COHESITY

Library successfully restores Cohesity-protected services after cyberattack

CERT Cyber Event Response Team

Industry: Public sector

Target: Unknown

Initial Attack Vector: Unknown

Overview

A major city's library system depends on more than 100 virtual machines (VMs), used for the library website, online catalog, in-person checkouts, self-checkout lanes, issuing library cards, free Wi-Fi, online homework help, and more.

> "Most companies follow Cohesity's security hardening guidelines when they start out. But as staff come and go, the configuration may drift. We strongly recommend frequently reviewing sensitive accounts and making sure that the DataLock retention period is appropriate."

Jonathon Mayor, Security Solutions Architect, Cohesity CERT

1: Detect

When the IT staff arrives on a weekend morning to perform routine maintenance, they discover that all systems are down. Suspecting a ransomware attack, they immediately disconnect the network switch to limit the attack's impact. They call an incident response firm, which confirms that a ransomware attack is in progress and all virtual machines (VMs) have been encrypted.

2: Respond

The library begins replacing its IT infrastructure. Early in the process they engage Cohesity CERT (Cyber Event Response Team) to advise on data restoration and operational recovery for the 60 VMs protected with Cohesity. (About 40 VMs are protected with other backup solutions.) The same day the case is opened, Cohesity CERT takes the following actions to contain and investigate the threat:

- Freezes the cluster to preserve potential evidence and assess the scope of the attack
- Gathers logs for forensics analysis by Cohesity security engineers, who confirm the Cohesity backups show no signs of unauthorized access

3: Recover

The incident response team collaborates with Cohesity to confirm that recovered VMs are validated and signed off for return to service. Then the IT team begins restoring the VMs, with Cohesity CERT standing by to help with any issues. All 60 VMs are quickly restored. In contrast, many of the 40 VMs protected with other backup solutions are lost. Rebuilding them takes weeks, disrupting normal library operations.

Cohesity CERT recommendations for stronger security and cyber resilience

- Enforce password policy that requires sufficient complexity and length
- Verify that the Cohesity cluster has not drifted from the recommended security configuration, and review the use of DataLock and MFA
- Validate that backups are successful

5000146-001-EN 1-2025