Recent Cyber Attacks Highlight Need for Municipal Data Governance and Security

This year has seen a rise in cyber attacks on government agencies and prompted official warnings. Notably, a recent joint statement from the FBI and CISA warned schools about probable attacks. And a data breach of federal court records further spotlighted the need for improved municipal data governance and security.

A perfect storm of cyber security risks makes municipal agencies particularly vulnerable to attack. In the first place, schools, courts, utility departments and other government entities store a treasure trove of sensitive information. Those same agencies often use legacy systems and lack critical cyber security infrastructure and data governance resources.

To counter the threat of cyber attacks and maintain public trust, agencies must implement municipal data governance and cyber security best practices. In its detailed joint statement to schools, the FBI and CISA highlighted several key actions to take, including those listed below.

Review and Update Incident Response Plans

A detailed incident response plan forms a critical component of the organization's ability to minimize exposure and risk. It includes immediate steps to take to contain the spread of infection, eradicate malicious code and ensure business continuity. The response plan also outlines a specific plan for internal and external communications.

Strengthen Backup Policies

Regular, reliable data backups provide an essential component of cyber security readiness. CISA emphasizes the need for agencies to ensure that regular backups include the data infrastructure of the entire organization. Backups should be tested regularly and encrypted, and the organization should maintain a copy of the backup offline.

Monitor Supply Chain Security

Time and time again, attackers have gained access to lucrative targets by first infiltrating a third party. For example, the California Department of Motor Vehicles suffered a ransomware attack last year that exposed thousands of driver and vehicle records. The attack began when hackers first breached a billing services company that contracted with the DMV.

Agencies should make it a policy to regularly review the security practices of third-party vendors. They should also monitor all external remote connections, including those with vendors, addressing any suspicious activity.

Strengthen Authentication and Access Management Practices

Bad actors commonly infiltrate their targets by compromising credentials to gain access to the network. Consequently, a critical element of cyber security includes addressing identity and access management. Begin with strengthening password policies and adopting multi-factor authentication (MFA) where possible.

Additionally, pay special attention to accounts with administrative privileges. Implementing risk-based authentication and zero trust policies helps to ensure that hackers cannot easily gain access to sensitive data and services.

Improve Patch Management

A critical, and too often overlooked, element of effective cyber security strategies involves patch management. Implement a plan to ensure that all software, firmware, and operating systems stay up to date. This includes installing and updating antivirus programs on all devices.

Improve Email Security

Because email remains a top attack vector, organizations must make email security a priority. This includes implementing high-quality email filters and properly configuring email services. CISA also recommends disabling hyperlinks in incoming emails and adding an email banner to alert users to external emails.

Cyber Security Grant Program to Assist Agencies with Municipal Data Governance and Security

Responding to increased cyber threats on government agencies, the recent Bipartisan Infrastructure Law includes a cyber security grant program for state and local governments. The program provides for $1 billion to help governments develop and implement cyber security strategies.

To qualify for the grant program, state and local governments must produce comprehensive cyber security plans. For agencies that lack sufficient security expertise, this requirement can prove daunting. The municipal data governance and security experts at Messaging Architects can help.