Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTERE DE L'INTERIEUR
DE L'OUTRE-MER ET DES
COLLECTIVITES TERRITORIALES

Responding to data breaches

Gendarmerie nationale

European Data Protection Supervisor

enisa European Network and Information Security Agency

European Parliament

Brussels, 23 octobre 2009

Lieutenant-colonel Eric Freyssinet, DGGN/SDPJ

Session 2
Management of data breaches

- A law enforcement perspective
  - The situation today -> Partnership
  - The investigative process and management of data breaches
  - Criteria for notification, for involving L.E.
  - Evidentiary issues
  - Only the telecommunications industry?

Situation

- Too few complaints about data breaches
  - > Too few investigations and arrests
  - Hope this legal initiative will improve those numbers
- Too few investigations and prosecutions on data protection crime
- The legal process is often seen as adverse:
  - Publicity of the trial
  - Investigations against companies which do not secure personal data appropriately
  - Fear of the impact of law enforcement activity on the system

Partnership

- Law enforcement and the justice need and want to be seen as partners:
  - We need confidence in the security of personal data managed by the industry, especially the telecoms industry, because it is used as evidence
  - We share the common goal of stopping those responsible of unlawful data breaches

The investigation process and the management of breaches

- Detect criminal action
- Receive complaints (before or after notification?)
- Collect evidence (and evaluate damages)
- Identify and arrest suspects
- Prosecute (and obtain compensation)

Trained personnel

(LE + Industry)

Criteria for notification, criteria for involving L.E.

- The proposed directive includes a number of criteria: personal data, scope and seriousness
- And personal data breach is (currently) defined: breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed [...]
- Room for adaptations at national level, but good practice at European level is of course advisable
- Those criteria should also take into account the nature of the attack and the impact on the system (not only on personal data)

Notification and complaint?

- In the case of an unlawful breach notified to the "competent national authority", an official complaint leading to a criminal investigation should always be considered
- It is not always possible to differentiate unlawful from accidental
- Hopefully, in many cases, serious attacks will be mitigated and personal data protected from illegal access: maybe would there be no notification, but a criminal investigation can still be necessary to stop the authors
- There is also a need for informal exchange of information about data breach incidents (statistics, trends, etc.), for a better understanding of the risks

Evidentiary issues

- We have shown that in all cases, criminal investigations are to be considered:
  - Preserving the evidence should always be a concern
  - Thus, evidence collection and preservation process must be included in recovery plans, as well as interaction with law enforcement
    - Availability and extensiveness
    - Admissibility (audit trail, digital signatures,...)
    - Format and procedures in place for the sharing of evidence

Not only the telecommunications industry

- Obviously, personal data needs to be protected, whatever the industry involved
- And obviously too, evidence that could lead to the arrest of people involved in attacks against computer systems even when no personal data is eventually at stake
- Balance between legal obligations and best practice: there is a common interest to share information about breaches and, when necessary, to initiate criminal investigations

Conclusion

- Partnership
- Involve law enforcement whenever needed
- Collect evidence
- Prepare for and plan it

Eric Freyssinet, lieutenant-colonel
Direction générale de la gendarmerie nationale
Sous-direction de la police judiciaire
35 rue Saint Didier
F-75775 PARIS Cedex 16

Tél: +33 1 56 28 66 27

Mél: eric.freyssinet@gendarmerie.interieur.gouv.fr