Assignment 12

1) According to 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?

Answer: The ENISA Threat Landscape report for 2023 identifies two main threat: Ransomware and Denial-of-Service (DOS) attacks. While the report doesn't definitively rank one above the other, ransomware appears to be a growing concern.

Here's why ransomware is particularly alarming:

Prevalence: The report indicates ransomware accounts for a significant portion (around 34%) of cyberthreat within the EU.

Increased Sophistication: Attackers are employing advanced tactics like "double extortion," where they steal data and threaten to release it alongside encrypting systems, putting more pressure on victims to pay.

Supply Chain Attacks: Targeting vulnerabilities in widely used software or service providers allows attackers to hit multiple organization at once.

Mitigation Ransomware Threats.

The ENISA report offers recommendation to mitigate ransomware threats. Here are some key strategies.

Regular Backups: Implement a robust backup implement a robust backup and recovery plan to restore data quickly in case of an attack.

Patch management System: Systematically identify and patch vulnerabilities and softwares and operating System promptly.

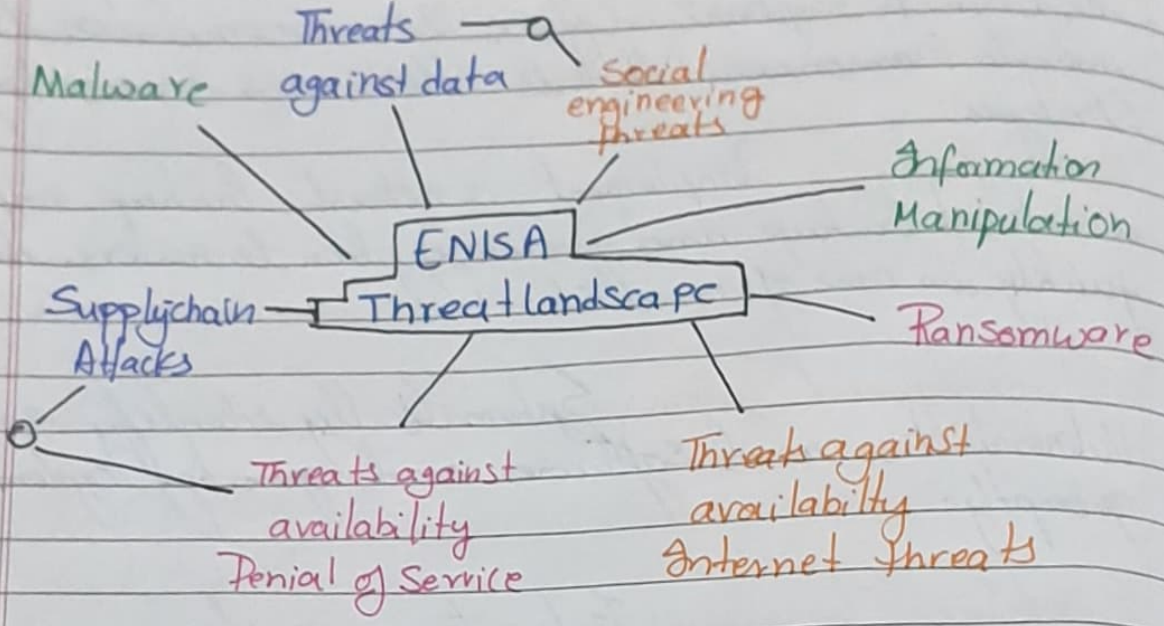
Employee Training: Educating employees on common social engineering tactics used in ransomware attacks phishing emails and suspicious attachment are commonly entry points

Multifactor Authentication (MFA): Enforced MFA to add an extra layer of security beyond passwords.

Network Segmentation: Divide your network into smaller segments to limit the reach of an attacker if they gain access.

Cybersecurity Incident Response plan:
Develop a clear plan for identifying, responding to, and recovering from a ransomware attack.

By implementing these strategies organizations can significantly reduce the risk of a successful ransomware attack and the associated damage.



ENISA Threat landscape 2022 - Prime threats

Ransomware and threat against availability ranked at the top during the reporting period
Resourceful threat actors have been observed to misuse legitimate tools primarly to prolong their cyber espionage operations.
geopolitics continue to have a strong impact on cyber operation.
Sexual threats actors further professionalised
By using Extortion only Techiniques
Increased operation by law enforcement
CLOP ransomware
One of the biggest malware threats is still information stealers
There is a steadily decline in classic mobile malware.

Analysis of the vulnerabilities landscape 2022-2023

NVD vulnerability severity rating CVSS v2.0 Ratings
CVSS v3.0 Ratings

Severity	Base Score Range
Low	0.0-3.9
Medium	4.0-6.9
High	7.0-10.0

Severity	Base Score Range
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

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

* According to the website, the following are some recommend best practices for securing personal computer:

→ The cyber Swachhta Kendra is a Botnet cleaning a malware Analysis Center (BCMAC), operated by the Indian Computer Emergency Response Team (CERT-In) as part of the government of India's digital India initiative under the Ministry of electronics and Information Technology (MeitY)

* Install genuine and updated Software

* Keep your operating System and Software up to date with the latest patches and updates to fix Security vulnerabilities.

* Use Strong passwords and change them regularly

* Install reputable antivirus and anti-malware Software and keep it update regularly.
Enable two-factor authentication whenever possible.

* Be Cautious when clicking on links or downloading attachments in emails, as they could be phishing attempts or contain malware

* Regularly backup your important data to an external drive or cloud storage to protect against data loss from ransomware or hardware failure

* Using a firewall to monitor and control incoming and outgoing network traffic

* Avoid using public wifi Networks for sensitive activities like online banking or shopping, or use a VPN for added Security.

* Disable Unnecessary Services and features on your computer to reduce the attack surface

* Enable the encryption for sensitive data to protect it from unauthorized access

* Educate yourself about Common CyberSecurity threats and practices to stay informed and vigilant.

* Security Tools

* Free Bot removal Tool - For Microsoft Windows.

* K7 Security Quick Heal eScan Antivirus for smart Phone CDAC Hyderabad has developed M-Kavach2 with the support of MeitY.

There are Several Current Threats which we need to lookout for.