Case Study:

Bullet Proof back up and protection against CryptoLocker virus. How proper planning and processes saved a company.

Disaster recovery isn't always a fight against Mother Nature. Sometimes it's a viral attack.

Challenge:

When we talk about disaster recovery we generally go to the worst possible natural disaster hitting our business. More realistically and frequently it's not Mother Nature causing the disaster but hackers and virtual threats. There are various levels of disasters and your business continuity plan should be able to help you carry on through any manor of scenario.

No one can promise prevention of cyber-attacks, the amount of time it takes you to recover from a security breach is how you can measure the impact it has on your business. How much does it cost to run your business for an hour? What would you lose being down for an hour, day, week?

The CryptoLocker Virus is malicious software which, once it's penetrated your computer, begins encrypting files and holding them for ransom. After encrypting your files Crypto sends you a message asking for payment to restore your files or to prevent them from destroying the information. With ransomware like this time if of the essence! The faster you detect and stop them from gaining more access the faster you can get your business back to normal.

Results:

Speed of recovery is key when it comes to keeping damage and costs to a minimum. When the CrypoLocker virus first arose, it was new to antivirus software and security companies. It attacked one of our clients and encrypted thousands of files within minutes. Through proper Anti-Virus management, our software detected the new variant of CryptoLocker virus within 7 minutes. In that short amount of time, the Crypto virus had already encrypted over 8 thousand files. Proper processes allowed us to move quickly once it was detected. Within minutes we were there to restore them to full working order and allow them to conduct business as if nothing had ever happened. In under an hour our team had removed and restored the encrypted files. The client's business was unaffected.

Having proper backup processes in place takes the power away from ransomware. Just backing up your data on site isn't always the answer. Depending on your environment your backup strategy may include cloud, colocation, and geo-redundancy. We can help you determine if your business which solution is the best fit for your company and help you devise a complete business continuity plan.

The best offense is a great defense! Education and proper training on how to protect yourself from malware is just as important as your recovery processes. We inform our clients when we gain knowledge of an active malicious campaign so they can help prevent access to their systems. Our blog is a great resource for our current and future clients. If you're interested in learning more please visit www.TheEpochTeam.com or email us at info@theepochteam.com.

8/12/2016

EPOCH INC.
3273-A PINE ORCHARD LN
ELLICOTT CITY, MD 21042
410.465.3955
INFO@THEEPOCHTEAM.COM

www.TheEpochTeam.com

Follow us on LinkedIn