darby techforce

powered by HTI

Ransomware 101:

Your Guide to Prevent, Detect and Respond

With ransomware attacks on the rise, cybersecurity should be a top priority for your practice this year. These costly attacks can devastate businesses through prolonged downtime, lost data, and substantial financial damages – the average cost of which was $178,254 in 2020! Plus, when it comes to the healthcare and dental industry, HIPAA compliance is also at stake. Read on to stay informed about this growing threat and ensure your systems are protected.

What is ransomware?

Ransomware is a type of malware that denies businesses access to their data by encrypting files until a ransom has been paid. According to Bitdefender, ransomware attacks have increased by more than 74% from the first half of 2018 to the first half of 2019 – and they show no sign of slowing down. Common symptoms to look out for include inaccessible files, corrupted messages, warnings of a file lock, a countdown clock with instructions or seeing "decrypt" added to your locked file names.

What do I do if I've been infected?

If you suspect you've been infected, immediately unplug all wired devices and disconnect wireless devices. If possible, determine workstation zero and do not attempt to run any "clean up" programs or erase anything from your devices. Do not attempt to pay the ransom or negotiate with the cybercriminals. This encourages attacks to continue and plus, there is no guarantee that if you do pay the ransom, the hackers will honor the terms of your agreement.

Once you've completed these steps, contact your IT provider so that they can determine the scope of the attack and evaluate possible responses. Your provider should already have a comprehensive data backup and business continuity strategy in place in case of such an attack.

How can I prevent an attack?

First, ensure that you and your staff are well-versed in prevention methods such as not clicking on suspicious links, thinking twice before opening email attachments, only downloading files from trusted websites, and using strong computer passwords. Aside from staying vigilant, the best way to prevent an attack is to secure your systems with a ransomware protection software, which provides an extra layer of protection on top of an antivirus software. While conventional antivirus programs protect against viruses that already exist, ransomware is constantly evolving and requires something a bit more sophisticated.

Introducing RansomGuard from Darby TechForce

Ransomware protection is best left to the professionals! At Darby TechForce, our new software "RansomGuard" offers a unique single product that covers prevention, detection and response. This all-in-one endpoint software is focused on identifying and stopping ransomware attacks, even if the technique has never been used before. RansomGuard features:

- **Real-Time Behavioral Detection**: Using a real-time code execution engine, RansomGuard monitors all endpoint processes and is able to predict advanced attacks based on the execution behavior of the suspicious software. By looking for symptoms rather than specific viruses, RansomGuard can detect and prevent ransomware that evades conventional antivirus software.

- **Predictive Execution Inspection**: RansomGuard is able to detect and respond to what is happening on the endpoint, as it happens, which is why it is so effective in finding extremely advanced ransomware. With an antivirus software alone, you are only able to analyze files through "static filters", which are historical and based on what the software has already seen rather than what is happening in real time.

- **Cloud Intelligence**: RansomGuard uses cloud intelligence to block known threats using a unique approach called "passive scanning." It constantly monitors every file and process on the endpoint of the server and sends information to the cloud intelligence service, where it is scanned in real time by dozens of scan engines and leading reputation services. When a known threat is found, it is immediately blocked before the user is exposed to any risk.

- **Roll-Back Feature**: Ransomware specifically relies on encrypting the operating system and files and many of the more advanced variants can eliminate the victim's ability to recover their data. With RansomGuard's roll-back feature, it is able to restore files that have been maliciously encrypted or deleted to their previous state – all with a single click!

To learn more about how Darby TechForce can defend your practice to keep you running safely and smoothly, visit www.darbytechforce.com or call us at (800) 866-2093.