Human Error, software flaws, and system integration complexity are the main sources of vulnerability, while cyber attacks, insider threats, and DDoS attacks are the main threats faced. The impact of these threats can be detrimental financially, reputationally, and legally. To address these challenges, organizations must develop robust security policies, adopt cutting-edge security technologies, and conduct regular audits and monitoring. With effective mitigation strategies, organizations can improve their AIS security and reduce the risks associated with vulnerabilities and cyber threats.

REFERENCES

Angraini, G. (2014). Analisis Kemampuan Literasi Sains Peserta Didik SMA Kelas X di Kota Solok. Jurnal Pendidikan Matematika dan Sains. *Jurnal Pendidikan Matematika dan Sains.*, *1*(4), 161–170.

Latifah, N., & Arisyahidin. (2022). Analisis Sistem Informasi Akuntansi dan Pengendalian Internal terhadap Kinerja Karyawan (Studi Kasus PT Bintang Kediri). *Otonom*, *22*(8.5.2017), 2003–2005.

Muchsam, Y., Sucipto, B., Rismawati, R., Rusdianti, I. S., & Raharja, A. R. (2023). Forming the Character of a Physically Healthy Young Generation Through Military Education. *TGO Journal of Community Development*, *1*(2), 90–95. https://doi.org/10.56070/jcd.2023.015

Raharja, Agung Rachmat, H. I. (2024). *Design of EMR (Electronic Medical Record) Applications Using RFID Cards to Record Patient Medical Record Data at The Sukajadi Bandung Health Center*. 66–72.

Raharja, A. R., Pramudianto, A., & Muchsam, Y. (2024). Penerapan Algoritma Decision Tree dalam Klasifikasi Data " Framingham " Untuk Menunjukkan Risiko Seseorang Terkena Penyakit Jantung dalam 10 Tahun Mendatang. *nawalaeducation*, *1*(1). https://doi.org/10.62872/cwgzp962

Raharja, A. R., Setiyono, R., & Hariyanti, I. (2024). PERANCANGAN DAN IMPLEMENTASI CALIFORNIA BEARING RATIO (CBR) DENGAN MENGGUNAKAN C# DAN ARDUINO. *Jurnal Responsif : Riset Sains dan Informatika*, *6*(1), 54–62. https://doi.org/10.51977/jti.v6i1.1425

Sutisna, T., Raharja, A. R., Hariyadi, E., Hafizh, V., & Putra, C. (2024). *Penggunaan Computer Vision untuk Menghitung Jumlah Kendaraan dengan Menggunakan Metode SSD (Single Shoot Detector)*. *4*, 6060–6067. https://doi.org/doi.org/10.31004/innovative.v4i2.10071

Tuasamu, Z., M. Lewaru, N. A. I., Idris, M. R., Syafaat, A. B. N., Faradilla, F., Fadlan, M., Nadiva, P., & Efendi, R. (2023). Analisis Sistem Informasi Akuntansi Siklus Pendapatan Menggunakan DFD Dan Flowchart Pada Bisnis Porobico. *Jurnal Bisnis Manajemen*, *1*(2), 495–510.