Asigra.

Recovery is Everything™

Datasheet

Why 3-2-1 Backup has Become an Ineffective Ransomware Defense

The traditional 3-2-1 backup process has been regarded as an effective defense against ransomware, but that is no longer the case.

3 copies of data stored on…

2 different types of media with…

1 copy stored offsite "air-gapped."

Backup software vendors, tape library vendors, cloud vendors, and BRaaS/DRaaS managed service providers say it is so. And as recently as 2017, the 3-2-1 defense may have been an effective ransomware defense, but no longer. Ransomware is a big multi-billion-dollar business. It's organized and, sometimes, state sponsored. Reliable backup processes have become a threat to that revenue stream. The people making huge money on ransomware recognize that threat. This has resulted in them pouring those $ billions back into research and development (R&D) to neuter the backup defense. It is a classic struggle of offense (ransomware) versus defense (backups).

The ransomware industry's first efforts were to have the ransomware utilize published backup software APIs to delete the backups before the ransomware actually detonated. It's crucial to recognize the difference between ransomware infections and detonations. A ransomware infection means the malware has penetrated a system, is live, but has not started encrypting the data. Detonation is when the ransomware encrypts the system's data and then disposes of the key. Increasingly sophisticated ransomware utilizes the infection stage to eliminate backup defenses tied to the detonation stage.

As it became clear ransomware was attacking, deleting, or encrypting backups of popular backup software, the 3-2-1 defense was deployed to stop or at least mitigate the ransomware's efforts. The logic being that when a copy of the backups is air-gapped such as a tape sitting on a shelf, it can't be erased or encrypted. This works but reverses a multi-year effort to make recoveries nearly instantaneous. Recoveries from tape are slow and cumbersome.

This has led to a more effective defense known as multifactor authentication. Ransomware has not yet been able to delete or encrypt a backup if multifactor authentication is required for either process to happen. Multifactor authentication keeps intact the small recovery time objectives (RTO) users expect and demand. Multifactor authentication is what Asigra employed in our latest release v14 named "Backup Evolved."

However, deleting or encrypting the backups was only the criminals first effort. Ransomware has continued to evolve. As mentioned, the latest ransomware versions do not detonate right away. They first spread to as many systems as they can utilizing the permissions of the compromised systems. Then they wait a week, a month, two months, four months, etc. before they detonate. Backup and data protection systems see ransomware as just another file to be protected. They then unwittingly back it up with all of the other data during the timeframe the ransomware is sitting idle before detonating. When the ransomware finally detonates, the backup administrator goes to their most recent backup, sees it has not been deleted, and recovers the data. But wait. As soon as it has been recovered, it detonates again. They then go to an older backup, repeat the recovery, and the ransomware detonates again. This is known as a ransomware attack-loop. It's effective because it's very hard to know when you initially backed up the ransomware file.

How far back in time must the backup be to get a clean uninfected backup? How much data can the organization afford to lose? It becomes a tradeoff between losing weeks or months of precious data or paying the ransom. Most security experts suggest that you never pay the ransom because it marks your organization as a "ransom payer" and a repeat target. It will be hit again and again. The 3-2-1 backup defense does nothing for ransomware attack-loops. It becomes part of the problem.

Stopping the attack-loop requires a different approach. The infected files cannot be allowed to be backed up. And if by some chance an old backup with infected files occurred before defenses were in place, those infected files can't be allowed to be recovered. This means backup software must detect infected but not detonated ransomware before it is backed up and before it is recovered. That defense stops ransomware infections, including attack-loop, in their tracks.

Ransomware has evolved and continues to evolve. Your backup software must evolve with it. Asigra v14 recognized this threat and implemented a cybersecurity feature that stops ransomware infected files or any malware, even zero-day exploits, from being backed up or recovered.

An ineffective defense against attack-loops such as 3-2-1 is worse than no defense. It provides a false sense of security increasing the organization's vulnerability.

Asigra v14 Backup Evolved is an effective ransomware defense. To explore further contact us by email at info@asigra.com.

MALWARE-IN-YOUR-BACKUP
Attack-Loop™ Prevention.

Asigra.