HYCU

Safeguarding your critical data from the ransomware threat

BEST PRACTICES FOR BACKUP AND RECOVERY

Ransomware happens. Be prepared.

Think a ransomware attack can only happen to someone else?

Think again.

Ransomware attacks are on the rise and targeting organizations of all sizes and industries.

Given the value of data to business today and the alarming rise in cyberattacks, securing and protecting critical data assets is one of the most important responsibilities in the enterprise.

To help you fulfill this essential mission, we've pulled together some best practices to help you lock down your data and reduce the risk posed by ransomware and other security breaches.

Losses due to ransomware are projected to exceed $20 billion in 2021.[1]

1 Source: https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/

Follow the 3-2-1 rule

Creating a robust backup, copy and archival strategy is an essential first step for protecting your most critical data and systems.

A traditional approach is the 3-2-1: rule:

- **3 copies** of data
- on a minimum of **2 separate storage solutions**
- with **1 medium being offsite**/alternate location or in the cloud

While this is still a good approach, it's critical to carefully select the types of backup targets you use with this kind of approach.

For some key considerations, keep reading.

Put a WORM to work

WORM

One of the most useful ways to safeguard backup data is to implement a copy or archival strategy that incorporates a **WORM** (Write Once, Read Many) capability. Nearly every cloud-based or on-prem object storage solution offers this capability.

BLOB

WORM is designed to provide data immutability, meaning it is unchangeable. The technology implements a retention policy that prevents data from being overwritten or deleted for a period of time you specify. **An Object Storage** bucket or Azure **BLOB** (Binary Large Object) container are great options for copy or archival backups.

DARE

When considering cloud storage providers, look for one that offers security measures such as **DARE** (Data-At-Rest-Encryption), **secured transport technologies** (VPNs and HTTPS/TLS), and the **AES 256 encryption** for data destined for cloud targets.

Cover your on-prem bases

There may be situations where on-premises NAS (block) storage options are used for initial backups, before copy and archival. These demand special consideration.

NAS appliances typically employ standards like NFS (Network File System) or SMB (Server Message Block). Without additional enhancements to your backup system and/or network safeguards, these standards can be vulnerable to attack.

A best practice is to ensure primary storage targets are **dedicated for backups** and are not used and mounted to other systems.
In addition, look for a backup and recovery solution that offers **detection, notification and prevention** features to help safeguard your initial NAS backups.

Create smart policies

Another best practice is employing a policy-driven approach to protecting critical VMs, data, and applications.

This requires some careful thinking about setting the proper policy options around snapshots, backups/copies/archives, data retention, and RPO (Recovery Point Objective)/RTO (Recovery Time Objective). Make sure your backup and recovery solution offers the ability to easily establish and enforce policies to ensure your applications and data are protected with the right degree of consistency.

Backup and recovery policies are not a “one and done” proposition. Things change, so revisit policies on a periodic basis to ensure they continue to meet the needs of the organization - and the evolving cyber threats.

Secure network access

The last step in the process of protecting your backups is to focus on securing the pathways to and from your sources, hosts and targets.

Based on your selected target, consider the following:

1. If using an **NFS target for primary backups**, be aware that appliance may require a whitelist setting to permit traffic to the network storage from your backup solution.

2. If you opt for an **SMB target**, you will need to configure an account with access to a share that you create. It is also important to disallow (or not improperly allow) any unauthorized network access to your backup data share - and do not attach it to other machines in your environment.

3. If you select an **iSCSI target**, consider enabling/configuring CHAP (Challenge-Handshake Authentication Protocol) on the target and on your backup solution.

4. For **cloud object storage targets**, you will need to configure accounts and/or secret/access keys to grant access. Then decide if you need an encrypted high-speed isolated connection (configured with peered connection points and appropriate routes), a site-to-site VPN connection, or if you can simply go over the public internet with HTTPS/TLS.

5. Other common sense measures include not permitting internet access to servers, paying close attention to admin workstation hygiene and selecting storage targets that provide anti-ransomware features. For added protection, look for a backup and recovery solution that allows use of a customer or provider-generated PKI (Public Key Infrastructure) certificate.

Don’t wait until it’s too late.

A ransomware or other cyberattack can happen at any time. Your best protection is making sure critical applications and data are safely backed up and isolated from potential intrusion.

Following the best practices summarized in this e-book is a good start.

It’s equally important to choose a backup and recovery solution that makes implementing strong data protections simple and flexible. That will make it easier to keep pace with the changing needs of your organization and the evolving threat landscape.

Still have questions about securing your critical data?

Connect with us at info@hycu.com.