KnowBe4

Ransomware Attack Response Checklist

STEP 1: Disconnect Everything

□ a. Unplug computer from network

□ b. Turn off any wireless functionality: Wi-Fi, Bluetooth, NFC

STEP 2: Determine the Scope of the Infection, Check the Following for Signs of Encryption

□ a. Mapped or shared drives

□ b. Mapped or shared folders from other computers

□ 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. Cloud-based storage: DropBox, Google Drive, OneDrive etc.

STEP 3: Determine Ransomware Strain

□ a. What strain/type of ransomware? For example: CryptoWall, Teslacrypt etc.

STEP 4: Determine Response

Now that you know the scope of your encrypted files as well as the strain of ransomware you are dealing with, you can make a more informed decision as to what your next action will be.

Response 1: Restore Your Files From Backup

□ 1. Locate your backups
   - a. Ensure all files you need are there
   - b. Verify integrity of backups (i.e. media not reading or corrupted files)
   - c. Check for Shadow Copies if possible (may not be an option on newer ransomware)
   - d. Check for any previous versions of files that may be stored on cloud storage e.g. DropBox, Google Drive, OneDrive

□ 2. Remove the ransomware from your infected system

□ 3. Restore your files from backups

□ 4. Determine infection vector & handle

Response 2: Try to Decrypt

□ 1. Determine strain and version of the ransomware if possible

□ 2. Locate a decryptor, there may not be one for newer strains

If successful, continue steps...

□ 3. Attach any storage media that contains encrypted files (hard drives, USB sticks etc.)

□ 4. Decrypt files

□ 5. Determine the infection vector & handle

Response 3: Do Nothing (Lose Files)

□ 1. Remove the ransomware

□ 2. Backup your encrypted files for possible future decryption (optional)

Response 4: Negotiate and/or Pay the Ransom

□ 1. If possible, you may attempt to negotiate a lower ransom and/or longer payment period

□ 2. Determine acceptable payment methods for the strain of ransomware: Bitcoin, Cash Card etc.

□ 3. Obtain payment, likely Bitcoin:

a. Locate an exchange you wish to purchase a Bitcoin through (time is of the essence)

b. Set up account/wallet and purchase the Bitcoin

□ 4. Re-connect your encrypted computer to the internet

□ 5. Install the TOR browser (optional)

□ 6. Determine the Bitcoin payment address. This is either located in the ransomware screen or on a TOR site that has been set up for this specific ransom case

□ 7. Pay the ransom: Transfer the Bitcoin to the ransom wallet

□ 8. Ensure all devices that have encrypted files are connected to your computer

□ 9. File decryption should begin within 24 hours, but often within just a few hours

□ 10. Determine infection vector and handle

STEP 5: ProtectingYourselt in the Future

□ a. Implement Ransomware Prevention Checklist to prevent future attacks

KnowBe4

Ransomware Prevention Checklist

First Line of Defense: Users

□ 1. Implement effective security awareness training to educate users on what to look for to prevent criminal applications from being downloaded/executed.

□ 2. Conduct simulated phishing attacks to inoculate users against current threats.

Second Line of Defense: Software

□ 1. Ensure you have and are using a firewall.

□ 2. Implement antispam and/or antiphishing. This can be done with software or through dedicated hardware such as SonicWALL or Barracuda devices.

□ 3. Ensure everyone in your organization is using top notch up-to-date antivirus software, or more advanced endpoint protection products like whitelisting and/or real-time executable blocking. You could also use Microsoft's free AppLocker but it's a bit cumbersome.

□ 4. Implement software restriction policies on your network to prevent unauthorized applications from running. (optional)

□ 5. Implement a highly disciplined patch procedure that updates any and all applications that have vulnerabilities.

Third Line of Defense: Backups

□ 1. Implement a backup solution: Software based, hardware based, or both.

□ 2. Ensure all possible data you need to access or save is backed up, including mobile/USB storage.

□ 3. Ensure your data is safe, redundant and easily accessible once backed up.

□ 4. 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.

KnowBe4
Human error. Conquered.

About KnowBe4

KnowBe4 is the world's most popular integrated Security Awareness Training and Simulated Phishing platform. Realizing that the human element of security was being seriously neglected, KnowBe4 was created by two of the best known names in cybersecurity, Kevin Mitnick (the World's Most Famous Hacker) and Inc. 500 alum serial security entrepreneur Stu Sjouwerman, to help organizations manage the problem of social engineering tactics through new school security awareness training.

More than 1,500 organizations use KnowBe4's platform to keep employees on their toes with security top of mind. KnowBe4 is used across all industries, including highly regulated fields such as finance, healthcare, energy, government and insurance.

- KnowBe4's infrastructure can scale up to very large enterprises, but also scale down to a small enterprise with just 50 employees.
- KnowBe4 wrote the book on cyber security (8 books and counting between Mitnick and Sjouwerman).
- KnowBe4 is the only set-it-and-forget-it security awareness training platform "by admins for admins" with minimum time spent by IT to get and keep it up and running.
- The platform includes a large library of known-to-work phishing templates.

KnowBe4
Human error. Conquered.

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755 | Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: Sales@KnowBe4.com