TEN TIPS TO AVOID RANSOMWARE

1. ACKNOWLEDGE AND UNDERSTAND THE THREAT

Crypto ransomware works by encrypting certain sensitive file types and then forcing the victim to pay a ransom to gain access to a decryption key for the data. With nearly all types of crypto ransomware it's virtually impossible to recover data without paying for the decryption key. Sometimes even paying the ransom won't decrypt the files.

2. EDUCATE USERS

It only takes a single bad decision by a user to unleash a costly ransomware attack. Ransomware is often delivered as a Trojan through malvertising, or through a phishing email. Prevention isn't possible 100% of the time, but in many cases attacks can be stopped if users have been trained to become familiar with the possible threats.

3. GET EXECUTIVES INVOLVED

When it comes to policy compliance, executives are often the most prone to breaking the very policies they authorized in the first place, (think CEO flying to Tokyo on a trip and streaming Netflix for several hours while roaming). On the other end of the spectrum, when executives take this stuff seriously, so do other employees.

4. TEACH A MAN TO PHISH? NOPE, TEACH A MAN NOT TO PHISH

Recent studies have shown that up to 50% of organizational end users will fall for a phishing attack in 2016. While security can be inconvenient, it is critical that users learn to avoid opening emails from unknown senders with attachments or links, while also learning how to spot suspicious emails even when they look like they're from known senders. Instruct users on spotting expressions or greetings the sender wouldn't normally use as clues to something "phishy." If all else fails, real-time anti-phishing protection can often block even zero-day phishing attacks.

5. MAINTAIN LAYERS OF ANTI-RANSOMWARE TECHNOLOGY

Reliable, cloud-based anti-malware can prevent nearly all ransomware attacks, but it's important to remember that new delivery vectors are being released constantly, so no endpoint security solution alone will provide a perfect security posture. Additional security layers like firewalls, Windows OS policy restrictions, and having proper back-ups in place will all help to secure your environment.

6. PATCHING AND PLUGINS

Keeping applications like Adobe Reader, Java, and other plugins up to date greatly reduces security vulnerabilities and prevents browser and application vulnerabilities that may bypass your anti-malware. Ad and pop-up blockers also greatly reduce user error by stopping users from clicking fake dialogue boxes that download ransomware.

7. DISABLE VOLUME SHADOW COPY SERVICE VSS

Shadow Volume Copies have been a Windows feature since the ill-fated Vista. This tool allows snapshots, or backups, of your files to be saved even when the files are currently in use. This same technology is also used by the Windows' System Restore feature that allows you to roll back Windows to a previously working configuration in case there is a problem. Since Vista, Microsoft has been bundling a utility called vssadmin.exe in Windows that allows an administrator to manage these copies that are on the computer, but with ransomware, this tool has become more of a problem than a benefit and in most cases, it should probably be disabled.

8. FILTER .EXE FILES IN EMAIL SERVERS

If your customers' email gateways can filter files by extension, you should consider denying emails sent with .EXE files, or denying emails sent with files that have two file extensions, the last one being an executable ("*.*.EXE" files). This is a common threat vector for ransomware.

9. ALWAYS HAVE A BACK UP

Nothing is more effective at mitigating a ransomware attack than knowing your organization can instantly restore data from business continuity backups. Ransomware such as CryptoLocker can even encrypt networked drives. Having offline air gaps or cloud back-ups with multiple copies of each file makes it virtually impossible for extortionists to infect backup data.

10. STAY CURRENT ON RANSOMWARE

It pays to keep up with ransomware developments. Some ransomware strains have been cracked, but these are limited successes. Ransomware, like all malware, will continue to evolve.