How Barracuda Cloud-to-Cloud Backup Can Protect You from Ransomware

https://campus.barracuda.com/doc/96020206/

In the last 18 months, malicious attackers have significantly increased their efforts to encrypt, take hold, and blackmail customers using their data. Microsoft 365 data is also subject to the same threats from malicious actors, and it is more important now than ever to have a backup solution to protect your organization from the worst scenario possible.

MIcrosoft 365 Data Impacted by Ransomware

There have been cases where synced files through SharePoint, OneDrive, and other clients that store data locally make those files susceptible to encryption if a malicious actor is already inside your network. Those encrypted files are then uploaded to the cloud after the encryption.

Microsoft 365 Data Protection Against Ransomware

Barracuda Cloud-to-Cloud Backup provides many capabilities to help prevent attackers from gaining access to your backups and protect your backup data from ransomware.

Backup is the Last Line of Defense

When infected with a ransomware attack, having a backup to restore from is the last line of defense to get your organization fully recovered. It's essential to have backups captured daily for your data so you are always prepared to act if the attack takes place.

Barracuda Cloud-to-Cloud Backup is a SaaS offering that provides a daily backup of your Microsoft 365 data and is always accessible to restore from when there is a ransomware threat or attack.

Immutable Backup Strategy

Barracuda Cloud-to-Cloud Backup maintains immutable backup copies by preventing direct access to the data as well as protecting against data modification or removal via API. This prevents access or removal of backup data by any means other than through the Barracuda Cloud-to-Cloud Backup interface, which can also be secured using multi-factor authentication (MFA). In addition, data stored in the Barracuda Cloud is written once and never updated providing an additional layer of protection.

Barracuda Cloud-to-Cloud Backup also protects against unexpected deletion by either cybercriminals and accidental or malicious acts by employees, preventing direct data purges from the backup

interface.

Air Gap Backup Strategy

Keeping your backup system and storage outside of your network creates a separation layer between production data and the backup copy. This mechanism will ensure that if your network gets infected with ransomware, the actual backup remains unaffected since it is not hosted within your network.

Barracuda Cloud-to-Cloud Backup is a fully SaaS based solution where all the backup system and data is kept separate from your network and the source data in Microsoft 365. Additionally, Barracuda Cloud-to-Cloud Backup uses separate containers to store each customer's data. Each backup is then stored as 3 separate copies as an extra security measure in the event the backup copies are impacted.

End-to-End Data Encryption

Encryption renders the backup data unreadable if an attacker has gained access to the data. Barracuda Cloud-to-Cloud Backup provides AES 256-bit encryption of data at rest in the cloud and TLS encryption for data that is moved from the source to the secure cloud location.

Multi-Factor Authentication (MFA)

Multi-Factor Authentication provides an additional layer of security to the accounts and credentials used to access Barracuda Cloud-to-Cloud Backup. With MFA, the attackers not only need the login and password, but they also need a secondary device and application to confirm the identity of the backup administrator.

Role-Based Access Control

Following the principle of least privilege, users accessing the backup system should only be given privileges that are essential to their specific role. With Barracuda Cloud-to-Cloud Backup, you can assign various user roles, including account administrators, limited users with specific permissions. This minimizes the chances of an attacker accessing the backup system with the most powerful administrative privileges.

Conclusion

Cybercriminals continue to advance their attacks to gain access and cause harm to many organizations. It is very important to consider all the different threat vectors cybercriminals are using to launch harmful attacks that can potentially run organizations out of business. Barracuda can help you find the optimal solution to detect, prevent, and recover from ransomware attacks. For more information on how Barracuda can further help protect you from ransomware,

see https://www.barracuda.com/ransomware.