CYBERMINUTE

Alberta Cybersecurity Insights

TLP: WHITE

Canadian Municipalities Impacted by Cyber Incidents

Throughout the first quarter of 2024 a number of Canadian municipalities faced cyber incidents that exposed vulnerabilities in their digital infrastructures.

Hamilton, ON: Since February 25, 2024, Hamilton has been experiencing a cyber incident that has seen some of its IT systems disabled. The ransomware attack led to the shutdown of almost all municipal phone lines and paralyzed city council, affecting services such as permit applications, the public transit app, and some public library services (such as wi-fi). According to the city's official statement, they took quick action to mitigate the impacts both to their systems and the public. Cybersecurity experts have been engaged to investigate the attack, and while critical services are operational, a full recovery timeline is presently unknown.

Ponoka, AB: The town of Ponoka's networks were impacted by a cyber incident on March 4, 2024. Per the notice on the town's website, the incident involved a breach of the system by an unauthorized external actor. Upon discovery of the breach, the town acted quickly to mitigate the impacts and is currently working with cybersecurity experts to investigate the breach. The town has emphasized its commitment to both privacy and security and has assured that any impacted individuals will be notified upon the conclusion of the investigation.

Huntsville, ON: Huntsville's municipal office was forced to close due to a cybersecurity incident discovered over the weekend of March 9-10, 2024. While there was no immediate evidence of compromised sensitive data, the town initiated its incident response protocol to secure their network against further unauthorized activity. As of March 21, some online services were still impacted by the precautionary measures taken in response to the incident as the town works with cybersecurity specialists to investigate the event.

These incidents serve as a reminder that cybersecurity is not just a technical issue, but a critical aspect of public trust and safety. As organizations continue to digitize their services, investing in cybersecurity measures is not just prudent but imperative for safeguarding the community's digital future.

Proactive cyber defences that organizations big and small can take include conducting regular risk assessments, adopting industry-standard cybersecurity frameworks, and implementing strong protective measures such as firewalls, encryption, and multi-factor authentication. The importance of having a practiced incident response plan can also not be overstated. Collaboration with other municipalities to share knowledge and resources is also vital in developing a collective defence against cyber threats.

Click Here to Read More!

Fujitsu Cyber Breaches

On March 15th,2024, Fujitsu released an incident notice in Japanese detailing the discovery of malware on their internal systems. Being as they are one of the

Critical Infrastructure Increasingly Targeted

Individuals and organizations are becoming increasingly dependent on digital systems everyday. With this, the critical

largest IT service providers on the globe, this incident was cause for concern amongst consumers. Subsequent investigations revealed that the exfiltration of personal information and customer data was probable. However, no leak has been confirmed and Fujitsu has informed customers who may experience down-stream impacts. In a separate incident, security researcher Jelle Ursem from the Dutch Institute for Vulnerability Disclosure, unveiled that Fujitsu had unknowingly exposed confidential and private customer data for a year. This data included thousands of client emails, passwords stored in plain-text, and much more. Ursem noted that he faced significant challenges reporting the breach to Fujitsu, citing the absence of a clear protocol for security disclosures as the crux of the problem.

The above incidents exemplify the increasing prevalence of supply chain threats, which saw a 430% rise in 2023 according to CrowdStrike. A supply chain attack is one in which the target is a trusted third-party vendor, critical to the supply chain. Such threats are diverse and can come from both internal and external sources, as shown by the Fujitsu incidents. Irrespective of the threat source, supply chain compromises result in downstream impacts which include but are not limited to infrastructure, which also relies on these systems and which underpins that same 'everyday' has become a prime target for cyber attacks. Throughout March several stories came to the forefront that US water and wastewater systems were being targeted by threat actors associated with the People's Republic of China and the Iranian government. In a letter from the White House, the US Environmental Protection Agency noted the following:

The Iranian Government Islamic Revolutionary Guard Corps was found to be using default manufacturer's passwords that had failed to be updated by the water facilities to spearhead their attacks,

The China-affiliated threat actor Volt Typhoon was less focused on active attacks, preferring to develop and enhance living off the land opportunities within critical infrastructure organizations, pre-positioning them for cyber espionage and quick action should tensions rise in the future.

These attacks come at a time where the public is less and less sure of the security of critical infrastructure. A survey conducted by Mitre and Harris Poll indicates that 81 per cent of Americans are worried about how secure their critical infrastructure is, with 78 per cent of people specifically stating a cyber attack as the greatest risk to

reputational damage, loss of customer trust, monetary loss, and loss of infrastructure.

There are several steps organizations can take to reduce the probability and impact of supply chain risk: firstly, organizations are advised to identify critical vendors as if they were assets. Following this, the incorporation of the supply chain threats and vulnerabilities into risk management activities can aid in the identification, prioritization, and treatment of risks both to and from the supply chain. Further controls include exercising buyers' due diligence and applying a defense in-depth strategy which ensures no single point of failure. Benjamin Franklin said it best in 1735, "an ounce of prevention is worth a pound of cure," and so organizations are advised to be proactive in securing their supply chain. For more information, refer to our October 2023 Threat Intelligence Report: Digital Supply Chain Compromise.

Click Here to Read More!

critical infrastructure. Further speaking to this public perception of the vulnerability of critical infrastructure is the fact that 51 per cent were not confident in organizations' ability to recover from a cyber attack.

In Canada, there has been a push in 2024 to better protect critical infrastructure. This includes a joint effort between the Canadian Armed Forces and the Communication Security Establishment to conduct defensive and offensive cyber activities with the aim to better protect against cybercrime, with specific mention of protecting against attacks on power grids and other essential services.

However, safeguarding against cyber attacks works best as a multi-layered approach, rather than relying on any one organization to carry out the protections. Key strategies that all organizations can take to enhance their protections include regularly updating and patching systems to mitigate known vulnerabilities, building up employee recognition and understanding of social engineering tactics that could lead to a breach, regularly backing up information in case there is a need to restore systems after an attack, and ensuring an incident response plan is in place should an attack occur.

Click Here to Read More!