Colorado’s Ransomware Resolution Shows How to Avoid Cyber Catastrophe

Key takeaways include the value of partnerships and the importance of cloud security training.

James Mersol
Mon, 02/24/2020 - 19:47

When one thinks of a statewide emergency, a couple of examples come to mind: a wildfire, a snowstorm or a tornado. Few would think of a ransomware attack on the same level. Since 2018, however, ransomware has been on the rise, leading some state and local governments — including the states of Colorado and Texas and the city of New Orleans — to declare states of emergency after ransomware paralyzed services.
Ransomware is one of the biggest topics discussed at the 2020 RSA Conference during a seminar on emerging threats, as everyone from multinational corporations to local school districts look to reduce their ransomware risk and develop a response plan in the event of an attack.

State of Colorado CISO Deborah Blyth discussed how her office coordinated with the state’s office of emergency management after the Colorado Department of Transportation (CDOT) was hit with SamSam in 2018. The attack affected approximately 1,300 systems and 400 servers, bringing down CDOT’s VOIP phones and disabling the department’s employee and vendor payment systems.

Her office thought they had contained SamSam in a week, Blyth said, but after systems became infected again, she contacted the office of emergency management. The office referred it to the governor, who declared a statewide emergency and called in the national guard’s cyber defense unit to help resolve the issue.

One key takeaway from the incident and the government’s response was the importance of partnerships, including within the state government, with federal agencies such as DHS and FBI, and with vendors. Thanks to their combined effort, they restored most of CDOT’s systems in a matter of weeks, far more quickly than CDOT expected.

While the office of emergency management typically handles natural disasters, Blyth found that some of the same methodologies applied to cyber incident response. The office helped the office of information technology sync its priorities with CDOT, staggering department meetings so that CDOT meetings could include the latest findings from the response teams. They also helped with logistics, developing a schedule for response team members to ensure everyone took some time to recover and also delivering pallets of bottled water to teams who had become so focused on resolving the issue that they had become badly dehydrated.

Following the attack’s resolution, Blyth and her team developed an after-action report to identify the root causes of the attack and how to avoid a repeat attack in the future.
The attackers had gained entry to CDOT’s system through a misconfigured virtual server that used a domain administrator account, giving the server access to far more of the network than it should have. The server had initially been set up for a short testing period, but had never been disconnected from the network.

Misconfiguration is a common security issue that organizations face as they look to accelerate their technological implementation said Tim Woods, vice president of technology alliances at FireMon. In a recent report, FireMon found that nearly 60% of the security professionals surveyed believed security lagged behind cloud migration in their organizations. Woods explained that as more and more stakeholders get involved with security, responsibility on security becomes fragmented. He recommended that development and security teams ensure that everyone knows what part of the organization’s security policy and implementation they are accountable for, so that even something like a virtual server test does not become a serious vulnerability.

Thankfully, Blyth said, CDOT’s network was segmented, preventing SamSam from spreading to other states or to traffic operations, which would have been a literal “life or death” scenario. Additionally, the state had been careful to back up its systems, allowing them to recover essential data.

“We never considered paying,” Blyth said.

Another problem was that the IT team assigned to create CDOT’s cloud environment had no specialized training on how to create a secure cloud system and establish governance controls, underscoring the need for that training amidst the global cybersecurity skills gap.

A potential solution for resolving the skills gap in the short term is to implement automated security processes, Woods said. Automation doesn’t need to be high-level AI or machine learning, he said, but “simple automation for repetitive mundane tasks,” allowing security teams to devote their resources toward developing risk-based security assessments and eliminating legacy measures and access controls from security policy.
Blyth recommended that every organization concerned with ransomware builds information sharing and response partnerships as soon as they can before ransomware hits. She also recommended that security offices develop prioritized plans as well as a “business case” for additional security funding if needed. Her office used the after-action report to successfully lobby the Colorado state government to appropriate $11.8 million to address known risks as quickly as possible, ultimately doubling its annual cybersecurity budget.

The most important takeaway Blyth found from the attack was the importance of implementing security controls faster.

“If they had attacked a week later, they wouldn’t have been able to get in,” Blyth said.

Since the attack, the State of Colorado has implemented stronger controls around privileged access and developed greater visibility into its systems. About a year later, Blyth noted, her team identified ransomware that had entered the network — but was unable to execute, thanks to the new controls.