27th ANNUAL

FIRST CONFERENCE BERLIN

14-19 JUNE 2015

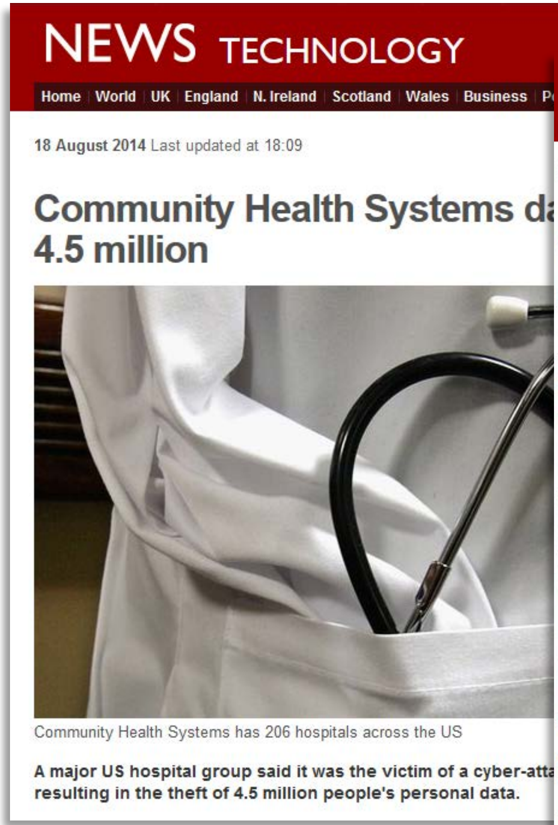
UNIFIED SECURITY: IMPROVING THE FUTURE

Protecting Privacy through Incident Response

Andrew Cormack, @Janet_LegReg

Chief Regulatory Adviser, Jisc Technologies

Incidents damage privacy



NEWS TECHNOLOGY

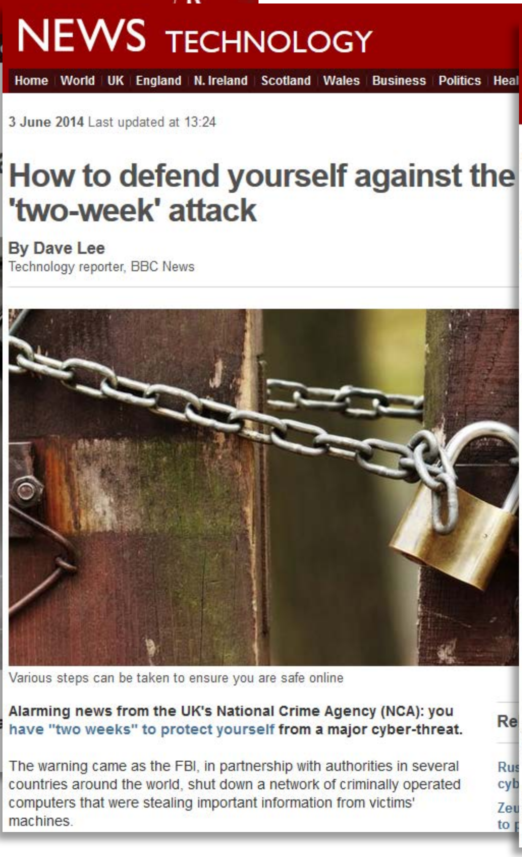
Home | World | UK | England | N. Ireland | Scotland | Wales | Business | Po

18 August 2014 Last updated at 18:09

Community Health Systems da
4.5 million

Community Health Systems has 206 hospitals across the US

**A major US hospital group said it was the victim of a cyber-atta
resulting in the theft of 4.5 million people's personal data.**



NEWS TECHNOLOGY

Home | World | UK | England | N. Ireland | Scotland | Wales | Business | Politics | Heal

3 June 2014 Last updated at 13:24

How to defend yourself against the
'two-week' attack

By Dave Lee
Technology reporter, BBC News

Various steps can be taken to ensure you are safe online

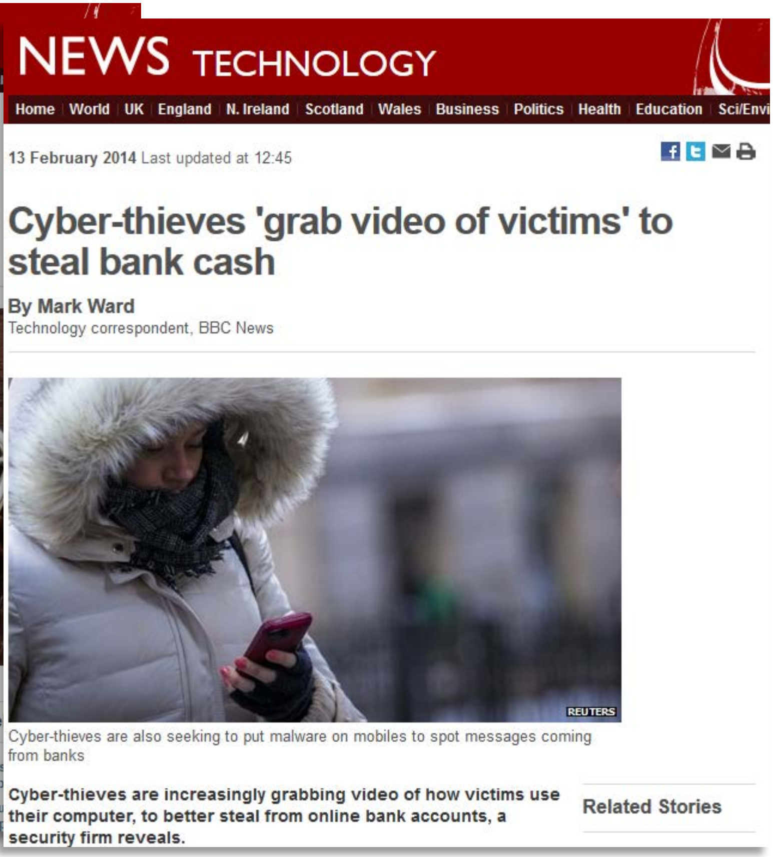
Alarming news from the UK's National Crime Agency (NCA): you have "two weeks" to protect yourself from a major cyber-threat.

The warning came as the FBI, in partnership with authorities in several countries around the world, shut down a network of criminally operated computers that were stealing important information from victims' machines.

Re

Rus
cyb

Zeu
to p



NEWS TECHNOLOGY

Home | World | UK | England | N. Ireland | Scotland | Wales | Business | Politics | Health | Education | Sci/Envi

13 February 2014 Last updated at 12:45

Cyber-thieves 'grab video of victims' to steal bank cash

By Mark Ward
Technology correspondent, BBC News

Cyber-thieves are also seeking to put malware on mobiles to spot messages coming from banks

Cyber-thieves are increasingly grabbing video of how victims use their computer, to better steal from online bank accounts, a security firm reveals.

Related Stories

Incident response…

- Can improve privacy
  - Notify victims, to reduce impact
  - Notify potential victims, to eliminate impact
- Can harm privacy
  - Collecting logs
  - Disclosing information
  - Identifying patterns
- Need to maximise benefits & minimise harm

How to get the balance right?

Some guidelines…

1) Focus on your constituency

- They are the ones it’s your business to protect
  - More likely to know you exist
    - Surprise makes privacy breach worse
  - Most likely to benefit from your activities
- You will learn of problems elsewhere
  - “Attackers” are compromised machines/accounts too
  - Notifying victim (via trusted 3rd party) probably OK
  - Wider dissemination prob. only for serious incidents

2) Avoid unnecessary processing

- Don’t collect/process information you can’t use
- Beware of “decorating” information
  - E.g. keep login/DHCP logs separate till needed
- Be very careful about (attempted) attribution

3) Think about information flow

- Direction of flow
  - “You have a problem: please fix it” (CSIRT)
  - “I have a problem: tell me who did it” (lawyer)
- Breadth of flow
  - Send information to those who can use it
- Quantity of flow
  - Don’t send them information they don’t need
    - E.g. indicate confidence, rather than disclosing source

Guidelines

- Focus on constituency
- Avoid unnecessary processing
- Think about information flows

- Mostly what you do already?

What about the law?

Look at EU, regarded as strictest…

Law supports incident response

- Notification of data subject/victim encouraged
  - Whether info received directly or indirectly
- Incident Response a “legitimate interest”
  - Now, if you’re a communications provider
  - Soonish, if you’re any other CERT/CSIRT/etc.

Draft Data Protection Regulation

“The processing of data to the extent strictly necessary for the purposes of **ensuring network and information security**, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data, and the security of the related services offered by, or accessible via, these networks and systems, by public authorities, Computer Emergency Response Teams – **CERTs**, Computer Security Incident Response Teams – **CSIRTs**, providers of electronic communications networks and services and by providers of security technologies and services, constitutes a **legitimate interest** of the data controller concerned. ...”

Draft Data Protection Regulation

“…This could, for example, include preventing **unauthorised access** to electronic communications networks and **malicious code** distribution and stopping ‘**denial of service**’ attacks and **damage to computer and electronic communication systems**.” [Recital 39]

Processing in “legitimate interest”

Three step test…

- Is interest (protecting your systems) legitimate?
- Is processing necessary for that interest?
  - i.e. no less intrusive way to achieve interest
- Does processing respect individuals’ rights?
  - A balancing test (see Article 29 Working Party)
  - Low-intrusion methods more likely to be OK
  - Major security threat may justify more intrusion

In other words…

Law

- Interest legitimate?
- Processing necessary?
- Rights protected?

CSIRT good practice

- YES: See Rec.39
- Minimisation
- Constituency focus
- Direction of disclosure
- Balancing test

e.g. Using DNS resolver logs

Interest

- Detect suspect external sites

Moderate

Rights protection

- pDNS discards local identity completely

Strong

e.g. Using DNS resolver logs

Interest

- Detect local bots etc.

Strong

Rights protection

- Requests for known bad domains
- Separate user lookup
- Don’t browse attributed logfiles

Moderate

Legal requirements ~= CSIRT good practice

To find out more…

- Ask a question now…
- See https://community.ja.net/blogs/regulatory-developments/tags/incident-response
- Read https://www.terena.org/activities/tf-csirt/publications/data-protection-v2.pdf

Other issues

- International sharing
  - Usually returning personal data to source
  - UK ICO – note privacy expectations of source country
- Big data/data mining
  - Legitimate interests probably still best legal basis
  - Might be worth developing good practice guidelines?