NETWORKS
CONSULTING RESOURCES

Top Ten Ways to Protect Your Business Against Cyber Attacks

Hope is not a strategy.

Cyber security for business has never been more important.

NETWORKS
CONSULTING RESOURCES

Businesses are expanding their dependency on computers, and hackers are getting increasingly more creative. It's imperative that companies educate themselves on the many facets of cyber attacks and prepare a defense against them. To help your business do this, we've compiled a list of ten solutions to address the most common vulnerabilities.

TOP 10 WAYS TO PROTECT YOUR BUSINESS AGAINST CYBER ATTACKS

1 Antivirus

Viruses are designed to damage, destroy or disrupt computerized operations which is why antivirus software must be a priority for every cyber-security plan. Unfortunately, updating antivirus software tends to drop off IT technicians' priority list because it's tedious and time consuming. Fortunately, it doesn't have to be. There are enterprise-level, antivirus products available that allow remote installation and updating from a central management server, and include built-in alerts to notify your technicians when antivirus programs need attention.

2 Anti Malware

More than just viruses, malware includes malicious programs that spread themselves, spy and steal data. Once they infect your computers, many times the only way to eradicate them is a complete rebuild. This is why a solid protection plan shouldn't rely on free or home versions of malware detection software such as the popular Malwarebytes. Invest in anti-malware programs that offer more robust protection and centralized management such as ABC Malware Program or DEF Malware Program.

3 Anti Ransomware

Ransomware is the worst of the cyber attackers because it quietly runs a virus, like the infamous Cryptolocker, that methodically sets itself up to launch a crippling attack. Once it secretly encrypts your data, it notifies you that it has locked your data and holds the only key. At that point your company's data is in a stranglehold that only paying a large ransom will release...maybe. Remember these are clever cyber criminals who know the future of your business is in their greedy hands. Your best defense against ransomware is to close the popular entry points into your systems and enlist anti-ransomware protection now before this happens.

4 Zero Day Threat Protection

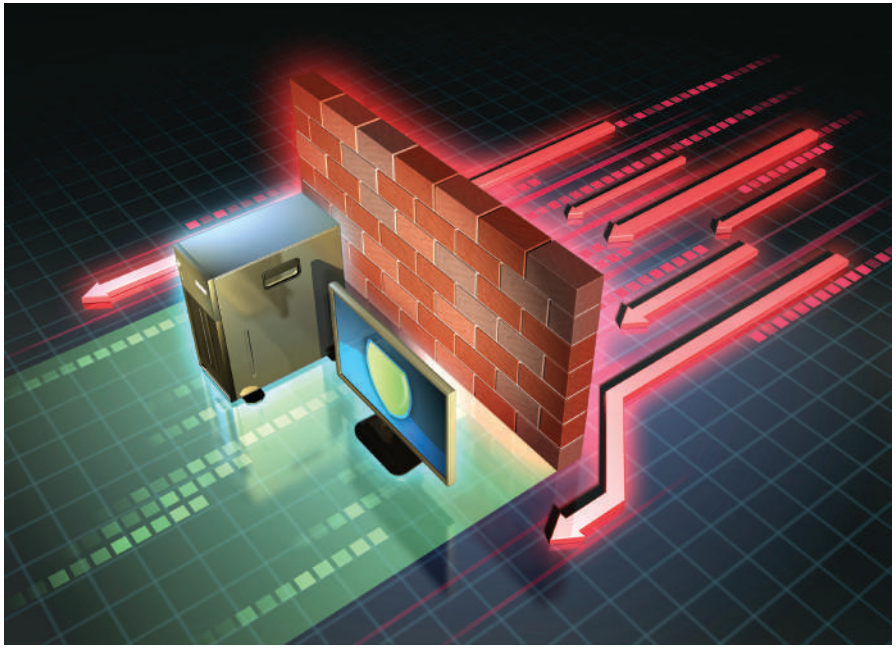
Hackers are the final testers of computer software. Instead of checking for properly functioning software however, they scan the code looking for security holes to exploit. A Zero Day threat in a software program is one where a security hole exists in a software release. Once the software is distributed and loaded on computers, these workstations have a security vulnerability that the software developers essentially have zero days to fix before hackers can capitalize on it. Hackers use these to take unauthorized control of your computers, install malware, corrupt files, copy contact lists, send spam or install spyware to steal your sensitive information and share it on the Dark Web. These are why we involve our partner, Dark Trace, when we create a complete cyber-security solution for our customers.

5 Email Vulnerability Solutions

Spam and Phishing are two email ways hackers enter your computer systems. Spam Filters scan emails in a background 'sandbox' where it safely opens attachments and investigates links before your user sees and clicks on them. Discovered threats are quarantined, disarming the potential harm. Phishing is another email method that utilizes convincing looking websites and links to trick users into clicking on them. Barracuda, is one such spam and phishing protection program that warns users if they've clicked on infected files and it includes a way to watch a training video to help users avoid these problems in the future.

6 End-User Training

One of the major security weaknesses in every organization is the end user. All of the software protection is worthless if your end users unknowingly open the door and let threats in. Hackers capitalize on unsuspecting users for many of their attacks. This is why any comprehensive security plan must include end-user training to educate them on the tricks and techniques utilized by cyber criminals to infiltrate your systems. Lunch and learns, regular reminders, new threat announcements, and automated training are essential ways to keep everyone aware and alert.



7 Firewalls and Filters

Firewalls are meant to shield systems, but can offer easy access to a company's systems when technicians treat firewall setup as "set it and forget it." Similar to cyber-attack protection software, firewall firmware must be updated regularly. In addition, there are ways to enhance the protective capabilities of your firewalls through filters that block passage to cyber dangers like the Dark Web, or setting up dual authentication with a Virtual Private Network connection.

8 Patching

Installing software patches in a timely manner is rarely the norm for IT departments. Yet it is an invaluable way to plug the holes that hackers exploit. Automatic patching and Active Directory processes make patching easier but don't reliably work. Improve your patching process by monitoring the patching, running patch reports and testing the patches to make sure they don't have bugs that cause other issues. If you have third-party software that only offers manual patching, be aware there are tools or PowerShell Scripts that can also be used to automate these processes.

9 Reliable Backups

While you are in the process of establishing a solid cyber attack plan, make sure you are creating, maintaining, and verifying the reliability and availability of your current system data backups. This is another area where IT departments tend to adopt a "set it and forget it" approach. They assume everything is running correctly and don't discover until there is a critical system failure that their automated backups became worthlessly corrupted and incomplete somewhere in the past. Make monthly file restoration part of your backup planning. A quality backup can save the life of your company after a devastating cyber attack.

10 Business Continuity Plan

Disaster Recovery (DR) plans are great for restoring your systems after a cyber attack, but a Business Continuity Plan (BCP) can take your DR plan to the next level. A comprehensive BCP helps your business proactively avoid disruptions rather than simply reacting to recover from them. Review your BCP often because new cyber attack methods are constantly knocking at your company's door. Also make sure your plan includes protocols for data breeches, and if you use Cloud services, be sure you understand their protocols and the timeliness of their resources to help you recover your data.

NETWORKS CONSULTING RESOURCES

Recap

Are your computers adequately protected against:

[ ] Antiviruses

[ ] Anti Malware

[ ] Anti Ransomware

[ ] Zero Day Threats

[ ] Email Vulnerability

Could your business profit from:

[ ] Staff Training

[ ] Firewalls and Filters

[ ] Patching

[ ] Reliable Backups

[ ] Business Continuity Plan

Net Works Consulting Resources is always available to help you plan your cyber defense, educate your users, and assist in establishing the pieces you need to help guard your company from the vicious cyber criminals eager to disrupt or destroy your business.

Request your free consultation today.

Give us a call at **888-638-9752** to schedule a meeting to discuss your needs.