Compulsory Data Retention: Issues for CSIRTs

Andrew Cormack
Chief Security Adviser, UKERNA
A.Cormack@ukerna.ac.uk
Why Now?

• Who wants data retention and why
  – Council of Ministers – crime and security (terrorism)
  – Commission – distort markets equally
  – Parliament – wants to be consulted

• Who doesn’t
  – European Data Protection Supervisor
  – EC Article 29 Working Party
    • General data retention not clearly justified
    • Retention periods not convincing
    • Safeguards not adequate

• Draft agreed Dec.2005 (not yet published)
Likely Content of Directive

• Concerns *traffic* data, i.e.
  – Users’ (real-world) identities and addresses
  – Login times, DHCP logs, etc.
  – Time, source, destination, etc. of communications
    • But NOT content of them

• Compulsory collection
  – By specified types of networks
  – Of data about specified services (see next slide)
  – Whether you need the data yourself or not

• Compulsory retention: 6 months to 2 years
  – Must disclose to competent authorities “without undue delay”

• Need to log and report access requests
Which Records?

- Internet e-mail
  - Source IP, userID and subscriber details
  - Destination userID and subscriber details
- Internet telephony
  - Source IP, userID, (number if passed to PTTY) and subscriber details
  - Destination userID, number and subscriber details
- All
  - Logon and logoff times to Internet and service
  - “Internet service used”
  - Calling phone number or DSL endpoint
Definition Problems

- What is/isn’t “Internet e-mail”?
- What is/isn’t “Internet telephony”?
- What if you only move the packets?
  - Must retain data you “generate or process”
- What about IM? IRC? Webmail? VoIP? Skype? ...
- Wording relates to domestic ISP connection
  - Not clear how it applies to business or NREN
Lost in Translation?

• Directive must be transposed into national laws
• Lots of flexibility/ambiguity for individual governments
  – Duration of retention (6 months to 2 years)
  – Which networks are included (“public” ones)
  – Whether new logs must be created
  – Which (if any) costs can be recovered
  – Purpose/process for authorised access
    • Just “serious crime” or any crime? And how to control this?
• Likely to be much uncertainty in short term
• And significant differences in long term
How are CSIRTs affected?

• Good news: should be more logfiles out there
  – But may not be lawful for you to use them
    • Use only permitted for serious crime investigations
    • Some countries restrict use of any data about crimes
  – How to separate it from routine logging?

• Bad news: logfiles are interesting
  – To good guys (so expect more requests)
  – To bad guys (so expect more attacks, and fake requests)
  – To interested parties (can MPAA demand them?)

• Bad news: now they do know you are a dog!
What should CSIRTs do?

• Minimum
  – Work out whether your organisation will be covered
  – Advise on secure/safe ways to store/search/access data
  – Ensure requests for disclosure are verified

• Recommended
  – Work with legislators to produce practical/effective law
  – Work with enforcers to ensure enforcement doesn’t make a network we can’t or don’t want to use
  – Security of storage and access processes are critical