computer dimensions
520.743.7554
info@computerdimensions.net
www.computerdimensions.net

Protect Your Business From Ransomware

On February 5th, Hollywood Presbyterian Medical Center declared a state of emergency. Cyber criminals had hacked into its system and were holding its files hostage. The hospital resorted to pencil and paper, transferred some patients to other hospitals, and temporarily shut down radiation and oncology. Ultimately, the hospital paid the $17,000 ransom in bitcoin to unlock its 'captive' data.

No doubt about it: We live in extreme times. And like practically everything else, ransomware has grown more extreme, emerging as one of the top cybersecurity threats of 2016. It's particularly concerning for mobile users on laptops, who may be working from home or on the road, beyond the enterprise's secure network perimeter.

For starters, ransomware is becoming more sophisticated, acquiring new stealth capabilities to invisibly encrypt data on systems as well as in backups. Other new ransomware variants may use kernel components to encrypt files on the fly, as the user accesses them.

Even the FBI, in fall 2015, warned that certain ransomware variants such as Cryptolocker and Cryptowall were so powerful, enterprises and organizations may not be able to retrieve their data without paying the ransom.

Analysts and experts expect ransomware to become more targeted in 2016, with a focus on the financial industry, local governments, and other organizations, especially those in the United States.

Ransomware will no longer be focused on Microsoft Office, Adobe PDF, and graphic files, as cybercriminals target additional file types used in business environments, McAfee Labs predicts.

Last year, 'Ransomware-as-a-Service' (RaaS), hosted on the anonymous Tor network, began giving even inexperienced cybercriminals access to the necessary extortion tools. Virtual currencies such as bitcoin enable cybercriminals to receive their ransoms anonymously.

Ransom32 is considered a particularly nasty, "undecryptable" new variant. Sold as a service, Ransom32 allows an application to be written once and used on Windows, Macs, and Linux computers, making ransomware easily cross-platform.

We can expect to see other types of digital extortion as well, which is bound to result in monetary gain for criminals, giving them even more incentives to attack. In January 2016, a survey from the Cloud Security Alliance and Skyhigh Networks found that 24.6 percent of companies would pay a ransom to prevent a cyber-attack.

520.743.7554
info@computerdimensions.net
www.computerdimensions.net

Aside from the ransoms paid, enterprises stand to experience significant system downtime, critical data loss, and even intellectual property theft as a result of ransomware.

And all of this is happening at a time when skilled security professionals are in short supply, with an expected shortfall of 1.5 million IT security professionals expected by 2019.

What to Do About Ransomware

*** Utilize VPN software.** Remain vigilant about IT security, and ensure that end user laptops are as secure as possible with VPNs (virtual private network) and up-to-date security software,.

*** Educate users.** Education of end users is the first line of defense. Make sure users are aware that ransomware is often spread through phishing emails and downloads (from compromised websites). Train them how to identify and avoid these and other security threats. Utilize email alerts and security presentations to help educate employees.

*** Perform regular security audits.** Be clear about all areas of potential risk and have a plan to counter them.

*** Back up critical data online as well as on premise.** Automatic, incremental, secure data backups to the cloud can help an enterprise recover files that are being held for ransom, especially if the ransomware has infiltrated on premise servers and backups.

Cybercriminals thrive on exploiting weaknesses in the system. But they make mistakes, too, inadvertently creating weaknesses in their own ransomware that the enterprise IT security industry can exploit. And so, along with the escalating risk of ransomware, we can expect enterprise IT security vendors to rise to the challenge, such as reverse-engineering malware to find its weaknesses.

In other words, the arms race between cybercriminals and IT security is going to be even more extreme in 2016.