Whalley Computer Associates

877.569.4227
wcabiz@wca.com
wca.com

Case Study Comparison: Ransomware Attack

Summary: This a case study comparison of two companies hit by the same ransomware attack within a 24-hour period. One company was protected under the WCA "Managed Services" and the other was not. Case study will examine the total damage of suffering a ransomware attack and the true cost of your company restoring your operations.

Company A: This client is a local major manufacturing company in the Military and Robotics industry that enlisted in our Managed Services programs which monitors their network and is prepared to help protect them against threats.

Approximately 7:30am on a Thursday morning an employee accidently clicked on a email link that was a ransomware attack. The client's PC was infected, but under the WCA Managed Services program the client's network was protected by a WCA installed program that immediately detected the attack and isolated the PC from the network limiting this attack to ONLY this PC. This program also notified our Managed Services team and within minutes they were working on the type of attack and resolution.

The threat was assessed, the PC was cleaned of the infection and WCA restored the most recent "pre-attack" back-up of the infected files. This PC was the only infected and isolated from the network for a total of 45 minutes while the ransomware attack was being eradicated and data was restored. Most importantly these services were covered under our Managed Services program and there were no additional costs incurred by company A.

Company B: This client is a local Public Safety Agency in a major city. This client was NOT enlisted in our Managed Services programs which monitors their network and is prepared to protect them against threats.

Approximately 7:30am on the Friday morning following company' A's attack an employee accidently clicked on an identical email link that was the same ransomware attack that hit company A the previous day. The client's PC was immediately infected and quickly started to infect other PC's throughout the network. The ransomware quickly spread throughout the entire network a total of 75+ PC's and 6 servers had their data encrypted by the ransom threat.

WCA was then called in to analyze, eradicate and restore the network. A team of 5 WCA engineers worked over the weekend and started to restore core PC's within 48 hours. TA team of senior engineers worked remotely to restore the server infrastructure recovering critical systems and data to an operational point. The process of cleaning and restoring 75+ PC's took about 2 weeks for most PC's to be restored. All systems were not back to fully operational for over a month and not all data was able to be restored. A total of about a weeks' worth of information had to be recreated
Benefits: WCA provided a smooth transition, with minimal disruption to the client. Client desired components were properly installed and configured to the clients existing infrastructure. All components were tested upon project completion.

Note: There was complications with certain PC's not being properly backeed-up. The restoration of the non-backed up PC's

877.569.4227
wcabiz@wca.com
wca.com

took another 2 weeks to restore all PC's to the network. The total cost of the attack was 48 hours complete downtown, core PC's and servers restored after 48 hours and a gradual recovery of the other 75+ PC's over the next month. Total expense of the WCA manpower to company B was over $50,000.00

Special Note: When hackers are unsuccessful with a ransomware attack, they will try again and if they are not successful then they will try to sell the information that they were able to obtain on the Dark Web to other criminals. The truth is that they might sell this information to many criminals, and they will try to login directly to the network. This makes accompany that has suffered from a Cyber-attack 100% more likely to be target of another attack.

FInal Thoughts: Ransomware attacks are going to happen, and it only takes a quick mouse click to start the process. By reviewing the case study, it should be clear that clients enrolled in the WCA Managed Services program are better protected against these threats and the total cost of your network being locked down and the cost to recover.

Another great protection to your company is to train your employees with "Security Awareness" training. WCA has created a training program is that can be held at your location to train your staff to be more informed about random emails. The weakest link in the protection of your network is an employee that launches a virus that Has been sent via email. Many organizations have started "Security Awareness for end users" trainings several times during the year to keep their staff up to date on new threats as well as reinforcing safe computer skills.

If you are interested in WCA's Managed Services program or Security Awareness Training for end users, please contact your Account Executive.