Strong Technology

WannaCry Ransomware Security Update

In light of the recent "WannaCry" ransomware outbreak that has been hitting businesses around the globe, we thought it pertinent to update you on the security practices we at Strong Technology are implementing to help prevent you from falling victim to malware.

Trend Micro:

There is no silver bullet fix when it comes to protecting your systems against infection. However, there are ways you can minimize your risks. Trend Micro Anti-Virus acts as your first line of defense against malware, protecting your business at every entry point and allowing us to monitor your systems for any potential, or active, threats.

Worry Free Business Security:

Trend Micro detected 99% of all ransomware threats in email messages or web links. That leaves 1% that could make it through to your endpoint. Trend Micro Worry Free Services minimizes the risk of ransomware to your endpoints through:

- **Behavior Monitoring** for suspicious behavior associated with ransomware, such as the rapid encryption of multiple files, so that the encryption process can be automatically stopped and the endpoint isolated, before ransomware can spread and cause more damage to your data
- **Real-Time Web Reputation** to determine if a URL is a known delivery vehicle for ransomware

Hosted Email Security:

- **Detects and blocks** ransomware with malware scanning and file risk assessment
- **Gives you advanced threat protection** with sandbox malware analysis and document exploit detection
- Uses **web reputation** to protect against web links in emails that are malicious

Daily and Weekly Monitoring:

As part of your Trend Micro monthly service agreement, Strong Technology runs reports on your Trend Micro protected systems on both a daily, and weekly basis, allowing us to monitor any influxes in threats and alert you to any potential vulnerabilities or infections.

Software Updates:

If there is anything to learn from this week's WannaCry attack, it is the importance of keeping your operating systems up to date. While Microsoft released a patch in March that addressed and fixed the Windows vulnerability used by the WannaCry virus, rendering it ineffective against updated systems, businesses in 150 different countries running legacy (unsupported) software, like Windows XP and Vista, were unable to receive this vital update.

Upgrading to new versions of Windows:

One of the reasons WannaCry's ransomware has been able to infect the computers of over 200,000 people across the globe is due to the number of companies and individuals running either pirated versions of Microsoft operating systems or legacy software such as Windows XP, both of which are unsupported by Microsoft and unable to receive updates, such as the one that addressed the vulnerability exploited by the WannaCry virus.

If you are currently using Windows XP on any of your computers, we at Strong Technology strongly suggest that you upgrade to a supported Windows operating system as soon as possible. If you are unsure whether any of your computers are currently running Windows XP or Vista, *feel free to give us a call at: (509) 468-1615.*

Monthly, Bi-Monthly, or Quarterly Updates:

While running supported versions of Windows (such as Windows 7, 8, and 10) ensures that you are able to access software updates from Microsoft, unless these updates are regularly installed your computers will still be open to malware attacks that exploit software vulnerabilities, such as the one used by this week's WannaCry virus.

Strong Technology can make sure that these updates are routinely and remotely installed on either a monthly, bi-monthly, or quarterly basis. If you are unsure if we are currently performing these updates, or would like us to begin providing this service for your business, *please give us a call at: (509) 468-1615.*

Intronis Cloud Backup and Recovery:

Your Backup and Recovery Strategy is just as important as your everyday security policies and procedures. That's why we recommend that you use Intronis Cloud Backup, allowing you to recover and restore data if disaster (like ransomware) strikes.

Staff Training:

It all starts with your users. They are the most vulnerable when it comes to ransomware- whether its falling for a phishing email or clicking on a malicious web link- making your staff your first, and last, line of defense.

Social Engineering:

Cybercriminals know that the easiest way for them to get into your system is by having a user open a door for them. That's why they use social engineering to trick users into downloading virus infected files or clicking on malicious links. However, with a little time and training you can teach yourself, and your staff how to spot these tactics and avoid falling victim to the various ways cybercriminals try to break through your defenses.

If you are interested in learning more about the common social engineering tactics being used by cybercriminals and would like to schedule a staff training or would like our assistance to review/create your own technology policies and procedures, *give us a call at: (509) 468-1615.*

(We also post a number of articles regarding this topic on both Facebook and LinkedIn)

Limiting Internet Access:

Unfortunately, there is no such thing as a system that is completely safe from viruses and malware. However, there are ways you can help mitigate your risk of getting infected. That is why we at Strong Technology strongly suggest that you limit internet access at your office. Work computers are for work, and while checking Facebook or reading the latest news during your break may seem harmless, it's not. In fact, you'd probably be surprised at just how easy it is to get a virus while browsing the web, even if you're only going to well-known and seemingly "reputable" sites. By only allowing your computers to access business-critical sites, you can help protect yourself from unwanted expenses stemming from ransomware and other malicious infections.

WiFi Access and BYOD:

In this day and age, it is especially important that your staff is aware of the dangers that can come with WiFi and BYOD (Bring your own devices) in the workplace. Many of us use laptops, cellphones, and other wireless devices to take our work with us wherever we go. However, these outside devices (anything that has connected to the web or other computers, such as USB devices) come with a number of security risks, mainly due to the number of unknown variables that they bring into the mix. Any one of these devices can, unbeknownst to us, be carrying a virus on it. As a result, connecting these devices to a production network via WiFi or USB can potentially allow these viruses to move onto your business network, thus giving cybercriminals easy access to important documents and sensitive information.

If you are interested in having Strong Technology help you review your current security policies and procedures or address any potential security vulnerabilities or concerns you may have, don’t hesitate to give us a call at: (509) 468-1615