Multi Layered Security: *It's a Must!*

Next Generation Firewall

Perimeter defense against any potential attack. Next-Gen Firewalls are designed to block unauthorized access to your computer system or network giving you granular control over inbound and outbound traffic.

Endpoint Protection

More than your traditional signature/hash based Anti-Virus, modern endpoint protection technologies provide behavior based protections, sandboxing, forensic analysis and more to help combat modern threats

Privileged Access Management

In an age of cloud computing and SaaS services management of access is critical, whether it be a simple password vaulting solution of full blown Identity management with Privileged Access Management, protection and control of credentials is essential.

File Level Backup

A good file sync and share tool is more than just a way for your team to collaborate on the go, it's a vital component to your organization's security strategy. With file level backup, you can ensure that even in the event of a site wide disaster, your team can maintain anytime access to their critical files.

Server Level Backup

Your last line of defense in a site wide disaster, backup and disaster recovery solutions allow you to recover at the systems level. An absolutely necessary piece of your organizational infrastructure, backup and disaster recovery delivers peace of mind that your systems will always be recoverable, even when disaster strikes.

DON'T WAIT

Start protecting your organization from inevitable downtime today. Contact our team to discuss your options for total system protection, both onsite and in the Cloud.

GET MORE INFO

512.472.6000

sales@myitpros.com

MY I.T. PROS

BETTER BACKUP. SAFER DATA.

Security At-a-Glance

*(un)*POPULAR THREATS TO AVOID

Advanced Persistent Threat

Cybercriminals typically use an advanced persistent attack to target larger organizations. Often with the objective of soliciting financial information. This type of attack can be executed over a long period of time and is difficult to detect.

Backdoor Trojan

A backdoor Trojan allows cybercriminals to take control of a system without permission. Posing as a legitimate program, a Trojan often spreads though phishing campaigns which fool users into accessing malware through everyday activities such as clicking links. Once the Trojan is installed it opens a "backdoor" to allow the malicious party access to the infected device.

Distributed Denial of Service Attack

A DDoS attack is meant to prevent users from accessing specific systems or URLs online. In this attack, a cybercriminal will flood a website with large quantities of information requests, which look like legitimate requests from multiple sources, which essentially renders the site inaccessible to legitimate users while under attack.

Flooding

In this security attack, hackers will send a large amount of data to a server or web location. The result is a break in the systems proper operation, due to a utilization of all resources on the victim machine, crippling its processing power.

Social Engineering

Social engineering uses psychological manipulation to persuade users to perform specific actions or reveal sensitive information. Lies, bribes, extortion and impersonation are often used in this type of attack. This is often considered the most effective attack vector.

SQL Injection

SQL Injection is an attack wherein an attacker uses a web application to access data or execute "true" statements on a database. Captured data could be anything contained within the database even if encrypted. By doing this, attackers can impersonate identities, modify or delete data or completely take control of an entire database.

Worm

A worm is an attack that has the ability to spread itself indefinitely and self-replicate. By exploiting Operating System (OS) vulnerabilities. This replication happens automatically and does not need human activity in order to spread.

ARE YOU RANSOMWARE READY?

When it comes to cyber threats, you've got a lot to look out for, from Trojans to Worms. But we've got some more bad news. Ransomware attacks are on the rise. Don't think so? In 2017 alone, ransomware attacks rose a whopping 250%, with those attacks hitting the U.S. the hardest1. What is ransomware? A type of malicious software, Ransomware encrypts critical data on a PC, desktop or mobile device and blocks access to those files by the data's owner. Aptly named, Ransomware requires a ransom be paid, typically in Bitcoins, to the attacker in order to regain access to the files.

Ransomware Attacks in Recent History

On average, small businesses lose over $100k per ransomware incident as a result of downtime2. Below are a few attacks to hit in recent years and how much they are estimated to have caused in damages.

- CryptoWall - $325M
- CryptoLocker - $30M
- Petya/NotPetya - $1.2B
- WannaCry - $4B

START PROTECTING YOUR DATA TODAY

512.472.6000

Call MyITpros for a free IT assessment