CASE STUDY

Ransomware (Large Municipality): INVESTIGATE, REMEDIATE, AND PROACTIVELY PROTECT

AT A GLANCE

A large U.S. city is struck by ransomware; after nearly two days of trying to resolve it with their own staff, they realized they needed a leader. They called in the Crypsis experts to help them remediate, respond, recover, and proactively protect for the future.

CLIENT CHALLENGE

A large city government was brought to a standstill by ransomware. The Crypsis Group and other forensic firms were hired to help the city respond, remediate, and recover. The city tasked Crypsis with leading the forensic investigation effort to ensure they could restore municipal services and protect citizen data as quickly as possible. Additionally, the city turned to Crypsis to provide strategic advice as they developed a plan to better protect itself.

CRYPSIS SOLUTION

For a city government, quickly restoring access to networks, systems, and applications is critical — citizens depend heavily on municipal services to conduct city business. After responding to the attack for almost two days, the city's office of the CISO realized they needed more expertise quickly. A Crypsis team of experts was brought in to lead and direct all investigative efforts and provide expert guidance to the city's CIO on ransomware response, remediation, and recovery. The Crypsis team worked quickly, directing investigative teams on which avenues to pursue and where to invest their efforts, while helping the city CIO determine how to best leverage city IT teams to remediate, recover, and implement solutions to stop new attacks before they could be realized.

The forensic investigators determined that several thousand systems were compromised by the ransomware. The Crypsis team developed a plan and processes for cleaning, replacing, and/or restoring these systems from backup as expeditiously as possible. In parallel, they investigated whether the malicious actor conducted any other detrimental activities in the network beyond the ransomware. As the investigation was concluding, Crypsis experts assisted the city in developing a plan to build their defenses, enhancing their ability to respond to future ransomware attacks. The plan was approved by the city and implementation began immediately.

The Crypsis team took protecting the city one step farther: They identified that the city's current governance policies were not sufficient to protect the city, and, working with the Office of the CISO, proposed an enhancement project that would greatly improve these policies to better align with security best practices and industry standards. Crypsis was selected to conduct this enhanced scope of work.

RESULT

Because of Crypsis' leadership, this municipality was able to get critical systems and applications back online, recover from the ransomware attack, and devise a strategy to better protect the city from future ransomware attacks. The team coordinated multiple investigative efforts into one cohesive strategy to achieve a more efficient result. The Crypsis experts identified governance policy gaps and worked with the city to create and implement policies based on best practices and industry standards, with the goal of better protecting municipal services and citizen data in the future.

The Crypsis Group provides the highest-quality incident response, risk management, and digital forensic services to over 1,700 organizations globally. To learn how we can help your organization, visit www.crypsisgroup.com.