ransomware.org
understand · prevent · recover

BY ActualTech Media

Developing a Ransomware-Resistant Backup

Ransomware victims need every advantage they can get during ransomware recovery and negotiation with ransomware groups. Reliable and tested backups are one such advantage and serve as an insurance policy to confidently restore files following an attack.

Ransomware groups want to make restoring from backup difficult, if not impossible, for victims. They seek out backups and through whatever means, they make sure the backups are unusable. Security experts typically advise that backups are "stored offline." Broadly speaking, offline backups are backups that aren't connected to the network and are ransomware-resistant.

THE 3-2-1 BACKUP RULE

Have Three copies of backed up data

Stored on at least Two different media types

One of the copies must be offsite

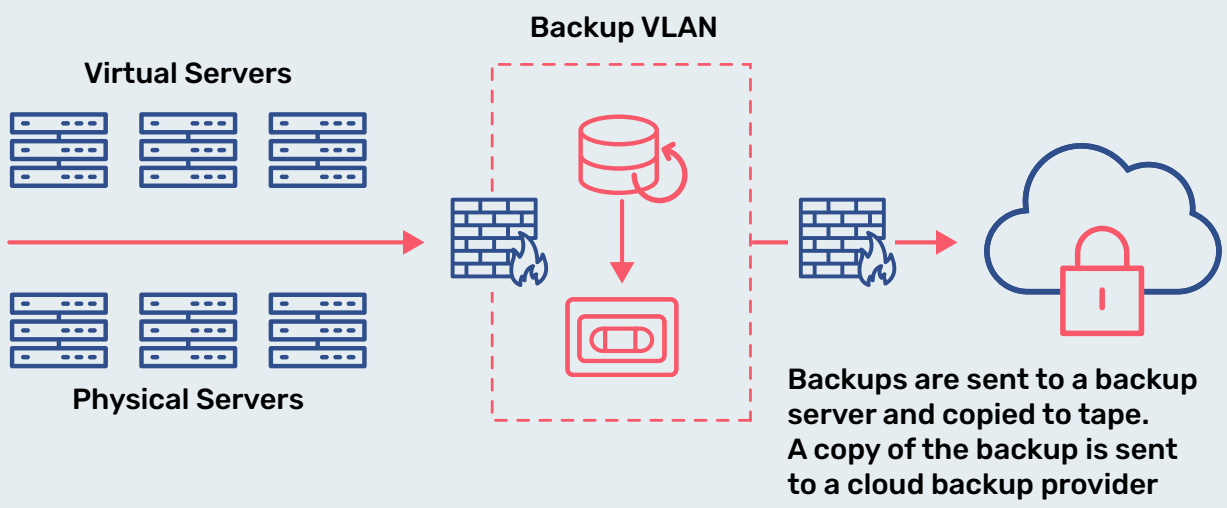
The reason for the emphasis on storing three copies of backed up data is that it creates more redundancy for backups. Having three sets of backup data makes it less likely a ransomware group will be able to encrypt all of your organization's backups.

Naturally, three copies of backed up data all residing on the same backup server doesn't offer additional protection. Therefore, the backups need to be stored on different media.

TYPES OF OFFLINE BACKUPS

1. **Tape:** Although some backup professionals don't like tape backups, no ransomware group has figured out how to encrypt or delete files backed up to tape.
2. **Cloud Provider:** Cloud backups are technically "offline" as they are not directly connected to the network.
3. **Disaster Recovery (DR) Network:** This is a network within your network that is behind a firewall.
4. **Offline Backup Storage Facility:** There are many back up storage companies that can act as your off-site backup.

Here is a backup network design with offline storage following the 3-2-1 rule of storing data on two different media types:



TEST YOUR BACKUPS

Be sure to test your backups regularly so that you can move quickly into action after an attack occurs and help the disaster recovery process run more smoothly.

These tests need to have three components:

- **Test from all backup sources—if the first two fail, it's important to know that the third works**
- **Don't just test by restoring a single file; conduct a full recovery**
- **Test the restoration of multiple systems at once to see how much bandwidth and processing power the DR team will be able to count on from the backup system**

When conducting a full recovery, use spare hardware and start by installing from the gold image to make sure the OS and applications load properly. Then conduct a full restore of the server and test it thoroughly to ensure everything works properly. Try the same test on several servers simultaneously. This serves as a stress test for both the backup software and the DR team.

Tip: Be sure to document your backup test and add it to your DR plan!

Want more ransomware information? Go to ransomware.org >