Case Study

Alamy

STORAGE > DISASTER RECOVERY AND BUSINESS CONTINUITY

How New Orleans Transformed Its Data Storage System After Cyberattack

A ransomware attack spurred the city of New Orleans to overhaul its data storage system. Learn about the project, which involved Pure Storage and Veeam technology.

Karen D. Schwartz | Jan 17, 2023

Hurricanes, tropical cyclones, floods – New Orleans has been through it all. With a history of natural disasters, city officials know they must batten down the hatches, both physically and digitally, to keep services running. Because of these realities, the city has long taken storage, backup, and disaster recovery seriously.

As far back as 2010, the city of New Orleans has worked on refining its data strategy. At that time, the city's data storage system was mostly disk-based, with active data housed on 3PAR disk arrays and older data housed on IBM SANs. The city kept all its resources in one of its data centers.

Related: Kitselas First Nation Improves Backup and DR After Disaster

New Orleans planned to gradually upgrade to flash-based storage to improve efficiency and prepare for a future of 20% annual data growth. To accommodate the expected expansion of data, the city's IT team began

complex and integrating the storage on 3PAR with backup on Data Domain was particularly difficult. The team also developed a plan that would relocate one of its data centers outside of New Orleans for disaster recovery

seemed off but chalked it up it as an internal issue. About an hour into the workday, however, the staff and service desk began to receive user complaints about interactions they were having. Within 30 minutes, the team realized systems were under attacked and immediately shut down the environment.

Much later, after a forensics investigation, the city uncovered the reason for the attack: A legitimate user with elevated privileges had clicked on a phishing email on-premises.

Finishing the Data Storage System

Because of the work the city had done, most of its data remained untouched during the attack. However, one of the recovery backups failed, which caused some data loss.

In the wake of the attack, Lagrue was adamant about finishing the storage and backup upgrade. “We were looking for clean storage and backup we could use to begin rebuilding, because we had to assume that everything in our environment was compromised because it had been touched,” Lagrue said.

The team investigated options before settling on Pure Storage FlashArray and FlashBlade for primary storage and disaster recovery. The team selected Veeam for backup across its data centers.

In addition, the city moved its secondary data center out of the New Orleans area to improve disaster recovery.

With this infrastructure, Lagrue is convinced that the city is fully prepared for the next disaster, whatever it might be. Data is constantly sent to the secondary data center, so if the production data center is compromised, it would be easy to simply disconnect from the first data center and begin operating out of the second. And because everything is actively backed up throughout the day, interruptions to routine work, especially in production and payroll, are no longer a problem.

To further lock things down, the city requires a two-step verification process to access backups. “Insurance requires having offsite and offline backups, and we have had to explain to our insurance carrier several times that we don’t do it that way because our active backups actually go offline if a threat is detected,” Lagrue said. “Effectively, they become offline backups at the point where someone actively tries to access the backups and our backup environment. It’s immediately shut down and requires personal verification from someone on our team to someone on the Pure team before that access can occur. That’s our security blanket.”

Cloud on the Horizon

Next up for the city of New Orleans is a large-scale move to the cloud, which Lagrue said is basically a cost decision.

As Lagrue sees the cost of cloud storage leveling off, she expects to invest more into the move. While there are no plans to close the data centers, there are areas within city that make more sense to move to the cloud, including centralized criminal justice projects and public safety. One option for these and other workloads are cloud-based data lakes, she said.

About the author

Karen D. Schwartz is a technology and business writer with more than 20 years of experience. She has written on a broad range of technology topics for publications including CIO, InformationWeek, GCN, FCW, FedTech, BizTech, eWeek and Government Executive.