Here are four recommendations to help companies protect their backups against ransomware attacks.

1. Be careful using network file servers and online sharing services.
Network file servers can be easy to use and are always available, two attributes that make network-accessible "home" directories a popular way to centralize data and make it easy to back up. However, when exposed to ransomware, this type of data architecture has serious security weaknesses. Most ransomware programs encrypt connected drives, so the victim's home directory would be encrypted as well. In addition, any server that runs a vulnerable and highly targeted operating system like Windows could be infected, which would lead to every user's data being encrypted.

Thus, any company with a network file server needs to assiduously back up the data to a separate system or service, and specifically test the system's restore capability if faced with ransomware.

Cloud file services aren't immune to ransomware either. In 2015, Children in Film, a business providing information for child actors and their parents, got hit with ransomware. The company extensively used the cloud for its business, including a common cloud drive. Within 30 minutes of an employee clicking on a malicious e-mail link, more than 4,000 files stored in the cloud were encrypted, according to an article in KrebsOnSecurity. Fortunately, the company's backup provider was able to restore all of the files, even though it took almost a week to complete the process.

Depending on whether the cloud service provided incremental backups or easily managed file histories, recovering data in the cloud could be more difficult than an on-premises server.

2. Get visibility into your backup process.
The earlier that a company can detect a ransomware infection, the more likely that the business can prevent significant corruption of data. Data from the backup process can provide early warning of a ransomware infection. A program that suddenly encrypts your data leaves signs in your backup log. Incremental backups will suddenly "blow up" as every file is essentially changed, and the encrypted files can't be compressed or deduplicated.

Monitoring vital metrics such as capacity utilization from the backup process on a regular basis — essentially, every day — can help companies detect when ransomware has infected a system inside the company and limit the damage from the compromise.

3. Consider your solution options.
If ransomware can directly access backup images, then it will be very challenging if not impossible to stop it from encrypting corporate backups. For that reason, a purpose-built backup system that abstracts the backup data will be able to prevent ransomware from encrypting historical data.

By separating backups from your normal operating environment and making sure the process is not running on a general-purpose server and operating system, your backups can be hardened against attack. Backup systems based on the most commonly targeted operating system, Microsoft Windows, are prone to being attacked and make it much harder to protect your backup data.

4. Regularly test your recovery process
Finally, backups are no good unless you can recover both reliably and quickly. Some victims of ransomware have had backups but still have had to pay the ransom because the backup schedule did not perform backups with enough granularity, or they were not backing up the data they thought they were backing up.

Part of testing the recovery process is determining the window of data loss. A company that does a full backup every week will lose up to a week of data should it need to recover after its last backup.

Doing daily or hourly backups greatly increases the level of protection. More granular backups and detecting ransomware events as early as possible are both key to fending off damage.

In the end, companies should aim to detect ransomware attacks early through monitoring or anti-malware defenses, use a purpose-built system to maintain a separation between the backup data and a potentially compromised system, and regularly test the backup and restore process to ensure data is properly protected.

These efforts will keep backups at the top of the list of ransomware defenses and will reduce the risk of losing data in the event of an attack.

- Author: Rod Mathews - https://www.darkreading.com/author-bio.asp?author_id=4825
-
-
-