INVASION FROM THE SKY HEALTHCARE BECOMES HIGH-RISK CYBER ATTACK TARGET

Over the last one decade or so, web applications and servers of banks, defence establishments, emails and financial institutions have been the main targets of hackers, and the inducement for such cyber-attacks are financial gains, or an act of revenge, or just for the fun of it. But now the hackers have widened their sphere of action and striking at newer targets, including the healthcare sector.

The healthcare industry collects and stores a vast amount of data of patients, including medical reports and other clinical data, and of course sensitive information of various pharmaceutical companies. Presence of this massive data in the cyber world catches the attention of cybercriminals and they are compromised, primarily because a large number of healthcare institutions do not comply with the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR) guidelines.

Even though hospitals have started using technology tools and automotive devices rapidly in order to improve the quality of treatment and patient care, non-compliance of standard operating procedures (SOPs) leaves gapsfor hackers to exploit the vulnerabilities.

Medical reports, life-critical information, doctors' data, and Internet of Things (IoT)-connected medical devices could well be compromised as the hackers aim to cause scientific, financial and reputational loss to healthcare providers.

Such attacks can, of course, be focused on organisations but they can also affect individual lives: a little negligence on the part of the organisation's cyber security team could prove fatal for a patient. So, trending cyber-attacks and data breach techniques call for stringent measures to ensure complete security of hospital devices and healthcare data through a secure ecosystem for computer devices, frequent cyber security audits, cyber awareness training, vulnerability assessment and deployment of latest security tools.

Six major cyber-crime

threats to healthcare

Unauthorised workplace access: Unauthorised access is mostly gained by insiders but sometimes it may be an outsider as well. An unauthorised person can reach the data center, server room, portable devices such as laptop, USB, or other data traveller devices to steal life-critical information about patients. Generally, the healthcare industry or hospitals do not pay much attention to data security and put the server rack in an open room without any biometric access or CCTV surveillance.

Ransomware Attack: Nowadays, international cyber-criminal gangs are also targeting healthcare industries to make money. Attackers encrypt data and files of the hospital server or computer so that the staff cannot access these files until the hospital pays them the ransom. Attacker binds the ransomware file either with genuine software or files like PDF and sends across to the victim via email. Lack of improper firewall configuration, network intrusion detection system and antivirus software, ransomware can easily encrypt valuable files.The actual user can decrypt such files only using a specific key which he would get after paying the ransom.

> “
> EVEN THOUGH HOSPITALS HAVE STARTED USING TECHNOLOGY TOOLS AND AUTOMOTIVE DEVICES RAPIDLY IN ORDER TO IMPROVE THE QUALITY OF TREATMENT AND PATIENT CARE, NON-COMPLIANCE OF STANDARD OPERATING PROCEDURES LEAVES GAPSFOR HACKERS TO EXPLOIT THE VULNERABILITIES

DDoS Attack: In their race to better facilitate patients and gain financial edge, healthcare institutions sometimes often try to pin other rivals down. If a healthcare outlet manages to deploy a Distributed Denial of Service (DDoS) attack against its business rival, the DDoS system starts shooting multiple requests per second to the computer resources to keep it engaged, thus making them redundant for real use. Every computer resource can handle only a fixed number of requests per second. In case of excessive load, the server may not be able to respond properly to the actual user. An improper arrangement of security checks and firewall leaves room for DDoS attacks.

Hacking: Data hosted on the hospital web server can be accessed from any location on the globe for research and medical purposes by doctors. Hacker sitting at a remote location can hack website or server of the healthcare institution and steal critical data about patients. If the web server is not deployed with proper security and firewall, it could be vulnerable to SQL Injection, Remote Code Execution and Command Injection, among other high-rated vulnerabilities. By exploiting these vulnerabilities, a hacker can take dump of the complete database of patients and doctors. He can even modify, delete or insert an entirely fake record in the

> “
> ONE NEEDS TO MAINTAIN A DATA BACKUP WITHOUT FAIL, WITH THE BACKUP SERVER KEPT AWAY FROM THE MAIN SERVER AND NOT DIRECTLY LINKED TO THE SAME NETWORK. A BACKUP SERVER ACCESSIBLE ONLY THROUGH AN INTERNAL NETWORK IS RELATIVELY MORE PROTECTED AGAINST CYBER-ATTACKS

database to misguide the doctor with regard to a patient's line of treatment.

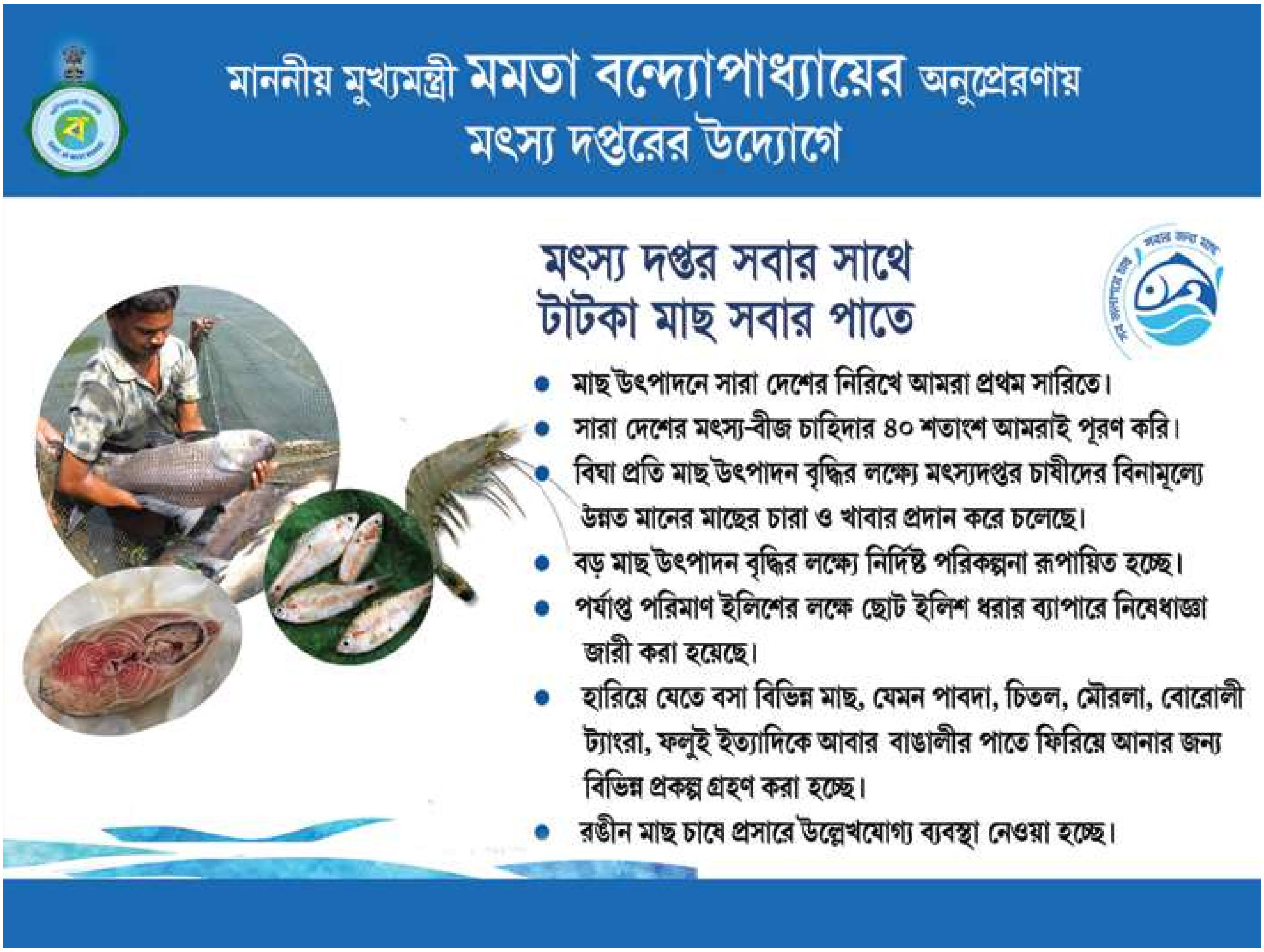
Malware Attack: All the above-mentioned types of attack can affect the industry only once – just after the attack, but malware is a malicious tool using which an attacker can get complete access to the industrial server and system. After securing access, the attacker may create persistence in the computer network to perpetuate his reach. Malware can cause spying and data leakage in the hospital and pharmaceutical industry.

Phishing Attack: Phishing is a fraudulent attempt to obtain sensitive information such as usernames, passwords and other critical details by disguising as a trustworthy entity in electronic communication. In order to hack healthcare units, an attacker can design a phishing web page to grab server, email, router and firewall passwords. The moment one visits the link received on email, it would redirect the visitor to a different website and open a fake web page looking similar to the genuine one and could ask to insert login credentials. And the damage is done.

Segment-wise Risk Analysis

Hospital and clinic: Hospitals are a high-risk target for a hacker since most of them have shifted to an automated collection and digital management system of patient'srecord. If the data is lost or tampered with, the hospital may lose the trust of patients, thereby affecting the credibility of the healthcare outlet. Hacker can even defame the hospital taking advantageof a small security lapseon its part, causing immense damage to the institution. Of late, hospitals have started looking to migrate to cloud-based hosting to protect data, but without proper encryption and adequate security checks, it could actually turn out to be an address for data loss.

IoT-based medical systems: The new generation of healthcare systems come with smart and automated medical devices, like smart



> ATTACKER BINDS THE RANSOMWARE FILE EITHER WITH GENUINE SOFTWARE OR FILES LIKE PDF AND SENDS IT ACROSS TO THE VICTIM VIA EMAIL. LACK OF IMPROPER FIREWALL CONFIGURATION, NETWORK INTRUSION DETECTION SYSTEM AND ANTIVIRUS SOFTWARE, RANSOMWARE CAN EASILY ENCRYPT VALUABLE FILES

beds, and scanning and surgery machines, where all medical equipment and treatment procedure arelinked and operated through internet-based tools, mostly without proper security mechanism in place. This renders the system a soft target for cyber attackers. By accessing those devices, a hacker can steal scanning report and other confidential treatment records. If the hacker is able to break the automated surgery machine, they can misguide doctors and cause the predefined surgery to go astray.

Pharmaceuticalcompanies : It is one of the crucial areas with much bigger implications. As the pharmaceutical companies have started using automated machines to mix salts in proper ratio and for packaging medicines in a standard dosage, ifanattackercausesthemachine to malfunction by tampering with its programming, it may cause a major medical crisis. A microgram of salt in excessin a medicine is good enough to claim one's life. Besides, sensitive information about specific medicine's composition can also be stolen by the attackers, much to the disadvantage of the company.

Atomization industries: Nowadays,a sizable number of hospitals prefer robotics-based medical services to cater to larger number of patients, andscientists are busy inventing newer devices which can perform automated medical observation and surgery. Hackers can misguide those automated devices at various stages of medical treatment, which can harm both patients and reputation of such hospitals.

Call for action:Fool-proof cybersecurity

Improve in habits: There is a needto keep complex passwordsfor hospital devices (computer, server, control panel of scanning machines, etc.). Proper access control on critical computer infrastructure is a must for the hospital. Server room and critical operating systems should be accessible only by authorised persons and protected through surveillance systems likeCCTV.

Technical up-gradation: High-tech medical devices and operating software should always be updated with the latest security patch Deployment of both software and hardware firewall on the network and server with updated rules needs to be ensured. In this regard, effective anti-virus software is essential to guard against cyber-attacks. Network intrusion detection and prevention system by experts can also prevent data loss to a great extent. Besides, regular audit of security standards must not be ignored.

Educating the staff: Every employee of the hospital should be educated on cyber security. A cybercriminal can target anyone in the organisation to gain access to sensitive information of the

> HIGH-TECH MEDICAL DEVICES AND OPERATING SOFTWARE SHOULD ALWAYS BE UPDATED WITH THE LATEST SECURITY PATCH. DEPLOYMENT OF BOTH SOFTWARE AND HARDWARE FIREWALL ON THE NETWORK AND SERVER WITH UPDATED RULES NEEDS TO BE ENSURED

organisation. If doctors and other hospital staff are aware of the social engineering techniques of cyber-attack then it would not be easy to hack into a hospital's data.

Data recovery plan: Cyber intrusion can happen to anyone and anywhere. So, one needs to maintain a data backup without fail, with the backup server kept away from the main server and not directly linked to the same network. A data backup server accessible only through the internal network is relatively more protected against cyber-attacks.

Conclusion: Apart from the attacks on computer or network devices, red-teaming allows cyber-criminals to target individuals to get into the network. It is not thattough to get control on the whole network once the attacker gets access to any one device in the network.That being the reason, cyber security must be applied on each and every node of network. Developinga habit for complex password maintenance should also be discussed regularly. Healthcare outlets collect and store sensitive patient information all in one place,from where cyber criminals can lift data for identity theft, extortion and bill details. It is time hospitalsbecame HIPAA and GDPR-compliant as these regulatory mechanisms provide for operational safeguards to securepatient records.

(Ummed Meelis a well-known cyber expert - police and defence trainer, and works closely with various police forces, Indian Air Force, Border Security Force and Comptroller & Auditor General of India, among other high-profile government establishments. He has conducted over 100 workshops for the police of Delhi, Uttar Pradesh, Rajasthan, Haryana and Himachal Pradesh and trained more than 8,000 police and other personnel in cyber security, vulnerability assessment and penetration testing, cybercrime investigation, digital evidence seizure and digital forensics.)

পশ্চিমবঙ্গ সরকার
কৃষিতে সাফল্য
আজ বাংলার ঘরে ঘরে
কৃষি বিপণন ব্যবস্থার এক নতুন দিগন্ত
পশ্চিমবঙ্গ রাজ্য কৃষিজ বিপণন পর্ষদ

KOLKATA POLICE - WITH YOU ALWAYS

CONTENT

The Kolkata PROTECTOR

NEW MEDIA

The Kolkata
PROTECTOR

JUNE - JULY 2019

Rs. 50/-

www.theprotector.in

A Magazine for the Kolkata Police

PROMOTING PEACE

PRAYER FOR PEACE, PROSPERITY