NETSCOUT

BECKER'S HOSPITAL REVIEW

Information security during COVID-19 and the era of remote care: Challenges and safety measures for health systems

Healthcare is increasingly reliant on digital information. To support this critical need, the size and complexity of hospitals' IT infrastructures have grown exponentially. The added complexity has created new challenges and risks for hospitals and health systems.

Becker's Hospital Review recently spoke with two NETSCOUT technology experts about the digital complexities impacting healthcare institutions. Eileen Haggerty, AVP, product and solutions marketing, and Tom Bienkowski, director of product marketing, shared perspectives for how IT leaders can overcome challenges and mitigate risks.

COVID-19 has accelerated the size and complexity of hospitals' digital infrastructure

The importance of digital technologies within hospitals continues to grow. These include technologies to improve patient outcomes – like EHRs and imaging – and technologies to improve the patient experience, such as smart beds. Hospitals now provide internet connectivity to numerous "internet of things" devices, including tablets and phones that run myriad mobile applications. Digitally-connected food carts deliver food to patients' rooms, and patient devices monitor cardiac or diabetic patients in the hospital and after they leave.

Ms. Haggerty said, "The applications themselves are more demanding and complex, and they've become more sophisticated because they're managing everything from patient records to diagnostic tests to radiology and prescriptions." Increasingly, hospitals are using cloud-based business services and various software-as-a-service offerings alongside these applications.

This increase in the number of devices, users, and applications on the network has forced hospitals to increase their network bandwidth. Ms. Haggerty has seen hospitals with 10 gigs of bandwidth increase to 40 gigs, and many are now deploying 100 gigs.

In addition to these trends, COVID-19 has spurred the exponential increase in telehealth services. One customer informed Ms. Haggerty that during the last two weeks of March, the hospital experienced a fourfold increase in telehealth volume. This increased network traffic has strained the capacity of some healthcare organizations. Even after the pandemic, the use of telehealth will remain high.

"These are some of the big evolutions happening," said Ms. Haggerty, "which are dramatically altering many aspects of the hospital IT environment."

Healthcare is unique since hospital networks operate 24 hours every day, seven days a week, 365 days per year. Having optimal network performance is critical in executing the hospital's mission. Ms. Haggerty emphasized, "Any unplanned disruption can be truly catastrophic, and even planned migrations, application upgrades, or system changes can be disruptive."

Achieving the required performance level is complicated in environments where organizations leverage technologies from multiple vendors, which is the case in most hospitals. In such environments, IT teams must deal with integration and interoperability challenges and issues related to visibility.

Ms. Haggerty explained that each vendor typically provides visibility related to their equipment's or application's performance that assesses how they're working. However, a report might show that each application appears to be performing well, the databases look good, and all the network and cloud tools are operating well. Yet a patient might still experience a slow load time for a web page or have difficulty accessing their medical record. "Each one of the siloed tools says that it's working fine, but IT is still receiving help desk tickets," states Ms. Haggerty. In her view, the major problem is the lack of visibility across the entire IT infrastructure.

Hospital IT leaders need visibility into the performance of all of the organization's applications regardless of which vendor provides the products and solutions. This functionality evaluates the data, traffic, voice, video, and more to understand any errors or disruptions throughout the infrastructure and look at performance holistically for the entire end-to-end patient experience.

The emphasis on complete visibility is part of NETSCOUT's mission since network performance is essential to ensure that healthcare providers can deliver consistent, safe, high-quality patient care. As Ms. Haggerty conveyed, "We're going to give you visibility across your private data center, your public cloud, your user experience, and your SaaS."

Focus on distributed denial-of-service attacks as they are often overlooked and misunderstood

IT leaders must be attuned to a wide range of security threats to the hospital's network and data. As Mr. Bienkowski pointed out, "There's been a major uptick in malware, phishing and all kinds of attempts to penetrate hospital IT infrastructure." The threat of ransomware has generated a great deal of attention with frequent reports of hospital attacks.

"Flying under the radar," Mr. Bienkowski observed, "is the threat of DDoS (distributed denial-of-service) attacks. One of the biggest threats to the performance of the hospital's digital infrastructure, as well as the availability of services, is a DDoS attack."

Recent statistics shared by Mr. Bienkowski illustrate how the threat of DDoS attacks has increased during the pandemic.

In the first half of 2020, when much of the world was locked-down, there were over 4.3 million DDoS attacks, which is a 15 percent increase from the same period in 2019, according to NETSCOUT research. Analyzing the period from March 2020 through the end of June, DDoS attacks increased by 25 percent compared to a year ago. During this time, NETSCOUT saw around 12,000 DDoS attacks within the healthcare industry, representing an increase of 12.5 percent compared to 2019. Mr. Bienkowski concluded, "The number and sophistication of DDoS attacks have increased not only during the first half of 2020 but during the COVID-19 pandemic itself."

Mr. Bienkowski expressed admiration for IT leaders for what has occurred over the past few months. "IT has had to absorb this massive uptick in need for higher bandwidth performance while also dealing on the front lines with a rise in DDoS attacks."

As threatening and disruptive as DDoS attacks can be, in Mr. Bienkowski's experience, a majority of enterprises don't have a good understanding of these attacks, which take three forms.

1. *Large volumetric, bandwidth-consuming events.* When most people think of a DDoS attack, this is what comes to mind. This type of attack aims to saturate routers and circuits.
2. *Application layer attacks.* These attacks go after specific applications, such as web servers or database servers. The objective of this type of attack, which comes in low and slow, is to exhaust the servers' resources. These attacks are difficult to detect but can be just as damaging as the large volumetric events.
3. *State exhaustion attacks.* These are stealthy attacks that go after stateful devices, such as firewalls and virtual private network concentrators, sitting at the edge of healthcare networks. During the pandemic, with more people working from home, VPN concentrators have become primary targets.

Unfortunately, many vulnerable IoT devices are becoming part of large botnets. By using free Do-It-Yourself attack tools or inexpensive DDoS for Hire Services, anyone can easily use these botnets to launch sophisticated DDoS attacks.

Mr. Bienkowski recommended, "The very first thing that leaders should do to protect your organization is to become educated about the true threat of DDoS. Many folks believe that a DDoS attack is a volumetric event. But this is not true. The modern-day DDoS attack is quite complex and uses multiple attack vectors." After becoming educated, the next step is to put various forms of protection in place.

For protection against the volumetric attacks, which saturate internet-facing circuits, on-premises security measures are obsolete. For these attacks, you need a cloud-based solution. NETSCOUT provides a cloud-based mitigation service, Arbor Cloud, with worldwide scrubbing and mitigation centers to handle the world's most significant attacks. Attack traffic redirects to these off-premise centers.

To stop the smaller application layer and state exhaustion attacks, NETSCOUT provides an on-premise solution, Arbor Edge Defense, that sits just inside the internet router in front of stateful devices like firewalls and VPN concentrators. It protects devices from stateful and block attacks targeting application servers.

Conclusion

A hospital's IT network and infrastructure have never been more critical. Technology and information are imperative for clinicians to operate efficiently in providing safe, consistent, high-quality healthcare. But providing adequate bandwidth, access, availability, and security is challenging. Using technologies from multiple vendors makes interoperability and visibility more difficult. New applications such as telehealth demand more bandwidth, and the increase in sophisticated DDoS attacks threatens the entire infrastructure.

IT leaders must have a solid understanding of their organizations' security and visibility issues within the complex healthcare environment. It is also important to partner with organizations with the in-depth knowledge and expertise required to address these performance and security challenges. ■