LEARNING MADE EASY

10 Tips for Preventing and Recovering from a Ransomware Attack

Ramsomware, or malware that allows an attacker to hold an organization's data for ransom, is one of the most feared types of cyber attack. Most organizations depend on their data to carry out day-to-day operations, and denying them access to it can be detrimental to business operations and even its future trajectory.

The best-case scenario is preventing a ransomware attack from happening. But if your organization is attacked, you'll want to recover as fast as possible — without paying the ransom, of course. That probably seems like a daunting task, but it doesn't have to be. With some preparation and a plan in place, your organization can restore normal operations quickly with minimal data loss. This checklist gives you ten tips for first preventing and, if that isn't possible, recovering from a ransomware attack.

1. Train your users to avoid a ransomware attack

The best kind of attack is the one that never happens. In this case, that means training your users to not fall victim in the first place. Teach everyone in your organization how to recognize common ransomware attack methods, and provide a way for them to report suspicious messages or websites.

2. Turn on email filtering

Today's mail servers either include options or support add-ons to filter mail messages and attachments for suspicious content. Research how to enable this feature for your mail server and use it.

3. Identify critical applications

Take inventory of your organization's critical business functions as well as the applications and data each one needs to operate. Create an inventory of data that is critical to your organization's operations.

REMEMBER

The inventory of critical data should be the focus of your protection and recovery efforts.

4. Back up data to an immutable destination

Frequently back up all the data from your inventory of critical data to a cyber recovery provider that ensures immutability so bad actors can't encrypt or modify your backups.

5. Use backups to minimize the impact from attacks

Choose a backup service provider that provides insights on data that is at risk for exposure and data that might have been affected by threat indicators to reduce impact and accelerate recovery.

6. Develop and validate a recovery plan

Develop a formal plan for recovering data. Document the conditions under which you should recover, who will carry out the recovery operations, how to identify what to recover, and how to recover identified data. Have automated testing and validation procedures to continuously test if recovery plans will actually work.

7. Train and deploy an incident response team

Assemble a team of personnel with the express purpose of responding to a suspected ransomware attack. The team should be fully versed in the recovery plan and comfortable with their clearly defined roles.

REMEMBER

Ensure each team member participates in frequent tests to keep everyone ready to respond whenever the demand arises.

8. Create templates for automated recovery

When you need to activate your plan, all you should need to provide is a list of data to recover. That means your plan should include script templates to carry out the recovery process for just the data you need to recover. Script templates also give you the ability to test the recovery process and fine-tune it.

9. Test your plan frequently

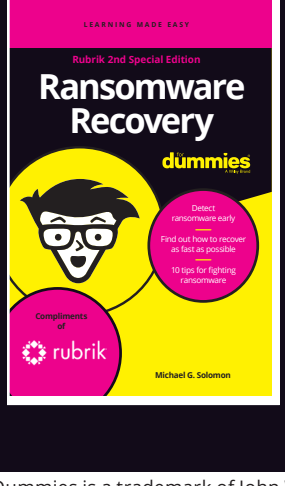
Test the entire recovery plan frequently. The only valid plan is one that meets your recovery point objective (RPO) and recovery time objective (RTO) requirements. Ensure everyone on the incident recovery team is comfortable with their roles and the plan flow.

REMEMBER

Frequently test to validate the plan's effectiveness in changing environments and keep personnel fresh and ready to go.

10. Monitor data for suspicious changes

Implement file integrity monitoring on production filesystems to detect suspicious changes, such as those consistent with ransomware. You should also implement monitoring for backup locations. Any unauthorized backup changes or unusual changes to previously backed up data should be noted. Ensure your cyber recovery provider delivers alerts for suspicious changes.



Learn more about how you can protect your data and your organization with *Ransomware Recovery For Dummies, Rubrik Special Edition.*

Read the ebook

rubrik

for dummies®
A Wiley Brand

Wiley part no.: 9781394188413