allmountain technologies

(970) 748-8880
www.allmtntech.com

Solutions & Success

The Inside Story

All Mountain Technologies Helps New Client Recover From Ransomware Attack

Ransomware would have caused a lot more damage to this brokerage firm if they hadn't gotten in touch with our team for help. Do you have someone to help you respond to a ransomware attack?

You've probably heard a lot about ransomware and other cybercrime threats.

It's easy to hype up the doom and gloom about cybercrime—fear is often a great motivator. Here's a reminder of just how real cybercrime is...

Vail Valley Brokerage Firm Gets Hit With Holiday Weekend Ransomware Infection

Originally, this local real estate brokerage firm approached AMT because their current IT staff member was leaving, and they were looking to replace him.

While our initial audit uncovered serious cybersecurity vulnerabilities, the firm protracted the process of reviewing our service offerings and singing the contract we proposed to them. Then, on Thanksgiving eve, they got infected with ransomware…

That's When This Brokerage Firm Hired AMT

Having been infected with ransomware, the firm opted to hire us outright as their IT partner. Fortunately, we were able to recover the database files because they had file level backup.

We then had to rebuild all the servers because of ransomware and then we methodically put back the files and had them running the same day. Next, we closed up the firewall gap that the threat entered through and deployed a range of key security measures to protect them from further attacks in the future. We then audited the firewall, closed all unnecessary ports, and added MDR to their security suite.

Once the dust settled, we were able to have a conversation with the firm's leaders about IT best practices and what is necessary in order to stay secure. They agreed to all terms and implemented our best practices, and they have been confidently secure ever since.

How Does Ransomware Work?

Ransomware is a type of malware that encrypts the target's data *(making it unreadable and inaccessible)* and holds it for ransom. It targets all data on the target's systems, making it impossible for them to ignore until they pay the ransom or restore the data from backup.

Typically, an unsuspecting employee clicks on an emailed attachment that appears to be a bill or other official document. In actuality, the attachment installs a malicious software program *(malware)* onto the computer system.

There are a number of ways that hackers can trick targets into downloading ransomware:

Phishing

Phishing is a hacking technique that "fishes" for victims by sending them deceptive emails. Phishing attacks are often mass emails that include ransomware as an attachment.

Malvertising

Hackers have found vulnerabilities in many popular, modern browsers like Google Chrome and Mozilla Firefox. They spam users with official-looking pop-ups informing them of an “infection” or “security alert” prompting them to download a file or click a link. As with so many of these methods, it just comes down to getting the user to interact with malware in some way without them knowing it.

Out Of Date Hardware

Many of the most common malware and viruses used by cybercriminals today are based on exploiting those programming flaws; to address this, developers regularly release software patches and updates to fix those flaws and protect the users.

What Would Happen If You Were Infected With Ransomware Right Now?

Do you have a plan? Are your system endpoints protected? Are your backups recent, tested, and viable?

It’s a mistake to assume that just because you haven’t been hit by ransomware yet, that you won’t be anytime soon. You may think you can put off investing in effective cybersecurity support, but without warning, you may get hit.

Don’t assume you’re safe—working with the AMT team, you’ll know for sure.