rubrik

Langs Building Supplies Stops Ransomware Attack Due to a Next-Gen Backup Solution

LANGS BUILDING SUPPLIES

RESULTS

- 25 minutes to write script to restore files to VM from latest snapshot
- 1 hour to normalize threat and running
- 0 data lost

THE CHALLENGE

- Ransomware attack on system through email link
- One production file server infected by CryptoLocker
- 15,000 files encrypted

THE SOLUTION

- API-first architecture
- Global real-time file search
- Converged data management for backup and recovery

"Having a top-notch data management solution in place means I can go about my day-to-day job without worrying about data loss. I know I have it covered," says Matthew Day, ICT and Support Manager at Langs Building Supplies, a leading manufacturer and supplier of products for the construction industry based in Stapylton, Queensland, Australia. The business was recently hit by a ransomware attack. Due to its effective backup infrastructure, the company was able to thwart the threat and restore its data without paying a ransom.

THE GROWING THREAT OF RANSOMWARE

Ransomware is a special type of malware in which an attacker holds users' data hostage until a ransom is paid. Many forms of ransomware use strong cryptography to encrypt a victim's data using an encryption key known only to the attacker. After a specified length of time, the attacker deletes the encryption key, and the victim's data is lost forever. Even if the victim pays the attacker prior to this deadline, the attacker may or may not provide the victim with the required decryption key.

Ransomware attacks are increasing exponentially. There has been a reported average of over 4,000 ransomware attacks per day since January 1, a 300-percent increase over the approximately 1,000 attacks per day in 2015.[1] The usual victims are in industries where accessing a computer is required for critical activities. Usually, they don't have modern technologies in place everywhere and end up paying the ransom in order to regain access to their data. In the past, there has been no effective way to get around these attacks, and the frequency of ransomware attempts are increasing.

LANGS BUILDING SUPPLIES' REAL-LIFE EXPERIENCE

In early June, one production file server at Langs Building Supplies was infected by CryptoLocker through an email link clicked by an employee. The IT team was alerted within 10 minutes of the attack through monitoring tools that tracked high change rates in data structures. As a result, only 15,000 files out of millions were renamed as .encrypted, a file extension that prevents those files being accessed without a passcode from the attacker.

RANSOMWARE ATTACK PREVENTED DUE TO NEXT-GEN DATA MANAGEMENT SOLUTION

After receiving an alert from the monitoring system, Day was able to isolate the affected VDI desktop and prevent the attack from spreading to the rest of the firm's infrastructure. "We were able to write a script to restore files back to the VM from the latest version of the file because of our backup. We had all of our files back to the file server in approximately one hour. No damage done," stated Day.

[1] Source: Symantec Internet Security Threat Report, 2016

There were a few key aspects to Langs Building Supplies' data management solution that allowed them to mitigate a potentially damaging situation:

1. Modern technology: "Modern technology does not necessarily mean low-touch but really that it works when you need it and how you need it to. Our converged backup appliance really helps manage our data. It can easily manage and protect our VMs, set our protection policies as general or as granular as we want, and search across our data protected for specific VMs, objects, or specific files to restore."
2. Programmatic Interface & API-driven: "The typical use case of finding a single file here and there via the UI is simple, but finding thousands of files would have been time consuming. Having a programmatic interface that allows custom workflows for third party services allows us to automate and orchestrate the management of our environment even further. Since Rubrik has RESTful APIs, we were able to write a script to search for and restore our affected files without having to go through a painful dig and recover process manually."
3. Incremental-forever: "We can take snapshots more often since less data needs to move to our backup location at any point in time with an incremental forever approach. This allowed us to discover the exact time when our files were renamed and recover our files from just before the attack occurred."
4. Quick Restore: Recover fast VMs and applications by mounting directly onto Rubrik. Day stated, "We had our production servers normalized and running in an hour."

"There was no potential for real long-term financial damage because we have Rubrik. We have systems in place to cover these eventualities. You need to have not only end user education and group policies, but also disconnected backups being managed by a system that is totally separate from your production environment, so no attack can get to them. That's where Rubrik steps in," said Day.

The best way to mitigate ransomware attacks is a defense-in-depth by integrating security with data protections. As Day explains, "You'll always have weaknesses. That's why you need rock solid data management. You always have to be moving forward instead of looking back. Since we plan for these failures, this threat was reduced to a minor convenience. The next day, it was like nothing happened."

LANGS BUILDING SUPPLIES

"Having a top-notch data management solution in place means I can go about my day-to-day job without worrying about data loss. I know I have it covered,"

Matthew Day, ICT and Support Manager at Langs Building Supplies

rubrik

Global HQ
299 South California Ave. #250
Palo Alto, CA 94306
United States

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

Rubrik provides the industry's leading Cloud Data Management platform to accelerate how enterprises protect, manage, and secure data everywhere. Fortune 500 companies trust Rubrik's single platform to deliver data protection, search and analytics, archiving and compliance, and copy data management to deliver instant data access, cut TCO in half, and slash daily management time down to minutes.