Syllabus subtopic: Basics of Cyber Security

Prelims and Mains focus: about the report: its findings and concerns associated; about PACS

News: Greenbone Sustainable Resilience, a German cybersecurity firm recently published an updated report on medical data leaks.

About the report

- The first report was published in October last year, in which Greenbone revealed a widespread data leak of a massive number of records, including images of CT scans, X-rays, MRIs and even pictures of the patients.

- The follow-up report, which was published in November, classifies countries in the “good”, “bad” and “ugly” categories based on the action taken by their governments after the first report was made public.

- India ranks second in the “ugly” category, after the U.S.

Key findings of the report

- Medical details of over 120 million Indian patients have been leaked and made freely available on the Internet.

- What is even more worrying is that the number of data troves containing this sensitive data went up by a significant number in the Indian context a month after Greenbone’s initial report was published.

- Maharashtra ranks the highest in terms of the number of data troves available online, with 3,08,451 troves offering access to 6,97,89,685 images. The next is Karnataka, with 1,82,865 data troves giving access to
The report says that in 60 days after the first report was put out, the number of data troves bearing the patients’ information went up from 6,27,000 to 1.01 million, and that the images of patients’ details rose from 105 million to 121 million.

It is a notable fact for the systems located in India, that almost 100% of the studies (data troves) allow full access to related images.

Why is it a concern?

The leak is worrying because the affected patients can include anyone from the common working man to politicians and celebrities. In image-driven fields like politics or entertainment, knowledge about certain ailments faced by people from these fields could deal a huge blow to their image.

The other concern is of fake identities being created using the details, which can be misused in any possible number of ways.

How was the data leaked?

Greenbone’s original report says the leak was facilitated by the fact that the Picture Archiving and Communications Systems (PACS) servers, where these details are stored, are not secure and linked to the public Internet without any protection, making them easily accessible to malicious elements.

The fact that PACS servers are vulnerable to attack or are accessible is not new information, and there have been a number of reports on this topic in the past. No report, however, has dealt with the breadth and depth of the problem associated with unsecured PACS servers.

About PACS
A picture archiving and communication system (PACS) is a medical imaging technology which provides economical storage and convenient access to images from multiple modalities (source machine types).

Electronic images and reports are transmitted digitally via PACS; this eliminates the need to manually file, retrieve, or transport film jackets, the folders used to store and protect X-ray film.

A PACS consists of four major components:
1. The imaging modalities such as X-ray plain film (PF), computed tomography (CT) and magnetic resonance imaging (MRI)
2. a secured network for the transmission of patient information
3. workstations for interpreting and reviewing images, and
4. archives for the storage and retrieval of images and reports.

Combined with available and emerging web technology, PACS has the ability to deliver timely and efficient access to images, interpretations, and related data. PACS reduces the physical and time barriers associated with traditional film-based image retrieval, distribution, and display.