Lost Data Retrieval Project
Cybersecurity

By Shourooq Shaath

Lost Data Retrieval

Ransomware data recovery procedure for data retrieval skills
Focus on restoring the effected system from backup then build a plan building data

THE PUPOSE OF THIS PROJECT

Is to restore lost and damaged/ encrypted system data from a recent ransomware attack from cyber criminals. Those cyber criminals who hold your data and systems hostage. Often ransom attackers demand to decrypt your data in exchange for payment in cryptocurrency since it's anonymous and less traceable.

IMPACT OF MY CONTRIBUTIONS

By understanding data protection strategies in place this can result in saving your business from catastrophic data breach by a ransomware attack that disrupt business continuity.

DATA RECOVERY PROCEDURE:

Best practices are to recover data from a cloud backup system. Using a cloud tool to back up your system data is an effective way to break the ransomware encryption placed on your files and systems using algorithms developed by security experts. Most cloud-based backup system have Decryption tool added to them.

1. ***Define the scope of the attack***
   The first step in responding to virtually any ransomware attack is to determine how much data was affected, and how many systems were breached. Was the attack limited to a single server or a single S3 bucket, for example, or was all the data within your data center or cloud environment impacted?

2. ***Disable affected systems***
   Once you've identified the affected systems and/or data, your next step should be to disable them to prevent the attack from spreading further. **The purpose of this steps is to make sure the attack is no longer active and spreading in your network.

3. ***Assess the damage***
   This step is to determine and assess the extent of the damage. How much data was held for ransom?

4. ***Disclose the attack***
   Are you a government office, public body. Is customer information leaked? In some cases, offices are required by law to disclose the attack the information breached.

5. ***Prepare a recovery plan***

At this step is you put your plan to recover lost, damaged, or stolen data

6. ***Recover & restore system data and other data from back up***
   With your recovery plan in place, you are removing ransomware infections from your network and execute it to recover data depending on how your data was backed up

7. ***Removing Ransomware infections***
   In this step you must quarantine your network, close all suspected ports, scan all computers, disable system restore, quarantine infected computer, restart computers, disable system restore and install Firewall (if necessary). Its' also recommended to install security updated and keep your network machine up to data, change ay shared passwords for shared resources. Once this all completed reconnect local network and internet access as this will prevent further infection from an external source.

8. ***Preform a security Audit***
   Once the data is recovered and operations have been restored, take time to determine how your systems were breached. Did the ransomware enter your environment via phishing, malware, a malicious insider, or something else? Identifying the source of the breach will help prevent it from happening again.

9. ***Create an incident report***
   This report must include details of the attack, the data & systems it affected, and the steps you took in recover and restore them. The purpose of this report is bringing a summary of the attack so that it can provide and understanding of what it takes to prevent a similar attack from happening in the future.

10. ***Provide Employee training***
    As technology evolves, cyber threat actors also continue to evolve their attack tactics and techniques. A lack of awareness of cyber threats can lead to cyber incidents. Your organization should focus on creating tailored cyber security training to help users avoid cyber incidents and strengthen the overall cyber security culture in the workplace.

    Educating employees about common cyber threats can protect your organization and minimize risks. Your organization should consider addressing topics such as the following examples:

    - Creating unique passphrases and complex passwords for all accounts
    - Using the Internet and social media safely in the workplace
    - Using approved software and mobile applications
    - Identifying malicious emails

11. ***Implement Zero trust policy***
    Zero Trust is a security framework requiring all users, whether in or outside the organization's network, to be authenticated, authorized, and continuously validated for

security configuration and posture before being granted or keeping access to applications and data. **Zero Trust assumes that there is no traditional network edge**; networks can be local, in the cloud, or a combination or hybrid with resources anywhere as well as workers in any location.

Zero Trust is a framework for securing infrastructure and data for today's modern digital transformation. It uniquely addresses the modern challenges of today's business, including securing remote workers, hybrid cloud environments, and ransomware threats. While many vendors have tried to create their own definitions of Zero Trust, there are several standards from recognized organizations that can help you align Zero Trust with your organization.

PLAN AND APPROACHES:

In this section we plan to restore affected systems from a **Cloud backup**; and extract corrupted or deleted data from storage devices.

1. ***Approach 1: Restore from the Cloud Backup***

   The fastest way to recover from ransomware is to simply restore your systems from cloud backups.

   For this method to work, you must have a recent version of your data and applications use the cloud as the place where you store backup data.

   This approach to cloud-based disaster recovery allows clients to take advantage of the low-cost data storage options available from cloud vendors. Also, backup routine is simplified by allowing to store backup data from all your system in a single location within the cloud.

2. ***Approach 2: Restore from on- premises backup to the Cloud***

   A second approach of cloud disaster recovery is to back up data on-premises but recover it to virtual machines and databases running in a cloud platform.

   This approach eliminates the need for physical on-site infrastructure to remain available following a disaster. Instead, you can quickly recover data to virtual environments running in the cloud. The major risk, however, is that, if you store data backups on-premises, your backups may be destroyed if a disaster impacts your local environment.

3. *Approach 3: Restore Cloud-to- Cloud*

You can achieve the best of both worlds by storing backup data in the cloud and recovering to the cloud at the same time.

Under this approach, you would spin up virtual machines and databases in the cloud, then populate them with data from your cloud-based backups in the event of a disaster that impacts on-premises resources.

In addition to separating both your backup data and backup infrastructure from your local data center, this strategy may speed disaster recovery, because it will typically take less time to transfer backup data from cloud storage to cloud VMs and databases than it would to move data between the cloud and an on-premises environment, or vice versa. That's because networks within the same cloud offer much more bandwidth than the public Internet that connects a cloud to external environments.

The downside of disaster recovery in the cloud is that it is likely to cost the most because it requires you to maintain both backup storage and backup infrastructure in the cloud.

The most straightforward cloud disaster recovery configuration is to back up data from on-premises to the cloud, then recover data from the cloud when is needed. This approach will cost the least and is the simplest to administer. The major limitation to consider, however, is whether you'll be able to move and recover data quickly enough from the cloud to your on-premises environment.

References

- https://cloudian.com/guides/ransomware-backup/ransomware-data-recovery-5-ways-to-save-your-data/
- https://www.msp360.com/resources/blog/designing-a-ransomware-response-plan/
- https://www.riskdiversion.co.za/useful-tips-to-remove-malware-from-a-local-network
- https://www.msp360.com/resources/blog/cloud-disaster-recovery/
- https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/#:~:text=Zero%20Trust%20is%20a%20security,access%20to%20applications%20and%20data.
- https://www.cyber.gc.ca/en/guidance/provide-employee-awareness-training