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?

Answer:

The ENISA Threat Landscape 2023 report provides valuable insights into the current state of cybersecurity threats. The primary threat identified in the report is ransomware, which accounts for 34% of all threats in the European Union. Following closely behind are Distributed Denial of Service (DDoS) attacks, making up 28% of the threats. Ransomware has targeted various sectors, with manufacturing being the most affected at 14%, followed by health at 13%. Public administration and services sectors also experienced significant impacts from ransomware, at 11% and 9% respectively.

The prominence and impact of ransomware make it an alarming threat. Its widespread occurrence poses considerable risks to both organizations and individuals. The financial losses, operational disruptions, and potential data breaches that result from successful ransomware attacks further emphasize the urgent need to address this threat.

To effectively mitigate ransomware threats, organizations can adopt several strategies. These include maintaining regular backups of critical data to restore systems in case of an attack, providing security awareness training to employees to prevent inadvertent infection through phishing and social engineering tactics, isolating critical systems from less secure networks through network segmentation, keeping software and systems updated to address vulnerabilities that attackers exploit through patch management, deploying robust antivirus and anti-malware solutions on endpoints for endpoint protection, and developing and testing an incident response plan to handle ransomware incidents effectively.

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

Answer:

Securing desktops requires a comprehensive approach that addresses various aspects of security.
Here are some best practices to consider:

1. Software Installation and Updates: Install licensed software and promptly update operating systems and applications. Read and understand the terms and conditions before installation to avoid compromising security.

2. Physical and Internet Security: Keep the computer and its components clean, organize cables, and avoid spills near the system to minimize hardware damage. Practice ethical browsing, verify SSL certificates, and download from trusted sources. Scan downloaded files with updated anti-virus software to protect against threats.

3. Data and Browser Security: Enable auto-updates, use trusted anti-virus and anti-spyware software, and encrypt sensitive data for enhanced security. Use strong passwords and regularly back up data. Keep web browsers up to date, adjust privacy settings, and monitor startup programs to mitigate risks.

4. Wireless and Modem Security: Change default passwords, enable WPA/WEP encryption, and implement MAC address filtering for wireless connections. Regularly change modem passwords and turn off the modem when not in use. Set up a BIOS password to restrict physical access to the computer.

By following these best practices, users can significantly reduce the risk of security threats and protect their personal information. Remember, prevention is always better than cure when it comes to desktop security.