RISK ANALYSIS RESEARCH

Abstract

Identify and perform a risk analysis of any possible threat to the North-West University networks

OMPHEMETSE SENNA

omphesenna@gmail.com

TABLE OF CONTENT

1. INTRODUCTION

The North-West university network comprises servers, network gadgets, and more computers that are connected to permit correspondence of the clients, sharing data, and furthermore, contains the information of students. The North-West University network associates a great many students everywhere in the world utilizing NWU sites consistently. Therefore, there are high prospects that digital assailants can attempt in all ways to enter the university network and abuse the university policies in other to profit from it. This report serves to examine the potential dangers that can happen to the northwest University networks.

2. PURPOSE

The purpose of this assignment is to Identify and perform a risk analysis of any possible threat to the North-West University network.

3. IDENTIFY THREATS

North-West University is an institution of high-level education providing different facilities for students to sharpen them for their roles in their dream jobs after making research and obtaining their degrees or even going further up.

Who is the vendor?

- Employees
- Students

Who uses the institution system?

- Employees
- Students
- Visitors or guests if given authority by the institution

There are numerous potential dangers that can be carried out on the network of the North-west university. During this age, innovation is ascending at a higher speed contrasted with the past ages and it is arriving at its pinnacle. The present world depends on innovation whereby individuals can utilize innovation to create merchandise and ventures.

Every single year, new cyber-attacks happen to various associations relying upon the security of that association. Associations experience various dangers in their organizations consistently and this issue rises each year.

There are numerous manners by which digital aggressors assault associations, people, or anything they are focusing on that will profit them.

Examples of cyber-attacks that can be used in the North-West university network:

- Man in the middle attacks (MITM),

- Phishing.
- SQL injection.
- Ransomware
- Cross-site scripting.
- Code injection.
- Viruses
- worms.
- Spyware.
- Information extortion

The above can be used to attack the network of the institution:

- Unauthorized access to the network.
- Disturbing of the network.
- Data leakage.

The primary focal point of this report will be on Unauthorized access to the network of the institution using SQL injection.

Structured query language (SQL) injection is an infusion procedure that is utilized by digital hackers to attack networks or the database of an association. They insert pernicious codes in the organization of the association to approach the database. At the point when assailants have full access to the organization of the North-West University, they can add their data to the site, they can erase any record or alter it in any capacity. Each association has its own information base where information is remained careful and can be changed whenever. Furthermore, this information is kept hidden and must be gotten to by the university individuals who have been given authority by the division of the university.

System Components or Assets that can be exposed to intruders:

Assets 1:

- People
  - Employees
  - Students

Assets 2:

- Data
  - Information related to employees and students
- Software
  - Applications, operation systems.
- Hardware
  - Power supply
  - CPU

North-West University is outstanding amongst other perceived universities all throughout the planet and hackers realize that they can hit an extremely immense big stake in this organization. Information about graduates of various ages is kept in the framework as confirmation to show that they have passed and have once been admitted to the university. When the information has been erased by the hackers there will not be verified to show that the alumni have been conceded to the university or even passed since not all matriculants approach universities.

The hackers can add anybody they allude to the framework or even open their own positions of adding any defenceless matriculants to the university and keep them as graduates with the goal that they can be utilized without any problem. They can hush up about the data so they can compromise the university by requesting ransom to deliver the information.

Breaching of the North-West university network may also affect the following:

- The reputation loss of the university.
- Financial loss.
- Numerous attacks may occur whenever every one of the entryways will be opened.
- Closure of the university.
- Disruption of the work.
- Employees may lose their jobs.

4. **RISK ASSESSMENTS:**

Determining the Loss Frequency:
Impact ratings that can be done in the institution can be categorized as:

- High: substantial damages are not easily retrieved, and the costs of repair are more than 60%.
- Medium: damages can be recuperated, and the costs of repairs may be between 30 and 50%.
- Small: damages and that bad and can be highly recovered and the costs of repairs can be between 0 and 30.

The reputation:

- This damage can be categorized as High since reputation is the adage of the institution, and once the institution misfortunes its reputation, numerous individuals won't confide in it again and the organization will lose its capability to capital and more prominent harm to its firm.

Disruption of work:

- Classified as High category because once the institution has been hacked, this may bring about the stop of specific exercises and others might shut down completely. For instance, the continuation of studies, and the business tasks.

Financial loss:

- Classified as High category because the institution might lose its future incomes since quantities of matriculants will proceed with their studies in different organizations and this may result in less pay for the business.
- Investors will lose their investments.
- The Institution may lose cash in fixing damages.

Numerous attacks may occur whenever every one of the entryways will be opened:

- Classified as Low since activities of the institution can be changed and the new security might be executed therefore chances of infiltrating are less.

Likelihood:

The North-West University is probably going to be targeted by intruders at the rate of 4.99 out of 5 every 5 years, and the annualized likelihood of attackers is 4.5 / 5, which is 90% out of 100.

Attack success probability

North-West University has been excellent regarding planning for any episodes. It is a very much ensured institution that is the reason why there are lower cases of threats to its networks for the past 5 years. Therefore, the organization may appoint a quantitative estimation of 85%.

Calculations of loss Frequency:

Likelihood in percentage = 90

Attack success probability = 85

Loss frequency = likelihood * attack success probability

= (90 * 85) / 100

= 76.5%

Assets 1 which includes employees and students demonstrate less level of being assaulted. It can be assessed that the potential for the success of being attacked stands at 10%. On the off chance that the attackers choose to attack assets 1. The odds of being hacked effectively are assessed to be 30% in a year with a score of 100%. The assets are esteemed at a score of 50 on a size of 0 to 100. The assessed loss of resources might be esteemed at 40% possibilities relying upon the administration of the establishment whether to save a portion of the representatives after an effective attack.

Assets 2 which includes data, software and Hardware shows less level of being attacked. It can be estimated that the potential for the success of being attacked stands at 1%. If the attackers choose to attack assets 2. The odds of being hacked effectively are assessed to be 10% in a year with a score of 100%. The resource is esteemed at a score of 17 on a size of 0 to 100. An expected loss of resources might be esteemed at 10% possibilities on the grounds that the assets are constantly overseen by the IT department.

Therefore, the risk ratings for the two vulnerabilities are:

Assets 1: has higher possibilities dependent on the attacks and targets since Students and employees don't follow measures of protection sometimes than **Assets 2**, where resources are secured by the IT department.

The following can put the security network of the institution at risk if not monitored.

- If the software of the are not updated
- Not enough security management
- Employees and students who are careless mainly when online
- Changing passwords after a long period of time.

5. **RISK CONTROL:**

The attackers realize that the likelihood of penetrating the organizations using assets 2 is less because of tight measurements that are carried out by the IT department. The odds of utilizing Students' mobiles or PCs are high. As a result, that will not take them anyplace since the students are allowed, to utilize less level of the institutional assets. Students have less percentage to the database of the framework, and they utilize the above construction of the data set.

Employees have a more noteworthy possibility of being utilized by the attackers since they got a more prominent possibility of getting to the foundation information base. Thusly, attackers may send vindictive codes through messages or emails to the workers. From that point, these vindictive codes will be carried out to the systems and networks of the institution, and this will give the attackers more access.

Risk management control on people:

- Institution must train students and employees on how to use the resources of the institution and, also how to identify and avoid certain attacks that might be used by intruders to penetrate the system and networks of the institution.
- Their passwords must be changed regularly.
- Password must contain at least 8 characters
- Conduct background check
- Download and install recommended software

There are certain measures that can be implemented and followed by the institution to contain and control the risks.

For Assets 1: Students and employees Defence:

- Computers and mobiles of assets 1 will have to be monitored.

Acceptance:

- The institution will have to accept any news whether the attackers used staff to penetrate the system.

Transference:

- Risks must be transferred to other departments that have more power to control and contain the problem.

For Assets 2: Data, Software, and Hardware Defence:

- Anti-viruses can be applied to the systems.
  Example: Computer desktops, Wi-Fi networks
- Use firewalls Acceptance:
- Once the institution has been attacked, acceptance must be taken by the institution to manage everything and to accept what it is dealing with. And the institution will have to face and deal with everything that is coming its way depending on the level of damage.
  Transference:
- Risks must be transferred to other departments that have more power to control and contain the problem.

Mitigation:

- That’s where insurances get involved in this platform because, with funding, the institution can fix the problem and implement other technologies to prevent attacks again.

Termination:

- Certain assets that have high risk must be terminated for the business to function very well.