Hello class,

Computers are everywhere, in our cars, phones, appliances, our grocery stores, airplanes, banks, and more… they are part of every critical infrastructure that our daily lives depend on. Thus, it is crucial to understand and implement cybersecurity measures. That is, measures that safeguard the functionality of our computer systems and the information stored in those systems.

In the context of operating systems, the key to safeguarding a computer system's functionality and the integrity of the information stored in it, is to prevent “malicious software (malware) from gaining unauthorized privileges on the system and, in particular, from gaining root access” (Stallings, 2018. P. 631).

Different types of malware exist, and each can affect a system in uniquely destructive ways. From viruses that replicate themselves and ransomware that encrypts crucial data to spyware that monitors and steals sensitive information. Figure 1 depicts a list of 12 types of malware that you are most likely to come across. For each type, a small description and real-world examples are given.

**Figure 1**

*Malware List*

A screenshot of a computer

Description automatically generated

*Note*. From *12 types of malware + examples that you should know,* by Baker, 2023, (<https://www.crowdstrike.com/cybersecurity-101/malware/types-of-malware/>). Copyright 2023 by crowdstrike.com.

Therefore, it is essential to implement countermeasures or security controls to prevent security incidents. That is to prevent malware from accessing a computer system's functionality and data. Countermeasures The Federal Information Processing Standard state code (FIPS) defines security controls as “the management, operational, and technical controls (i.e., safeguards or, countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information” (FIPS 199, n.d.).

Below is a list of countermeasures that can be implemented:

1. **Antivirus/Antimalware Software** detects and neutralizes threats like viruses, worms, and spyware. They work by comparing files on a computer to a database of known threats and behaviors.
2. **Firewalls** are a barrier between a trusted network and an untrusted network. They can prevent unauthorized access to a network and can often detect and block many types of attacks.
3. **Intrusion Detection System (IDS)** is a system that monitors network traffic and system activities for malicious activities or policy violations and generates an alert when such activity occurs (Lutkevich, 2021).
4. **Intrusion Prevention System (IPS)** is an IDS that detects potential threats but also takes actions to prevent them from causing harm.
5. **Patch Management** is the action to manage software or systems patches. It is important to regularly update and patch systems, it can help prevent security incidents.
6. **Penetration Testing and Vulnerability Assessments**. A vulnerability assessment identifies and measures security weaknesses in a system. .A penetration test is a simulated cyber attack designed to identify vulnerabilities in an organization's security system (Escobar, 2021).
7. **Security Awareness Training**: Educating users about the signs of a security incident can prevent many attacks. Users should be trained to recognize and report phishing attempts, suspicious behavior, and potential malware.
8. **Access Controls and User Permissions**, it is important to implement controls on which users can access what data and to ensure that users have the appropriate amount of access to perform their duties.
9. **Encryption**, which involves encoding sensitive data. This data can only be decrypted by authorized applications and users who have access to the data.
10. **Systems Event Management (SIEM)** is a security solution that helps organizations recognize and address potential security threats and vulnerabilities before they have a chance to disrupt business operations (IBM, n.d.).

-Alex

**References:**

Baker, B. (2023, July 19). 12 types of malware + examples that you should know[Figure 1]. *crowdstrike.com*. <https://www.crowdstrike.com/cybersecurity-101/malware/types-of-malware/>

Escobar, E. (2021, August 19). Vulnerability assessments versus penetration tests. *Secureworks*. <https://www.secureworks.com/blog/vulnerability-assessments-versus-penetration-tests>

Lutkevich, B. (2021, October 7). What is an intrusion detection system (IDS)? *Techtarget.com*. https://www.techtarget.com/searchsecurity/definition/intrusion-detection-system?Offer=abt\_pubpro\_AI-Insider

IBM (n.d.). What is Security Information and Event Management (SIEM)? *Ibm.com*. https://www.ibm.com/topics/siem

*FIPS 199, standards for security categorization of federal ... - NIST.* (n.d.). National Institute of Standards and Technology. Retrieve from: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

Stallings, W. (2018). *Operating Systems: Internals and design principles*. Pearson