PSNI CYBER CRIME CENTRE

Ransomware – Thoughts of a victim

01/09/2020

This information sheet has been compiled by the Police Service of Northern Ireland Cyber Crime Centre and is intended to raise awareness of current threats and available guidance: **Contact us:** cyberprotect@psni.pnn.police.uk

Ransomware – Thoughts of a victim

Irrespective of your role or the organisation you may belong to, many of you will have an understanding of ransomware, be that through personal experience, taking part in cyber awareness sessions or simply reading of incidents such as Garmin, Travelex, Norse Hydro or Wannacry.

Over recent years, ransomware has been reported across all sectors in Northern Ireland, be that a small family firm, a charity or a large enterprise and a common question asked is ok it's a threat, but how might it affect my organisation?

We recently engaged with a NI victim of ransomware to find out how the incident in question impacted their organisation. To help raise awareness of the threat posed and the lessons learnt, they have kindly allowed us to share their experience.

As a company, how prepared did you feel your organisation was before this incident took place?

We had suffered from a smaller attack 18 months previous and we implemented additional measures (procedures and various new technologies) to combat the threat so we believed we had sufficient protection in place. But we have extensive legacy systems which are harder to protect.

How did this incident impact on your ability to carry out day to day business?

For the first 4 working days over 70 - 80% of day to day business was impacted. It took 10 working days for the majority of day to day working for the core business to be restored, smaller business operations took longer.

What advice would you provide a local organisation looking to prepare for an event such as you experienced?

Change your mind set from ***"if it will happen"*** to ***"it is going to happen"***.

Cyber security and Information security is a combination of having dedicated and skilled staff (internal & external), dedicated technologies and processes.

- Maintain your software with the latest upgrades and patches.
- Consider the adoption of Cloud technologies as these vendors have vastly more capability to protect your systems.
- Have an incident response plan / partner.
- Have each department create a business continuity plan i.e. how could our department survive without business systems for ***x*** days?

What have you learned from this experience?

Mostly that Cyber security is an ongoing and evolving threat that needs a bigger percentage of the business focus.

- Implement absolute information security procedures for access and control - even if that slows down business innovation.
- Accelerate the removal of older legacy systems.
- Implement IT info & cyber security best practice and without exception.
- Dedicate more resources to information security.

Why not just pay the ransom?

We had excellent backup and recovery systems so we had the ability to recover 99% of all information. Also we would fear paying the ransom would encourage further attacks or raise our profile as a soft target for Cyber Criminals.

What cost would you place on the impact this incident had on your organisation? - Well into six figures

NCSC Guidance on Mitigating Malware and Ransomware Attacks

Useful websites

www.actionfraud.police.uk
www.cyberaware.gov.uk
www.nicybersecuritycentre.gov.uk

Twitter

@PSNIBelfast
@cyberawaregov
@NICyberSC

we care · we listen · we act