EIGHT HOT TIPS TO PROTECT YOUR SYSTEMS AGAINST RANSOMWARE

Simple steps to prevent ransomware attacks

myriad digital

1 BACKUP REGULARLY

A robust backup and recovery strategy goes a long way to safeguard against being a victim of ransomware. This strategy has to be aligned with the importance of your data and include recovery point and time objectives. Please note that many conventional backup methods may be compromised.

2 PATCH YOUR SYSTEMS

Attacks are designed to penetrate vulnerabilities in common software apps e.g. Internet Explorer. Therefore applying security updates and patches promptly and reliably is critical. This extends to all OS and application environments. A fully patched system will go a long way in protecting against a range of cyber threats, including ransomware.

3 EDUCATE YOUR STAFF

Education & awareness are paramount when it comes to defeating ransomware so spread the word. Be aware of suspicious looking email by looking at the senders domain name. Look out for spelling mistakes, check the signature and the legitimacy of any request. Check links by hovering over them & see where they go. These are all signs of bogus email that should be avoided.

4 PROTECT YOUR NETWORK

Anti-virus, anti-spyware and other intrusion prevention technologies should be in place on devices at the network perimeter. A layered approach can stop ransomware by avoiding a single point of failure in your security architecture

5 SEGMENT YOUR NETWORK

Ransomware is designed to spread from the endpoint to the server/storage where it can create the most havoc. By segmenting the network and keeping critical apps, data and devices isolated on a separate network or virtual LAN can limit this spread. Split your guest WIFI from your internal to prevent intrusion from 3rd party unprotected devices.

6 SECURE YOUR ENDPOINTS

Many users connect to your networks with personal and corporate devices so it is essential that all of these are adequately protected. Most anti-virus solutions are signature-based so can be detected however recent ones are hash based and undetectable with conventional methods.

7 PROTECT ANDROID DEVICES

Almost 85% of all smartphones are at risk.The Google Android OS has become a popular target for ransomware attacks. Once these devices are infected it can not only nail the phone but your entire network and data. Deploy anti virus and malware protection on all Android devices. Only install apps from Google Play, Disable installation of apps from unknown sources.

8 QUARANTINE ROGUE FILES

Consider implementing technologies such as sandboxing that can move suspicious files to quarantine before they can enter the network. Once quarantine is passed they can enter your network but not before. Once a threat is identified, protective measures such as policies can be provisioned blocking further threats associated by IP or domain.

At myriad digital we have extensive experience of implementing system security that works. Call us so we can help secure your future

Call Us on 01626 360011