HealthManagement
Promoting Management and Leadership

Cybersecurity: Key Best Practices for Protecting Health Data

With digital technology now widely used in healthcare, from doctor appointment scheduling apps to telehealth systems, risks of patient data being hacked have increased immensely. As such, the concept of "patient wellbeing" has evolved to include data privacy and protection.

This change is not surprising considering that, given recent high-profile cyberattacks –notably the Quest Diagnostics breach that left nearly 12 million patient records exposed, including credit card numbers and medical information – data thieves remain focused on their favourite targets: healthcare organisations.

As shown in a recent Carbon Black study, done in collaboration with 20 of the industry's leading CISOs, there has been a surge in cyber incidents over the past year with the average healthcare endpoint seeing 8.2 attempted attacks per month. In addition, two thirds (66%) of healthcare organisations taking part in the study noted how cyberattacks have become more sophisticated.

You May Also Like: Common Healthcare Cyber Threats

Monetary incentives are behind hackers' appetite for healthcare provider data, which is some of the most highly valued information on the dark web, alongside Personal Health Information (PHI), forged prescriptions, and health insurance login information.

Carbon Black said provider data mostly comes in the form of administrative paperwork that would help a hacker forge a legitimate doctor's identity. This information is sold by a hacker on the dark web to buyers who then pose as the doctor and submit fraudulent insurance or Medicare claims, or even claims for costly surgeries; pocketing the cash and leaving the victims to deal with the costs. This type of data regularly sells at $500 per listing.

With adoption of medical and IoT devices on the rise, the study noted the surface area for healthcare attacks is becoming even larger. "The silver lining has been that awareness of the problem has never been higher," Carbon Black said.

Strengthening Cybersecurity Management

This set of key best practices, the report points out, should help the healthcare industry boost its security posture and build a safer world for everyone.

- **Increase endpoint visibility:** CISOs need to start viewing the attack surface as including anything and everything that is connected within their organisation: medical-record systems, networked medical devices, payment processing systems, etc. Remember that if something is online, it's on your radar as a security risk.
- **Establish protection from emerging attacks:** With increased attack surface, providers need to use every tool at their disposal to detect and shutdown attacks once they inevitably occur. From security tools, to streaming analytics, to training: leave no stone unturned.
- **Run automated compliance and vulnerability assessments** : Island hopping attacks are a constant risk, hence organisations must regularly audit their network security and establish robust, quick-response procedures for remediation when gaps in the security infrastructure are identified.

- **Work with healthcare-focused Managed Detection & Response providers (MDRs):** One of most efficient ways to improve organisational security posture is to turn to experts in the field, as their wisdom and insights can help bring an organisation's cybersecurity into the 21st century.
- **Back up your data:** Cyber attackers infiltrate networks for the express purpose of destroying data. Being prepared is key, so make sure that data is stored off network for quick recovery in the event of a successful attack.

Source: securitymagazine.com

Published on : Tue, 19 Nov 2019