RANSOMWARE
Hostage Rescue Checklist

NEW EDITION

Cybercrime Has Gone Pro

Ransomware attacks cause downtime, data loss, possible intellectual property theft, and in certain industries a ransomware attack is considered a data breach.

Wouldn’t it be great to have an actionable checklist of what to do when you get hit and how to prevent it in the future? Now you do!

• Ransomware Attack Response Checklist
• Ransomware Prevention Checklist

Don’t be taken hostage by ransomware.

www.KnowBe4.com
KnowBe4
Ransomware Attack Response Checklist

STEP 1: Initial Investigation
☐ a. Determine if it is a real ransomware attack
☐ b. Determine if more than one device is exploited

If so, continue:

STEP 2: Declare Ransomware Event and Start Incident Response
☐ a. Declare ransomware event
☐ b. Begin using predefined, alternate communications
☐ c. Notify team members, senior management and legal

STEP 3: Disconnect Network
☐ a. Disable networking (from network devices, if possible)
☐ b. Power off devices if wiperware is suspected

STEP 4: Determine the Scope of the Exploitation
Check the Following for Signs:
☐ a. Mapped or shared drives
☐ b. Cloud-based storage: Dropbox, Google Drive, OneDrive, etc.
☐ c. Network storage devices of any kind
☐ d. External hard drives
☐ e. USB storage devices of any kind (USB sticks, memory sticks, attached phones/cameras)
☐ f. Mapped or shared folders from other computers

Determine if data or credentials have been stolen
☐ a. Check logs and DLP software for signs of data leaks
☐ b. Look for unexpected large archival files (e.g., zip, arc, etc.) containing confidential data that could have been used as staging files
☐ c. Look for malware, tools and scripts that could have been used to look for and copy data
☐ d. Of course, one of the most accurate signs of ransomware data theft is a notice from the involved ransomware gang announcing that your data and/or credentials have been stolen
**Determine Ransomware Strain**
- a. What strain/type of ransomware? For example: Ryuk, Dharma, SamSam, etc.

**STEP 5: Limit Initial Damage**
- a. Initial investigators should try to stop/reduce any damage they discover, if possible

**STEP 6: Gather Team to Share Information**
- a. The goal is to make sure the team correctly understands all information, including scope and extent of damage

**STEP 7: Determine Response**
- a. Pay the ransom or not?
- b. Repair or rebuild?
- c. Invite in additional external parties?
- d. Notify regulator bodies, law enforcement, CISA, FBI, etc.?

**STEP 8: Recover Environment**
- a. Repair only or rebuild
- b. Need to preserve evidence?
- c. Use business impact analysis to determine what devices and systems to recover and the associated timing
- d. Restore critical infrastructure first

**Step 9: Next Steps**

Prevent the Next Cyber Attack:
- a. Mitigate social engineering
- b. Patch software
- c. Use multi-factor authentication (MFA) where you can
- d. Use strong, unique passwords
- e. Use antivirus or endpoint detection and response software
- f. Use anti-spam/anti-phishing software
- g. Use data leak prevention (DLP) software
- h. Have a good back up and regularly test
First Line of Defense: Software
- Ensure you have and are using a firewall.
- Implement antispam and/or antiphishing. This can be done with software or through dedicated hardware such as SonicWALL or Barracuda devices.
- Ensure everyone in your organization is using the very latest generation endpoint protection, and/or combined with endpoint protection measures like whitelisting and/or real-time executable blocking.
- Implement a highly disciplined patch procedure that updates any and all applications and operating system components that have vulnerabilities.
- Make sure that everyone who works remotely logs in through a VPN.

Second Line of Defense: Backups
- Implement a backup solution: Software-based, hardware-based, or both.
- Ensure all possible data you need to access or save is backed up, including mobile/USB storage.
- Ensure your data is safe, redundant and easily accessible once backed up.
- Regularly test the recovery function of your backup/restore procedure. Test the data integrity of physical backups and ease-of-recovery for online/software based backups for at least three or four months in the past. Bad actors lurk in your networks for months and can compromise your backups.

Third Line of Defense: Data and Credential Theft Prevention
- Implement Data Leak Prevention (DLP) tools.
- Use least-permissive permissions to protect files, folders, and databases.
- Enable system logs to track data movements.
- Use network traffic analysis to note any unusual data movements across computers and networks.
- Encrypt data at rest to prevent easy unauthorized copying.

Fourth and Last Line of Defense: Users
- Implement new-school security awareness training to educate users on what to look for to prevent criminal applications from being downloaded/executed.
- Your email filters miss between 5% and 10% of malicious emails, so conduct frequent simulated phishing attacks to inoculate your users against current threats; best practice is at least once a month.