FACTSHEET:

Protect yourself from Ransomware

Know your ransomware…

Ransomware has been around in some form or another for the past two decades, but it really came into prominence in 2013 with CryptoLocker.

The word CryptoLocker has now become sononymous with ransomware however there are several major variants including –

- CryptoWall
- CTB-Locker
- Locky
- TeslaCrypt
- TorrentLocker
- KeRanger
- Sality

With so many threats being used and created by criminals daily; your staff must remain vigilant to avoid infection.

SUMMARY

Ransomware is a type of malware that targets servers, home computers and endpoints within a network to encrypt files so you cannot use them. Files can be seen but cannot be opened or used and in some cases your whole system is locked down.

The pain point for businesses targeted by this type of attack is mainly loss in productivity, financial losses to restore systems and files and the permanent loss of sensitive or proprietary data.

Once your system has been attacked the hackers then demand a ransom to "unlock" the files (usually paid in untraceable Bitcoin) which does not necessarily guarantee the recovery of files or system access. After all, the reality is you can't trust the bad guys!

Malicious sites make up over 22% of all websites. There is a 50% chance that your staff will encounter an unsafe site while using their computer in 2017.

BACKGROUND

There has been a rampant increase in the use of ransomware in the last few years. With each successful attack the top hacking groups are becoming more targeted in their approach and more sophisticated in the use of their resources. In 2013 there were approximately 82 million malware variants. By mid-2014 there were over 96 million variants or a growth trend of 14,640 new variants per hour (Webroot, n.d.). That number has risen exponentially since then.

The most common modes of entry for a ransomware attack are through staff visiting unsafe or fake websites, opening emails or email attachments from unknown senders or clicking on unsafe links within social media posts, instant messenger chats or emails.

SOLUTION

So which security solution will offer 100% prevention and protection from ransomware? The simple answer is none. Cybercriminals are constantly innovating their product to circumvent or disable your security defences to get a successful attack on your system. However, there are things you can actively do to avoid the costly repercussions of a ransomware attack.

The best tactic to avoid ransomware attacks is to ensure that your staff are educated about suspicious emails, fake websites and malicious links. Staff should be mindful and ensure the email in their inbox is from a sender they trust, take extra caution with those emails containing attachments and be vigilant against fake websites or links.

If your staff are allowed to use USB drives, consider employing a group policy to perform a virus scan each time the device is plugged in. This measure safe-guards against people bringing a potentially infected device into the network and releasing the infection.

Use reputable security measures, such as Ategra Digital Shield, that includes antivirus, antispam and antispyware to ensure you have multi-layer protection for your computers, networks and equipment. Most importantly make sure it's always monitored, maintained and up to date.

Ensure you have all the latest updates and patching applied to your computer, servers and other equipment. Ransomware can attack by exploiting system vulnerabilities so it's important to be protected by the latest system updates.

Ategra Computer Technology
No problems, just solutions!

Contact Us

Ategra Computer Technology
35 Georgina Crescent
Yarrawonga NT 0830
P: 08 8932 7888
E: ategra@ategra.com.au
W: www.ategra.com.au

Most importantly, put strong backup practices in place and consider your business continuity plan in response to a potential attack. Backups should be multi-layered and include onsite and offsite backup solutions such as cloud storage. Again, your backups should be monitored and maintained to ensure data integrity.

CONCLUSION

Malicious email can be used by hackers and criminals at any time unless steps are taken to protect your systems and crucial data. Education, secure backups, maintenance and reputable multi-layered security resolutions can help avoid the costly repercussions of an attack. Don't fall victim to cybercriminals!

Contact Ategra at **08 8932 7888** or send us an email at **ategra@ategra.com.au** for more information on how to best protect your data.