BACS CONSULTING GROUP

Ransomware Attack Response Checklist

STEP 1: Initial Investigation

□ Determine if it is a real ransomware attack

□ Determine if more than one device is exploited

If so, continue:

STEP 2: Declare Ransomware Event and Start Incident Response

□ Declare ransomware event

□ Begin using predefined, alternate communications

□ Notify team members, senior management and legal.

Depending on contracts with 3rd parties and/or business partnerships, they may need to be informed as well.

STEP 3: Disconnect Network

□ Disable networking (from network devices, if possible), or isolate from production network.

□ Disable Bluetooth if enabled.

□ Power off devices if wiper malware is suspected

STEP 4: Determine the Scope of the Exploitation

1. Check the Following for Signs:

- □ Mapped or shared drives
- □ Cloud-based storage: Dropbox, Google Drive, OneDrive, etc.
- □ Network storage devices of any kind
- □ External hard drives
- □ USB storage devices of any kind (USB sticks, memory sticks, attached phones/cameras)
- □ Mapped or shared folders from other computers

2. Determine if data or credentials have been stolen

- □ Check logs and DLP software for signs of data leaks
- □ Look for unexpected large archival files (e.g., zip, arc, etc.) containing confidential data that could have been used as staging files
- □ Look for malware, tools and scripts that could have been used to look for and copy data
- □ 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, and your files may have been encrypted.

3. Determine Ransomware Strain

- □ What strain/type of ransomware? For example: Ryuk, Dharma, SamSam, etc.

STEP 5: Limit Initial Damage

- □ Initial investigators should try to stop/reduce any damage they discover, if possible

STEP 6: Gather Team to Share Information

- □ The goal is to make sure the team correctly understands all information, including scope and extent of damage

STEP 7: Determine Response

- □ Pay the ransom or not?
- □ Repair or rebuild?
- □ Invite in additional external parties?
- □ Notify regulator bodies, law enforcement, CISA, FBI, etc.

STEP 8: Recover Environment

□ Repair only or rebuild

□ Need to preserve evidence?

□ Use business impact analysis to determine what devices and systems to recover and the associated timing

□ Restore critical infrastructure first

Step 9: Next Steps

Prevent the Next Cyber Attack:

□ Mitigate social engineering

□ Patch software

□ Use multi-factor authentication (MFA) where you can

□ Use strong, unique passwords/pass-phrases

□ Use anti-virus or endpoint detection and response software Use anti-spam/anti-phishing software

□ Use data leak prevention (DLP) software

□ Have a good back up and regularly test

First Line of Defense: Software

1. Ensure you have and are using a firewall.
2. Implement anti-spam and/or anti-phishing. This can be done with software or through dedicated hardware (SonicWALL or Barracuda devices to name a few).
3. Ensure everyone in your organization is using the very latest generation endpoint protection, and/or combined with endpoint protection measures like white-listing and/or real-time executable blocking.
4. Implement a highly disciplined patch procedure that updates any and all applications and operating system components that have vulnerabilities.
5. Make sure that everyone who works remotely logs in through a VPN.

Second Line of Defense: Backups

1. Implement a backup solution: Software-based, hardware-based, or both.
2. Backups should be stored off site, (a secured facility or in the cloud), in case a natural disaster occurs (fires, floods, etc) at the physical business location.
3. Ensure all possible data you need to access or save is backed up, including mobile/ USB storage.
4. 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

1. Implement Data Leak Prevention (DLP) tools.
2. Use least-permissive permissions to protect files, folders, and databases.
3. Enable system logs to track data movements.
4. Use network traffic analysis to note any unusual data movements across computers and networks.
5. Encrypt data at rest to prevent easy unauthorized copying.

Fourth and Last Line of Defense: Users

1. Implement security awareness training to educate users on what to look for and how to react in order to prevent malicious applications from being downloaded/ executed.
2. 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.

Ransomware Attack Response Checklist

(650) 383-4248

BACS CONSULTING GROUP