Zero Trust Data Management foils **ransomware attacks**

By following certain best practices, agencies can ensure their data is secure and instantly available

Jeffrey Phelan
Public-Sector CTO,
Rubrik

THE WIDESPREAD SHIFT to remote work during the pandemic introduced new vulnerabilities to government systems. Employees' personal devices and home networks were not as secure as on-site workstations, and adversaries took advantage of the situation to increase their social engineering and ransomware attacks.

Agencies need to enhance their cybersecurity training for employees, and they need to think more strategically about protecting data and networks. Adversaries who successfully breach a government network will try to penetrate the identity and access control system and invariably attempt to take down the backup infrastructure so the agency won't have protection against ransomware.

Therefore, agencies need to adopt best practices for protecting data and IT infrastructure.

4 steps to secure data

First, agencies should apply a logical air gap, which means the backup infrastructure is readily available but not accessible from the network. A physical air gap — for instance, an off-site data center — tends to be expensive and has other limitations. Think of it like a moat around a castle: The drawbridge must be down while data is being backed up, and during that time, bad actors can follow an authorized user into the castle. That's why Rubrik recommends using a logical air gap.

Second, agencies need to make sure their file system and data are immutable and that no one can alter, change or edit the backup data. Any system that can be edited is NOT immutable. Additionally, some vendors play games with the term and will say backups are immutable for a specific time frame or under certain administrative controls, but that approach makes it possible for an adversary to pose as an authorized user and make changes to or delete the backups. Conversely, Rubrik delivers the data management industry's only patented immutable file system as the core security capability that underpins its zero trust solution.

Third is retention lock. Think of it in terms of the protocol for launching a nuclear strike: The secretary of defense must verify that the order came from the president before complying. With retention lock, a human presents challenge questions to an individual who wants to make policy or other changes to a government IT system. Even authorized users can't do such activities without making a phone call and talking to a person in Rubrik's organization.

Fourth is data encryption. Rubrik encrypts data when it lands in our system, travels within our system and moves off

Shutterstock/FCW Staff

> **Recoverability service-level agreements of minutes and hours are possible** and delivered today across the whole of government and the Defense Department.

our platform. Our philosophy is trust nothing and suspect everything, so we issue challenges at every point of access or movement of data and use the latest technologies to validate identities every step of the way.

Recoverability is the only KPI that matters

Agencies must ensure recoverability because none of these protections matter if they can't recover data and systems that run their critical missions and operations. Agencies need to gather and protect data at the edges of their networks, in their data centers and across different clouds. Regardless of where agencies decide to store that data, they need to be able to access it instantly. Recoverability service-level agreements of minutes and hours are possible and delivered today across the whole of government and the Defense Department. Gone are the days of weeks and months to get back online.

It's therefore no surprise that Rubrik's industry-leading Zero Trust Data Management solution drove Microsoft's recent equity investment in Rubrik, bringing our leading immutable file system, multi-layer approach to security and seamless data management capabilities to combat ransomware for both on-premises and cloud environments. ■

Jeffrey Phelan is public-sector CTO at Rubrik.