Munich RE

Cyber update
Global ransomware attack: WannaCry

A ransomware attack, known as the 'WannaCry', has affected more than 200,000 computers globally. Individuals, businesses and organisations in over 150 countries were reported to have been impacted by the attack.

Risk Solutions

May 2017

HSB Engineering Insurance
www.munichre.com/hsbeil

What is ransomware?

Ransomware is a type of malicious software that infects computer hard drives and encrypts the data so that it is inaccessible. This is accompanied by a demand for a ransom payment. The suggestion is that if the ransom is paid, the affected party will be provided with the decryption key (effectively, a password) which will unlock the data. However the advice from leading organisations, in the wake of this incident, has been not to pay ransoms. Payments do not always have the desired outcome, as data is not always restored and may potentially make businesses more vulnerable to a future attack.

In the case of the WannaCry attack, affected businesses and computer users were faced with a ransom request of $300-600 in Bitcoin in order to restore their systems.

Ransomware attacks are not new and have been identified as one of the fastest growing trends in cyber-crime. In 2016, research showed an 80% rise in cases compared with 2015*, and this increase in incidents is continuing at an alarming rate.

How did the attack happen?

The WannaCry ransomware attack exploited a known vulnerability in older versions of Microsoft Windows. Although Microsoft released a fix ('Patch') for this in March, after the vulnerability was identified, not all systems had been updated.

The malicious software may have been downloaded onto computers by links in emails. WannaCry also appears to have the capability to spread between computers that have the same vulnerability.

What is the impact?

In the UK, the greatest impact appears to have been centred on healthcare services. The attack targeted the vulnerabilities in their computer systems, in the same way that other global businesses and organisations were affected.

The biggest issue facing businesses and users is the inability to access systems and data, which has caused the loss of productivity and disruption whilst systems are being restored back to working order. So far, there are no cases reported of data breaches where private information has been accessed and compromised.

HSB Engineering Insurance

*Source: McAfee Labs Threats Report December 2016

Reducing the impact

Whilst this particular attack has largely been halted, the true extent of the impact will not be realised for weeks to come. The warnings are that other variations of the same ransomware could develop and spread as quickly.

There are some fundamental measures businesses and individuals can take to reduce the risks of falling victim to a ransomware attack. The National Crime Agency (NCA) leads the UK law enforcement response to cyber threats together with the National Cyber Security Centre. These organisations and industry best practice supports the following advice:

1. Backup data

Ensure that you backup your data regularly and disconnect the backup device from your computer so that malware infection cannot spread to your data backups. Ransomware works by locking your data, but if you have backups then you cannot be held to ransom and you can restore your systems from backups.

2. Install the latest updates

Ensure that systems, software and devices are kept up-to-date with the latest updates as soon as they become available. Microsoft has released an update for the older (non-supported) version of Windows. These updates should be carried out immediately.

You should also consider updating your software to the current versions where possible.

3. Install anti-virus software

Install anti-virus software on all devices and keep it updated, where possible enable automatic updates. Leading developers of anti-virus software work tirelessly to track developments in malware and to keep their software current, but this only takes effect when the users install the latest updates.

4. Download legitimate software and apps

Only download ‘apps’ and software from known and trusted sources such as Google Play Store or Apple’s App Store.

5. Enable security protections

Ensure that security protections on your devices are not disabled. Whilst this might be more convenient in some cases, it can make your devices more susceptible to malware infection.

6. Be vigilant

Be vigilant and suspicious of unexpected emails requesting personal or bank account details, and do not click on attachments or links unless you are sure you can trust the source. If an email is requesting information claiming to be from a legitimate source, contact the alleged source directly and not via links or telephone numbers in the email. Banks and other similar organisation will not ask for your PIN numbers or full passwords.

7. Ensure you are prepared

Be prepared for when a cyber incident occurs. Have you considered how you would continue to operate if you could not use your computer systems? Making plans ahead of time can significantly reduce the impact.

If you have been a victim of a ransomware attack, you should:

- Contact your IT service company, if you have one.
- Report it to Action Fraud. Website: www.actionfraud.police.uk
- Contact your cyber insurance company if you have purchased cyber cover.

How can cyber insurance help?

Depending on the extent of cover provided by the policy, cyber insurance can provide important protection and can help businesses to recover quickly from cyber incidents.

In the case of a ransomware attack, there are a number of ways a cyber insurance policy can respond:

- Provide access and cover the cost of experts who can provide advice and help to restore computer systems to working order and recover data.
- Cover lost business income and additional expense incurred to minimise disruption.
- Cover the cost of damage to software and hardware if repair or replacement is necessary.
- Cover the costs of investigating and responding to a data breach if data has been compromised, or you suspect that it has been compromised as part of the attack.

For more information on HSB Cyber Insurance, please contact your local HSB office.

HSBEI-1754-0517