Municipalities vs. Ransomware Attacks - Who's Winning?

01/28/2020

Ransomware attacks on municipalities were on the rise in 2019, with two-thirds of known ransomware attacks in the United States targeting governments, and the trend is expected to continue for 2020.

It is important for city governments to be vigilant in regards to their cybersecurity, regardless of the city's size. Recent attacks show that city population size does not necessarily correlate with demand. For example, in response to an attack Lake City, Florida paid a ransom in the amount of $460,000. The city of New Bedford, Massachusetts, although it ultimately did not pay, also experienced a similar ransom demand in the amount of $5.3 million. Lake City has a population of approximately 12,000 and New Bedford has approximately 95,000 residents. Compared to 2018's $52,000 ransomware demand on the city of Atlanta, it is easy to see that city size does not provide much comfort or protection against cyber threats.

Another complication trending in the area of ransomware attacks is the publication of victims that have been hacked and have yet to pay the ransom demand on public website. Attackers add pressure to the situation by threatening to publish the compromised data or actually publishing further information in the interim, such as the attack dates, number of files stolen, IP addresses and machine names of servers infected.

Why are municipalities easy targets for ransomware attacks? In short, because they are ill-prepared to defend themselves. Small and medium-sized cities do not have the resources or funds they need to invest in IT security. Cities also struggle to keep the pace with technology. For example, refresh cycles may not be timely because of the required continuity of their services for its citizens or new IP-based delivery activities are implemented on aging computer systems. Additionally, municipalities deal with fractured organizational structure and public-sector bureaucracy, which lead to slower deployment of security measures.

Attackers also bet on municipalities paying a ransom to resolve an operational crisis as quickly as possible, given the nature of their business. Many security firms and law enforcement may discourage this course of action because there is no guarantee of receiving a decryption key once a ransom is paid. Paying ransoms also increases the likelihood an organization will experience a second attack once an attacker knows a victim is willing to pay. Generally, conceding to demands encourages continued "bad behavior" and leads to more attacks, higher ransom demands and repeated strikes.

However, there are some tactics cities can employ to mitigate and prevent these attacks:

Create a Security Strategy. A security strategy should be ahead of all city activities. New attacks are emerging everyday, so it is important that this strategy addresses more than reactive approaches to trending attacks. It is also imperative that this strategy is enterprise wide – not just for IT. A cohesive

approach is important in a landscape where its victims often work in silos. Finally, a strategy needs to be not only defined but also efficiently implemented. Once a strategy is in place, a city's workforce should be trained and tested to ensure successful results in a worst case scenario. Employee training can't be stressed enough!

Develop Cohesive Relationships. As cybercriminals often count on the interconnectedness of local governments and the threat of political embarrassment, it is key to have pre-existing relationship with outside resources that can assist in the event of a ransomware attack. More and more local governments are working with the states and emergency management offices to create an orderly process for addressing a ransomware attack. It can also be helpful to have formal or even informal information sharing practices amongst peer cities and government agencies.

Build a Continuity Plan. As part of an organization's security strategy, municipalities should give consideration to its business continuity and disaster recovery plan. In focusing on disaster recovery, it is important to understand the difference between disaster recovery and backup – and that the two are not mutually exclusive. Disaster recovery is the ability to run a workload in a different location so that the workload will remain online and available in the event of a disaster. Backups are point in time copies used to restore data or machines to its previous state. In analyzing a BCDR plan, it may be prudent to have both disaster recovery and backup components as part of that plan. Another consideration is whether to invest in cybersecurity or business interruption insurance. In evaluating insurance, a municipality should determine: which devices, files and users are covered under the policy; whether ransom demands are included in the coverage and whether the amount of coverage is sufficient to tackle a worst-case scenario.

Ransomware attacks are expected to continue to rise, so it is important for municipalities to remain diligent in safeguarding their assets. Municipalities can be prepared by having a strategic plan and following through with a training program to reduce the risk presented by these attacks.