Assignment 12

1. According to the ENISA Threat Landscape report for 2023, what emerges as the primary threat within cyberspace? Why is this particular threat deemed particularly alarming? Furthermore, based on the insights provided in the document, what strategies are recommended to effectively mitigate this threat.

In the ENISA Threat Landscape report for 2023, ransomware emerges as the primary threat within cyberspace. This form of malware encrypts files or systems, rendering them inaccessible until a ransom is paid. Ransomware attacks have surged in recent years due to their profitability and relative ease of execution, making them particularly alarming for several reasons.

Firstly, ransomware attacks can cause significant disruption to essential services, such as healthcare, finance, and transportation, leading to potentially life-threatening situations and substantial economic losses. Secondly, the evolution of ransomware tactics, such as double extortion (wherein stolen data is threatened to be leaked if the ransom is not paid), escalates the severity and impact of these attacks. Thirdly, the proliferation of ransomware-as-a-service (RaaS) models has lowered the barrier to entry for cybercriminals, enabling even those with minimal technical expertise to carry out attacks.

To effectively mitigate the threat posed by ransomware, the ENISA report recommends a multifaceted approach. Firstly, organizations should prioritize proactive measures, such as regular backups of critical data and robust cybersecurity training for employees to recognize and respond to phishing attempts, a common entry point for ransomware. Secondly, implementing defense-in-depth strategies, including network segmentation, endpoint protection, and intrusion detection systems, can help contain and prevent the spread of ransomware within networks. Thirdly, fostering collaboration and information-sharing among public and private sectors can enhance threat intelligence capabilities and facilitate a coordinated response to ransomware campaigns.

By adopting these strategies, organizations can bolster their resilience against ransomware attacks and mitigate the associated risks to their operations and data.

2. Visit the website www.csk.gov.in and outline some of the recommended best practices for securing personal computers.

Software Installation and Updates:

Always install licensed software to ensure regular updates for the operating system and applications. For open-source software, make sure to update frequently.

Enable automatic updates for the operating system and keep it regularly updated.

Install antivirus and antispyware software from trusted websites, ensuring they automatically update with the latest virus signatures and definitions.

Physical Security:

Regularly clean the computer and its components, turning off the PC before cleaning.

Organize power cables and wires to prevent damage from water and insects.

Be careful not to spill food or liquids on the computer.

Use the "Safely Remove" option when disconnecting USB devices.

Set a BIOS password to prevent unauthorized access.

Internet Security:

Follow internet ethics while browsing and check copyright issues before using online content.

Use websites that implement HTTPS for online transactions and downloads.

Verify SSL certificates on websites by clicking the lock icon and checking certificate details.

Download files from original websites, not third-party sites, and scan them with updated antivirus software.

Install and configure a software firewall to protect against malicious traffic.

Data Security:

Use encryption to secure valuable information and remember the password used for encryption.

Use strong passwords for the admin account and other important applications like email clients and financial applications.

Periodically back up computer data on CDs, DVDs, or USB drives to prevent data loss due to hard disk failures or system reinstallation.

Wireless Security:

Change default administrator passwords.

Turn on WPA (Wi-Fi Protected Access) or WEP encryption.

Change the default SSID.

Enable MAC address filtering.

Turn off the wireless network when not in use.

Modem Security:

Change default passwords.

Switch off the modem when not in use.

Browser Security:

Keep the web browser updated with the latest patches.

Use built-in privacy and security settings.

Use content filtering software.

Enable "Safe Search" in search engines.

Scan email attachments with updated antivirus and antispyware software before opening them.

Regularly empty the spam folder.

Monitor and control startup programs for optimal system performance.

E-Mail Security:

Always use strong passwords for email accounts.