HealthManagement
Promoting Management and Leadership

Role of AI in Healthcare Cybersecurity: a Double-Edged Sword

Artificial intelligence and machine learning have featured heavily at healthcare technology conferences so far this year, building on public interest that has only grown since the end of 2022. Most of the conversations have highlighted the potential benefits of AI/ML solutions for healthcare organisations. But AI-powered tools also come with some serious cybersecurity considerations for organisations. Earlier this year, for instance, scammers used deepfake technology to create a bogus conference call in order to trick a finance employee at a multinational company in Hong Kong into paying out $25.6 million. Government agencies have also been warning everyday consumers about voice cloning scams. Amid this rapidly evolving AI and cybersecurity landscape, what do healthcare organisations need to know to strengthen their own strategies and protect their patients and staff members?

AI-Powered Cybersecurity Risks in Healthcare: A Call to Vigilance

Healthcare organisations are increasingly relying on AI to leverage the immense volume of data they collect, aiming to derive actionable insights and enhance clinical decision-making. Additionally, AI-powered solutions are sought after to alleviate the administrative burdens on staff and streamline workflows across the industry.

However, the proliferation of data in healthcare also makes these organisations prime targets for cybercriminals. These malicious actors are employing AI to bypass traditional cybersecurity measures, posing a significant threat to both small community hospitals and large health systems alike.

Various AI-related attacks are being deployed by cybercriminals. Among these are commoditized AI-powered attacks, which involve the use of readily available AI kits or services purchased from the dark web. Examples include data-intensive password cracking, assisted hacking, and the utilisation of deepfake technology to enhance social engineering schemes.

Furthermore, emerging AI-assisted cyberattacks, such as ransomware, advanced persistent threats (APTs), and business email compromise (BEC), are becoming increasingly prevalent. In these instances, AI is integrated into existing attack kits to enhance their effectiveness. For instance, the use of AI-powered ransom negotiators can exacerbate ransomware situations, making them more challenging to resolve.

AI-assisted APTs present a particularly insidious threat as cybercriminals leverage AI to continuously probe and attack healthcare systems through various avenues. These attacks often involve prolonged surveillance and remain undetected for extended periods, enabling the gradual exfiltration of sensitive data while evading conventional security measures.

As cyber threats continue to evolve and become more sophisticated, C-suite personnel and other organizational leaders are increasingly targeted by cybercriminals seeking access to valuable information that can impact multiple health systems. Thus, healthcare organisations must remain vigilant and implement robust cybersecurity strategies to mitigate these evolving threats effectively.

Empowering Cybersecurity with AI: Strategies and Frameworks for the Future

The integration of AI into cybersecurity solutions is on the rise, with major vendors like Cisco and Google Cloud partnering to strengthen defences against cyber threats. While the use of AI by malicious actors is a significant concern, industry leaders like Google CEO Sundar Pichai are optimistic about AI's potential to bolster cybersecurity.

AI-powered solutions offer several benefits, including aiding in data discovery and classification to identify security gaps and establish access privileges. They also assist in enforcing identity access policies based on business value and workflow considerations. AI response systems enhance infrastructure design by detecting intrusions and responding in real time, providing robust analysis and rapid responses to cyber threats.

In terms of cybersecurity strategy, the National Institute of Standards and Technology's Cybersecurity Framework 2.0 plays a crucial role. It promotes inclusivity by involving diverse stakeholders, standardizes terminology to improve communication, and empowers decision-makers across the organisation. Implementing this framework enterprise-wide fosters confidence and ownership among all involved parties in combating cyber threats.

While the use of AI introduces new challenges in cybersecurity, it also presents opportunities for healthcare organisations to enhance their defences. By leveraging AI-powered solutions for data discovery, access control, and threat detection, organisations can bolster their cybersecurity posture. Moreover, embracing frameworks like the NIST Cybersecurity Framework 2.0 facilitates cohesive and inclusive approaches to cybersecurity strategy, ensuring that all stakeholders are equipped to tackle evolving threats effectively. As the landscape continues to evolve, proactive adoption of AI-driven cybersecurity measures will be essential for safeguarding patients and staff members against malicious attacks.

Source: **HealthTech's MonITor**

Image Credit: **iStock**

Published on : Fri, 26 Apr 2024