elastic

How State and Local Agencies Stay Ahead of Cyber Attacks

State and local government networks continue to be pummeled by digital assaults, including damaging ransomware attacks that can yank public websites offline, reap financial havoc and even sever essential lines of service between states and their citizens.

Some state and local agencies have evolved their cybersecurity postures but others, facing budget and logistical challenges, struggle to keep up with the furious pace of threats.

During a recent roundtable "Holding Data Hostage," IT decision-makers and experts explored recent developments in the space, sharing trends and insight for improving agencies' cybersecurity postures. The roundtable was hosted by Elastic, the company that builds real-time, scalable enterprise search, observability, and security solutions on a single free and open technology stack that can be deployed anywhere.

Focus on Full Visibility

Internal IT talent and expertise at the state and local level is more critical than ever — but glaring shortages across the public sector persist. That's one of the main takeaways of a recent survey of state and local IT decision-makers from the Government Business Council and Elastic.

Many state and local organizations are turning to managed service providers to fill the gaps in IT workforces, but agencies can face challenges when they outsource too many of their operations and don't retain enough visibility into the operations of their third-party partners. Alternatively, adding new data sources with an existing security solution to achieve full visibility can be costly, which is a challenge as budgets and resources shrink.

"The problem is that a lot of these state and local agencies are not getting a 360-degree view or holistic view of all of their data and all of their data traffic and all

their networking," says Jared Pane, a principal solutions architect for state and local government at Elastic. "In other words, it's hard to manage — let alone secure — what you can't measure."

The focus placed on improving visibility into your infrastructure, network and workforce has never been greater, especially with the steep increase in remote workers during the COVID-19 pandemic.

"People are the biggest problem. … How many cities have been hammered by ransomware? And that really just scares us very much. I think our organization has gotten better. I wouldn't say we're invulnerable. Nobody's invulnerable. I think we made improvements but you're always one person away from causing a disaster, and I think that's what keeps everybody up at night and why my hair is so white."

Bill McLeod | *mayor of Hoffman Estates, Illinois, a Chicago suburb*

15%

of state & local decision-makers say their agencies have comprehensive visibility into their attack surfaces

34%

say they have moderate confidence

18%

say they have limited to no visibility

32%

said they didn't know or weren't aware

"Organizations have invested a great deal of time and energy into making the perimeter of their networks hardened," says Jamie Butler, the lead security engineer for Elastic. "This has meant an ever-greater focus on intrusion-detection systems and strong firewalls."

The issue, says Butler, is that an environment where a large number of state and local government workers are logging on from home "scrambles" the traditional models.

"You're no longer within that network; you might no longer have a perimeter, or in the best case the perimeter became a lot more porous. In the worst case, your perimeter just became your employees' home WiFi," Butler adds. "Because MSSPs are usually in a highly privileged position in their customers' environments, some have been targeted by ransomware actors. To help provide visibility to things such as logins, organizations can use Elastic Beats to have better situational awareness across their environment."

Even with an MSP approach, it's important for agencies to maintain situational awareness of their networks. Agencies are awash in data, including threat data. But there are event-management tools and automated logging tools and dashboards, such as those offered by Elastic, that help agencies keep track of the critical data and provide a real-time look at the state of their networks and IT infrastructures.

Such tools are essential to creating a smoothly running and effective security operations center or a security information and event management solution.

See Value Before Making an Investment

It's no secret state and local agencies face budget constraints that make implementing new approaches challenging.

But effective leaders can push for investments that need to be made to shore up agencies' security posture.

"I think one of the most essential things is for IT folks to learn to 'speak mission.' Not IT, but mission," says Ron Sanders, the staff director for the Florida Center for Cybersecurity. "They need to be able to present the mission case for the investments in ways that senior leaders and their peers in public works and public safety ...understand."

Starting with an open source solution is one way to see and be able to communicate value before making a significant investment. Solutions like Elastic Security offer a completely free option to get started and start seeing value right away. "It's a low-risk platform for building a production system, proving that it works to desired specifications, and getting from data to insight quickly. Once the project has been validated, agencies then have the option to deepen the investment in the platform, cloud, or additional solutions to get to mission success even faster," said Pane.

>> Learn more at elastic.co/