BioSpectrum
the business of Bio & Health Sciences
ASIA EDITION

Securing interoperability from cyber threats in healthcare organisations

October 1, 2021 | News | By Hithaishi C Bhaskar

In conversation with Vincent Goh, Senior Vice President at CyberArk (Asia Pacific and Japan)



As hospitals and healthcare ecosystems continue to grow in sise and complexity, adopting digitised operation models is inevitable. Healthcare is becoming one of the major targets of cyberattacks with the increase in adaptation of Infocomm network-driven technologies. The enablement of remote monitoring tools and frequent data maneuvers is prompting the ransomware and cyberattack risks on confidential healthcare data. Tackling this will leverage unlimited possibilities in advanced medical technology and healthcare innovations. **Vincent Goh, Senior Vice President at CyberArk (Asia Pacific and Japan)** provides more insight on multi-layered cybersecurity threats and solutions for healthcare organisations.

- **What are some common breaches in healthcare?**

Frontline healthcare providers are able to offer patients new models of care and technologies, allowing advanced patient services and improved clinical outcomes. Digital transformation has played a big part in improving healthcare, but, at the same time, it increases the threat surface as far as an attacker is concerned, introducing additional cybersecurity risks for the sector.

While the adaptation to digital – given the clear benefits – is well underway, healthcare organisations are a little behind in adopting the “cybersecurity mindset” when compared to other industries, which are perhaps more used to being cyber targets. It is important to change this, embracing an Identity Security approach is built on Zero Trust principles and an “assume-breach” mentality. Without this, hackers have an easier path to infiltrate, potentially disrupting patient care and being able to access private patient records.

The top three common breaches witnessed in the healthcare industry include:

Ransomware Attacks

In 2020 alone, ransomware attacks on the healthcare industry reached nearly $21 billion. These attacks on healthcare organisations can be particularly devastating as cybercriminals are becoming more aggressive, viewing the healthcare sector as an easy target as they hit multiple endpoints such as printers, biomedical devices, the internet of things and the imaging suite.

Insider Attacks

Outdated and unsupported software and rapidly evolving technology have left hospitals and healthcare systems vulnerable to internal threats – whether resulting from human error, which could be due to limited cybersecurity literacy, or otherwise.

Third-Party Attacks

Cyber criminals will exploit any weak point along the continuum of care. This means that partners such as business services, management consultants, legal counsels, and other external parties connected to the healthcare organisation can be seen as targets.

- **What are the most common ways attackers use to enter a company's network to steal their data?**

Phishing remains one of the top forms of social-driven breach. Attackers nearly always take the path of least resistance by using this tried-and-true approach: start with a phishing scam targeting a user's endpoint then crack weak passwords to access credentials in the device. Using these credentials, the attacker can move from one workstation to another to steal sensitive data and privileged credentials (such as local admin rights) to easily escalate to higher-value assets and information.

In addition, the attack surface has expanded dramatically as connected devices proliferate, including computers for medication, treatment and surgical procedures.

- **What are the implications faced by a healthcare organization if it is attacked by cyber criminals?**

Damage may stem from the disruption of a healthcare organisation's business operations by making workstations, software and servers inoperable and/or extorting the victim with threats. Cyber attacks do not stop at the endpoint but seek to propagate deeper for more valuable data. It is imperative for healthcare institutions to demonstrate regulatory compliance, not only to avoid financial penalties, but also to avoid unwanted, severe repercussions.

Once in, attackers will disable endpoint security and security monitoring wherever possible. Their next objective is to harvest credentials for an even higher privilege escalation, to look for more machines and valuable data. As they propagate, they disrupt backups, delete shadow copies and unlock files to maximise the impact of the attack.

In some cases, it can lead to loss of lives. In 2020, a ransomware attack invaded 30 servers of the Düsseldorf University Hospital, resulting in a disruption of its treatment and emergency services, where a patient who had to be transferred to another hospital died from treatment delays. The incident is the first known death due to a cyberattack.

- **What can the security team in hospitals do to secure themselves against such attackers?**

Firstly, hospitals and other private healthcare organisations should focus on electronic patient health information (ePHI) records, which includes personally identifiable information (PII). These records must be compliant with global and local regulations and standards.

As hospitals and healthcare ecosystems continue to grow in size and complexity, providers face ever-increasing challenges in protecting highly targeted ePHI. Secure interoperability – or the safe sharing of ePHI – would not be possible without the use of privileged access management. Managing access to privileged information is an effective way to limit the moves of an intruder throughout the network after a breach.

To combat today's multi-layered threats, healthcare organisations must ramp up employee cybersecurity training, back up data regularly and adopt an Identity Security approach to their cyber defences, whereby the organisation assumes that any identity – whether IT admin, remote worker, third-party vendor, device, or application – can become privileged under certain conditions, creating an attack path to an organisation's most valuable assets. Tools are put in place to ensure that all these

identities are authenticating accurately, allocated proper permissions allowing them access to privileged assets in a structured way.

Hithaishi C Bhaskar