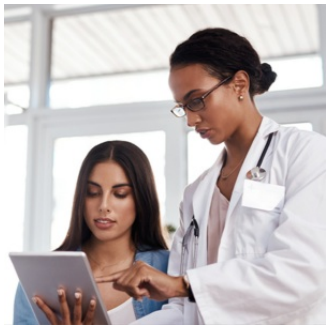
HealthManagement
Promoting Management and Leadership

Cyberattacks Are on the Rise – How Healthcare Organizations Can Stay Ahead



The healthcare industry is transforming in unprecedented ways — from advances in medical technology to care delivery models. This transformation is a quantum leap forward for clinical outcomes.

At the same time, it also introduces a new challenge: **opportunities for malicious actors.** Today's networks extend beyond the traditional hospital perimeter, exposing organizations to a greater risk of breaches. Healthcare is hit with ransomware attacks more than any other critical sector, according to the U.S. Federal Bureau of Investigations.

So what's driving the surge in cyberattacks on healthcare organizations? How should IT and security teams respond? Let's look at the different trends behind these attacks, and how healthcare organizations can effectively defend against today's latest threats.

3 Cybersecurity Trends in Healthcare

Several trends in healthcare are driving the latest changes in the threat landscape. Understanding these is the first step to building cyber resilience and readiness within hospitals and health systems.

1. The Rise of Remote Care

From telehealth to remote patient monitoring (RPM), innovations in care models are improving patient satisfaction dramatically. Patients experience more access to care while hospitals and health systems achieve better patient engagement and outcomes.

The challenge: Remote care requires tools and services to be administered outside the hospital — and perimeter. The wide range of under-protected devices (computers, smartphones, RPMs) exposes sensitive patient data to malicious actors, who could infiltrate a home network much more easily than a hospital network.

2. Connected Healthcare Devices Continue to Evolve

Connected devices such as heart monitors, dialysis machines, and infusion pumps are now widely used in a wide range of healthcare scenarios, as are non-medical connected devices such as digital wall boards, kiosks, and video screens.

The challenge: The surge in connected devices brings an unprecedented number of new endpoints to every hospital — which means more opportunities for threat actors to exploit.

3. Complex IT Environments and Resource Constraints

Healthcare organizations are constantly deploying new tools, applications, and services — delivered from data centers, cloud providers, SaaS providers, and internet-based services. These digital innovations enhance the care quality given by practitioners and enable patients to access and consume care conveniently.

The challenge: Hospital networks are quickly becoming tangled and unmanageable. IT leaders lose visibility into specific areas of the perimeter, which hinders resource allocation and troubleshooting. Paired with the industry-wide shortage of cybersecurity/IT talent and perpetual budget constraints, this level of IT complexity puts a huge strain on risk posture.

Other important factors fuel cyber risk in healthcare, including the highly sensitive nature of healthcare data such as PHI and PII, the growing rate of ransomware attacks, and the increasing number of legacy systems with outdated security.

How Can Healthcare Organizations Stay Ahead?

The healthcare industry's cybersecurity challenge is unique. Attacks aren't only business and operational in nature — they threaten continuous care delivery and put human lives at risk. Improving patient outcomes should always be our number one priority, and that means mitigating cyber risks, preventing breaches, and speeding up incident response.

Hospitals need a security approach built upon cyber resilience. One that prevents attacks before they occur, reduces mean time to detect and respond, protects all devices and users, and ensures effective care continuity. To do this, we recommend prioritizing these key areas:

1. Reduce IT complexity
2. Enable security automation
3. Safeguard patient data

In our latest white paper, *Cybersecurity Transformation in Healthcare: Three Priorities for 2023 and Beyond*, we delve into these recommendations and discuss the changing threat landscape of healthcare. We also discuss how a platform approach to cybersecurity helps hospitals and health systems stay ahead of today's emerging threats, saves lives, and supercharges care delivery across organizations.

At Palo Alto Networks, we work with healthcare providers to ensure that care from anywhere is uninterrupted. Our best-of-breed platforms across network, cloud, and security operations transform disparate and complex point solutions into integrated healthcare security so your organization can focus on what matters most: patient outcomes.

Download the white paper here.

Source: HIMSS

Published on : Tue, 30 Jan 2024