Data Breach Notifications

Requirements from a Civil Society Perspective

Andreas Krisch <andreas.krisch@edri.org>

www.edri.org

Introduction

- My name is: Andreas Krisch ...
- ... and I do have identities:
  - President of EDRi
  - President of VIBE!AT
  - CEO of an Austrian company
  - Private Person
  - User of Social Networks (maybe :-)
  - Hobbyist
  - Holder of bank accounts and credit cards
  - Member of diverse associations, networks, ...

Introduction

- My name is: Andreas Krisch ...
- ... and I do have identities:
  - President of EDRi
  - President of VIBE!AT
  - CEO of an Austrian company
  - Private Person
  - User of Social Networks (maybe :-)
  - Hobbyist
  - Holder of bank accounts and credit cards
  - Member of diverse associations, networks, ...

Introduction

- My name is: Andreas Krisch ...
- ... and I do have identities
- ... and I keep these identities separated
  - by using different e-mail accounts and nicknames
  - by selectively sharing information
  - by selectively revealing certain aspects to others
- ... and I'm convinced this is necessary
  - to protect my privacy
  - to maintain a correct frame for all of my activities
  - to mitigate risks

Data breaches

- are a potential threat to my identities
  - aspects of different identities might be combined
  - identities might be revealed
- are a potential threat to my financial situation
  - misuse of financial information
  - identity theft
- are a potential threat to my reputation
  - some aspects of my identities might
    - be harmful for some of my other identities
    - be misinterpreted when taken out of their context

Data breaches

- Identity management
  - helps to maintain the right context
  - helps to protect personal data
- Data breaches
  - endanger identities
  - endanger financial well-being
  - endanger personal data
- Leaked data
  - adds to the amount of published personal data
  - is out of control

Data Controllers

- should conduct risk assessments
  - before the data breach event
  - based on the sets of data processed
  - from the view of the controller **and** the data subject
- should improve data security
  - data minimisation
  - PETs
  - technical measures
  - organisational measures

Data Breach Notifications

- should be mandatory
  - for all relevant breaches
  - regardles of the business or sector of the controller
- Guidlines how to respond to breaches
  - as data controller **and**
  - as individual
  - should be developed based on risk assessments
  - before the breach event

Data Breach Notifications

- should be issued
  - when it is likely that
  - personal data (Art. 29 WP 136) or
  - privacy (see: identities!) of an individual are adversely affected
- Notifications
  - should be provided in written form
  - via usual (from individuals point of view) direct secure communication channels
  - if needed via forms of mass communication (ads in newspapers, ...)

Data Breach Notifications

- should provide at least the following information
  - specific sets of data affected
  - amount of data affected (e.g. usage data of 3 years)
  - kind of data breach (loss, illegal access, ...)
  - duration of the data breach
  - number of persons that illegally had access **or**
  - potential magnitude of persons having access
  - potential dissemination of affected data
  - potential misuses of this data (result of risk assessment)

Data Breach Notifications

- should provide the following information
  - actions that have / will be taken by the controller
  - actions that have / will be taken by authorities
  - actions that can be taken by the individual
    - whom to inform about the breach (bank, ...)
    - what actions to take (change passwords, ...)
    - how to detect misuses (observe account movements, ...)
    - whom to inform about misuses or suspicious incidents
    - how to prevent identity theft
    - where to get more information and help
    - ...

Thank you for your attention!

Andreas Krisch

andreas.krisch@edri.org

http://www.edri.org/