CYBER SECURITY

ASSIGNMENT -12

NAME: B. SHANMUKH

Reg.no: 282023-024

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?

ANS:

The ENISA Threat Landscape report for 2023 identifies ransomware as the primary threat within cyberspace. Ransomware continues to dominate, accounting for 34% of all reported threats in the European Union. This threat is particularly alarming due to its extensive impact across multiple sectors, including manufacturing, healthcare, public administration, and services. The sophistication and frequency of ransomware attacks, often involving double extortion tactics (where attackers steal data in addition to encrypting it), significantly disrupt operations and pose severe financial and reputational risks to organizations (CyberPilot) (Homepage).

To mitigate the threat of ransomware and other prominent cyber threats, ENISA recommends several strategies:

1. **Asset Management and Risk Assessment**: Maintain a comprehensive inventory of assets, conduct regular risk assessments, and perform vulnerability scanning to identify and address potential weaknesses (CyberPilot) (Security Boulevard).

2. **Secure Remote Access and Configuration**: Implement secure configurations for remote access technologies and ensure strong password policies with phishing-resistant multi-factor authentication (MFA). Apply the principles of least privilege to minimize access to critical systems (Security Boulevard)

3. **Data Backup and Recovery**: Establish a secure, redundant backup strategy with offline, encrypted backups that are regularly tested. This ensures data can be restored quickly in the event of an attack (CyberPilot) (Security Boulevard).

4. **Incident Response Planning**: Develop and regularly test incident response plans, including clear communication and notification protocols. Incorporate key suppliers into business continuity and incident response exercises (Security Boulevard).

5. **Security Awareness Training**: Conduct regular security training tailored to different departments to address evolving threats such as social engineering and phishing. Specific training for IT and security staff is crucial to bolster defense mechanisms (Security Boulevard).

6. **Zero-Trust Architecture**: Adopt a zero-trust approach, ensuring continuous verification of users and devices trying to access network resources. This reduces the risk of unauthorized access (Security Boulevard).

- By following these strategies, organizations can enhance their cybersecurity posture and better protect themselves against the pervasive threat of ransomware and other cyberattacks.

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

ANS:

The Cyber Swachhta Kendra website recommends several best practices for securing personal computers:

1. **Install Genuine Software**: Ensure all software is genuine and updated regularly.
2. **Be Cautious with Links**: Think before clicking links in emails or social media.
3. **Security Awareness**: Stay informed about potential threats.
4. **Heed Security Warnings**: Act on security warnings promptly.
5. **Strong Passwords**: Use strong, regularly changed passwords.
6. **Regular Backups**: Maintain backups to prevent data loss from ransomware.
7. **Disable AutoPlay**: Prevent automatic launching of files from removable drives.

➢ For more details, visit Cyber Swachhta Kendra.