Hitachi Vantara Federal

CHECKLIST

Ransomware Disruption Prevention Checklist

A Three Step Process to Guaranteeing Federal Data Integrity During a Ransomware Attack

Do you have the tools/technology in place to guarantee the integrity of your data in the event of a ransomware attack?

When ransomware attacks happen, there are two possible ransomware scenarios: either a user inside the firewall network opens a bad file or link that immediately executes a harmful payload, or the execution of a malicious file that's been lying in wait for months to bypass restore capabilities executes upon a trigger event.

The first situation often has limited impact that can be quickly remedied with redundancies and reliable backup and recovery programs that can restore data to a specific point in time. The second situation is much more challenging. Someone knowingly or unknowingly loads a trojan file that was improperly scanned or otherwise not detected. The malware can go undetected for months until a triggering event. Triggers are usually timed to happen beyond the backup window, and the frequency of backups means storage space can be limited.

As we've seen, without restore points, the victim's choice is to pay the ransom or lose their data for good. Their recourse has been to expand backup and restore capabilities to a bigger time window, and at greater expense.

However, implementing different processes and technologies can render this danger moot. Below is a step-by-step overview of the technology and processes your agency needs in place to guarantee the fidelity of sensitive agency information in the event of a ransomware attack.

◊ Step One – Identify all the data stored in your system

- **Understand** what is valuable vs unnecessary data in your system
- **Eliminate Data ROT** (Redundant, Obsolete, or Trivial Data Sets)
    - ROT is digital data that an organization is retaining beyond any legal or defined time (retention) period and may pose a liability risk that ransomware targets because it is not managed properly. It becomes a burden for capacity management and is often captured in other retention tools. By keeping ROT, you can slow down searches, impact proof of compliancy, and makes data management less agile.
        - Examples include:
            - » Junk mail, spam, deleted items in mail, duplicate copies of email
            - » Any temporary files
            - » Employee records held beyond any legal justification
- **Reduce Spillage** by identifying instances where data has grown out of control. There are three main types of data spills:
    - **Inadvertent** - If someone had no reason to believe their actions would lead to a data spill, it can be called inadvertent.
    - **Willful** - When an individual purposefully disregards procedures or policies and causes a data spill. Intentionally bypassing security controls is an example of this.
    - **Negligent** - Occurs when a person acts unreasonably and causes an unauthorized disclosure. This can happen through careless attention to detail or a reckless disregard for procedures.

◊ Step Two – Monitor what is happening in the system

- **Implement Log Analysis** technology, such as Security Information and Event Management (SIEM) tools, for compliance and vulnerability management, real-time insights, threat reporting and log aggregation abilities.

♦ Step Three – Respond to new data as it is being added to the network

- **Utilize WORM-based (write once read many) object storage** technology, which has no executable files, prohibiting any corrupted files from executing while stored and nullifying the triggers. Modern object storage has come a long way from its roots, making it a more secure, high performance alternative to solutions such as Network Attached Storage (NAS). However, when implementing Object Storage to mitigate ransomware, agencies should ensure their capabilities include:
  - The ability to combine object storage, file sync and share, cloud storage gateways, and sophisticated search and analytics for a simple, integrated cloud storage
  - Massive scalability and multiple storage tiers backed by security, support and configurability
  - Content validation, replication and object versioning to protect from accidental deletions
- **Create one path for data to flow.** Whether it is on premise, in the cloud, or via a hybrid approach, move data to a singular location where it can be controlled, accessed and managed. The "One Path" strategy provides a holistic approach to next-generation data management, helping your organization evolve beyond IT-centric goals such as storage and performance, to more business-oriented outcomes such as improved productivity and time to market based on data intelligence. This allows your agency to build a more dynamic and effective digital workplace while addressing security and compliance demands.

LEARN MORE ABOUT AN UNLIKELY ALLY IN RANSOMWARE PREVENTION

Hitachi Vantara Federal

Corporate Headquarters
11950 Democracy Drive, Suite 200
Reston, VA 20190 USA
hitachivantarafederal.com

Contact Information
USA: 1-703-787-2900
hitachivantarafederal.com/about/contact-us/

August 2021