Press Release

amicus its

Understanding the latest in ransomware threats

Ooops!
Your files have been encrypted!
Sent $1000 worth of bitcoin to address xxxxxxxxxxxxxxxxxxxx
Your files will be lost. Time left 48 hours
47 : 28 : 19

28th June 2017

Understanding and defending against WannaCry, Petya and Adylkuzz threats

Latest Threat Reports

The Department for Culture Media & Sport (DCMS) and the National Cyber Security Centre (NCSC) published the Cyber Security Breaches Survey 2017 on 19th April 2017. Yet again, the stats remain alarming:

- Nearly 46% of UK businesses had identified at least one cyber breach in the last 12 months.
- 72% of breaches came from fraudulent emails (users don't even need to open or download an attachment – the attack can be triggered by sending an email, through malicious website visits or instant messaging. All this highlighting the importance of training and educating staff about cyber threats facing business.
- Only 20% of companies surveyed provide their staff with cyber training
- Only 30% have formal policies in place - despite an overwhelming 74% of directors and senior managers claiming that cyber security is a high priority.

Worryingly 33% of all UK businesses didn't spend a penny in cyber security in 2016 with the confidence in thinking that they couldn't be a target being strongest in firms with less than 10 employees and a sub £2m turnover group. All businesses are a target as they are part of a supply chain and larger firms of 250 employees+ at highest risk with 68% affected and suffering the highest costs.

- May 2017 saw around 200,000 reports of infected computer systems from 150 countries worldwide. It was the dawn of WannaCry and Adylkuzz ransomware cyber attacks, followed in June by Petya and confusingly NotPetya attacks. For IT Managed Service Providers everywhere, one thing is critical - to be able to prevent outbreaks against customers.

Security Layers Every Organisation Needs

There is no single solution against malware, it requires a joined up system of defence measures:

Ransomware Guide

Don't pay the ransom – there is no guarantee you will recover your data

Backup your data regularly – this is your best line of defence

Don't open unrecognised email attachments

Educate staff – what to look out for and what to do with suspicious emails

Implement software updates – these help your software run well and contain security updates

Look for decryption keys – sites like No More Ransom publish decryption keys if you become infected and don't have a valid backup

Have up to date anti-virus software installed – but don't rely on it to protect you on its own

Director of Technology Security & Governance, **JP Norman** commented: *"As we stated very recently in our blog on 6th June it's people who are so often at the forefront of defending security systems today. So we need to ensure that we people as much as software at the heart of the process of information security, if they are not to be the weakest link. Only by placing education and regular training at the forefront of compliance can you have a reasonable chance of withstanding a cyber attack".*

Chronology of Pain – Payment by Bitcoin

- 5th September 2013 – **Cryptolocker** - ransomware that used a Trojan to target computers running Microsoft Windows, spread by infecting email attachments and encrypting certain file types in local and mounted network drives
- 12th May – **Wannacry** outbreak – certain files locked. Victims include: NHS, Renault, Nissan and Fedex. Not particularly profitable for the hackers but highly damaging for the victims.

- Mid May – **Adylkuzz** malware enters the threat scene. This bug gets in the IT system, mines it to slow performance down and feeds of the computer's energy and downloads a series of commands to create a cryptocurrency that fills the hackers coffers, with eventual failure of the IT. With servers around the world, Adylkuzz searches for vulnerabilities in systems mainly those which don't have the latest Microsoft patches.
- 27th June – N**otPetya** – entire disks locked, rendering them useless. Victims include shipping giant Maersk, plus radiation monitoring stations at Chernobyl.
  NB. Of note, the Internet Service Provider for the hackers duly followed good practice by closing down the mail and domain accounts that were being used to exploit the attack. However, this now means that even if you were willing to pay the ransom (which is not recommended practice), the hackers have no way of knowing that you have paid, or reply with the encryption keys!

If you are concerned about any type of data threat to your organisation, or taking steps to mitigate against the threat of cyber attack, please contact our Sales team in confidence on **+44 02380 429429** or email enquiries@amicusits.co.uk