B&FC
BLACKPOOL AND THE FYLDE COLLEGE

Cyber security briefing

Paul Dewhurst
Chief Information Officer

Background on the recent cyber attacks.

- The IT security community expected that the release of Vault7 NSA tools archive by WikiLeaks would prompt a new wave of innovation in cyber-crime.

- WannaCry absolutely changed the landscape for ransomware, from ‘point to point’ encryption to a ‘point to multi point’ model, with a single infected machine able to damage the entire infrastructure.

- It also changed the economics of the attack, making the challenge to the attacker to simply infect a single machine and let a single previously unknown vulnerability take care of the rest.

- The scale of the ransoms were relatively small – just a few hundred dollars. But with dozens or hundreds of systems affected, over an estimate 45,000 target organisations in 75 countries the income for the criminals is potentially very lucrative indeed.

What is the most significant vulnerability to a cyber-security threat?

PEOPLE

Application of common sense

Cyber-security threats are highly technical, however prevention is largely common sense.

- Phishing is still the primary access point
  - Awareness, communication and training
  - Monitoring news and blog sites
- Passwords
  - Do you have enforced strong passwords
  - Awareness and training
- Patching
  - Update date virus detection and end-point protection
  - Application of critical patches
  - Routine patching schedule

Prevention

- Useful
  - Staff training, induction and regular refreshers
  - Employ qualified IT staff and ensure they are continually trained to keep them current
  - Provide “password safe” software
  - Routine patching and rapid critical patching
  - Restrict or block access to files outside span of your security controls (e.g. personal email accounts)

- Optional
  - USB blocking
  - Threat monitoring
  - Threat and vulnerability audit
  - Penetration testing

Impact reduction

- Useful
  - Fragment and restrict access to shared files and drives
  - Frequent back-ups
  - Zero day incident response plan

- Optional
  - Breach detection
  - Early warning systems
  - Network (VLAN) monitoring