Cyber Suraksha Dishaanirdesh Vol. 12

Cyber Attacks in Healthcare Industry

Health care industry has been an eye candy for all the hackers worldwide in the past many years. 15 million records got compromised in 2018 and thrice the year before. Following are few case studies of the previous year and the reasons behind such breaches:

DOMINION NATIONAL: Breach of 2.96 million patients' healthcare information due to improper data server security

Insurer Dominion National reported a hack on its servers, which potentially breached the data of 2.96 million patients which stayed unnoticed for 9 straight years. When the investigation was held the reason identified was unauthorized access to the data servers.

INMEDIATA HEALTH GROUP: Breach of 1.5 million patients' healthcare information

A misconfigured database led to a personal health data breach of 1.57 million Inmediata Health Group patients. The internal website, which contained patient's data was visible on the all search engines. The information had been made available to employees through an internal web page, but the failure to configure that page correctly allowed the data to be made accessible over the internet without the need for authentication.

OREGON DEPARTMENT OF HUMAN SERVICES: Successful phishing attack leading to compromise of 6 lakh patients healthcare data

Mail inboxes remain flooded with promotional offers that attract the users. Such mails can be malicious trying to gain credentials, in Oregon this compromised the employee credentials and exposed 645,000 patient's data and 2.5 million mail IDs.

COLUMBIA SURGICAL SPECIALIST: Ransomware attack blocking the access of 400,000 patients' records

Ransomware attack has been a big talk in Cyber attacks, which restricts the access to all the data and asks huge amounts to be paid to regain access. On January 7, 2019 Columbia Surgical Specialist reported a ransomware attack that blocked the access of medical records of 400,000 patients. The hospital had proper backups in place and did not have to pay the ransom and restored the backed up data.

Cyber Suraksha Dishaanirdesh Vol. 12
Learnings for NHA

Be aware of Social Engineering

Never disclose potentially sensitive information to an unknown source, and never give out more information than seems necessary.
Being vigilant in detecting phishing emails and educating employees in NHA to be proactive is a crucial step in protection. Key pointers on how to spot and handle phishing email:

- Check the email signature
- Be careful with attachments
- Check for spelling errors
- Is the email asking for personal information

Maintaining proper information backup

Backup copies allow patient information to be restored from an earlier point in time will help the NHA recover from an unplanned event. Storing the copy of the information on separate medium is critical to protect against primary data loss or corruption.

Security Guidelines for workplace

Stay alert while websurfing: Whenever any confidential detail that must not be on the internet, is visible then it should be immediately reported to NHA. Since, it could be a result of any technical misconfiguration.
Regularly check if system is updated: In case any update gets missed because of any reason, it should be reported. This might make the system open for attack.
Report any abnormality: If any problems are faced during the daily processes, then reporting should be done, so that the issue could be identified and system stays safe from any data breach, loss or failure.

Stay Safe from Ransomware

Do not click on pop-up ads in unknown websites, do not give everyone full user permissions. Install all security updates for your computer. Keep automatic updates enabled. Do keep your security software patches and operating systems up to date