GDPR – How to determine the “appropriate technical and organisational security measures”?

Stéphane Adamiste
Agenda

1. Information security in a nutshell
2. Threat modelling
3. Case study
4. Tools
About the speaker

- Works for one of the largest Swiss software development and integration company
- Delivers consulting mandates directly to clients
- Assists projects on information security and data protection aspects
- Works on internal security governance

PROFILE

- 17 years of experience as an Information Security and Data Protection specialist
- Deep knowledge of audit and risk assessment methodologies, compliance to data privacy regulations, Information Security best practices and governance.
- Apprehends Information Security aspects from both a business and technical perspectives

PREVIOUS JOBS

- COO of a Swiss-based audit and consulting firm specialized in Information Security and Risk Management.
- Senior Consultant and Auditor within a Big4 company (Enterprise Risk Management division)
Information security in a nutshell
Information security in a nutshell

- Systems process data

- Systems process various types of data

- Data has a value (and therefore is called information assets)

- The value of data can be defined by evaluating the adverse impact caused to the owning organization if:
  - Data is disclosed to unauthorized people (loss of confidentiality)
  - Data is modified by unauthorized people (loss of integrity)
  - Data is not accessible when needed (loss of availability) (=! performance)
Information security in a nutshell

- An **adverse impact** is caused by a **threat** that materializes

- **Threats** materialize by exploiting **vulnerabilities** in a system

- **Information security** consists in **protecting information assets** against **threats** that may affect their **confidentiality, integrity** and/or **availability** by implementing proportionate **security controls**.
Information security in a nutshell

**Threat:** Attack on website by Internet hacker

**Vulnerability:** SQL injection

**Impact:** The back-end database can be viewed, modified and deleted, leading to productivity, legal, reputational and financial issues

**Security controls:** input validation, use of parameterized requests
Information security in a nutshell

- Information Security Management is Risk Management

- Information Risk (~ cyber-risk) = Operational risk linked to the use of information systems

Risk = Likelihood of a threat x Impact

- Hacking
- Denial of service
- Environmental hazard
- Insertion of malware
- Etc.

Impact areas:
- Safety & health
- Reputation
- Finance
- Legal
- Productivity

- Attack surface?
- Target visibility?
- Reward for an attacker ($, fame)?
- Exploitability of vulnerabilities?

- Value of data?
- Security requirements?
The car metaphor

- Car ~ Information system
- Car passenger ~ information assets processed by the system

Conclusion: To build the appropriate system, you need to consider assets processed and applicable threats
Information security management in projects

Managing information security aspects in an IT project implies:

- Identifying data types (a.k.a. information asset type) to be processed by the system
- Identifying confidentiality, integrity and availability requirements for each data type
- Identifying threats to the information assets
- Determining security measures (a.k.a. security controls) that will prevent threats from materializing

A.k.a perform a risk assessment / ISDP concept (Information Security and Data Protection)
Security controls

- Technical security controls
  - Application layer
    - Authentication
    - Access control
    - Audit (= traceability)
    - Secure Development Lifecycle
  - Infrastructure layer
  - Physical layer

- Organisational security controls
  - Human resources security
  - Data breach management
  - Etc.
Threat modelling
Threat modelling: Definition / characteristics

- Allows **early** risk detection and prevention process
  - Conducted during the design phase

- Simple
  - Pen and paper activity

- Didactic
  - Bridges the gap between tech and business

- **Editable**
  - Can be updated along with the target of evaluation
  - Can be applied iteratively

- Elastic
  - Focus on main threats vs exhaustive approach

- **Objective**
  - Provides rationale basis for decision making

**a process to identify and document threats to a particular system and their most appropriate countermeasures**
### Threat modelling flavours

**Asset-centric**
- Asset = something of value (vague)
- Determine assets
  - What we want to protect
  - What attackers want
  - Stepping stones
- Identify threats
  - No direct line from assets to threats?

**Attacker-centric**
- Identify types of “profiles” likely to threaten the system
  - E.g. script kiddie vs state
  - E.g. Human unintentional / human intentional (insider, outsider), natural (flood, fire, lightning, etc.)
  - Subjectivity / projection

**Software-centric**
- Focus on the system being built
- Based on a graphical representation of the system
- More objective / systematic
Prerequisites for threat modelling

- Get an accurate view of the system’s architecture
- Understand the business processes supported by the target system
- Have the technical security knowledge to identify threats in the architecture
Data Flow diagrams

- graphical representation of the "flow" of data through an information system, modelling its process aspects
- Popularised in the 70’s by computing pioneers Ed Yourdon and Larry Constantine in their book *Structured Design*
External entity: an outside system that sends or receives data, communicating with the system being diagrammed.

Process: any process that changes the data, producing an output.

Data store: files or repositories that hold information for later use.

Data flow: the route that data takes between the external entities, processes and data stores.
Case study
https://gaisf.org/

Application functionalities

— Purely informative site
Application features

— Purely informative site
Information assets

<table>
<thead>
<tr>
<th>Information asset</th>
<th>C</th>
<th>I</th>
<th>A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Website content</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Connection logs</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Admin credentials</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

Threat scenarios

<table>
<thead>
<tr>
<th>#</th>
<th>Scenario</th>
<th>Threat agent</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1</td>
<td>Denial of service</td>
<td>Internet hacker</td>
</tr>
<tr>
<td>T2</td>
<td>Defacement</td>
<td>Internet hacker</td>
</tr>
<tr>
<td>T3</td>
<td>Impersonation</td>
<td>Internet hacker</td>
</tr>
<tr>
<td>T4</td>
<td>Insertion of malicious code</td>
<td>Insider, Internet hacker</td>
</tr>
</tbody>
</table>
T2: Defacement, content modification

1.1 Obtaining a valid admin login
- 1.1.1 Traffic interception
- 1.1.2 SQL injection allows access to DB
- 1.1.3 Phishing attack
- 1.1.4 Account brute forcing
- 1.1.5 Account guessing
- 1.1.6 Account guessing

1.2 Obtaining a valid admin session ID
- 1.2.1 SQL injection allows authentication bypass
- 1.2.2 Session ID's are predictable
- 1.2.3 Etc.

1.3 Bypassing access control
- 1.3.1 Etc.

1.3.1 Etc.

1.1.6.1 Etc.
Generic threat trees

Web application threats
- forced sensitive operation
- credentials brute forcing
- credentials guessing
  - bad password complexity
  - bad lockout mechanism
  - bad login error mechanism
  - social engineering
  - use unique temporary activation link
  - use strong random session IDs
- session hijacking
  - poor or predictable session identifiers
  - session fixation
    - change session ID after successful authentication
    - session ID cannot be set client-side
- cross site scripting
  - use output encoding
  - set cookie "http only" flag
- long session time out
  - short session time out & log out mechanism leading to session destruction
- use "no cache" tag
- make the request that encap
Corporate risks & mitigation controls
Tools