Mains Practice Question

Q. Ransomware attacks and cyber espionage are growing threats to national security. Discuss the evolving nature of cyber threats faced by India and suggest potential solutions to enhance cybersecurity measures.. **(250 words)**

29 May, 2024 GS Paper 3 Internal Security

Approach

- Introduce by defining ransomware and cyber espionage
- State the evolving nature of cyber threats faced by India
- Suggest potential solutions to enhance cybersecurity measures
- Conclude suitably.

Introduction

Ransomware is malicious software that **encrypts victims' data a**nd demands payment to restore access. **Cyber espionage** involves unauthorized access and theft of sensitive information, often by state-sponsored actors, for economic, political or military gains.

- **They are indeed grave threats to national security, and India, like many other countries, is grappling with these evolving cyber threats.**

Body

The Evolving Nature of Cyber Threats Faced by India:

- **Increasing Ransomware Attacks:** India has witnessed a surge in **ransomware attacks.**
  - **Example:** The **2022** ransomware attack on the **All India Institute of Medical Sciences (AIIMS) in Delhi.**
- **Cyber Espionage and Data Breaches:** Sophisticated cyber actors, including state-sponsored groups, are targeting India's critical infrastructure and sensitive data.
  - **Example**: the data breach at the **Kudankulam Nuclear Power Plant.**
- **Deepfakes and AI-powered Attacks:** India faces risks from emerging cyber threats like deep fakes, AI-powered social engineering, and autonomous cyber weapons.
  - **Example**: Deepfake videos of Indian political leaders spreading disinformation during elections.
- **Internet of Things and Operational Technology Risks:** The proliferation of IoT devices and the convergence of IT and OT systems in industrial control systems create new attack surfaces.
  - Vulnerabilities in IoT devices used in **smart cities** or industrial control systems could be exploited for disruptive attacks.
- **Doxing and Hacktivism:** Indian entities face risks from hacktivist groups and individuals engaging in doxing (leaking sensitive information) for ideological or political motivations.
  - Hacktivist groups recently attempted a malware entrapment bid on the **Indian Air Force.**

Potential Solutions to Enhance Cybersecurity Measures:

- **Investing in Cyber Defense Capabilities:** Enhancing India's cyber defense capabilities by investing in advanced threat detection and mitigation technologies.
    - Developing a skilled cybersecurity workforce through specialized training programs and public-private partnerships.
- **Promoting Secure Software Development Practices**: Encouraging the adoption of **secure software development life cycle (SDLC) p**ractices to address vulnerabilities in software and systems.
    - Incentivizing the use of secure coding practices and vulnerability disclosure programs.
- **Cybersecurity Sandboxes and Deception Grids:** Implement sandboxes and deception grids to detect and analyze advanced cyber threats by luring and containing them in isolated environments.
    - The **Indian Computer Emergency Response Team (CERT-In)** could create a honeypot network to attract and study the tactics of threat actors targeting Indian infrastructure.
- **Bug Bounty Programs:** The Indian government could launch a bug bounty program for its e-governance platforms, to incentivize ethical hackers and security researchers to identify and report vulnerabilities in critical systems and applications.
- **Cybersecurity Exercises and Simulations:** Conduct regular cybersecurity exercises and simulations involving various stakeholders to test incident response capabilities, identify gaps, and improve preparedness.

Conclusion

Cybersecurity is a continuous battle. By proactively adopting a multi-layered approach that combines **technological solutions, user awareness, and international cooperation,** India can effectively counter evolving cyber threats and safeguard its national security.

PDF Refernece URL: https://www.drishtiias.com/mains-practice-question/question-8308/pnt