RansomCloud

10 things your business must know
to survive an attack

backupvault.co.uk

BACKUPVAULT

Traditional ransomware rides high in the cyber underworld, but a young upstart is on the rise. Loosely titled 'RansomCloud', this rearmed and reinvented strain of malware is bred for a sole purpose: to target the cloud apps and services your business increasingly depends upon.

So, if you use Office 365, or Google's G Suite, you could suddenly find your emails and your stored files and data paralysed by encryption (in *real-time*) – with a chilling ransom note demanding payment to release them.

In this guide, we look at what your business needs to know and do in order to prevent a RansomCloud attack from taking your data prisoner – and dealing a blow to your finances at the same time.

01 Back up your data – because the cloud apps don't

Backing up your data effectively can render RansomCloud's attempts to separate you from it toothless. But don't rely on your cloud service providers to take care of these backups – because they don't. If you read their Terms & Conditions carefully you will see that your data is still **your** responsibility.

Run dedicated backup software within your business, on the other hand, and you can constantly protect your data by copying it automatically to a secure offsite cloud datacentre, provided by the backup vendor.

But make sure they also offer a 'mirror site' – an additional secure datacentre that ensures your data is backed up and accessible even if one datacentre suffers an interruption.

02 Remember the restore!

Many a business has failed to bounce back from a ransom attack because its backed-up data simply couldn't be reinstated into the organisation quickly and smoothly enough.

The key metric to look for here is Recovery Time Objective (RTO), and the choice of backup type will influence it to a great degree.

A backup service that makes large files immediately usable even when they're only partially restored, for example - rather than having to wait for them to restore in their entirety – will offer a far superior RTO, enabling your business to get back on its feet that much more quickly following a RansomCloud incident.

03 Scrutinise the support and the small print

Before you choose your backup provider in your bid to protect your business against RansomCloud, find out what level of support they can offer and what degree of integrity the data centres themselves have.

Are support staff available 24/7, to hold your hand if a RansomCloud incident hits? To what standard is your precious data encrypted both on its way to the data centre and at rest there? And where are the data centres situated – is their location compliant with current data protection legislation, for example?

Backup can beat a RansomCloud attack – but not all backup is created equal.

04 Make sure all your data's covered

'Data' is an understandably useful catch-all term for backup providers – but you need to delve deeper to understand what is and isn't protected, and to what degree of granularity.

Standard 'file and folder' backup won't capture often critical data elements like user preferences and permissions, and system settings, potentially leaving you trying to do a full restore with only half the story.

A 'system image' backup, on the other hand, can capture pretty much everything, but you need to make sure it can work with all your data sources too. Depending on the size and nature of your organisation, these can include:

- Virtualised servers
- Desktops and laptops
- Mail servers
- On-premise
- Hybrid systems, and more.
- Remote machines
- File servers
- Data servers
- Cloud

So choose your backup provider carefully – your data depends on it.

05 Use web filtering

Web filtering detects suspicious websites and domains contained in links within email - which is typically how ransom attacks are often triggered – and stops users from accessing them.

As ever, prevention is better than cure.

06 Foil attackers with multi-factor

Multi-factor authentication (MFA) can be an effective protection against RansomCloud, because it introduces an extra layer of manual user identification that a RansomCloud attacker simply can't provide. This is often in the form of a PIN or password request sent to the mobile device of the user whose account the ransomware is attempting to compromise.

The RansomCloud attacker doesn't have access to the user's device, therefore they can't authenticate their request to access the user's account.

Consequently, they can't have their wicked way with the data it contains.

07 Get your people onside

Are your staff able to recognise the tell-tale signs that an email might contain a link that could, if opened, trigger a RansomCloud attack?

Does the mail seem relevant to their job role, or is it strangely off-topic? Does it address them by their name, or use a generic salutation like 'Friend'? Is the spelling and grammar poor? And does that genuine-looking link, when you mouse over it, reveal that it's actually leading you up the garden path?

If your people aren't savvy to these (and more) signs, you need to bring a qualified trainer in to get them up to speed – and keep them there.

08 Serve phish once a week

The Friday fry is a great British tradition, but what we're talking about here is a very different kettle of you-know-what.

Regularly subjecting your business to mock phishing emails (there are vendors who specialise in providing this kind of software) will enable you to gauge and improve internal awareness of the kind of tactics a RansomCloud attack typically relies on to dupe the user into executing it.

Only when you know exactly where your organisation's understanding of ransom attacks is weak can you guard effectively against it.

09 Develop a disaster recovery plan

This isn't just good practice to protect your business against the effects of RansomCloud attacks, it's good practice to help get your business up and running after many other kinds of outage, too – fire, flood, natural disaster, hardware failure, accidental data loss or deletion, and so on.

And central to your disaster recovery plan is data backup that can take your data back to a specific point in time, of your choosing, before the disaster struck.

This power to choose a specific 'Recovery Point Objective' (RPO) is a critical difference between a true backup system and mere data replication, which often only stores copies from a few hours previously.

It could spell the difference between a disaster recovery plan that gets your business back to normal and one that's actually not worthy of the name.

10 Don't pay. Invest.

Tempting as it may be to bite the bullet and give in to the RansomCloud attacker's demand for money, to get your business back on its feet, don't even let it get that far.

Firstly, there's no guarantee that the attacker will indeed decrypt your data and emails once they've been paid (in fact, there's a great deal of empirical evidence to suggest they won't).

Secondly, there exists a 'sucker list' – a database shared between ransom attackers - of those businesses that have paid once to free their files and are therefore more likely to do so again. You do not want to be on that list.

It's ultimately a choice between investing in effective backup before the worst happens, or paying someone to rip you off again.

Remember: *prevention,* not cure.

Know all this - and use this guide to keep your business RansomCloud-free.

Ransom-Proof Your Data

with BackupVault Cloud Backup and Office 365 Backup

100% of our customers have fully recovered from a ransomware attack.

And we've been in business for over 15 years.

Start your FREE 30 day trial today...

Ransom-Proof My Business

Or, get a quote from our friendly team on

020 3102 0040

BACKUPVAULT

backupvault.co.uk