rubrik

South Louisiana Community College Recovers Before Receiving a Ransom Note

SLCC
SOUTH LOUISIANA COMMUNITY COLLEGE

INDUSTRY

Education

CHALLENGES

- Ransomware attack initiated through a forgotten desktop
- Hundreds of servers and virtual machines encrypted
- Infected servers attempting to attack other servers

RESULTS

- Zero data lost
- $0 paid in ransom
- 100% recovery within 2 hours

Nick Pitre, Director of IT at South Louisiana Community College (SLCC) had a funny feeling something was brewing. The Ryuk ransomware variant had been making its rounds at colleges and universities, so he knew it would not be long before SLCC was also targeted.

Sadly, he was right. "I noticed odd behavior when my team was not able to log in. Our servers were being encrypted," Pitre recalled. The infiltration occurred by way of an administrator loading new software onto a forgotten Windows 7 desktop collecting dust in a closet. Without proper security measures, the admin's credentials were captured, and the ransomware immediately activated and began, spreading to a handful of servers.

But when the attack hit, Pitre was ready—so ready that the hackers never even had the opportunity to deliver a ransom demand. As soon as the ransomware started encrypting files, Pitre's team quickly responded by recovering data from backups stored in Rubrik and preventing any damage from taking place.

PREPAREDNESS PAYS OFF

The reason SLCC was able to avert disaster came down to preparedness. The school received a suggestion from the State of Louisiana to turn off backups because previous attacks had compromised backups, but Pitre overruled, "We're not doing that. I trust Rubrik's immutability." Turns out it was the right move. Rubrik thwarted the ransomware from doing any damage at all.

"Each recovery took five to 10 minutes. In two hours, the situation was 100% contained, which I was pleasantly impressed by," said Pitre.

Where the ransomware was able to infiltrate the network's defenses, Rubrik's Live Mount point-in-time recovery helped identify the risk of reinfection if wrong snapshots were used for recovery.

RUBRIK RECOVERED SLCC IN 2 HOURS

This breach could have led to loss of learning coursework, financial and student records. "Without Rubrik backups, recovery could have taken weeks, which is exactly what happened to another college in Louisiana." Pitre remarked, "They were completely out of luck and had to spend a few weeks recovering."

Using Rubrik, Pitre said, "There was no data loss. Thanks to Rubrik's immutable backups, this breach was simply an inconvenience for the two hours that we were rebooting backups."

"I told everyone within our college system that Rubrik saved us big time. They were all evaluating other backup vendors, which resulted in five different community colleges within Louisiana trusting Rubrik to increase their security and protection against cyber threats."

"Since the ransomware incident, we have doubled down on Rubrik, purchasing a second set in another data center to ensure every server we are backing up is being backed up in two locations."

MORE FROM THE IT DIRECTOR

- **Zero data lost**: "We walked away unscathed, with zero data lost thanks to Rubrik's immutable backups. That was a big factor—not having to worry about our backups getting taken over."
- **$0 paid in ransom**: "From the time we realized there had been an incident, it took just two hours to bring all affected VMs back up and running. We caught it so early on that the hackers never even had a chance to deliver a ransom note."
- **Nightmare averted**: "Ransomware never reached our Active Directory (AD). If the attackers had gotten on our AD, it would have been a nightmare."
- **Ease of use**: "The initial reason I liked Rubrik so much was the ease of use. I never even felt the need to call Rubrik support during the attack because we had the recovery under control, which speaks to its simplicity."
- **Reliable support**: "Support has always been incredible when I have called them. I often go months without having to speak to support because Rubrik is so reliable, truly a 'set it and forget it' product."

South Louisiana Community College, in Lafayette, Louisiana, currently offers more than 50 programs, leading to associate degrees, technical diplomas, and certificates, to 10,000 students annually. The College also offers a wide range of non-credit instruction and training. For more information visit solacc.edu.

rubrik

Global HQ
3495 Deer Creek Road
Palo Alto, CA 94304
United States

1-844-4RUBRIK
inquiries@rubrik.com
www.rubrik.com

cs-slcc / 20220306