Research Article

Risk Assessment Technology on the Application of Admission of New Students in High School

Jaka Purnama, Yayuk Ike Melani

[1]Information System, STMIK PalComTech, Indonesia

Abstract.
The rapid development of technology makes almost all service activities use information technology, including service activities in schools. One of the services provided by the school is to facilitate prospective students who are interested in registering as new students at school by building an open source-based new student registration application so that prospective students can register anywhere without having to come to school directly. The use of this application has several technological obstacles such as the system being locked due to being hacked by hackers, phishing, attacks from viruses, attacks from previous people who know the security of data from a computer system, unstable computer networks that affect the operational process to be slow, and low level of computer security. The purpose of this study is to provide recommendations for controlling the risk of using information technology in new student registration applications so as to minimize future losses to schools by measuring the likelihood and impact of using computer technology. The risk assessment model uses the NIST SP 800-30r1 framework, which is used as a tool to measure how big is the threat level and the impact caused by attacks that attack the application. The NIST SP 800-30r1 framework has stages such as recognizing system characteristics, threats, vulnerabilities, analyzing system handling, determining likelihood, determining impact, risk determination, recommending control, and determining results. The results of this study were used as recommendations to minimize losses obtained by schools and as a benchmark for controlling the risk of using technology to improve the quality of schools.

Keywords: risk assessment technology, admission, high school

Corresponding Author: Jaka Purnama; jaka_purnama@palcomtech.ac.id, Yayuk Ike Melani; email: yayuk_ike@palcomtech.ac.id

Published 26 May 2023

Publishing services provided by Knowledge E

Selection and Peer-review under the responsibility of the ICASI Conference Committee.

1. Introduction

Rapid development of technology makes almost all service activities using information technology including service activities in school. One of the services provided by the school is to facilitate prospective students who are interested in applying to become new students in school by building a new student registration application based on open source so that prospective students can register anywhere without having to come to school directly. In this covid-19 pandemic, most schools already use new student registration applications as a support tool to conduct student admissions. The use of applications can not be separated from the risks of using technology such as

phishing attacks, insider terror, various viruses that attack, installation failures and so on. In the realm of engineering, risk is described quantitatively and more focus on technology. Social information provides information that helps how individuals interact, make decisions, structure, and respond to change. The application of Risk Management is built to avoid losses caused by the occurrence of a risk threat or event [2]. Indonesia is the country with the largest Threat Exposure Rate. Threat Exposure Rate is down from the percentage of computers affected by malware attacks within a 3-month period[3].

The research was focused on how to assess the risk of the use of information technology from a new student admission application used by one of the high schools in Palembang. Assessment of the risks to the use of technology is needed to measure how much risk will be faced by the school so that the school can anticipate the risk of using technology so that the applications used run smoothly without obstacles. The assessment conducted has a scale of probability of occurring from the lowest (0.1) with the category is not dangerous to the highest (1.0) with a very dangerous category that can be at risk of causing harm to the company. Previous research has discussed the importance of doing good security in terms of login applications using passwords that can be encrypted. Encrypted passwords can use MD5 as the original password scrambler[4]. The role of system security methods used is also important to maintain the security of information stored in a system. Similar research has also revealed that there are some risks of using information technology is still often ignored by system users so there are often obstacles such as users can not open the system because it has been hacked by hackers and the level of security of the system used is classified as weak . Based on the definition of risk can be described the magnitude of the possibility of a danger with the severity grouped into levels of frequency to severity [7].

The purpose of this study is to assess the risk of how likely the threat is and how much of a risk impact on the use of new student admission applications and provide some risk control recommendations in accordance with the problems of computer security that pose a threat that causes impact such as losses that will be faced by schools.

2. Methods

2.1. Data Collection Techniques

This study uses data collection techniques in the form of interview techniques and observation techniques. Interviewing is one of the few techniques in data collection that is widely used in research. There are three types of interviews: structured interviews, semi-structured interviews and unstructured interviews. The interviews conducted by researchers were using semi-structured interviews. The interview conducted by the researcher is to conduct an interview directly to the informant in the study. The informant in question is the head of the Business Administration at the school concerned. The data obtained in the interview that has been done is data in the form of information on how the process of using new student admission applications that have been running. What kind of hardware and software are used in building applications. Any obstacles that often occur during the use of new student admission applications. Any attack that often attacks new student admission applications. What has been done so far to overcome the obstacles and attacks that attack new student admission applications.

The next data collection is to use observation techniques. Observation is one of the data collection techniques that researchers perform by observing directly to the target of the study [10]. Observation is a way of collecting data by making observations and recording all the phenomena targeted by observations. Observation made by researchers is to make direct observations of the process of using new student admission applications used by prospective student users and user admins. One of the observation processes carried out is observing how prospective students open the application, using what browser. Whether at the time of opening the application already uses a security protocol that is already secure. The data obtained is some information such as what threats have attacked the application and how the handling process is carried out so far.

The next data plan is to use a questionnaire. Questionnaires are one of the techniques of data collection by relying on communication with data sources and providing multiple questions according to the object of the study [12]. The questionnaire contains a list of structured questions followed by several answer options [13]. The questionnaire used by the researchers adopted questions that had been provided by the NIST Special Publication 800-30 revision 1 framework. The result of the questionnaire is any threat information that can attack a new student admissions application.

2.2. Risk Assessment Process

The risk assessment process used by researchers is to use the NIST Special Publication 800-30 revision 1 framework. NIST SP 800-30 revision 1 is a standardized document developed by the National Institute of Standards and Technology[14]. Dnature conducts risk assessment,this framework has nine stages, namely the characteristics of stem, threat identification, vulnerability identification, control, possibility of occurring, impact analysis, determining the level of risk and finally providing recommendations for control against threats that have attacked.

1. Characteristics of the system

   Identify information technology that supports new student admission applications. Identification of the characteristics of this system is necessary to ensure the risk measurement process is carried out in accordance with the vision and mission of the company. Identification is identified to identify the hardware used, the software used, anyone involved in the management and use of the application.

2. Identify threats

   Identifying threats to application use. Identification is done by determining what sources of threats can attack the new student admissions application. The source of the threat can come from people within the company or from outside the company.

3. Identify vulnerabilities

   Identify vulnerabilities to the source of threats that attack the application. Vulnerability is a weakness in the system or internal control intentionally or unintentionally in the utilization of the system used.

4. Control

   Identify any controls that the data builder performs on new student admission applications.

5. Possibility of happening

   Used to get how much value is likely to occur against weaknesses in new admissions applications. The probability of it happening is whether it is high, moderate or low. A high level of threat sources will be very able to prevent vulnerabilities that are done no longer effective. At a moderate level, the source of the threat

is able to penetrate the defense but can still be overcome by the system. Low-level, threat source cannot penetrate at all the security defense systems used. The highest level in probability of occurring has a value (1.0), medium (0.5) while low (0.1).

6. Impact analysis

   Used to get how much impact a threat will have from the use of new admissions applications. The impact on applications also has high, medium and low groups. High levels of causing severe damage or loss of the system's ability to perform operations in other words, intruders have successfully crippled the security of the system. Moderately, it causes major damage to the system but is still active and preventable. While low, resulting in minor damage that is not too severe. The highest levels in impact have values (100), medium (50) while low (10)

7. Determination of the level of risk

   To determine the level of risk using a 3x3 matrix. The risk matrix is a tool used during risk assessment.

8. Control recommendations

   Recommendations in the form of advice on how to take precautions and controls to reduce the risks that occur in the application.

3. Result and Discussion

There are several stages that researchers do in conducting risk assessments, namely:

1. Characteristics of the system

   Hardware used based on personal computers or PCs that currently still use third parties as an outside server to store data that has been processed by the application. The data processed is data on prospective students, school facility data, extracurricular data, registration data and admin data. The application user is a prospective student while the data manager of the application is the administrative staff.

2. Identify threats

   Threat identification is obtained through interviews and questionnaires conducted by researchers. The result of interviews and questionnaires conducted is that there

are threats coming from outside that try to enter into the admissions application of new students by entering passwords and usernames randomly, changing plug ins in applications, scanning networks, flooding, wireless jamming and Ddos in applications, the entry of malware into the system that can damage some data inthe hardware used and damage to data storage media such aslong-standing hard drives. Used is never replaced.

3. Identify vulnerabilities

Vulnerability identification is obtained through interviews and questionnaires that have beenshared. From the ahsil interview and questionnaire obtained some threats that attack the system seen in table 1.

TABLE 1: Identify vulnerabilities.

Types of Risks	Vulnerability
User is the manager of the system but does not work in the school environment	Users know hardware and software in building new student admission applications
The operating system used is not updated.	Outdated operating systems affect the security of the systems used
Power supply tools	Power supply tools that are less treated will experience damage even though the power supply is one of the important tools in the system.
Natural events such as fires	Improper security and arrangement of cables in network installations will make the possibility of fire.
Hurricanes and earthquakes	Can be used as one of the threats on new student admission applications
Spearphising attacks	Data managers must be careful in receiving phishing emails in the form of viruses.
Malware	Being late in virus updates and not using tighter security allows malware viruses to enter the computer system.
Flash drive	Negligence of staff who perform removal of applications containing malware
System use training	Training that lacks understanding of the system often makes mistakes in the system.
New student admissions app users use smartphones in registering	Intruders benefit from firewall protection used to protect the system.

4. Control

The controls obtained in the interviews that have been carried out are poured into documents that include standards and procedures in the operation of new admission applications.

5. Possibility of happening

After identifying the vulnerability, it can further determine the likelihood of it happening. The probability of this happening can be seen in table 2.

TABLE 2: Probability of happening.

Types of Risks	The degree of likelihood of occurring
The user is the manager of the system but does not work in the school environment	High
The operating system used is not updated.	High
Power supply tools	Low
Natural events such as fires	Middle
Hurricanes and earthquakes	Middle
Spearphising attacks	High
Malware	High
Flash drive	High
System use training	Low
New student admissions app users use smartphones in registering	Middle

6. Impact analysis

The impact value is derived from the results of measuring how much impact is caused by the threat that attacks the application. Dampat values are obtained from questionnaires that have been distributed. The results can be seen in table 3.

7. Determination of the level of risk

The level of risk obtained by using a 3x3 matrisk can be seen in table 4.

8. Control recommendations

Recommendations in the form of advice on how to take precautions and controls to reduce the risks that occur in the application.

Table 3: Impact.

Types of Risks	Impact	Level of risk impact
The user is the manager of the system but does not work in the school environment	Users who are system managers but do not work in school environments may be able to commit data theft.	High
The operating system used is not updated.	May result in some functions on the system not working because the operating system used does not support some of these plugs in applications.	High
Power supply tools	Damage to the power supply can be one of the obstacles in the process of supporting applications.	Low
Natural events such as fires	Damage to hardware and software used hampers the process of running new student admission applications	Middle
Hurricanes and earthquakes	Hardware damage and even loss of hardware can hamper the process of running new student admission applications.	Middle
Spearphising attacks	Create a user who opens a fake email that convinces that the email is a submission from a close friend so that the system processor is interested in clicking on the submitted URL	High
Malware	Pops upspam ads on the monitor screen used for new student admissions apps	High
Flash drive	Flash drives that contain viruses can move to the computer used for processing system data so that the computer is in poor condition.	High
System use training	Training in the use of less systems will be one of the threats in making mistakes on the system.	Low
New student admissions app users use smartphones in registering	Weak firewalls on smartphones cannot protect the system so intruders can freely use user data.	Middle

4. Conclusions

Risk assessment is carried out using the NIST SP 800-30 Revision 1 framework which has nine stages in conducting risk assessment. To get information on what attacks and threats have attacked the admissions application of new students researchers use data collection tools such as interviews, observations and the dissemination of questionnaires to system processing users. From result of data collection obtained various threats such as malware viruses, the use of flashdrive, neglect in system maintenance and so on. These risks are used in decision making to provide risk control recommendations.

Table 4: Risk Levels.

Types of Risks	Possibility of happening	Impact value	Risk value	Level of risk
The user is the manager of the system but does not work in the school environment	High (1,0)	High (1,0)	100	High
The operating system used is not updated.	High (1,0)	High (1,0)	100	High
Power supply tools	Low (0,1)	Low (0,1)	10	Low
Natural events such as fires	Middle (0,5)	Middle (0,5)	50	Middle
Hurricanes and earthquakes	Middle (0,5)	Middle (0,5)	50	Middle
Spearphising attacks	High (1,0)	High (1,0)	100	High
Malware	High (1,0)	High (1,0)	100	High
Flash drive	High (1,0)	High (1,0)	100	High
System use training	Low (0,1)	Low (0,1)	10	Low
New student admissions app users use smartphones in registering	Middle (0,5)	Middle (0,5)	50	Middle

Acknowledgments

References

[1] Wulandari S, Wahyudi A. ”Risk management in the development of organic agriculture in Indonesia.” Proceedings of the national seminar on organic agriculture. Bogor. 2014.

[2] Prasetyo, Zico, Afriyeni A. ”Implementation of operational risk management at PT. West Sumatra Regional Development Bank Branch painan South Coast Regency.” 2019.

[3] Prakasa JE. Improved security of information systems through the classification of attacks on information systems. *Sci J Inf Technol Asia*. 2020;14(2):75–84.

[4] Khairina DM. “Login system security analysis.” Mulawarman Informatics: Scientific. *J Comput Sci*. 2016;6(2):64–67.

[5] Umar R, Riadi I, Handoyo E. Information system security analysis based on THE COBIT 5 framework using capability maturity model integration (CMMI). *J Bus Inf Syst*. 2019;1:47–53.

[6] Melani YI, Mahmud M. Risk assessment on the monitoring system of teaching and learning activities in private universities. *J Technol Inf Sys. Jurteksi*. 2020;7(1):23–32.

Table 5: Control Recommendations.

Types of Risks	Level of risk	Control recommendations
The user is the manager of the system but does not work in the school environment	High	Use clear agreements in purchasing systems that use third parties
The operating system used is not updated.	High	Always update your operating system.
Power supply tools	Low	Keep maintenance on power supplies and other tools
Natural events such as fires	Middle	Prevention such as backing up data is not just one place
Hurricanes and earthquakes	Middle	Prevention such as backing up data is not just one place
Spearphising attacks	High	Use anti-spam and anti-phishing tools
Malware	High	Perform a file malware scan
Flash drive	High	Use an antivirus that can detect the visrus in the flash drive
System use training	Low	Create an app usage guidebook
New student admissions app users use smartphones in registering	Middle	It is recommended for prospective students to be able to open applications on a secure network

[7] Isnaini KM. Ade. “Analysis of the influence of risk assessment (risk assessment) on mining accidents on coal mining activities (case study at Pt. Baturona Adimulya).” *J Eng Patra Akademika*. 2017;8(02):19–25.

[8] Edi FR. Psychodignostic interview theory. LeutikaPrio Publisher; 2016.

[9] Mayasari, Silvina. ”The effectiveness of Instagram social media in the publication of the anniversary of the National Museum of Indonesia (MNI) to the community.” 2018:190-196.

[10] Ayudia A, Suryanto E, Waluyo B. Analysis of Indonesian language usage errors in the observation report in junior high school students. *BASASTRA*. 2017;4(1):34–49.

[11] Sari N, Achnes S. Tourist satisfaction with culinary tourism in the beautiful beach attractions Selatbaru District Bantan Bengkal is. Diss Riau University; 2016.

[12] Risanty, Dewi R, Sopiyan A. ”The creation of a teaching and learning evaluation questionnaire application using Telegram Bots at the Faculty of Engineering,

University of Muhammadiyah Jakarta (Ft-Umj) with polling methods." Proceedings semnastek (2017).

[13] Nugroho, Eko. Principles of compiling questionnaires. Universitas Brawijaya Press; 2018.

[14] Aha D, et al. "UCI repository of machine learning database." 1987.

[15] Meilani YI, Syamsuar D, Kunang YN. "Technology risk assessment on E-university academic information system implementation." *J Comp Dev 1.1*. 2019;54-

[16] Catal C, Diri B. "A systematic review of software fault prediction studies". *Expert Syst Appl*. 2009;36(4):7346–7354.