Agenda

- Wales, eCrime Wales, eCrime European Partnership
- Research & Working with the Media
- Infrastructure – Fibrespeed
- Foundation Wales – Collaboration with EADS/Cassidian
- Social Engineering and Other threats
- Coch Bach y Bala
Wales

3m population = Rome

20,000km² = Slovenia

Welsh language
Welsh Language Dictionary Attack Lists?!
e-Crime Wales Partnership

Partnerships are key to success
£974m e-Crime cost to Wales
Overview

**e-Crime is a barrier to the take up and use of Innovative ICT**

Innovative Character of the Project:

- A unique collaboration of Police, Government and Private Sector
- A comprehensive and inclusive awareness raising strategy
- A one stop shop for reliable e-Crime prevention

www.ecrimewales.com
Progress to date

- Project funded in 2008
- ERDF funding of €1.3m
- Businesses in Wales will:
  - Be better prepared against e-Crime
  - Have a place to report e-Crime

Wales will be a safer place to do business
Progress to date

• Police will:
  Have a centralised record of e-Crime
  Be better prepared to tackle e-Crime

Wales will be a safer place to do business
Wales Leading the way...

• Biggest business-focused e-Crime event in Europe
• Commercialisation and Private Sector Investment
• Sharing Best Practice globally:
  
  Europe, South Africa & Middle East

• Creation of European e-Crime Partnership
2nd November 2011
Cardiff City Stadium
Cardiff,
Wales, UK
Register at www.ecrimewales.com

Keynote speakers from:
Blackberry/RIM
NBC Universal
US Dept. Homeland Security
Experian
Microsoft
Sophos
Barclaycard
European Partnership

• Share best practice and information across Europe

• Work together to understand the level and impact of e-Crime on European businesses by sharing reporting and recording information.

• Bring together those organisations involved in e-Crime detection and prevention activities in Europe.

• Educate businesses about the identification and seriousness of e-Crime.

• Offer comprehensive and coordinated high quality advice and support for business about actions to take to avoid becoming a victim of e-Crime and what to do if they are, or suspect they are.

© crimewales
© droideddcymru
14 Regions across Europe
Research & Working with the Media

• Annual Benchmarking Report
• Effectiveness of Programme within the Welsh Police Service
• Effects on eCrime on the Tourism Sector
• Effects on eCrime on Micro Businesses
• Work with FSB, and other Stakeholders
• Situational Awareness Trial with Glamorgan University
600% rise in Malware in 2009
25% Welsh Businesses Victims of e-Crime
Cyber crime is costing over £1 billion a year

By Andrew Boyd
andrew.boyd@wnn.co.uk

Electronic crime is costing the Welsh economy almost £1 billion a year, an expert has claimed.

North Wales Police e-crime Wales liaison officer Andrea Barnard is warning people to be aware of potential computer criminals after new figures from the Cabinet Office suggest such offences may be hitting the Welsh economy for a staggering £974 million.

The figure in The Cost of Cyber Crime report represents a sharp increase on last year's Welsh estimate of £373 million, but e-Crime Wales offices fear the real total is far higher.

"The report concludes that cyber crime is seriously under-reported," said Andrea Barnard, e-Crime Wales' dedicated business liaison officer for North Wales Police. "As a result the real cost of cybercrime in Wales could be different to the figure included in the report, it could be higher or lower.

"Technology provides greater opportunities to commit offences, and with fewer risks."

"In comparison to physical crime, the perpetrator of an electronic crime is far more difficult to find." Offences such as illegal file-sharing were omitted from the report, indicating the level of e-Crime may be higher.

Ms Barnard said e-Crime offenders often live in countries outside where the crime was committed, sometimes making prosecution impossible.

She added: "We can't stop criminals committing we can protect our constantly evolving organisations and to stay vigilant to..."
Situational Awareness Trial – October 2009
Gathering the Intelligence

WG Laptop with intrusion detection software analysing and logging inbound malicious packets

Company X Office Network

Internet Router & Firewall

Data In/Out

Internet
Situational Awareness Trial

USA 9%
GERMANY 5%
ITALY 8%
COLUMBIA 5%
CHINA 48%

approx. 60 Countries in total

Welsh Government
October 2009
Situational Awareness Trial

• 25,486 targeted attacks to Welsh Businesses over 5 days

• Networks ports open: (In) SSH, FTP, POP3, IMAP, SAMBA 445,139,135,137,138, HTTP 80, LDAP 389,389U,3268, ICMP type8.

• Detected co-ordinated attacks from countries

• Specifically targeting supply chains (defense areas)

• Bruteforce attacks against sensor equipped laptops
Infrastructure - Fibrespeed

- UK’s 1st Open Access Network – a Welsh Government Initiative
- £30m partnership between Welsh Government & Geo Networks

DROP & RPZ Lists

Reputation Policy Zone (RPZ – List of known bad domain and host names)

Provided by Spamhaus
ROGUE SPAM ATTACKS

DROP LIST PROTECTION

BAD TRAFFIC
Cassidian / EADS Foundation Wales

• Cyber Security Centre Based in Newport, Wales
• Employ 1000
• An EADS Company
• eCrime Wales Partner / Sponsor
EADS Foundation Wales

• The Foundation is a not for profit Company setup between Welsh Government, EADS & Cardiff University.

• To Discover understand, through a programme of world class research, technologies that will support sustainable development

• To grow and strengthen regional industrial and academic capabilities of strategic importance to the partners

• To promote and facilitate the exploitation of technologies developed, to the economic benefit of the regions involved.
EADS Foundation Wales – Projects:

- Apollo
- IPSE
- ISiOCA
- Nectar
- PuLSE
- RECEPTOR
- Tethys
- Universe
- Vulcan

www.eadsfoundation.com
Social Engineering & Other Threats

• Geo location data could be manipulated to reveal a company location – some companies and organisations need to work at undisclosed locations.

• Geo location data could also be used to aid stalkers, child abusers and thieves by providing them with *involuntary* geo location information – eg clicking on an email link with payload/code eg via MSN, opening an infected PDF file with malicious Java Script.
“Created a proof of concept HTTP-based service where router MAC addresses are mapped to approximate GPS coordinates from other data sources”

http://www.samy.pl/mapxss/?mac=00-13-46-18-57-5a
(This Router was exposed to Street view car).

http://www.samy.pl/mapxss/?mac=00-50-7F-66-07-B1
(Router A has never been exposed to google street view car – it is located down a long private drive).

http://www.samy.pl/mapxss/?mac=001CF07B843
(However, on the entrance of the long private drive (close to the public road) is an IP WiFi CCTV which is connected to Router A.
Some protection measures

Consider purchasing a new/or swapping your router.

Switch off the wireless functionality in your new or unaffected router.

Change its WLAN Mac Address (if supported)

Switch off all wireless devices in your premises – as they may associate with other wireless broadband routers in the area which could reveal your location.
Social engineering is the act of manipulating people into performing actions or divulging confidential information.

Social engineering can be used to gain access to any system, irrespective of the platform.

It’s the hardest form of attack to defend against because hardware and software alone can’t stop it.
Would **you** let this man into **your** building?

*Courtesy of First Base Technologies*
Helpful Staff

- People security is weak in most organisations
- If an attacker has confidence, they will succeed
- Help desks are too helpful!
- If an attacker is in the building, they’re trusted
- People are too polite!
- Robust policies, awareness raising and lots of training is the defence
What kind of devices are placed in offices?

• Portable Wireless transmitters - accessible up to 1 mile away

• Planted and Connected to an internal network point, powered by AA batteries.

• Is accessed using equipment readily available to purchase on the internet
MiFi – Handy Gadget Data Leakage Device?

- Portable 3G WiFi Router with SIM Card
- Has built in firewall / DHCP server
- Can be accessed remotely
- WiFi devices connected to it can also be accessed remotely
- Cheap to purchase £50.00
- Small wireless footprint
- Has Data Card Storage Facility
Powerline Adaptors

• Uses electric wiring to create a circuit
• Limited to internal wiring only
• Wireless models can broadcast company networks to the outside world
Keyboard loggers

- Logs all keystrokes
- Does not log mouse movements
- Cheap to purchase
- Easy to install
- Can store up to 1 years keystrokes
USB Keylogger
Wireless Keylogger

@crimewales
@droseddcymru
(PC) PCI Card Keylogger
(Laptop) Mini PCI Card Keylogger
Caller ID Spoofing
Do you know who’s really calling you?
Did you know this service exists today?
Coch Bach y Bala - ‘The Welsh Houdini’

• Poacher & Thief from Bala, North Wales
• Escaped out of several jails
• Known and pursued by Police

Modern Day Cyber Criminal

• Can operate from anywhere
• May deliberately ‘appear’ to be based overseas
• Will make more money than Coch Bach y Bala ever made – and may well get away with it
Thank you
Diolch yn fawr
Dank u
Gracias
Merci

Grazie
Danke
Kiitos
Děkuji ti
Dziękuję

Peter Gwyn Williams
LinkedIn
twitter.com/petergwyn

“Most laws were conceived in and for a world of atoms, not bits”
Nicholas Negroponte; Being Digital (1995)
“Wales hasn't waited for other countries to decide what best practice is, Wales has actually done it!”

*Ed (the Fed) Gibson, Director, PwC*

“e-Crime Wales is a stand-out initiative, it brings many organisations together to really make a difference and make the Internet a safer place…”

*Garreth Griffith – Operations Director, Wonga*

“Wales is at the forefront in the fight against e-Crime, Why Wales? Wales took the initiative…”

*Richard Cox, CIO, Spamhaus*