FEDInsider

State and Local Governments Tackle Evolving Cyber Threats

Agencies are relying on advanced tools, federal collaboration and security tactics to thwart, detect and respond to threats

Cyberattacks are getting more sophisticated and frequent, particularly impacting state and local governments with fewer resources for security. According to a Sophos research report, more than 50% of state and local governments faced ransomware attacks in 2021 and only one in five organizations were able to stop them.

To discuss how to combat cyber threats in government, members of government and industry recently spoke in a series of panels at FedInsider's live event, CyberSmart 2023: Combating Cyber Crime in Austin, Texas, on June 8.

Evolving Tech & Evolving Threats

Nation-state actors, the rise of artificial intelligence and ransomware continue to pose cyber risks – and ransomware groups are taking their tactics to new levels. Jeremy Wilson, deputy chief information security officer for the Texas Department of Information Resources, said he's seeing global ransomware groups like LockBit threaten double or triple extortion, launch distributed denial-of-service (DDOS) attacks and even leak mock data to try and trigger a response.

Texas is responding to those threats with both designated state teams and help from nationwide partners. "One of the things I'm proud about is our Department of Information Resources cybersecurity response team," he said. "Through them, we have added a dark web and deep threat analysts capacity. And we also now get great threat intelligence from the FBI, CISA, the Department of Homeland Security and other incident response partners."

With the rise of remote work and remote access to services, endpoints and the pace at which they're being added are also posing challenges for security. For the city of Austin, Texas, overcoming these complexities is done with a concentrated effort centered around partnerships, a zero trust strategy and a continuous detection program loaded with proper threat intelligence.

"Zero trust bias gets baked into everything," said Bart Lauwers, security operations manager for the city of Austin. "Let's not connect anything that we don't need. And if something is connected, it has to be secured. For us, zero trust is a whole philosophy, and it's proved highly effective to keep things secure."

Collecting only what is needed is critical to keeping citizen and client data safe, especially as data is requested to access online services. "When you are developing technology software, you need to make sure that you are only taking what you need," said Tony Lauro, director of security strategies at Akamai Technologies. "Developers have a tendency to take everything and sort it out later. But that is not a good policy when it comes to data collection, and it is certainly not a good policy when it comes to privacy and citizen rights."

Power in Numbers

State and local governments are increasingly relying on collaboration and federal funding to help address cybersecurity needs. For ex-

Featured Experts:

- Bart Lauwers
  Security Operations Manager, City of Austin
- Jeremy Wilson
  Deputy CISO, Security Ops., TX Dept., Information Resources
- Tony Lauro
  Director of Security Strategies, Akamai Technologies
- Gayle Combs
  Cybersecurity Advisor, CISA – Region 6, Arkansas
- Tim Roemer
  President & General Manager, Public Sector, ThriveDx
- Brian Osterman
  Solutions Engineer, Recorded Future
- Mario Chavez
  Chief Information Security Officer, Texas Dept. of Insurance
- Anil Koindala
  Chief Security Officer, IT Service, Texas Railroad Commission
- David Morgan
  IS Security Manager, Texas Dept. of Public Safety
- Skylar Barnes
  Solutions Engineer, Okta
- Fadi Fadhil
  Field CTO, Palo Alto Networks

ample, the Infrastructure Investment and Jobs Act of 2021 established the State and Local Cybersecurity Grant Program, which appropriated $1 billion in awards over four years.

These efforts are needed to help address the rapidly accelerating rise of well-funded threat actors equipped with new tools, training and methodologies. There's also been an increase in attacks made against supply chains and those which employ phishing and well-designed social engineering campaigns. In addition to all that, the number of state-sponsored threat actor groups that can attack with the explicit permission of their government is increasing.

State and local agencies need advanced detection tools and better methodologies to prevent those kinds of advanced attacks coming from highly-skilled adversaries. "Part of that defense will involve a heavy emphasis on machine learning and AI," said Brian Osterman, solutions engineer at Recorded Future. "With AI and machine learning, we can have a machine that goes through all that data and identify all the relationships regarding how everything is connected." Doing that can uncover even the most advanced or subtle threats that attackers try and hide.

Funds should also go towards cybersecurity training. "The worst thing you can do is throw money at the problem, because you end up throwing a bunch of it away on advanced tools," said Tim Roemer, president and general manager of public sector at ThriveDx. "Unless somebody is highly trained at how to use those advanced tools, they don't do any good and most organizations can't properly use them."

Agencies can also turn to CISA for a host of additional no-cost resources and services. "Cybersecurity is a collective effort and it matters to all of us," said Gayle Combs, cybersecurity advisor for CISA – Region 6, Arkansas. "We are only as strong as our weakest leg…and when we talk about critical infrastructure, we are talking about that part of the infrastructure that impacts all of us." That is why CISA strives to help other agencies and government organizations with a variety of free cybersecurity programs.

Securing Government Networks

It is imperative that in today's threat environment, agencies provide mission continuity and secure access to a dispersed base of internal and external users. According to Mario Chavez, Texas Department of Insurance CISO, this requires having a good identity and access management strategy, strong fraud detection, clearly defined objectives, strong knowledge of users and assets, and clean data in a distributed user base.

"Refining policies and procedures, defining technology requirements as well as finding the right vendor to partner with are all critical," said Chavez. All of that might be difficult at first, especially if agencies are still running legacy applications, but they shouldn't stop modernizing, he added.

Finding and retaining talent are also critical components to securing government networks. Fadi Fadhil, field chief technology officer at Palo Alto Networks, said considering it's such a competitive market, agencies should foster competition as much as they can.

"We should also be providing some incentives to promote from within, and to provide professional development for workers who are already within an organization," Fadhil said.

Training is key for professional development, talent retention and proper use of security tools. "The Texas Department of Information Resources and the legislature have done a good job by requiring certain criteria, for instance, making sure there are certain governance requirements met, even in contracting," said David Morgan, IS security manager for the Texas Department of Public Safety. "It's not just about getting a new tool, but also making sure that there is adequate training among the staff so that they can effectively use it."

Risk management also plays a critical role in achieving secure yet accessible government services as users are accessing them from all sorts of devices and locations. "For example, NIST provides a risk management framework that details specific things that an agency or municipality can do when taking a look at all of their infrastructure and the systems they have in place," advised Skylar Barnes, solutions engineer at Okta.

And securing access also means securing a web gateway. Anil Koindala, a cybersecurity officer for IT service at the Texas Railroad Commission, said that one way to achieve that would be with a standalone gateway technology which acts as the delegated license service as well as a security-as-a-service component for edge computing devices.

"With that, we can have a common risk indicator based on access controls," Koindala said. "And that is one area which we can definitely improve on." Once that kind of security service platform is fully adopted, organizations will have a single agent that generates unified reports.

But no matter what cybersecurity products or frameworks are employed, ultimately, security for agencies won't ever be found in a one-size-fits-all solution. Instead, Koindala added that customizing the perfect tools for the environment and having tight collaboration efforts across both government and industry will be the key to success.

FEDInsider

Hosky Communications Inc.
3811 Massachusetts Avenue, NW
Washington, DC 20016

(202) 237-0300
Info@FedInsider.com
FedInsider.com
Facebook.com/FedInsiderNews
Linkedin.com/company/FedInsider
@FedInsider

carahsoft.

Carahsoft
11493 Sunset Hills Road, Suite 100
Reston, VA 20190

(703) 871-8548
Info@Carahsoft.com
Carahsoft.com/Akamai
Facebook.com/Carahsoft
Linkedin.com/company/Carahsoft
@Carahsoft