Assignment-12

Lohendra P

2406CYS124

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 (European Network and Information) Security Agency) Threat Landscape report for 2023 identifies several significant threats, but one of the most concerning appears to be ransomware attacks . Here's why it's alarming and how to mitigate it according to the report: Prevalence: The report suggests ransomware accounts for a significant portion of cyberattacks, with some sources stating it comprised over half (54%) of attacks in the healthcare sector. Disruptive Impact: Ransomware encrypts critical data, essentially holding it hostage until a ransom is paid. This can cripple essential services, cause financial losses, and erode public trust. Evolving Techniques: Attackers are constantly developing new methods, making it harder to defend against them. The report also highlights the concerning rise of AI□powered manipulation tactics used in these attacks. Here are some mitigation strategies suggested in the report: Regular Backups: Having up-to-date backups allows restoration of data in case of an attack. Patching Systems: Keeping software and applications updated with the latest security patches helps address vulnerabilities exploited by attackers. Employee Training: Educating staff on cybersecurity best practices, like phishing email awareness, can significantly reduce the risk of successful attacks. Incident Response Plans: Having a clear plan for how to respond to a ransomware attack can minimize downtime and damage. By staying informed about the evolving threat landscape and implementing these mitigation strategies, organizations can improve their cybersecurity posture and become less susceptible to ransomware attacks.

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

Answer :

According to the website www.csk.gov.in, here are some of the recommended best practices for securing personal computers: Install genuine and updated software. This includes your operating system, applications, and antivirus software. Outdated software often has security vulnerabilities that attackers can exploit. Use strong passwords and change them regularly. A strong password is at least 12 characters long and includes a mix of uppercase and lowercase letters, numbers, and symbols. Avoid using easily guessable passwords such as your name, birthday, or pet's name. Maintain regular backups of important files. This will allow you to recover your data in case of a ransomware attack or other data loss event. Disable AutoPlay. AutoPlay can be a security risk because it can allow malware to run automatically when you insert a removable drive or connect to a network. These are just a few of the many best practices for securing personal computers. By following these tips, you can help to protect yourself from cyberattacks