BLOG POST

Cloud backup options for mitigating the threat of ransomware

The increase in cyber attacks related to COVID-19 (and the number of people now home working) means it is more important than ever to ensure your information is backed up securely.

Jamie H

The NotPetya cyber attack back in 2017 caused widespread damage to multi-national corporations including Maersk, TNT Express, and Mondelez International. Each of these corporations reported losses as a result, with indications that backups were either limited or non-existent.

The COVID-19 situation has already forced organisations to make rapid changes in response to the demand for increased home working. Many organisations have put in place a 'change freeze', to prioritise the reliability of their IT. Despite this, it's important to ensure that your critical data is backed up securely. If you already have a data backup regime in place, you can use this blog to check it's fit for purpose.

The NCSC's recently published guidance:

Offline backups in an online world
and
Mitigating malware and ransomware attacks

are great starting points for you to check that you have set up your cloud backups correctly. Despite being internet-connected, using the cloud as your backup is suitable as long as you have procedures in place to prevent your backup being corrupted during an incident.

The most important factors to consider are:

1. Could ransomware overwrite your backup, preventing your recovery? Look for a service that keeps **multiple versions of backed up data**, or which allows you to undo changes to backups.
2. Does the cloud service provider you have chosen have **multi-factor authentication (MFA)** available to protect the backup? If it does, then ensure you have implemented it.
3. Do you carefully manage the ability to modify or delete backups ? Make sure you **limit the number of accounts** with the ability to access backups.
4. Will your cloud service provider **ship data back to you** to aid recovery from an incident?
5. If you have client software on-premise, **check the schedule** of incremental cloud backups.

By following these points you should be able to mitigate the risk of ransomware and other cyber attacks, in what has been a cultural shift for many organisations.

You may also find our recent guidance on preparing your organisation for an increase in home working to be useful.

Jamie H
Senior security researcher

WRITTEN BY

Jamie H

PUBLISHED

8 April 2020

WRITTEN FOR

Large organisations

Small & medium sized organisations

Public sector

Cyber security professionals

PART OF BLOG

NCSC publications