ManageEngine
FileAudit Plus

Ransomware
Prevention and Response Checklist

Ransomware prevention checklist

Preventive measures at the user level

- ☑ Conduct security awareness training and educate your end users about ransomware attacks.
- ☑ Train your end users to spot and report phishing emails containing malicious attachments.

Preventive measures at the software level

- ☑ Ensure your firewalls are operational and up-to-date at all times.
- ☑ Logically separate your networks.
- ☑ Employ a strong email filtering system to block spam and phishing emails.
- ☑ Patch vulnerabilities and keep all your software updated.
- ☑ Set up rigorous software restriction policies to block unauthorized programs from running.
- ☑ Keep your antivirus fully operational and up-to-date.
- ☑ Conduct periodic security assessments to identify security vulnerabilities.
- ☑ Enforce the principle of least privilege.
- ☑ Disable Remote Desktop Protocol (RDP) when not in use.
- ☑ Disable macros in your Microsoft Office files.
- ☑ Use a strong, real-time intrusion detection system to spot potential ransomware attacks.

Preventive measures at the backup level

- ☑ Back up your files using a 3-2-1 backup rule, i.e. retain at least three separate copies of data on two different storage types, with at least one of those stored offline.
- ☑ Ensure that you back up critical work data periodically.
- ☑ Enforce regular checks for data integrity and recovery on all your backups.

Ransomware
response checklist

Time-sensitive reactive measures

- ☑ Shut down infected systems immediately.
- ☑ Disconnect and isolate infected systems from the network.
- ☑ Isolate your backups immediately.
- ☑ Disable all shared drives that hold critical information.
- ☑ Issue an organization-wide alert about the attack.
- ☑ Contact your local law enforcement agency and report the attack.

Analysis-based reactive measures

- ☑ Determine the scope and magnitude of an infection by identifying the type and number of devices infected, as well as what kind of data was encrypted.
- ☑ Determine the type and version of the ransomware.
- ☑ Identify the threat vector used to infiltrate your network.
- ☑ Conduct root cause analysis.
- ☑ Mitigate any identified vulnerabilities.
- ☑ Check if a decryption tool is available online.

Business continuity reactive measures

- ☑ Restore your files from a backup.

Additional **resources**

Step-by-step guide to detect and respond to ransomware attacks.

Know more >

8 best practices to prevent future ransomware attacks.

Know more >

Infographic on HIPPA guidelines on ransomware attacks.

Know more >

Infographic on how to protect your organization from ransomware attacks.

Know more >

Ebook FBI recommendations to prevent ransomware attacks.

Know more >

FileAudit Plus

FileAudit Plus is real-time Windows file server auditing and analysis software that monitors, audits, alerts, and reports on all file accesses and modifications made in your file server environment. Furthermore, it:

- Monitors file integrity.
- Provides detailed analysis on file storage.
- Streamlines compliance requirements.
- Generates instant, user-defined email alerts.
- Automatically executes predefined responses when security threats such as ransomware attacks occur.

Key features of FileAudit Plus

Audit file accesses & changes: Obtain detailed information on the quintessential four W's—who accessed what, when, and from where—for all file and folder accesses and modifications.

Analyze disk usage pattern: Analyze file storage capacity with visual representation and gain insight into the storage space usage patterns using disk space trend analysis graph.

Optimize file storage: Identify and discard old, large, unmodified, non-business files, hidden, and orphaned files to de-clutter your storage space.

Combat ransomware attacks: Detect and shut down ransomware attacks right at their inception with an automated threat response mechanism and also get notified with instant, user-defined alerts.

Monitor file permissions: Gain visibility into your file permissions and identify who has access to do what to your sensitive files.

File integrity monitoring: Detect and alert on unauthorized changes to your file server environment through continuous real-time monitoring.

Compliance reports: Ensure compliance with multiple external regulatory standards such as PCI DSS, HIPAA, FISMA, GDPR, SOX, and GLBA.