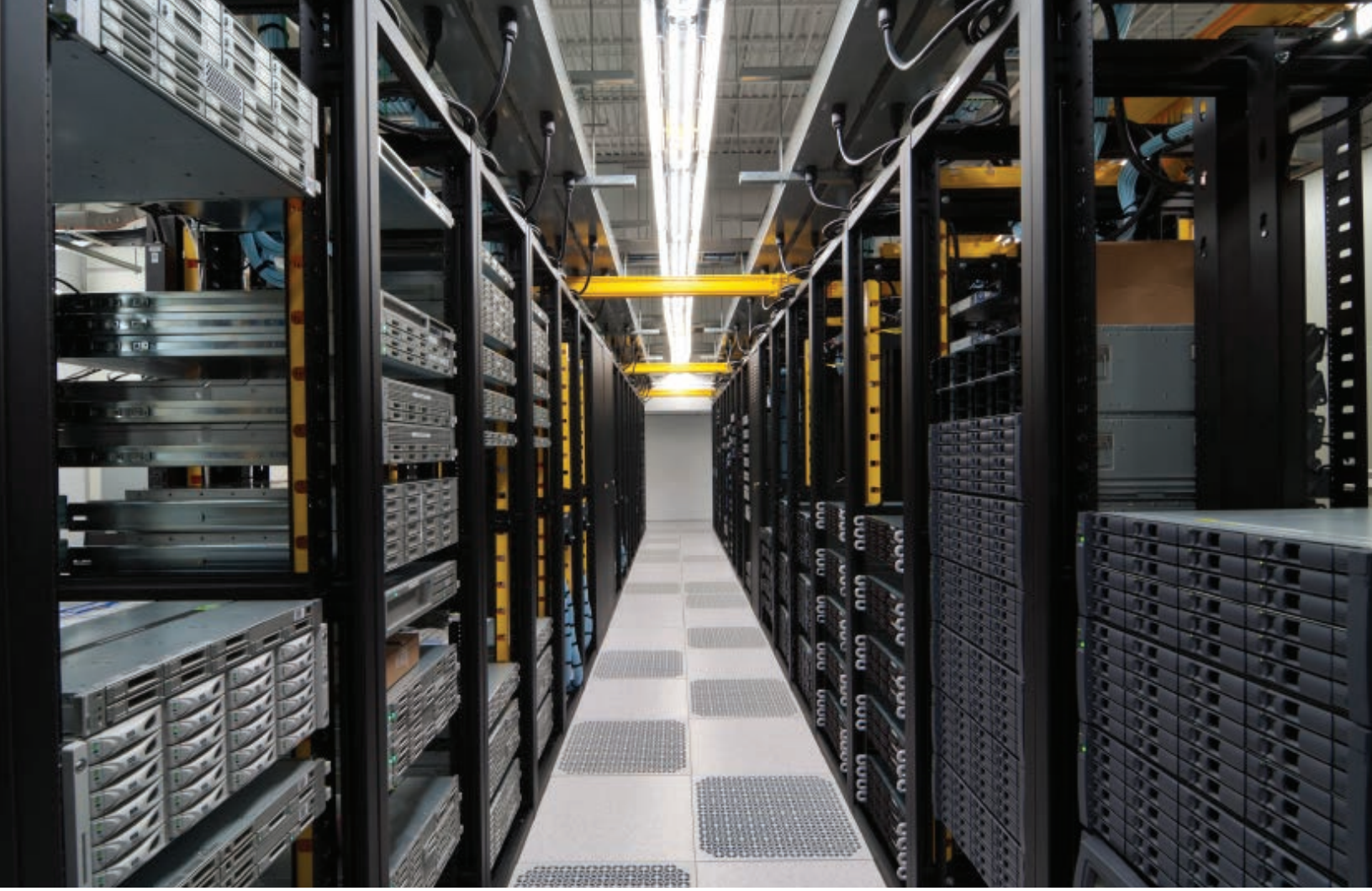
YOUR DATA OR YOUR BUSINESS: RANSOMWARE EXPLAINED

TechKnowledgey



YOUR DATA OR YOUR BUSINESS: RANSOMWARE EXPLAINED

This cyberattack scheme hasn't garnered nearly as much attention as the usual "break-in-and-steal-data-to-sell-on-the-Internet" type, but it can be even more debilitating.

Ransomware attacks have begun appearing in the last few years and its practitioners are so polished that in a few cases they even have mini-call centers to handle your payments and questions.

So what is ransomware? The business model is as old as the earliest kidnapping. Ransomware stops you from using your PC, files or programs. The attackers hold your data, software, or entire PC hostage until you pay them a ransom to get it back. Obviously, seeing that you are dealing with criminals, there isn't any guarantee you will ever get your data back just because you meet their demands.

The M.O. is pretty simple. You suddenly have no access to a program or file and then a screen appears announcing your files are encrypted and that you need to pay (usually in bitcoins) to regain access. There may even be a Doomsday-style clock counting down the time you have to pay or lose everything. Microsoft reports that some versions accuse you of having broken a law, and that you are being fined by a Federal agency, police force or other official enforcement office. Some versions use the FBI logo.

Interestingly, one of the more common "market segments" being targeted in the US has been

public safety. Police department data is held hostage, and in many cases, they have given up and paid the ransom. They had little choice. They aren't the only ones. Within a week, a hospital in southern California also fell prey, as did one in Texas.

Ransomware can be especially insidious because backups may not offer complete protection against these criminals. Such new schemes illustrate why you need to be aware of the latest criminal activities in the cyber world, and make sure your data protection efforts are up to date.

Here are 5 steps you can take right now to protect yourself from ransomware:

1) Make sure you continue to keep your antivirus software up to date.
2) Train your employees to be aware. People remain the biggest source of security breaches. Employees unwittingly open malicious emails or go to corrupted sites and expose their employers' networks and infrastructures to malicious software.
3) Backups are probably the most important method to restore your systems if you suffer a ransomware attack. Make sure that your backups are detached when the backup is not occurring. Otherwise, you risk that even backup files will be corrupted.
4) Keep all of your software programs updated. Software developers frequently patch vulnerabilities with new updates.
5) Use pop-up blockers. AdwCleaner is one of the best. It not only blocks unwanted pop-ups but also protects against browser hijacks, malware and adware. You can read more/download it here (http://windows.dailydownloaded.com/en/security-software/popup-blocker-software/293-adwcleaner-download-install)

These simple tips discussed work like the locks we put on our front doors. Just as you wouldn't leave your home unlocked and invite a robbery, you shouldn't leave your data vulnerable to an attack by miscreants.

CONTACT DETAILS

Jesse Good
Marketing Coordinator | TechKnowledgey, Inc.
Email: jgood@tkiapps.com
Phone: 574-971-4267
https://www.techknowledgeyinc.com/