Prescient Solutions

Ransomware Attacks on Municipalities

Ransomware Attacks on Municipalities

- Ransomware is an increasing problem for municipalities, including small ones.
- There have been at least 170 ransomware attacks on state, county, or city governments since 2013.
- Of 70 attacks during the first half of 2019, more than two-thirds targeted cities.
- Small municipalities are frequent targets due to lack of strong cybersecurity defenses.
- Attacks target schools, libraries, airports, courts, and other municipal facilities.
- Recovery can take weeks and be costly.
- Some recent attacks:

Date	Location	Impact	Resolution
09/2019	Orange County, NY	Delayed first day of school.	Unknown.
08/2019	Two school districts in Long Island, NY	Student and staff information unavailable.	One district restored from clean backup. One district paid $88,000 ransom.
08/2019	22 municipalities in Texas	Unable to accept payments, issue birth/death certificates, perform other functions.	Unknown.
05/2019	Baltimore, MD	Systems including email down. Unable to perform functions including property transfers and sending out water bills.	More than a month and more than $18 million to recover.
04/2019	Cleveland, OH	Airport flight and baggage info screens could not display data.	Additional staff required for two weeks to perform manual operations.
04/2019	Augusta, ME	City Center shut down for several days.	Systems rebuilt from scratch. Costs include overtime and additional software licenses.
03/2019	Albany, NY	Police unable to access crime reports or schedules; City Hall unable to generate birth certificates, marriage licenses, and other documents.	More than a week for full recovery.

Ransomware Explained

- Ransomware is a type of malware.
- Like other malware, gains access through phishing, exploit kits, and malvertising.
- Unlike malware that steals data, malware encrypts data and makes it unreadable.
- Some ransomware can spread through network to connected drives and other servers.
- Requires bitcoin or other untraceable cybercurrency ransom for decryption key.
- If ransom isn't paid by deadline, ransom amount may increase; eventually, the encryption key is thrown away and data becomes unrecoverable.

Blocking the Ransomware Threat

- Defending against ransomware is like defending against any other kind of malware.
- Develop a strong cybersecurity strategy including antivirus, firewall, and other tools.
- Keep patches up to date to close known vulnerabilities.
- Train employees to recognize phishing attempts and use other safe computing practices.
- Scan email for known malware to prevent it from reaching employees.
- Restrict privileged access and limit employees' ability to install programs.
- Use application whitelisting to block ransomware from executing.

Recovering from Ransomware

- No defense is 100% effective, so you need a plan for recovering from an attack.
- As soon as you recognize an attack, disconnect infected systems and disable Wi-Fi and Bluetooth to keep it from spreading.
- Should you pay the ransom? This may be cheaper than other recovery strategies, but is not recommended. There is no guarantee you'll receive the key, you encourage hackers to attack others, and you may be victimized again.
- Identify the specific ransomware that attacked you. Some variants have known solutions to decrypt data and recover.
- In most cases, you will need to restore from a good backup before the ransomware hit.
- **Your disaster recovery strategy applies!**

1515 Woodfield Rd, Suite 880, Schaumburg, IL 60173
141 W. Jackson Blvd, Suite 3850, Chicago, IL 60604

Phone: (847) 240-3900
Phone: (888) 343-6040

www.PrescientSolutions.com