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?

Common primary threats often include:

Phishing and Social Engineering: Deceptive tactics to trick individuals into revealing sensitive information or performing actions that compromise security.

Ransomware: Malicious software that encrypts data or blocks access to systems until a ransom is paid, causing significant disruptions.

Supply Chain Attacks: Targeting vulnerabilities in third-party suppliers or service providers to gain access to larger networks.

Zero-Day Exploits: Attacks exploiting unknown vulnerabilities before they are patched, making them highly effective against unprepared systems.

These threats are alarming due to their potential for widespread damage, financial losses, and loss of trust.

Mitigation strategies often recommended include:

User Awareness and Training: Educating users about common cyber threats, how to recognize phishing attempts, and the importance of cybersecurity best practices.

Patch Management: Regularly applying security patches and updates to software and systems to address known vulnerabilities.

Access Control: Implementing strong authentication mechanisms, least privilege access policies, and monitoring user activities to prevent unauthorized access.

Backup and Recovery: Maintaining regular backups of critical data and systems to quickly restore operations in case of a ransomware attack or data loss event.

Segmenting networks to limit the impact of a cyber incident and prevent lateral movement by attackers.

Incident Response Plan: Developing and testing an incident response plan to quickly detect, respond to, and recover from cyber incidents, including communication protocols and roles/responsibilities.

These strategies, when implemented comprehensively and regularly updated, can help organizations mitigate the risks posed by primary threats within cyberspace.

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

1. **Use Strong Passwords**:Create complex passwords with a mix of letters, numbers, and special characters. Avoid using easily guessable information like birthdates or common words.

2. Keep Software Updated:Regularly update your operating system, antivirus software, web browsers, and other applications to protect against known vulnerabilities.

3. Enable Firewall:Activate the firewall on your computer to monitor incoming and outgoing network traffic and block unauthorized access.

4. Install Antivirus Software: Use reputable antivirus software and keep it updated to detect and remove malware, viruses, and other malicious programs.

5. Be Cautious with Email and Downloads: Avoid opening suspicious email attachments or clicking on links from unknown or untrusted sources. Be cautious when downloading files from the internet and verify their legitimacy.

6. Use Secure Wi-Fi: Secure your wireless network with a strong password and encryption (WPA2 or WPA3) to prevent unauthorized access to your internet connection.

7. Enable Two-Factor Authentication (2FA): Whenever possible, enable 2FA on your accounts to add an extra layer of security beyond just a password.

8. Backup Regularly: Keep regular backups of important data on an external hard drive or cloud storage to protect against data loss from hardware failures, theft, or ransomware attacks.

9. Limit User Privileges: Use standard user accounts instead of administrator accounts for everyday tasks to limit the impact of potential malware or unauthorized software installations.

10. Educate Yourself: Stay informed about common cyber threats and best practices for online security. Regularly update your knowledge and practices to adapt to new threats.

Implementing these best practices can significantly enhance the security of your personal computer and reduce the risk of cyberattacks and data breaches.