GAZI UNIVERSITY

ENGINEERING FACULTY

COMPUTER ENGINEERING

CENG482 INTRODUCTION TO COMPUTER SECURITY

Gamze AKSU – 171180005

Assignment-3

MARCH 2022

İÇİNDEKİLER

Sayfa

1. RISK

The dictionary meaning of risk is the danger of being harmed, the possibility of being harmed. That is the probability of something bad happening. It includes uncertainty. It is the probability that something people value will be damaged. Risk definition, risk assessment, risk management differ for different areas. [1]

Risk for cybersecurity is the impact of uncertainty on information and technology [2]. Technological systems are likely to be damaged. In other words, it is the possibility of loss of data and information or loss of reputation that may occur after a cyber-attack [3]. Represents loss of confidentiality, integrity, or availability for computer systems. These three concepts are the basic elements of information security. It's called the CIA for short. The opposite of these three concepts is called DAD (Disclosure, Alteration, Destruction). [4]

- Confidentiality: To ensure that data and information are not seen or accessed by unauthorized persons. It is necessary to protect data from unauthorized access.
- Integrity: It is to ensure that as the data is being moved, it is the same at the end as it was at the beginning. It is necessary to prevent data corruption, modification, addition and deletion of new data.
- Availability: It means that the system is available and accessible for the determined, targeted, needed time. The system must be running when needed.

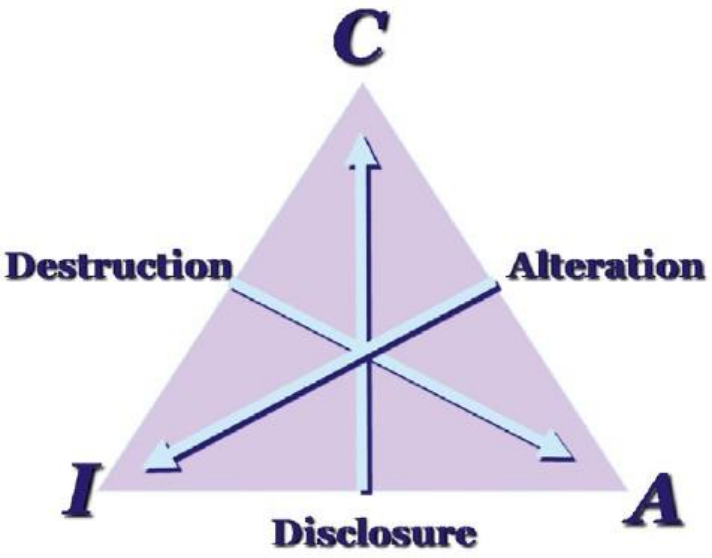

Figure 1 : CIA Triad

1.1. Available Risks and Risk Components

The risks that may arise in the field of cyber security may include theft of sensitive information, malicious software, hardware damage, compromised credentials, company website failure or damage to servers. [5]

Cybersecurity risk is generally defined by three components. [3]

1. **Threat**: Threat factors can be internal or external to an organization. It can happen through a social engineering attack, DDoS attack, or other types of attacks. It is generally done for financial gain.
2. **Vulnerability**: It refers to the security vulnerabilities in the system. This could be any flaw, weakness, or error in the system. Threat actors can infiltrate the system using these flaws.
3. **Effect**: It is the result of an attack or a disruption. When an organization is attacked or encounters a problem, there are consequences that they have to face before or after the organization fixes the problem. These results can affect the reputation and operation of the organization or cause the company to lose money.

1.2. Threat Types

There are 4 different types of mobile security threats that organizations can encounter. [6]

- **Mobile Application Security Threats:** They are threats that occur with applications that people download to their mobile phones. An app may appear normal and legitimate, but may actually be a malicious app.
- **Web-Based Mobile Security Threats:** Some sites that are normal in the visible part may have malware running in the background. When people visit these types of sites, they may have downloaded malware on their phone.
- **Mobile Network Security Threats:** When people connect to public WiFi networks, threat actors can also perform some attacks on people over the same network.
- **Mobile Device Security Threats:** This species includes physical threats. This includes the loss, corruption or theft of devices. This threat is important because the hardware is directly in the hands of threat actors.

1.3. Possible Threats for Mobile Devices

Table 1 lists the threats found in the literature for the phones in the source [7]. Loss of confidentiality, integrity, or availability is also marked for each threat factor. The effects of these losses vary from person to person. Normally, the impact of these losses should be calculated separately for each threat.

Dimension	Threat	C	I	A
Network Connectivity	T1 Spoofing	✓	✓	✓
	T2 Scanning	✓		
	T3 Denial of Service, Network congestion			✓
	T4 Spam, Advertisements			✓
	T5 Eavesdropping	✓		
	T6 Jamming			✓
Device	T7 Loss, theft, disposal or damage	✓	✓	✓
	T8 Cloning SIM card	✓	✓	
	T9 Technical failure of device		✓	✓
Operating System	T10 Unauthorized device (physical) access	✓	✓	✓
	T11 Unauthorized Access	✓	✓	✓
	T12 Offline tampering	✓	✓	✓
	T13 Crashing			✓
Applications	T14 Misuse of Phone Identifiers	✓		
	T15 Electronic tracking/surveillance/exposure of physical location	✓		
	T16 Resource abuse			✓
	T17 Sensitive Information Disclosure (SID), Spyware	✓		
	T18 Corrupting or modifying private content		✓	✓
	T19 Disabling applications or the device			✓
	T20 Client Side Injection/ Malware	✓	✓	✓
	T21 Direct billing		✓	
	T22 Phishing	✓	✓	

Table 1: Mobile Phone Threats

2. RISK ASSESSMENT

2.1 Risk Level Evaluation

- **High**: High level means that their effects are huge. Corrective measures must be taken immediately.
- **Medium**: As with the high level, corrective measures need to be taken. However, before these measures, the measures to be taken for high risks have priority. A reasonable period of time is acceptable for the measures to be taken for the middle level.

- **Low**: It is up to the user whether corrective action at this level is necessary or not. If the user wishes, he can accept these risks and choose not to take any action.

2.2. Threats

All threats listed in Table 1 also apply to my phone. These threats can also happen to my phone.

2.3. Vulnerability

2.3.1. Outdated Operating Systems

As with every device, it is necessary to use up-to-date systems on phones. If an operating system has been updated because there is a security vulnerability, and the device used is not up to date, this vulnerability will be available for that device. Threat actors infiltrate the system using this vulnerability.

2.3.2. Poor Password Strength

Poor Password Strenght means that the passwords used are weak and easy to guess. When threat actors break this weak password, they can access the system and capture important information. Weak passwords should not be used. In fact, protection should be made with more than one factor. With multi-factor authentication, it will be difficult for an attacker to crack the password and gain access to the system.

2.3.3. Unsecured Public WiFi

Public Wifi networks are less reliable than private networks. Because it is not known how encryption is made in a public WiFi network or who is in the same network. Therefore, it is necessary to be careful when connecting to public WiFi networks. An attack called Man-in-the Middle Attack can be carried out by creating a public WiFi with a fake name. In this way, attackers can monitor the packets of people connecting to the network. This is why companies often force employees to use VPNs.

2.3.4. End-to-End Encryption Gaps

While carrying important information from one place to another, this information should be sent in encrypted form along the way. However, if encryption breaks anywhere along the way, it's called an end-to-end encryption gap. By exploiting this vulnerability, threat actors can capture important information. Unencrypted WiFi networks are an example of this. In addition,

unencrypted applications or services are also dangerous. It is necessary to ensure that encrypted transport occurs throughout the entire path.

2.4. Asset impact

When a phone is lost, it is important not only how much physical value it has, but also how valuable the information in it is. How this phone will affect people when it is lost and how much damage it will suffer if it is lost are also included in the asset impact. For example, losing a phone can affect someone's finances, psychology, work or school life, social life or entertainment.

The types of information that can be found on the phone can be listed as personal, financial, business, government, authentication, connection. The types of information available on my phone are as in Table 2. High indicates that the loss of the CIA has very significant effects, and Low indicates that the effects of the loss are not very significant.

Information Type	Impact
Personal	High
Financial	High
School	Low
Authentication	High
Connection	High

Table 2: Impact Table

2.5. Results

Threat Likelihood, Impact and Risk calculations have been made for each of the threats found in Source [7]. These calculations are shown in Table 3. For each threat, the likelihood of the threat and the impact of the threat are considered. For some threats, the likelihood is low, while for others, the likelihood is high. The risk is calculated with the likelihood of occurrence of the threat and the effect it will create. For example, if the likelihood of occurance of a threat is low but its impact is very high, the risk medium is calculated as a result.

Threat	Threat Likelihood	Impact	Risk
Spoofing	Low	Low	Low
Scanning	Medium	Low	Low
Denial of Service, Network congestion	Low	Low	Low
Spam, Advertisements	High	High	High
Eavesdropping	Medium	High	High
Jamming	Low	Medium	Low
Loss, theft, disposal or damage	High	High	High
Cloning SIM card	Low	High	Medium
Technical failure of device	Medium	High	High
Unauthorized device (physical) access	Medium	High	High
Unauthorized Access	Medium	High	High
Crashing	Low	High	Medium
Misuse of Phone Identifiers	Low	Low	Low
Electronic tracking/surveillance/exposure of physical location	Low	Medium	Medium
Resource abuse	Medium	Medium	Medium
Sensitive Information Disclosure (SID), Spyware	High	High	High
Corrupting or modifying private content	Low	High	Medium
Disabling applications or the device	Medium	Low	Medium
Client Side Injection/ Malware	Low	Low	Low
Direct billing	Low	Medium	Low
Phishing	High	High	High

Table 3: Risk Results

REFERENCES

1. Wikipedia contributors. (2022, February 25). Risk. In *Wikipedia, The Free Encyclopedia*. Retrieved 15:10, March 23, 2022, from https://en.wikipedia.org/wiki/Risk
2. NIST COMPUTER SECURITY RESOURCE CENTER. (n.d.). Cybersecurity Risk. Retrieved from https://csrc.nist.gov/glossary/term/cybersecurity_risk
3. Security Scorecard. (2021). What is Cybersecurity Risk? Definition & Factors to Consider. Retrieved from https://securityscorecard.com/blog/what-is-cybersecurity-risk-factors-to-consider
4. Başaranoğlu. E, (2016) Bilgi Güvenliği Unsurları (CIA Ve Diğerleri). Retrieved from https://www.siberportal.org/white-team/securing-information/bilgi-guvenligi-unsurlari-cia-ve-digerleri/
5. Sotnikov, İ. (2022) How to Perform IT Risk Assessment. Retrived from https://blog.netwrix.com/2018/01/16/how-to-perform-it-risk-assessment/
6. Gontovnikas, M. (2021). The 9 Most Common Security Threats to Mobile Devices in 2021. Retrieved from https://auth0.com/blog/the-9-most-common-security-threats-to-mobile-devices-in-2021
7. Theoharidou, M., Mylonas, A., & Gritzalis, D. (2012). *A Risk Assessment Method for Smartphones. Information Security and Privacy Research, 443–456.* doi:10.1007/978-3-642-30436-1_36
8. Shih, D., Lin, B., Chiang, H., & Shih, M. (2008). *Security aspects of mobile phone virus: a critical survey. Industrial Management & Data Systems, 108(4), 478–494.*