Dear ORNA Customer,

We are sending you this report to provide critical information and recommendations regarding the cyber threats related to the healthcare sector in Canada.

Summary

The healthcare sector in Canada faces significant cyber threats, including state-sponsored cyber espionage, ransomware attacks, and misinformation campaigns. Since 2015, at least 14 significant cyberattacks have targeted Canadian health information systems, as reported in an article published in the Canadian Medical Association Journal in November 2023. State-sponsored actors from nations such as China, Russia, Iran, and North Korea target healthcare institutions to collect sensitive information and disrupt operations. Ransomware attacks have become more frequent and sophisticated, causing severe disruptions and financial losses, as seen in notable incidents like the LifeLabs data breach, SickKids Hospital ransomware attack, and the Newfoundland and Labrador health system attack.

The COVID-19 pandemic has exacerbated existing vulnerabilities, with the rapid adoption of telehealth services and digital tools creating new entry points for cyber attackers. Emerging technologies like cloud computing and IoT devices have further expanded the attack surface.

By understanding and addressing these evolving threats, healthcare organizations can enhance their cybersecurity resilience, protect patient data, and ensure the continuity of critical healthcare services.

Notable Incidents

Cyber incidents in Canadian healthcare have been a growing concern due to the increasing reliance on digital systems and the sensitive nature of medical data, including:

- 2019 - LifeLabs experienced one of the largest cyberattacks in Canadian healthcare history, impacting approximately 15 million patients. The attackers accessed personal information, including names, addresses, emails, login credentials, health card numbers, and lab test results. Although LifeLabs paid a ransom to secure the data, the company faced significant public backlash and regulatory scrutiny.

- 2021 - A cyberattack on the Newfoundland and Labrador health system caused widespread disruptions across multiple hospitals. The attack compromised the province's healthcare IT infrastructure, including electronic medical records and email systems. As a result, patient care was significantly impacted, with delays in procedures and services due to the attack.

- 2022 - The Hospital for Sick Children (SickKids) in Toronto was targeted by a ransomware attack. This attack disrupted multiple services, including appointment bookings, diagnostic test results, and treatment schedules. While SickKids managed to restore affected systems without paying the ransom, the incident underscored vulnerabilities in the hospital's IT infrastructure.

- 2023 - A ransomware attack on five Ontario hospitals and their shared IT provider, TransForm, caused online service outages and forced the postponement of surgeries and appointments. The attack, which affected Bluewater Health, Chatham-Kent Health Alliance, Erie Shores HealthCare, Hotel-Dieu Grace Healthcare, and Windsor Regional Hospital, resulted in the theft of patient, employee, and professional staff data. The hospitals are working with cybersecurity experts and law enforcement, including local police, OPP, INTERPOL, and the FBI, to restore systems and investigate the breach.

State-sponsored cyber threats from nations like China, Russia, Iran, and North Korea, along with ransomware attacks by cybercriminals, significantly endanger the healthcare sector due to its valuable personal and medical data. The COVID-19 pandemic exacerbated these vulnerabilities as healthcare providers rapidly adopted digital solutions like telehealth and electronic health records, creating new entry points for attackers. Emerging technologies such as cloud computing and IoT devices have further expanded the attack surface, making healthcare a prime target. Additionally, the increasing use of misinformation and disinformation by state-sponsored actors poses a significant challenge, potentially undermining public trust and disrupting operations.

Conclusion

The healthcare sector in Canada confronts profound and evolving cyber threats, ranging from state-sponsored espionage to increasingly sophisticated ransomware attacks and the pervasive use of misinformation campaigns. Since 2015, numerous significant cyber incidents have targeted Canadian healthcare, underscoring vulnerabilities in digital systems and the sensitive nature of medical data. The COVID-19 pandemic intensified these risks, accelerating the adoption of digital solutions like telehealth without always commensurate cybersecurity measures. As healthcare organizations navigate these challenges, enhancing cybersecurity resilience and safeguarding patient data remain paramount to ensuring the uninterrupted delivery of critical healthcare services. By staying vigilant and proactive in addressing these threats, Canada's healthcare sector can better protect against cyber risks and uphold trust in its operations.

Recommendations

Recommendation #1: Stay up do date
Stay informed through threat intelligence feeds and news updates on cyber attacks targeting the healthcare sector in Canada

Recommendation #2: Multi Factor Authentication
Ensure that multiple forms of verification are required to access sensitive systems and data.

Recommendation #3: Conduct Regular Risk Assessments
Identify and address potential vulnerabilities in the systems.

Recommendation #3: Users Awareness
Conduct simulated attack scenarios to make sure that the employees are well aware of phishing and other risks, and also to make sure that they report the incident to the internal cybersecurity team.

Recommendation #4: Prepare for the Worst

ORNA strongly recommends that organizations ensure that all critical systems are backed up appropriately and that incident response plans are rehearsed regularly so that all participants understand their role.

References

1. Medium: https://medium.com/@aardvarkinfinity/canadian-cyber-threat-landscape-an-assessment-for-2023-2024-7152c5951f52
2. Global News: https://globalnews.ca/news/10063578/ontario-hospitals-ransomware-attack/

If you have any additional questions, please reach out to your ORNA representative at sme@orna.app.

Sincerely,
ORNA Team