Lancashire
Cyber Foundry

What can your business do to defend against Ransonware?

READ TIME: 2 MINS

AUDIENCE: INFORMATION SECURITY

Ransomware is a growing concern for many large business'. We've all seen news stories where large business have been frozen out of their data because someone's holding it hostage.

1. WHAT IS RANSOMWARE?

Although there are different strains of ransomware they all work on the same principle. A malicious person accessed your data, encrypts it and then refuses to decrypt it until you've paid a ransom. Sometimes they honour this and sometimes they don't.

A real world example would be if you biked into town and locked your bike to a lamppost. Imagine someone else coming along and putting their own lock on it too. When you return they say they will only remove their lock if you pay them.

Technical they've not taken your bike, and your bike is still there but you only have access to it through them.

Ransomware currently aims for big business. The bigger the business, the more money; the more money, the more likely they are to pay the ransom.

However, that's likely to change as bigger business start to protect themselves more against malware and ransomware attacks. Ransomware will move towards small to medium sized business with far less cyber security infrastructure.

EXAMPLE: WANNACRY

WannaCry is probably the most famous example which hit the NHS but also a lot of other less known organisations. Once inside the network it propagated to every single machine on the network. Those with the latest Windows 7 updates were spared but those behind got infected. Additionally, lots of the NHS IT Infrastructure was taken out of action as a precautionary measure.

Eventually a freelance information security analyst analysing the virus was able to disable the virus by triggering a deliberate failsafe in the virus which stopped it from continuing further.

European Union
European Regional Development Fund

NORTHERN POWERHOUSE
HM Government

Lancaster University

2. HOW TO PREVENT IT?

Just don't click on dodgy links right? Wrong!

Ransomware is now so sophisticated that once in your network or organisation you don't need to do anything to trigger it. It will spread on it's own. It's also only a matter of time before ransomware can jump from network to network without anything actively doing anything.

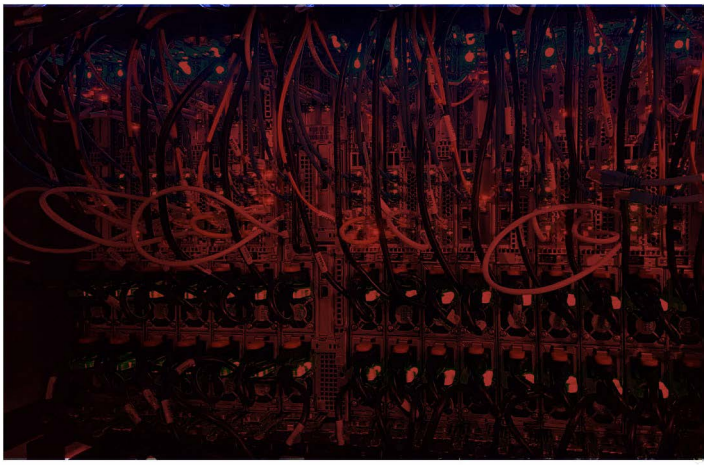
Outside of normal cyber hygiene such as regularly changing passwords and good password management, blocking spam emails, turning your network and machine off when you're not using them, there's actually very little you can do to stop ransomware. It's almost inevitable.

But all is not lost, whilst it's hard to prevent it's a very treatable virus.

Restore from your backup. If the nature of this attack is that they've got your data hostage on your machine; restore the data from somewhere else.

A few rules for engagement on this though:

- Backup regularly (minimum daily)
- Backup externally (somewhere not always connected to your machine)



- Double check your backup before you need it.

The best antidote to ransomware is to make sure you have a copy of everything you do something else. This will change ransomware from a totally disaster to an inconvenience.

3. FIND OUT MORE

Lancashire Cyber Foundry runs a programme designed to support businesses facing cyber challenges in Lancashire. Digital Innovation support is part of this programme but there is also business stategy support available too.

To find out more about how your business can access support and register on one of upcoming workshops contact us: *cyberfoundry@lancaster.ac.uk*

ABOUT THE AUTHOR

Geraint Harries

Before starting at Lancaster University over 4 years ago, Geraint had worked in software development roles in both IBM and the Civil Service. In addition to being a qualified teacher, Geraint has worked freelance with a varied client base as a software developer and graphic designer.