SOUTH WEST REGIONAL CYBER BRIEFING

⬤⬤⬤ EVENTS

Events of interest in the coming fortnight:

- **Friday 9th – Saturday 10th June** - Get Safe Online and Dorset Police Cyber are running a pop up event in the Dolphin Centre in Poole. Go along for free cyber advice and security info.

- **Thursday 15th June** - Cyber Security talk at Jurys Inn Cheltenham 17:45 – 20:15 hours.
  Cheltenham Cyber

⬤⬤⬤ ADVICE

Patching

- Apply security patches to software running on all devices within 7 days of its release
- Remove out of date or unsupported software
- Update all smart phones and tablets including application updates as soon as they become available.
- Perform frequent vulnerability scans of your network
- Disable unnecessary user accounts including guest accounts, particularly those with administrator rights.

⬤⬤⬤ CURRENT THREATS

Samba 3.5.0 – The importance of patching.
Samba has released a security advisory in response to vulnerability.
All versions of Samba from 3.5.0 onwards are vulnerable to remote code execution vulnerability, allowing a malicious client to upload a shared library to a writable share, and then cause the server to load and execute it. SambaPatch

South West Cross Site Scripting (XSS) Attack
A company in the SW has been a victim of a XSS attack whereby hackers injected code into the website that gave them admin access. Once in, they injected malicious java script into the header in order to collect card payment details of online customers. The company failed to patch the vulnerability.

⬤⬤⬤ VIDEO

A short video explaining the importance of software updates:

https://www.youtube.com/watch?v=xc20JvvTLO4

⬤⬤⬤ 10 STEPS CYBER SECURITY

Monitoring

Establish a monitoring strategy and produce supporting policies.
Continuously monitor all systems and networks.
Analyse logs for unusual activity that could indicate an attack.

⬤⬤⬤ NEWS

Google to prioritise ranking to websites with HTTPS

At the start of 2017 Google began marking sites without HTTPS as non-secure and lowering them down the result rankings. Having a secure site means that the data is encrypted so that cybercriminals intercepting those details, will be unable to read or use that information. **Google HTTPS   Google Ranking**

WannaCry: Two Weeks and 16 Million Averted Ransoms Later

A review documenting recent experience with managing, mitigating, and tracking the propagation and evolution of the WannaCry outbreak, and the true extent of its reach.
Kryptos Research

⬤⬤⬤ CYBER DICTIONARY

Patching

Applying updates to firmware or software to improve security and/or enhance functionality.