emazzanti technologies
TECHNOLOGY STRATEGIES FOR BUSINESS GROWTH.

Cyber Security in Municipalities, Is Your City Safe and Secure in 2024?

In January 2023, a ransomware attack hit the Royal Mail in the UK, disrupting international mail operations for several days. As a result, the agency suffered a significant decline in revenue and a serious reputation hit. The attack highlights the cyber risks faced by public agencies and the need for improved cyber security in municipalities.

Local Governments a Target

Municipalities represent a particularly attractive target for threat actors for several reasons. In the first place, local governments store large amounts of valuable information, from driver's license numbers and credit card data to medical information. Hackers, including nation-state threat actors, can sell this information or hold it for ransom.

Secondly, research shows that many local governments lack the funding and staff to build adequate defenses against cyber attack. They often run on antiquated systems, with outdated cyber security technologies and practices. Cyber criminals know this perhaps better than the agencies themselves.

Thirdly, the same connected technologies that allow governments to streamline services and improve quality of life also greatly expand the attack surface. Smart cities operate on tightly integrated systems with thousands of IoT devices. Each device represents a possible entry point for threat actors seeking to acquire data or disrupt critical operations.

Top Security Challenges Facing Municipalities

Municipalities deal with the same cyber threats as other organizations, from ransomware and DDoS attacks to phishing and supply chain attacks. In addition, they face some challenges unique to the public sector.

For instance, while the cyber security workforce shortage affects everyone, the problem proves particularly acute for local governments. With limited budgets, they often find it difficult to compete with the private sector when trying to attract and retain cyber security talent.

In addition, municipalities control critical infrastructure, from electricity to transportation, communications, and water. A breach in one area can have far-reaching implications, even beyond the government offices. Consider the damage a threat actor could inflict by shutting down the electrical grid or interrupting traffic patterns.

For smart cities, the challenges extend even further. The complex systems involved depend on a vast network of interconnected IoT devices. Protecting and monitoring those devices requires automation, which can introduce additional vulnerabilities. Once attackers breach one endpoint, they can potentially move laterally through the network.

Best Practices for Cyber Security in Municipalities

To protect critical data and infrastructure and minimize the damage when attacks occur, local governments should implement key cyber security practices. Best practices include:

- Cyber security risk assessment – Cyber security risk assessments involve evaluating the organization's security systems and practices to identify vulnerabilities. Use the risk assessment to update the agency's cyber security strategy.
- Zero-trust architecture – Zero trust means verifying every request to access the system. It also involves using the principle of least privilege, granting only the minimum access necessary to complete the task at hand.

- Network segmentation – By dividing the network into smaller segments based on risk levels or business needs, organizations limit the exposure of critical assets. Segmentation also reduces the impact of a security breach by preventing attackers from moving laterally through the network.
- Security training for all employees – Human error plays a significant role in the vast majority of security breaches. Regular, engaging security awareness training, targeted to specific job roles, can help.
- Robust backup and recovery strategy – Backups enable organizations to navigate cyber threats and prevent data loss more smoothly. An effective backup and recovery strategy includes creating multiple copies of essential data, capturing endpoints, automation, and regular testing.
- Patch management – Be sure to apply security patches to software and firmware quickly to close vulnerabilities. With thousands of devices and applications, this can prove tricky. Automation will help. With legacy systems, segmentation and limiting connectivity may prove necessary.
- Continuous monitoring – Security monitoring provides alerts to suspicious activity and unsecured devices, giving early warning of potential attacks or vulnerabilities.

Enlist Expert Help

The municipal cyber security experts at eMazzanti Technologies understand the unique cyber security challenges local governments face. They also understand the budget pressures for improved efficiency and cost reduction. Our consultants will help tailor a security strategy to each agency’s budget and specific needs.