Exercise sheet 01

Individual submissions only. Talk, discuss, debate. Write separately **in your own words**.

1. Current Attacks

Find a report – that is not older than three months – about a **malware attack on a company** or public institution. 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? What protection mechanisms do you recommend against malware?

2. Known Vulnerabilities

The NVD National Vulnerability Database is a compilation of known vulnerabilities in products. What are **known vulnerabilities published for SOGo Web Mail** in 2023? (Note that date of discovery and date of publication might be different.)

For each vulnerability, state the CVE-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 include a possible solution that IT operations could apply for a customer. Note that the options for customers are different than for developers. Developers could remove the vulnerability from a product. Customers may apply a patch if one is available, but have to reduce functionality, change a configuration, use a workaround etc.

3. Application Whitelisting

Get familiar with built-in techniques for **application whitelisting in Microsoft Windows**.

1. How does application whitelisting work with **Windows Defender Application Control (WDAC)**? How does it differ from AppLocker?
2. How does WDAC restrict users/processes with respect to executing code?
3. How does WDAC restrict users/processes with respect to reading files?
4. How does WDAC restrict users/processes with respect to writing files?
5. What are the different **file rules** hat you can use with WDAC?
6. What is the purpose of the **audit mode** in WDAC?
7. How do you debug WDAC policies, i.e., how do you find out that they are effective and what are the logging resources that you can use in case a WDAC policy does not work as expected?

Answers must be submitted in Moodle as PDF files following the naming convention:
Exercise01-YourLastName-YourFirstName.pdf
Example: Exercise01-Mustermann-Erika.pdf