The Guide to Ransomware Prevention

An Introduction to Ransomware: The Basics

Ransomware is a type of malicious software (malware) that restricts access to files on the infected system, or makes data on your computer unreadable by encrypting it; it then demands payment to un-restrict or un-encrypt them. Once you pay (to the tune of several hundred USD via prepaid voucher or virtual currency known as Bitcoin), you get your files back. The malware even puts a deadline on how long you have to pay the ransom.

Ransomware typically propagates as a trojan, such as CryptoLocker, and is usually disguised as a legitimate file from an email, USB drive, or website.

Is Your Cloud Data Secure?

The fact that you are backing up data to the cloud is a good thing – but it's not the act of backing up that's the issue. The problem with typical cloud backup implementations is that they're set to synchronize; your backed-up data in the cloud is maintained as a mirror copy of what's currently on your computer. Ordinarily that's ideal – unless those files are encrypted, in which case they'll be synchronized to the cloud by your backup software. Your backup isn't what you thought it was, just like that. Later in this document we'll look at how you can ensure your backup doesn't get corrupted.

NETWORKS PLUS

Ransomware malware prevention tips

Prevention is key when it comes to protecting your business from ransomware.

Follow these eight prevention tips:

1) Install a reputable anti-virus/anti-malware software that has on-demand scanning. *(Be advised that anti-virus alone may not be able to prevent a ransomware infection and can do nothing once infected. A good anti-virus is only part of a good prevention program.)*

2) Schedule your anti-virus/anti-malware software to automatically run scans at least once per week.

3) Always double-check the sender of any emails you receive and if you don't know the sender, proceed with caution.

4) Never click on email attachments unless you know exactly what the attachment is.

5) Don't click on links within emails unless you know where the link is going.

6) Keep a separate backup of your personal files away from your computer.

7) Set up and stick to a regular backup schedule.

8) If you use cloud backup services, consider investing in a cloud-to-cloud secure backup solution as a plan.

9) Installing a "next-generation" firewall that is capable of unified threat management is an essential piece of a prevention strategy. A next-generation firewall can help prevent suspicious traffic from reaching your internal network.

Keep your backups safe with cloud-to-cloud backup

In the prevention tips above, we suggest making a backup of your backup via cloud-to-cloud backup. Cloud-to-cloud backup solutions offer an additional secure copy of your data that maintains prior versions – bingo, the un-encrypted files without the ransomware infection. These versioned files are inaccessible and unchangeable by the malware. They also insure against one of the leading causes of data loss, accidental deletion, by keeping any deleted files even if you were to remove them from your computer.

Cloud-to-cloud backup is a worthwhile preventative solution; it's a backup for your backup in other words. It backs up data you store in Google Drive for instance and not only creates an additional secure copy but stores previous versions. In ransomware terms, that means you would have the unencrypted versions. And of course with the second copy, it has the added benefit of preventing data loss via accidental deletion.

Conclusion

The moral of the story is that while the ransomware malware can be removed, prevention is crucial in order to protect your data from being encrypted or restricted. Install appropriate anti-virus software and firewalls, be wary of any emails that are sent to you from unknown senders, and have appropriate backup in place – whether it's a physical copy or a cloud-to-cloud backup solution.

Contact one of our local business consultants here or call 800.299.1704 to get a free network security proposal for your business.