Exercise Sheet 02

Individual submissions only. Talk, discuss, debate. Write separately **in your own words**.
If you use Generative AI, you need to document which AI tool you use and all the prompts. You are still fully responsible for the correctness of your submission.
Include your name on the first page of your submission pdf file.

1. Current Attacks

Find a report – that is not older than six months – about a **malware attack on a company** or public institution in Switzerland. Describe the attack and how malware was used to overcome security mechanisms and achieve the attacker's goals. Could the attack or its effects have been prevented? How?

2. Malware

Many institutions and individuals are exposed to attacks by malicious software. Helpful sources may be the current report "Die Lage der IT-Sicherheit in Deutschland" (available in German: https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html) or the "Common situational picture 2021" by German BSI and French ANSSI that has ransomware as a focus topic (available in English: https://www.bsi.bund.de/EN/Service-Navi/Publikationen/ANSSI-BSI-joint-releases/ANSSI-BSI-joint-releases_node.html).

2.1. How many new malware variants are reported daily? Name your source with report name, year, and page number.
2.2. What is a botnet? What is the most common operating system targeted by botnets? Name your source with report name, year, and page number.
2.3. What are typical attacker actions before executing ransomware? Name your source with report name, year, and page number.
2.4. What protection mechanisms are recommended by IT-Grundschutz against malware? Name the title and ID of the specific requirements and state whether these are required for basic protection, standard protection, or for increased protection needs.

3. Vulnerability Management

The EUVD European Union Vulnerability Database is a compilation of known vulnerabilities in products. What are **known vulnerabilities for Moodle** that have been assigned an ID in 2025 and that have a CVSS score of at least 8?
For each vulnerability, state the EUVD ID, give a short description, and state which assets and protection goals of users and the server operator may be affected. For each vulnerability, also find out if there is a workaround that IT operations could apply for a customer. Fixing the software or applying an update with a fix is not a workaround. A workaround is a measure that you apply in case no update is available or is not possible.

Answers must be submitted in Moodle as PDF files following the naming convention:
Exercise02-YourLastName-YourFirstName.pdf
Example: Exercise02-Mustermann-Erika.pdf