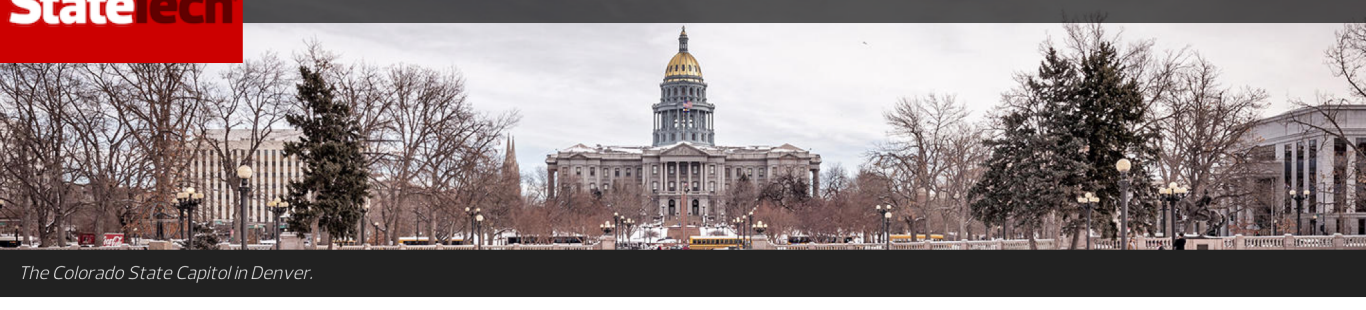


The Colorado State Capitol in Denver.

JAN 04 2019

SECURITY

How Colorado Mounted a Best Defense Against Ransomware

As more hackers target state and local agencies, governments can take measures to plan and defend their systems.

by Erin Brereton

Erin Brereton has written about technology, business and other topics for more than 50 magazines, newspapers and online publications.

In recent years, a number of city and state agencies have experienced damaging ransomware attacks.

In 2014, to protest the police shooting of unarmed 18-year-old Michael Brown, the online activist group Anonymous caused web servers for the city of Ferguson, Mo., to crash. A March 2018 ransomware attack disabled critical software programs used by the city of Atlanta. A month prior, ransomware infected approximately 150 of the Colorado Department of Transportation's servers and 2,000 of its workstations.

The initial CDOT attack — and a second incident in which the malware reactivated a week later — involved SamSam ransomware. This ransomware also was used against more than 200 municipalities, hospitals and other organizations, according to the Justice Department, which in November indicted two men in connection with the extortion scheme.

Due to a combination of previously instituted policies and responsive actions, the Colorado Governor's Office of Information Technology was able to avoid paying the hackers' requested ransom and mitigate much of the potential damage from the attack.

VIDEO: These are the cybersecurity threats that keep state CISOs up at night.

Colorado Was Ready for a Cyberattack

CDOT had segmented its network in recent years as part of the state's Secure Colorado strategic cybersecurity plan — which helped isolate the malware within one department, CDOT's business operations unit, according to OIT Chief Technology Officer David McCurdy.

"These groups' modus operandi is to attack the most critical system they can find and backup system, and spread the malware as much as they can so it makes it impossible for an organization to recover," McCurdy says. "We have a very segmented environment; that's why it didn't spread out to other parts of the system."

Offsite tape storage allowed the agency to restore data after the attack. OIT was also able to quickly mobilize a response team because it had previously created a cyberattack reaction plan.

"We do joint exercises with the National Guard and other cybercommunity members in Colorado, so we had actually been practicing these events for some time," McCurdy says. "A week into it, we reached out to the National Guard, as well as a wide variety of vendors."

The office of emergency management also helped to coordinate activities, and eventually recommended the state's governor declare the event an emergency.

"That made funds available to us, but more than anything, it sent a message to the community, CDOT and our partners that the state was taking this seriously and was going to apply the right amount of resources to get it resolved quickly, but with the most methodical process," McCurdy says.

Ransomware Recovery Can Require Additional Actions

The cost constraints state and local agencies face can mean their systems aren't as well-protected as those of other entities, drawing cybercriminals' interest. But agencies are becoming aware of the growing threat, according to Alison Brooks, research director for smart cities and public safety at IDC.

"Many state and local jurisdictions are just trying to limp along with existing technology investments for as long as they can; that's what structurally makes them vulnerable to attacks," Brooks says. "They used to think they wouldn't be an interesting target for this kind of warfare. Now that there's an increased focus on that, it's causing state and local agencies to up their resources in terms of what they're protecting and how."

There are many things a state or local government can learn after an attack, as well. To protect the state from future infection, CDOT's anti-virus solution vendor obtained a malware sample onsite that allowed it to create a new signature for it. OIT also bumped up its plans to implement a suite of east-west traffic-related security software, and forensics and inspection work was performed on approximately 350 servers and almost 4,500 workstations on the CDOT back office network, including machines that hadn't been impacted.

About 35 percent had some trace of being touched and were subsequently restored, according to Colorado spokesperson Brandi Wildfang Simmons.

From the time the issue was identified to the point where approximately 85 percent of the systems had been restored and normal operations could continue, the entire process took about a month, McCurdy says.

MORE FROM STATETECH: Find out how state CIOs and CISOs can make "bold plays for change" on cybersecurity.

Proactive Measures Help Safeguard Systems

In addition to both offering and measuring the results of cyberawareness training for all employees to reduce the risk of a breach, McCurdy suggests state and city governments review their cybersecurity plans to ensure they include proper network segmentation, inaccessible backup storage and other effective fortification techniques.

"The hard thing to communicate is just how fast the technology is advancing. Hackers are coming out with new tools and types of attacks every day," McCurdy says. "Make sure you have the appropriate layers of security. It's critical to do still do the basic things. Several other organiz[illegible]ere impac[illegible]h more than we were — and that had to do with the nature of their ba[illegible]ps a[illegible]heir ability to recover from the incident."

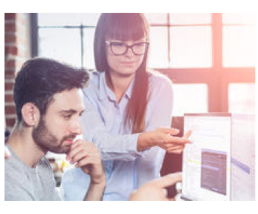
PYGMALIONK/GETTY IMAGES

More On SERVERS ANTI-MALWARE DATA PROTECTION NETWORK ACCESS CONTROL THREAT PREVENTION

Related Articles

Security

States Deem Midterm Election Security Efforts a Success — Mostly



Security

Why Cybersecurity Planning Should Be a Top Priority for Local Agencies

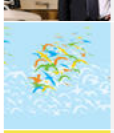
Security

The Network and IT Security Needed to Defend Smart Cities

Latest Articles

How States Benefit From Appointing A Chief Data Officer

Digital Signs Point The Way To A Brighter Future



What Your Agency Needs To Know About Windows 10 Migration

Review: Barracuda Load Balancer 340 Guards Access To Mission Critical Apps

NETWORKING

Risk vs. Reward with Internet of Things Deployments

DATA CENTER

Disaster-Ready State and City IT Systems Weather the Storm