2020

Advisory for Hospitals & Healthcare Industry

BY THE DATA SECURITY CENTRE OF INDIA (DSCI) ALONG WITH THE CYBERSECURITY CENTRE OF EXCELLENCE (CCOE), HYDERABAD.

CYBERSECURITY CENTRE of EXCELLENCE

A joint initiative of DSCI & Government of Telangana

DSCI PROMOTING DATA PROTECTION

A NASSCOM® Initiative

GOVERNMENT OF TELANGANA

Background

The current context of global Coronavirus pandemic or more relatively known as COVID-19, has forced Governments, businesses and other institutes globally to take necessary precautions, and impart health guidelines and advisories such as social distancing and hygienic measures to safeguard human lives at stake. Currently, hospitals and health care industry are the frontline responders across the globe and are increasingly scaling up their collective efforts to offer necessary care and treatment to the patients diagnosed with COVID-19 symptoms, trying to save lives selflessly.

While hospitals are working round-the-clock handling the inflow of patients, they have become soft targets for cybercriminals due to lack of contemporary IT infrastructure and willingness to pay the ransom- ***thanks to their critical nature of work!***

Rise in Cyberattacks

Cybercriminals are exploiting the current crisis by increasingly deploying wide range of cyberattacks ranging from phishing attacks, unsolicited emails posing as advisories from government agencies, malware attached to mails, exploiting vulnerabilities in network devices and to a greater extent, more sophisticated type of attacks such as ransomware. Last year, a hospital from Mumbai became victim of ransomware attack and lost access to patient's history and billing data[1]. It was also reported that an attempt was made by hackers to attack the e-health services website of Kerala government[2].

As noted by INTERPOL's Cyber Threat Response team, there has been a significant uptick in ransomware-styled attacks which are designed and deployed to lock out healthcare critical systems to extort payments. To counter and safeguard against such types of criminal activities, INTERPOL has issued a Purple notice alerting police in all its 194 member countries to the escalated and surging threat of ransomware. According to Healthcare IT News UK[3], a cyberattack on a hospital in Czech, also serving as a COVID-19 test facility was forced a tech shutdown in the midst of the outbreak, compromising life-sustaining medical equipment.

Other motives of cybercriminals include preventing access to critical healthcare systems, stealing sensitive information such as patient data, personally identifiable information, financial information. In addition to technology related issues, there is a rise in manufacturing and sale of falsified medical products like face masks, substandard sanitizers and unauthorised antiviral medications. The general public is also being targeted by the cybercriminals by luring them into online phishing scams in the name of government schemes. One of the fastest proliferating scams amid these times are donation scams related to Coronavirus. Cyber criminals are exploiting empathy and helping nature of citizens by tricking them and con money.

Clinical labs who are providing the COVID-19 diagnostics services also need to beef up their software and hardware security as the ramifications of any attack on them could be devastating.

---

[1] https://www.asianage.com/metros/mumbai/190718/cyber-attack-on-mgm-hospital.html

[2] https://keralakaumudi.com/en/news/news.php?id=259769&u=amid-coronavirus-scare-attempt-to-hack-official-website-of-health-department-no-documents-lost-says-minister-259769

[3] https://www.healthcareitnews.com/news/europe/cyberattack-czech-hospital-forces-tech-shutdown-during-coronavirus-outbreak

Healthcare organisations and institutions must proactively heed to relevant advisories and guidelines to protect their healthcare network, assets and resources from being exploited by cybercriminals.

In light of these developments, DSCI has prepared a simple Cyber Security Best Practices guide for hospitals & healthcare industry. These simple and easy tips will ensure basic security protocols are upheld which can help in minimizing cyberattacks.

Cyber Security to be a Top Priority

Hackers attempt to lure the healthcare staff by sharing unsolicited COVID-19 related emails, falsely claiming to contain information or advice regarding the coronavirus from a government agency, which encourages the recipient to click on an infected link or attachment. This would help hackers to launch their exploits on their machine & spread it across.

It may lead to data breach of sensitive information or end up with ransomware attack.

- **Data breach of sensitive information:** this leads to stealing of Protected Health Information (PHI) which contains patient information and personally identifiable information (PII), doctors information and credentials. Hackers may sell the stolen information on the deep web, blackmail, stalk, harass or engage in other fraudulent activities.

- **Ransomware attack**: this is a malware attack that prevent users from accessing their personal/organisation's data and demand ransom in order to regain access. Even though the ransom is paid soon after the attack, there is no guarantee of files getting decrypted. Paying ransom makes the criminals more profitable and incentivizes them for further attacks.

Cyber Security Best Practices:

There is no single silver bullet. Preventive measures and awareness are required from multiple stakeholders in order to make hospital networks more secure and resistant to attacks like ransomware.

Preventive measures at three different levels

At Staff Level

- Conduct security awareness trainings and educate your staff about ransomware attacks
- Train your staff to spot and report phishing emails containing malicious attachments
- Enable multi-factor authentication on all user accounts
- Create awareness & understanding amongst employees and external third parties about unauthorised disclosure of personal data
- Train employees to handle data breaches efficiently

Phishing: Cyber criminals are now exploiting the COVID-19 outbreak as an opportunity to send phishing emails claiming to have important updates or encouraging donations, impersonating trustworthy organizations.

Phishing uses fraudulent email messages designed to impersonate a legitimate person or organization and trick the recipient into downloading harmful attachments or divulging sensitive information, such as passwords, official data, bank account numbers, etc.

Few common indicators of phishing attempts are:

- **Suspicious sender's address** imitating a legitimate business closely resembling one from a reputable company by altering or omitting a few characters
- **Generic greetings and signature** such as "Dear Customer" or "Sir/Ma'am" and lacking direct contact information in the signature block
- **Spoofed hyperlinks and websites:** Hover the cursor over any link in the email body. If the link doesn't match the text that appears onscreen, it may be spoofed.
- **Spelling and layout:** Poor grammar, spelling mistakes and inconsistent formatting are other indicators
- **Suspicious attachments** are a common delivery mechanism for malware. Unsolicited emails request users to download and open an attachment.
- **Email forms** creating urgency or lottery wins asking users to fill personal/financial information

For more information: **Refer to DSCI WFH Advisory for Employees**

At IT Infrastructure Level

- Ensure your firewalls are operational and up-to-date at all times
- Logically separate your networks
- Employ a strong email filtering system to block spam and phishing emails
- Patch vulnerabilities and keep all your software updated
- Set up rigorous software restriction policies to block unauthorized programs from running
- Keep your antivirus fully operational and updated
- Conduct periodic security assessments to identify security vulnerabilities
- Enforce the principle of least privilege
- Disable Remote Desktop Protocol (RDP) when not in use
- Disable macros in your Microsoft Office files
- Use a strong, real-time intrusion detection system to spot potential ransomware attacks
- Conduct periodic privacy impact assessments
- Ensure de-identification of patient personal data, especially health data

At Backup Level

- Back up your files using a 3-2-1 backup rule; i.e., retain at least three separate copies of data on two different storage types, with at least one of those stored offline
- Ensure that you backup critical work data periodically
- Apply preventive measures at the backup level
- Enforce regular checks for data integrity and recovery on all your backups
- Ensure implementation of storage limitation checks on patient's personal data

For queries or more information, reach out to us at: safewfh@dsci.in