Ransomware prevention best practices

Ransomware is a sophisticated class of malware in which data is held hostage until a ransom is paid. Some of the most common ways ransomware infiltrates organizations is through phishing emails, corrupted websites, and malicious extensions. By adopting proactive security measures and developing a well-structured ransomware response plan, organizations can significantly reduce the risk of falling victim to these extortion-driven cyberattacks. Here are some effective strategies to protect against ransomware, methods for prevention, and steps for swift recovery in the unfortunate event of a ransomware attack.

8 best practices to protect against ransomware

Prevention plan

1. **Back up your files**
   Use the 3-2-1 backup rule: Keep at least three separate versions of data (one original and two backups), on two different storage types, and at least one copy offsite.

2. **Patch vulnerabilities**
   Reduce the vulnerabilities in your operating systems, browsers, antivirus software, and other applications by regularly updating them.

3. **Employ email filtering**
   Block malicious executables, spam, phishing, and other common email attacks that ransomware is known to use.

4. **Provide the least amount of privilege possible**
   Use robust access management to restrict unwarranted access and reduce the number of access points through which malware can enter your organization.

5. **Educate end users**
   Conduct periodic training for your employees on how to identify and avoid common ransomware pitfalls such as malvertisements, phishing emails, etc.

6. **Use an intrusion detection system**
   Cut off ransomware attacks in their early stages using continuous monitoring to detect signs of anomalous or malicious activity in real time, allowing you to respond instantly.

7. **Logically separate networks**
   Split your network into multiple logical segments so that you can isolate it in the event of a ransomware attack.

8. **Respond effectively after a ransomware attack**
   Response plan

Response plan

1. **Disable infected systems**
   Isolate and disconnect infected systems immediately from the network to prevent further spread and minimize damage.

2. **Report the attack**
   Notify the appropriate internal parties (incident response team, legal counsel, and shareholders) and external parties (law enforcement, compliance agencies, etc.) about the ransomware incident promptly.

3. **Assess patient zero**
   Determine the user account with which the attack was initiated, and decide if the user's permissions and privileges need to be revoked to prevent future attacks.

4. **Identify the ransomware variant**
   Check the file extensions, ransom note, and coding style to identify the type and variant of the ransomware.

5. **Restore backups and recover data**
   Use verified and clean backups, preferably one from an offsite location, to restore affected systems and data to their pre-attack state.

6. **Identify the root cause**
   Start a post-incident response analysis to find out how the ransomware breached the system, which vulnerabilities were exploited, and how to prevent future occurrences.

7. **Temporarily pause maintenance tasks**
   Disable regular maintenance tasks, such as deleting temporary files, analyzing disk usage, carrying out updates, etc., until the investigation is complete as they may interfere with forensic analysis.

8. **Create a prevention and response checklist**
   View checklist

How to prevent ransomware attacks in your organization

Monitor network and system activity for unusual patterns, such as a sudden increase in file modifications or encryption attempts. Advanced threat detection tools like DataSecurity Plus can identify such ransomware signatures and behaviors early on, and help you set up an alert and response system to shut down infected systems right at their inception.

See how DataSecurity Plus' automated ransomware response mechanism works in action

Next steps

- Free trial
  Set up and evaluate DataSecurity Plus's capabilities with a free, fully functional 30-day trial.
- Interactive demo
  View an online instance of DataSecurity Plus (available without signing up).
- Guided product tour
  Schedule a demo to have a product expert walk you through the software and answer your questions.
- Request a quote
  View pricing details and request a personalized quote

About DataSecurity Plus

ManageEngine DataSecurity Plus is a unified data visibility and security platform. It audits file changes in real time, triggers instant responses to critical events, shuts down ransomware intrusions, and helps organizations comply with numerous IT regulations. It also analyzes file storage and security permissions, deletes junk files, and detects file security vulnerabilities. Users can assess the risks associated with sensitive data storage by locating and classifying files containing PII, PCI, and ePHI. It also prevents data leaks via USBs, email, printers, and web applications; monitors file integrity; and audits cloud application usage.

$ Get Quote

⤓ Download free trial