Ransomware Response Checklist

LMGsecurity.com

When you are infected with ransomware, time is of the essence! Ransomware spreads very quickly, encrypting your computer, networked file share, and even attached cloud storage. Act fast and you may be able to save data, or at least recover it quickly. Here is a checklist for you, your colleagues and friends.

1. **Pull the network cable out and/or disconnect from your wireless network.** Immediately disconnect any USB drives. Remember, ransomware will crawl through your system encrypting files. You want to stop it from locking up files on any shared drives or backup drives that you have attached to your system.

2. **Call IT right away.** They may advise you to pull your computer's plug out of the wall or remove the battery if it is a laptop. The way you shutdown is important. If you try to shut your computer down by just pressing a button, some ransomware can prevent the computer from shutting down.

3. **Quickly figure out what was encrypted.** If you have backups for that data, GREAT! This really underscores the importance of taking regular backups, every single day, automatically.

4. **Check to see if the ransomware has a known bypass**. Especially, if you can't restore from backups. There are certain tools available for some kinds of ransomware that can decrypt your files. Here is a useful site: www.nomoreransom.org.

5. **If all else fails, you may choose to pay the ransom.** If you're going to do it, do it quickly before the price goes up. If you don't have Bitcoin on hand, call an experienced security firm (such as LMG) to take care of the transaction for you.

6. **Talk to legal counsel immediately.** If there's a chance you have sensitive or regulated data on any computer that was encrypted (such as personal information, Social Security Numbers, health care information, or other sensitive data). **Ransomware infections may be considered a data breach** in certain circumstances.

7. **Finally, consider reporting the ransomware attack to the FBI.** They are tracking these cases. Either contact your local field office, or go to the Internet Crime Complaint Center at www.ic3.gov.

To see ransomware in action, check out LMG's research project, "Watch Ransomware Wreak Havoc in the Cloud" on the LMG Security Blog: https://lmgsecurity.com/blog/