COM-402 exercises 2023, Session 1: Introduction, Cyber attacks

Exercise 1.1

Here are four security mechanisms and four goals. For which goal can each mechanism be used?

1. authenticity	a. duplicate/distribute system
2. availability	b. hash
3. confidentiality	c. isolation
4. integrity	d. message authentication code (keyed hash)

Exercise 1.2

In your opinion, what is the most important technical means you need to have in order to be protected against ransomware attacks?

Explain why.

Exercise 1.3

You are developing a website that sells cigarettes online in Switzerland. Imagine a cyber threat of each category below. For each threat, describe the goal of the threat and by which means the goal is achieved :

- Commodity threat
- Hacktivism

Exercise 1.4

In you opinion, is an anti-virus software a good protection against social engineering attacks carried out over e-mail? Explain why.

What would be the best way of protecting against these attacks?

Exercise 1.5

An anti-malware tool adds up the sizes of all files on a disk, adds the size of the empty space and compares it to the total disk size.

What type of malware is this software trying to detect? Explain why.

Solutions to the Exercises

Solution 1.1

- 1 – d
- 2 – a
- 3 – c
- 4 – b

Solution 1.2

Having backups of you data is key to protect against ransomware. Other protections, like anti-virus software, are also important but if you don't have a backup you may still end up having to pay the ransom.

If you have a recent backup, you can simply delete the encrypted data and restore the backup.

A complete backup solution would include some well-defined and tested procedures for restoring data, applications and operating systems.

Solution 1.3

- **Commodity threat:** Goal: get money from the victims. Technical means: The attackers send a phishing e-mail that tells the recipient to connect to their Paypal account in order to activate a new security feature. They use the collected passwords to automatically transfer the balance of the Paypal accounts to their account.
- **Hacktivism:** Goal: damage the image of the victim (e.g. tobacco industry). Technical means: The attackers exploit a flaw in the website of the victim that allows them to post a message that says that cigarette sellers are poisoning their customers.

Solution 1.4

An antivirus software might be able to detect some typical characteristics of a social engineering e-mail (e.g. a fake sender address, or some keywords like "please pay", etc.). Social engineering attacks can have so many different forms that it does not seem possible to create a software that can detect all of them.

The best protection is to raise the awareness of the users. This can be done through specific training of the users. This could include running a fake social engineering attack and informing them of the results.

Solution 1.5

The tool could be looking for a rootkit. Indeed, the goal of a rootkit is to hide the presence of malware on a computer. A difference between the total number of bytes used — the size of visible files plus empty space — with the total size of the disk, could be an indication that there are hidden files.