Sri Lanka Institute of Information Technology

Advanced Networking Technologies
IE2052

Assignment 1

Submitted by: -

Student Registration Number	Student Name
IT21049354	Athauda A.M.I.R.B

Date of Submission
07/08/2022

Table of Contents

1. Introduction

The term "Information Security" is used to refer to the methods and systems that businesses use to keep sensitive data safe. To put it simply, information security is the process of protecting sensitive information from being accessed by anyone other than the intended recipient. Data tampering and data deletion are among the consequences of security incidents. There is a monetary cost associated with an attack, in addition to the disruption of business operations and harm to a company's reputation. To protect themselves from threats like phishing, malware, viruses, malicious insiders, and ransomware, businesses must set aside funds for security and make sure they are prepared to detect, respond to, and proactively prevent attacks. As a guide to campus security, this document describes the logical and physical security management with specific examples.

2. Physical Vulnerabilities

2.1. Physical Security

Physical security is the safeguarding of company, agency, or institution’s personnel, equipment, software, networks, and data from any physical actions or events that could cause major loss or damage. Fire, floods, natural disasters, theft, vandalism, and terrorism are all covered. Even though most of these are covered by insurance, physical security's focus on damage prevention avoids the loss of time, money, and resources due to these events.

2.2. What are Physical Vulnerabilities?

Physical security is to do with closing the physical loopholes. We'll be wasting our security measures if we keep the server room door open despite our best efforts. So, the physical vulnerability means the probability of getting affected or damaged by unauthorized people in physical security of your infrastructure, which means your routers, switches, hubs, and servers are available to attackers who try to access.

2.3. List of Physical Vulnerabilities

1. Facial recognition and thermal alarm system failure
    - Facial recognition and thermal alarm systems at the entrance failed to recognize the student's face if the student wore a face mask. At once, it could not get the exact temperature of the student when more students were going one by one. from this, any unauthorized person could access the campus if there were a rush at the entrance.

2. The glass of the box that stores routers and switches in labs can be broken
    - Routers and switches stored in labs are placed in a steel box with a glass cover door. If someone is shot with a tool like a hammer, the glass will break at once. So any unauthorized person who tries to access the system can easily do their task with those routers and switches.

3. With ongoing power cuts, unauthorized people can easily access premises and buildings
    - With the prevailing situation in the country, a power cut is a normal thing in a daily routine. And then there's not enough fuel to run the backup generators. So if a power cut happens after the evening, as there's no backup electricity, there will be a blackout and even cannot identify a person in the evening. And also, the surveillance cameras go off if there's not much power. So it is a high risk that any unauthorized person can access buildings without security during power cut times.

4. Overloaded electrical items at the labs are a fire hazard
    - Labs are full of electrical devices. In the power cuts, backup generators can only run the fans in the air-conditioners. So the computer machines in labs get hotter when there's no air conditioning if we use those computers for a long time. And if an electrical leakage happens and causes a fire hazard, sometimes there's a risk that fire sensors won't turn on because of power cuts. So it is a very critical risk.

5. Steel door locks can be broken by using tools used for construction sites
    - there are ongoing projects on the campus premises, and there is a lot of equipment here and there. If any unauthorized person enters buildings, that person can brake the locked steel doors with that equipment. It will be significantly easier if there's a power cut.

2.4. Solutions

1. Facial recognition and thermal alarm system failure
    - Update the facial recognition system to recognize people's faces even with the face mask and increase the sensitivity of the thermal sensors using thermocouples made with special tolerance (also known as premium grade) wire can improve sensor accuracy. Wire made of higher-purity alloys is used to reduce the error. [1]

2. The glass of the box that stores routers and switches in labs can be broken

- We can use special tempered glasses for those racks to prevent those outside attackers. And we can place motion sensors to find out if any unethical work is happening. And also, we can use a passcode lock for those routers and switches stored boxes for more security and as a deterrent control to prevent the attacker from doing that.

3. With ongoing power cuts, unauthorized people can easily access premises and buildings
    - Use the backup generators only for activities like turning on the lights with low voltage and giving a separate backup generator to the surveillance cameras. And enabling night vision on those cameras will be easier to recognize the person who enters the building or the place. [2]

4. Overloaded electrical items at the labs are a fire hazard
    - With the ongoing power cuts, it will be hard to run air conditioners using a backup generator because they run on fuel. There is also a fuel crisis in the country. Because there's no cooling system in the lab environment, devices can get hot quickly if we run the computer machines in labs for an extended period. And the machines in the lab environment stick together. If some machine gets an electric leak, there's a possibility that it will spread like a chain. Therefore, we can use students' laptops other than the lab's computers if there is a power cut. If some student hasn't brought their laptop, only that student can use the lab machine. So it will be an effective way.

5. Steel door locks can be broken by using tools used for construction sites
    - There is ongoing construction on campus premises so that anybody can find sharp equipment. The doors of the labs are all locked with steel locks. So, using that sharp equipment, any unauthorized person can break the lock and enter the rooms. So if we can pack the gear in safely, we can get rid of it. Therefore, we must inform the workers who work on construction sites to manage the equipment in a specific place only the workers can access.

3. Logical Vulnerabilities

3.1. Logical Security

Logical security also known as technical security, is the tools, protocols, or anything else technological that can be used to try and secure systems or information being managed. You don't have to do anything more complicated than buy the necessary hardware or software and install it and configure it, and you'll have the security you need.

3.2. What are Logical Vulnerabilities?

Logical security for an organization's systems includes user identification and password access, authentication, access rights, and authority levels. In a network or on a workstation, these safeguards ensure that only individuals who have been granted access can carry out operations or access data. If we cannot secure those areas with enough security, they will be vulnerable to outsiders. And these are known as logical vulnerabilities or technical vulnerabilities.

3.3. List of Logical Vulnerabilities

1. Malicious activities and policy violations can happen
    - When considering the activities done on campus, we cannot look into each student's activities because many students come to a lab or any other campus building at once. So if any outsider party wants to do any malicious activity or policy violation, it can be done by using a student, worker, or any other person. And it will be a loss to the campus assets.

2. Outsiders can enter to the system through software bugs
    - As a lot of software is installed on a lab machine, there will be software with zero-day vulnerabilities. So if we cannot patch those vulnerabilities on time in the lab machines, it will be an easy exploit for unauthorized people who try to enter the system. For example, the MS Word "Follina"

vulnerability can be shown. You can get an idea about "Follina" vulnerability through the blog I published on the medium here.

3. Personal data can be stolen by unauthorized people when using public Wi-Fi
    - As we are using the public Wi-Fi and many students are accessing. If someone tracked you through your network traffic, others could steal your credentials.

4. If someone plugs a storage device with the virus, it will harm the computer
    - Lab machines are open to students, and they can do whatever they want with their machines while in the lecture. So, if someone plugs a USB or any other data storage device into the computer and if it has a virus in it, it will harm the machine in various ways, such as slowing down the computer, damaging or deleting files, and frequent computer crashes.

5. System resources can be changed
    - If someone gets access to the system resources on the computers, routers, and switches, they can change things according to their usefulness.

3.4. Solutions

1. Malicious activities and policy violations can happen
    - We can use an intrusion detection system(IDS) to get rid of this problem. This means that using this IDS can track suspicious network activity or policy violations, such as phishing. You can configure your intrusion detection system to respond immediately if an intrusion occurs. Intrusion-detection software is what it is (IPS). [3]

2. Outsiders can enter to the system through software bugs
    - As we deal with various types of software daily, there can be vulnerabilities in that software, and our computers can be hacked.

Therefore, we must be aware of the daily blogs about the cyberworld and update our software once we get an update from the developers. And we have to ensure we are using the latest version and there are no bugs.

3. Personal data can be stolen by unauthorized people when using public Wi-Fi
    - When we are connecting to public Wi-Fi, it's a precarious place because outsiders can track our network traffic and steal our data through the network. So, we must ensure our data cannot be followed by any packet or network traffic analyzing tool. Therefore, we can use VPNs to get rid of this network traffic tracking and surf the internet very safely. So, using a VPN, keep our data safe on public Wi-Fi and stop third parties from tracking us. [4]

4. If someone plugs a storage device with the virus, it will harm the computer
    - Nowadays, everyone has a portable data storage device with them. So, if we plug our data storage device into computers, we must ensure our device is free from viruses. Therefore, we must get a virus detection software called antivirus software. If someone plugs their devices into a lab computer for any reason, and if it has a virus, it will go through our computer and cause trouble. Sometimes it can be the worst. Therefore, we can install antivirus software on our computers to prevent those bad things. [5]

5. System resources can be changed
    - There are many students on campus, and each student has practical sessions. So, they must use the computers in the labs. Those computer system resources can be changed if they go into unauthorized people's hands. Therefore, we can use an Access Control List (ACL) to get rid of this issue. Using this, we can only give access to the places where students want to do their practical. We can manage control access if we use an ACL. It applies not only to computers but also to network devices such as routers and switches. And ACLs can be used as filters in routers and switches to control which traffic is allowed access to the network. [6]

4. Evidence

Figure 1:SLIIT new building during the power cuts in night

(With the prevailing situation in the country, I could not access the campus premises and take the evidence. So, I have attached the photo already on my gallery.)

5. References

[1] [Online]. Available: https://www.processindustryinformer.com/improve-process-temperature-measurement-accuracy/.

[2] [Online]. Available: https://www.agmglobalvision.com/How-do-night-vision-cameras-work.

[3] [Online]. Available: https://www.barracuda.com/glossary/intrusion-detection-system#:~:text=An%20intrusion%20detection%20system%20(IDS,information%20and%20event%

[4] [Online]. Available: https://www.avast.com/c-do-i-need-a-vpn#:~:text=What%20is%20the%20purpose%20of,Fi%20network%20%E2%80%94%20even%20at%20home..

[5] [Online]. Available: https://geekflare.com/advantages-using-antivirus/.

[6] [Online]. Available: https://www.techtarget.com/searchnetworking/definition/access-control-list-ACL#:~:text=An%20access%20control%20list%20(ACL)%20is%20a%20list%20of%network..