Solutions: Sheet 1

1. Attacks on IT-Systems

Research recent attacks on IT systems and briefly explain three attacks and their impact (reference your sources).

2017 WannaCry:

In May 2017, a global ransomware crypto worm called WannaCry attacked computers with Windows installed. WannaCry encrypted data and demanded payment in Bitcoin to decrypt the data. WannaCry contains mechanisms to spread in networks by searching for possible devices to infect. [1, 4] It used the ExternalBlue exploit (a computer exploit developed by the NSA) to gain access [2] and DoublePulsar (an implant tool developed by the NSA) to install and execute WannaCry. [3] About 200.000 computers were infected across 150 countries. National Health Service hospitals in England and Scotland were among the most affected. More than 70,000 devices were infected, including important medical devices. Depending on the extrapolation, the commercial losses amount to several hundred million to as much as 4 billion. [1]

Sources:

[1] https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

[2] https://en.wikipedia.org/wiki/EternalBlue

[3] https://en.wikipedia.org/wiki/DoublePulsar

[4] https://www.theguardian.com/technology/2017/may/12/nhs-ransomware-cyber-attack-what-is-wanacrypt0r-20

2021 Acer:

The company Acer suffered from a ransomware attack by the group REvil and where prompted to pay ransom in in the amount of 50.000.000$. [1] Once REvil had access to the network, they began stealing confidential data as leverage. A file with stolen user data was posted and additionally the stolen data was for sale at an auction. [2] Acer didn't confirmed if they paid the group. It seems that the hack had no influences on their side to improve their vulnerabilities, as Acer confirmed a second successful hack in the same year. [4]

Sources:

[1] https://www.bleepingcomputer.com/news/security/computer-giant-acer-hit-by-50-million-ransomware-attack/

[2] https://www.forbes.com/sites/leemathews/2021/03/21/acer-faced-with-ransom-up-to-100-million-after-hackers-breach-network/

[3] https://www.zdnet.com/article/acer-reportedly-targeted-with-50-million-ransomware-attack/

[4] https://www.zdnet.com/article/acer-confirms-second-cyberattack-in-2021/

2022 Ukraine cyberattacks:

Around January 2022, malware attacks took place which were first detected on January 13 by Microsoft Threat Intelligence Center (MSTIC). The malware infected devices belonging to several governmental, non-profit and IT organizations in Ukraine. [1]

On January 14, 2022, hackers replaced texts on 70 websites of the Ukrainian government in fake Polish and Russian language and wrote: "Be afraid and wait for the worst". Among the affected websites were those of the Ministry of Foreign Affairs, the Cabinet of Ministers, and the Security and Defense Council. [1]

Shortly after the Russia invasion, microsoft published an analysis of the cyberattacks. According to this, at least 6 different hacking groups believed to be linked to Russia have conducted cyber operations against Ukraine. Attacks are mainly on the telecommunication infrastructure and often correlate with attacks. [2] [3]

Sources:

[1] https://www.nytimes.com/2022/04/27/us/politics/russia-cyberattacks-ukraine.html

[2] https://www.theguardian.com/world/2022/feb/23/russia-hacking-malware-cyberattack-virus-ukraine

[3] https://edition.cnn.com/2022/04/27/europe/russia-cyberattacks-ukraine-war-microsoft/index.html

2. Security Objectives

Explain the security objectives (aka protection goals) *confidentiality*, *integrity* and *availability*, make sure that the three terms are clearly delimited in your explanations.

Furthermore:

- Find three examples of applications or application scenarios in each of which at least one of the security objectives plays a role and describe them.
- For each of the three security objectives, state measures to implement them.

Confidentiality:

Confidentiality means protecting information from access by unauthorized persons.

Measures to ensure confidentiality:

- Cryptographic encryption methods
- Access control
- Physical protection, e.g a room only specific persons can access

Example:

When a company is storing information about a person no one else should have access to the information. Confidentiality is no longer given if, for example, a hacker gets hold of this data.

Integrity:

Integrity means that data is complete and correct when an authorized persons created, transfered and stored. Intentional or unintentional changes can cause a violation of integrity.

Measures to ensure Integrity:

- Hash functions
- Store copies to compare them later
- Access and admission rules

Example:

An authorized person transmits data without error detection methods such as checksums, which can cause data to arrive corrupted.

Availability:

Availability of an IT-System means that the system is available and accessible to authorized person.

Measures to ensure availability:

- Replacements in the event of possible absences of persons
- Backups (e.g if a server is unavailable for a certain time, it is still accessible via another server)
- Redudant design of components

Example:

When you play an online game, it should be possible to play it even if, for example, one of the servers goes down, if you are authorized to do so. In case of e.g. a banned account, you should not be able to play because you are no longer authorized.

3. Protection Goal Availability

Availability is usually expressed as a percentage of uptime in a given time period (e.g. year or month).

a. Formula for Maximum Allowed Downtime

Derive a formula for the availability with which you can calculate the maximum allowed downtime depending on the guaranteed availability (percentage) for a certain total runtime.

$$\text{Downtime} = \text{Total Runtime} - (\text{Availability} \cdot \text{Total Runtime})$$

b. Calculation of Maximum Allowed Downtime

Calculate the allowed downtime for a particular percentage of availability, presuming that the system is required to operate continuously for the following settings:

Guaranteed availability of the following percentages:

- 90% percentage ("one nine")

per year: $8640 - (0.9 \cdot 8640) = 864 \text{ h}$

per month: $720 - (0.9 \cdot 720) = 72 \text{ h}$

per day: $24 - (0.9 \cdot 24) = 2,4 \text{ h}$

per hour: $1 - (0.9 \cdot 1) = 0,1 \text{ h} = 6\text{min}$

- 99% percentage ("two nines")

per year: $8640 - (0.99 \cdot 8640) = 86,4 \text{ h}$

per month: $720 - (0.99 \cdot 720) = 7,2 \text{ h}$

per day: $24 - (0.99 \cdot 24) = 0,24 \text{ h}$

per hour: $1 - (0.99 \cdot 1) = 0,01 \text{ h} = 0,6\text{min}$

- 99.9% percentage ("three nines")

per year: $8640 - (0.9 \cdot 8640) = 8,64 \text{ h}$

per month: $720 - (0.9 \cdot 720) = 0,72 \text{ h}$

per day: $24 - (0.9 \cdot 24) = 0,024 \text{ h}$

per hour: $1 - (0.9 \cdot 1) = 0,001 \text{ h} = 0,06\text{min}$

- 99.99% percentage ("four nines")

per year: $8640 - (0.9 \cdot 8640) = 0,864 \text{ h}$

per month: $720 - (0.9 \cdot 720) = 0,072 \text{ h}$

per day: $24 - (0.9 \cdot 24) = 0,024 \text{ h}$

per hour: $1 - (0.9 \cdot 1) = 0,0001 \text{ h} = 0,006 \text{min}$

Allowed maximum downtime for the following time periods:

- per year

$$24 \text{ h} \cdot 30 \text{ days} \cdot 12 \text{ months} = 8640 \frac{\text{h}}{\text{year}}$$

- per month

$$24 \text{ h} \cdot 30 \text{ days} = 720 \frac{\text{h}}{\text{month}}$$

- per day

$$24 \frac{\text{h}}{\text{day}}$$

- per hour

$$1 \text{ h}$$