BioSpectrum the business of Bio & Health Sciences ASIA EDITION

Healthcare's Cyber Battle: Seven threats afflicting the industry

11 July 2024 | Analysis

By Karthick ChandraSekar, Associate Director, ManageEngine

Under the Universal Declaration of Human Rights, healthcare is a human right. Yet, despite this, cybercriminals routinely target health services, which can cripple critical infrastructure and services. Just last year, a DDoS attack caused a seven-hour disruption to the web services of Singapore's public healthcare institutions. The Ministry of Health mentioned that attackers flooded servers with internet traffic to prevent users from accessing online services. Internet-reliant services then became inaccessible as the attack triggered the firewall to begin filtering out traffic indiscriminately.

Although there was no compromises to patient care or internal networks, nor evidence indicating data losses, the incident was a warning. It undeniably sheds light on potential weak links in the digital resilience of the national public health system. Indeed, the Cybersecurity Agency of Singapore (CSA) has warned that with the rise of ransomware, healthcare is consistently among the top-three most targeted sectors.

Why healthcare is in the crosshairs

Health service providers hold private patient information, which is lucrative for criminals. On the awareness front, because healthcare tends to be an intense field, many staff end up not having the time to adequately prepare themselves to understand the cyber risks they face. The following threats are the most common, and every individual involved in healthcare should acquaint themselves with what they are and how they are used by threat actors.

Ransomware

Ransomware has dominated the threat landscape in recent years. According to the CSA's 2023 Cybersecurity Health Report, ransomware was the leading incident category. Unsurprisingly, perhaps, ransomware was also the most opted-for attack vector when targeting healthcare. The way ransomware attacks play out usually begins with threat actors gaining access to data and then encrypting it. Cybercriminals are able to hold that data hostage, only releasing it after payment is made by the organisation being extorted.

Having robust data encryption and backup tools will cost a fraction of what is typically demanded from criminals, and will also equip the organisation to steer clear of hits to brand reputation.

Data theft

In a shocking revelation, the Centre for Internet Security (CIS) said that a hacker stands to gain more from selling personal health information (PHI) than from selling credit card details on the black market. The average cost of a single PHI record on the black market is USD 355. To put that into perspective, the average cost per record of credit card information stands at a measly USD 1 to USD 2. Not only that, the stakes are also considerably higher for healthcare, where the average cost of a breach by non-healthcare-related agencies stood at USD 158.

That's why it is crucial for healthcare service providers to equip themselves with advanced data leak prevention software that can counter both external and internal threats.

Unauthorised access

Securing patient medical records hinges on protecting them from the inside out. That can only be achieved by limiting access for those records to a specific group of users, including employees and authorised third parties. This ensures that critical PHI or personally identifiable information (PII) is secured from prying eyes—be they cybercriminals or people within the organisation who are not directly involved in the use of that data.

Hacked network servers

Healthcare network servers connect different parts of the organisation, including MRI machines, patient monitoring tools, workstations, operating systems, peripheral devices, and computers. These various components enhance the overall healthcare experience, but they also increase the attack surface.

The recommended way to mitigate these risks is through a combination of firewalls, intruder prevention systems, and vulnerability detection and remediation tools. This mitigation effort needs to be supplemented with a unified endpoint management solution to improve the visibility of the network.

Phishing

Humans are central to maintaining cybersecurity, but we're all too often the weakest link. This is especially true of phishing, which uses social engineering methods to get people to give up sensitive information. Training healthcare personnel, setting up privileged access, and enforcing multi-factor authentication are each critical to fighting back against phishing.

Unsecure servers or databases

Sometimes, health services providers store patient records on public-facing servers in a manner that is easy for anyone with an internet connection to access. While compliance mandates like Singapore's Cyber and Data Security Guidelines for Healthcare Providers aim to provide clarity, it is still on providers to maintain comprehensive security information and event management (SIEM). That includes solutions for advanced threat analytics, threat hunting, user and entity behaviour analytics (UEBA), among others.

With healthcare organisations increasingly dependent on IT, it is critical to remember that many of these tools are not designed with security in mind. Though digital transformation enables innovation and efficiency, that work will all be in vain without awareness and a well-thought-out approach to security.