How KPMG's cyber incident response team helped a Canadian municipality

Client challenge

A Canadian municipality suffered a ransomware attack by an external threat actor, which encrypted its entire IT infrastructure, including essential services such as water treatment and telephony systems. The attack rendered critical daily services unavailable to the community. The municipality lacked sufficient personnel and technological resources to respond effectively to the incident. Specifically, the municipality lacked 24/7 continuous monitoring of its IT environment which limited its ability to detect and respond to the attack in a timely manner. In addition, incomplete logging mechanisms and limited log retention cycles hindered its capacity to identify, analyze, and respond to the incident.

Solution

To respond to the incident, through its cyber insurance provider and legal counsel, the municipality engaged KPMG's multi-disciplined cyber incident response team. KPMG provided a full range of services, including incident containment, investigation, recovery support, and 24/7 continuous monitoring services. KPMG mobilized quickly, establishing clear communication with the municipality to assess the situation and prioritize breach containment activities.

Using advanced security tools, KPMG conducted an in-depth investigation of the municipality's IT environment to understand the activities performed by the threat actor. Regular status updates clarified the attack's scope and impact. In addition, KPMG analyzed the municipality's operational technology environment to ensure a complete understanding of the incident, while also deploying appropriate containment activities.

In parallel, KPMG assisted the municipality with recovering critical systems by restoring from available back-ups and providing recommendations to mature the municipality's cyber security controls and technology stack. KPMG also provided support for rebuilding telephony systems that had become inoperable due to the attack.

The Outcome

With KPMG's support, the municipality successfully contained the incident and restored critical services. A strategic roadmap was developed to enhance its cybersecurity posture, encompassing targeted recommendations across technology, processes, and personnel management.

KPMG played an important role in helping the municipality not only recover from the ransomware incident but also strengthen its defenses against potential future cyber threats. KPMG collaborated with the municipality to implement 24/7 continuous monitoring and to provide penetration testing services, both important components for proactive threat detection and resilience.

In addition to reinforcing internal security measures, KPMG enhanced third-party risk management by conducting detailed assessments of the municipality's reliance on external applications and infrastructure. This was important for identifying and mitigating risks associated with third-party services.

To learn more about our Cyber Incident Response services and how we can help your organization, click here: Cyber response - KPMG Canada.

If you have experienced or have a question about a cyber incident, contact our team of incident response specialists email us at cyberincident@kpmg.ca or call our Toll-free telephone number: 1-844-576-4911

Contact us

Our dedicated team is here to support your organization's unique needs.

Alexander Rau

Partner, Advisory Services - Cybersecurity
KPMG in Canada
+1 416-777-3450
alexanderrau@kpmg.ca

Guillaume Clément

Partner, Advisory, Cybersecurity
KPMG in Canada
+1 418-653-5335
guillaumeclement@kpmg.ca