Offline backups in an online world

How to protect your backups that are stored in the public cloud.

James L

The NCSC has seen numerous incidents where ransomware has not only encrypted the original data on-disk, but also the connected USB and network storage drives holding data backups. Incidents involving ransomware have also compromised connected cloud storage locations containing backups.

We have previously highlighted the importance of data backups for disaster recovery, most notably in our guidance on backing up your data and ransomware. If you've not read these yet, please do. They explain the importance of maintaining regular, reliable backups to minimise the impact of an incident like a ransomware infection.

In response to recent ransomware incidents, this post supplements our existing guidance to help you protect your backups stored in the public cloud. The four rules outlined below should be kept in mind when using the cloud to store any of your backups.

1. The offline rule

At any given time, are one or more backups offline?
The purpose of an 'offline backup' (sometimes called a 'cold backup') is to remain unaffected should any incident impact your live environment. You can do this by:

- only connecting the backup to live systems when absolutely necessary
- never having all backups connected (or 'hot') at the same time

With at least one backup offline at any given time, an incident cannot affect all of your backups simultaneously.

Using cloud storage to hold an offline backup is a good idea because it guarantees physical separation from your live environment. Crucially, when your offline backup isn't in use it also needs to be digitally disconnected. Unlike conventional backup storage, you cannot take your cloud storage offline by simply unplugging it. However, there are a few steps that can be taken to apply the same level of protection.

Identity management

The first step to protect cloud storage is secure account identity. For cloud services this almost always appears as username and password credentials. All users able to access cloud backups should be properly protected in line with NCSC guidance. Without a trusted identity, ransomware should not be able to request access to your cloud storage and encrypt it. For more information on secure identity management, please refer to the NCSC's password guidance and multi-factor authentication guidance.

Client management

A backup client is a device with credentials to access your cloud storage. Cloud backup clients should not have valid credentials while your cloud storage is not in use. The number of backup clients should also be kept to a minimum with standard user devices unable to modify cloud backups directly. Following this practice, a ransomware infection can only compromise your cloud backup if it occurs on an authorised client and while your cloud backup is being used.

Access control

Some cloud storage services offer more advanced access controls for identity and connectivity. If these controls are available, they should be configured to only allow authorised clients to create new backups (or append to existing ones), and deny connection requests while the storage is not in use ('cold'). If a ransomware infection occurs while your cloud backup is offline (denying connection requests), it will not be able to reach the cloud storage, giving you the same level of confidence as unplugging an on-premises storage drive. In the event of a ransomware incident occurring whilst your cloud backup is connected, ransomware acting with privilege to only create new data cannot overwrite your existing backups. This is comparable to traditional write-once storage (but is cheaper and more scalable).

2. The recovery rule

Is the data in cloud backups restorable and recoverable?
While all measures can be used to try and prevent a security incident from affecting your backups, it's best to have a backup plan for your backups. Some cloud storage services allow you to restore modified data back to an older version, and recover deleted data for a limited time after it was deleted. If ransomware does manage to affect your cloud backup, you can use these features to restore back to the last known-good state. When choosing a cloud storage provider, you should check that these features are included in the service.

3. The 3-2-1 rule

Is critical data saved in multiple backup locations?
It is vital to keep multiple backups and to logically separate them. Maintaining resilient backups means that if one is compromised, at least one other remains. The most common method for creating resilient data backups is to follow the '3-2-1' rule; at least 3 copies, on 2 devices, and 1 offsite. This strategy is popular because it scales effectively (including the use of the cloud for an offsite backup) and can give you confidence that your critical data is safe from a localised incident. However, it does not require any backup location to be offline – hence the need for our first offline rule.

4. The regular rule

Is critical data backed up regularly?
Finally, backups should be created on a regular basis. The more frequently backups are created, the less data is if you're forced to recover. Not only should

your backups be created frequently, they should also be regularly tested to check they work as expected.

I think that the saying 'every cloud has a silver lining' is quite apt in this situation. The silver lining of recent incidents is that cloud backups are being created. By asking yourself these questions and following the guidelines, you can make your cloud backups more resistant to incidents like ransomware.

James L

Cloud Security Researcher

WRITTEN BY

James L
Senior Security Researcher

PUBLISHED

13 August 2019

WRITTEN FOR

Small & medium sized organisations

Large organisations

Public sector

Cyber security professionals

PART OF BLOG

NCSC publications