Cybersecurity Challenges for State and Local Governments

State and local governments face unique challenges when it comes to cybersecurity. These organizations maintain and operate many of the most fundamental infrastructures, forming the foundation of a peaceful, productive society. Simultaneously, these organizations deal with rules and regulations at state and local levels, as well as Federal regulations and requirements. Securing all of this infrastructure against cyber attacks is typically the responsibility of understaffed, underfunded and stretched cybersecurity teams.

Meanwhile, the landscape for cyber threats increases every year with the adoption of technology into all aspects of life. Some of the most difficult areas to defend against these cyber threats exist at the state and local levels. These organizations are responsible for a host of critical infrastructures and essential services, such as:

- Energy
- Transportation
- Water systems
- Gas
- Electric
- Emergency services
- Law enforcement
- Public Health
- Education
- Elections

While the importance of these systems and services is self-evident, state and local governments are often accustomed to operating independently of one another and employing the use of different technologies (many of which may be outdated). This particular set of challenges provides an ideal target for threat actors who are both able and willing to carry out attacks that have the potential to harm thousands.

Threat Intelligence and Collaboration

Much of threat actors' success is due to their collaboration with one another. Malicious cyber actors frequently share tools and techniques, increasing their agility and precision in circumventing defenses. Adversaries then reuse these shared techniques because their targets are reluctant to share sensitive threat information that would prevent this. Collaboration is critical to defending against such tactics.

The most common place to begin collaboration is to share details about observed attacks and include any relevant investigation or analysis performed. This type of information is known as threat intelligence, which may be as tactical as providing file hashes, domains and IPs or as strategic as actor motivations and behaviors. Applying this context to internal security events can provide organizations with a means to more proactively defend against the threats that are relevant to their environment.

Sharing this information with peers offers significant benefits to both the sharing organization and the recipients. For example, collaboration brings multiple perspectives to bear on a specific threat. Not all groups have the same selection of security and monitoring tools in place. These different points of view can lead to stronger overall analysis. In addition, having a broad set of analysts with differing skills and expertise examining an attack leads to better overall knowledge of actors, campaigns, tools, attack patterns, and the like. The result for organizations is

© 2021 Anomali, Inc. All rights reserved.

a well-informed defensive posture against known and even suspected threats.

In light of such benefits, organizations have banded together to create formal threat sharing communities, often aligned within their own industry, known as Information Sharing and Analysis Centers (ISACs). State and local governments are beginning to develop and rely on their own sharing communities to exchange information for the benefit of public security as well.

Anomali ThreatStream is the leading global threat sharing platform for ISACs, ISAOs, industry groups, holding companies, and other threat intel sharing communities seeking to power secure collaboration.

Benefits for Anomali threat intel sharing community partners include:

- A branded threat sharing community portal
- A dedicated "Trusted Circle" on the Anomali platform
- Admin access to help screen and manage memberships
- A STIX/TAXII server for programmatic access
- Anomali licenses for community members
- Community training, education, and support

Use Case – Elections

Attacks against elections-related systems are no longer a passing concern but rather a reality for governments at the local, state, and federal level. Each state and jurisdiction is responsible for operating and certifying their own elections. It is incumbent upon each state to stay vigilant to any attacks that threaten the integrity of elections and voting processes or results.

As an example, one election jurisdiction may discover that their elections infrastructure or a particular model of voting equipment is being targeted by hackers or susceptible to a specific vulnerability. This information is extremely relevant to other elections commissions within the state or in any other state that may use similar infrastructure. This type of threat intelligence needs to be shared quickly and with as much context as possible, allowing the community at large to benefit from it. As further discussions between governing bodies take place, elections would become less susceptible to manipulation or direct attack. This is particularly true as capabilities are extended across governing levels (i.e., local, state, federal) and across state lines to provide equal and immediate participation for all members.

Use Case – Police, Fire, and Emergency Management Services

Police, Fire, and Emergency Management Services (EMS) are critical functions in both daily life and times of disaster. Each of these can have local and overlapping jurisdictions, and may also receive support from larger governments in times of need. These departments typically do not have budgets dedicated to cybersecurity.

Chicago's Cook County Department of Homeland Security and Emergency Management (DHSEM) began building a county-wide ISAC in 2016. DHSEM's mandate was to support the whole county, meaning they frequently provided backup to local police and fire districts. They also housed the Information Security Office, subsequently leading them to establish the The Cook County Cyber Threat Intelligence Grid (CCCTIG) to provide information security support at the local level. There are many possible applications of such a system, such as if Cook County learned of a cyber-attack on a water treatment plant that could lead to drinking water contamination across the region. They could then quickly and efficiently inform police, fire, and EMS to prepare and pool resources. This would also serve as an opportunity to prevent further attacks on other local facilities.

© 2021 Anomali, Inc. All rights reserved.