Medical Device and Malware

For Prelims: Medical Device and Malware, Ransomware, Cyberattacks, Trojan Horses, Cyber Surakshit Bharat, Cyber Swachhta Kendra.

For Mains: Implications of malware attacks on medical devices and the measures.

Why in the News?

Recently, some experts have warned that Common medical devices such as oximeters, hearing aids, glucometers, and pacemakers can be turned into **Ransomware.**

- Industry experts are now seeking urgent Central government intervention to recognize this threat and immediately put in place measures to plug any possible drain.
- The warning comes close on the heels of **the ransomware attacks suffered by India's top tertiary care hospitals,** leading to the siege of millions of medical records and vast amounts of health data at Delhi's AIIMS, Safdarjung Hospital etc.

What are the Concerns?

- **Data Breaches:**
  - The increasing use of medical technology devices and the lack of adequate cyber protection for these devices have **raised concerns about data breaches and cyberattacks in the healthcare industry.**
  - Such devices contain software as medical devices (SaMD) and software in medical devices (SiMD), and are typically connected to the internet, mobile phones, servers, and the cloud and thus vulnerable to attacks.
  - **Sun Pharma,** the fourth-largest generic pharmaceutical company in the world and an Indian multinational corporation, **was targeted in the recent cyberattacks along with the** Indian Council of Medical Research (ICMR).
- **Vulnerable Population:**
  - India is among **the world's top 20 markets for medical devices**, with the medical devices sector projected to reach USD 50 billion by 2025. However, the rapid economic growth, rising middle-class incomes, and increased market penetration of medical devices have left the **population vulnerable to cyber threats.**
- **Inadequate Systems:**
  - Furthermore, the **Indian healthcare industry lacks a centralized data collection mechanism,** which makes it challenging to determine the exact cost of data corruption.
  - Despite this, it is evident that data has become the **new oil and is seeing a significant threat from cyberattacks.**

How can we Address Such Cyber Threats?

- **Consultation with the Experts:** The government should consult with industry experts to identify the challenges that could pose a risk to national security.

- **Employee Training:** Employees should be trained in how to recognize and avoid phishing emails, which are commonly used to initiate ransomware attacks.
- Data protection is not a rocketing science, but requires legal and technical artisanship, the **allocation of adequate resources and the training of all professionals** involved in the processing of personal data.
- **Regular Software Updates:** Regular software updates can help address vulnerabilities that hackers might exploit.
- **Access Control:** Limiting access to medical devices to only authorized personnel can prevent unauthorized individuals from accessing the devices and infecting them with malware.
- **Encryption:** Encryption can be used to protect the data on medical devices from unauthorized access.
- **Network Segmentation:** Segmenting the network can help **prevent the spread of malware from one device to another.**

What are the Major Types of Cyber Threats?

- **Ransomware:** This type of malware **hijacks computer data and then demands payment (usually in bitcoins)** in order to restore it.
- **Trojan Horses:** A Trojan horse attack uses a malicious program that is hidden inside a seemingly legitimate one.
    - When the user executes the **presumably innocent program,** the malware inside the Trojan can be used to open a backdoor into the system through which hackers can penetrate the computer or network.
- **Clickjacking:** Act of tempting internet users to click links **containing malicious software or unknowingly share private information** on social media sites.
- Denial of Service (DOS) Attack: The deliberate act of overloading a particular service like website from multiple computers and routes with the aim of disrupting that service.
- **Man in Middle Attack:** In this kind of attack, the messages between two parties are intercepted during transit.
- **Crypto Jacking:** The term Crypto jacking is closely **related to cryptocurrency.** Crypto jacking takes place when attackers access someone else's computer for mining cryptocurrency.
- **Zero Day Vulnerability:** A zero-day vulnerability is a flaw in the machine/network's operating system or application software which has not been fixed by the developer and can be exploited by a hacker who is aware of it.
- **Bluebugging**: It is a form of Bluetooth hacking in which an **attacker exploits a vulnerability in a Bluetooth-enabled** device to gain unauthorized access to it. The attacker can then use the compromised device to make calls, **send messages, or access other data without the user's knowledge or consent.**

What are the Government Initiatives Related to Cyber Security?

- **Indian Cyber Crime Coordination Centre (I4C)**
- **Indian Computer Emergency Response Team (CERT-In)**
- **Cyber Surakshit Bharat**
- **Cyber Swachhta Kendra**
- **National Cyber security Coordination Centre (NCCC)**

UPSC Civil Services Examination, Previous Year Question (PYQ)

Prelims

Q.1 In India, under cyber insurance for individuals, which of the following benefits are generally covered, in addition to payment for the loss of funds and other benefits? (2020)

1. Cost of restoration of the computer system in case of malware disrupting access to one's computer

2. Cost of a new computer if some miscreant wilfully damages it, if proved so
3. Cost of hiring a specialised consultant to minimise the loss in case of cyber extortion
4. Cost of defence in the Court of Law if any third party files a suit

Select the correct answer using the code given below:

(a) 1, 2 and 4 only
(b) 1, 3 and 4 only
(c) 2 and 3 only
(d) 1, 2, 3 and 4

Ans: (b)

Q.2 In India, it is legally mandatory for which of the following to report on cyber security incidents? (2017)

1. Service providers
2. Data centres
3. Body corporate

Select the correct answer using the code given below:

(a) 1 only
(b) 1 and 2 only
(c) 3 only
(d) 1, 2 and 3

Ans: (d)

Mains

Q. What are the different elements of cyber security ? Keeping in view the challenges in cyber security, examine the extent to which India has successfully developed a comprehensive National Cyber Security Strategy. **(2022)**

Source: TH