ELCA for
GAISF
11.06.2018

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

Stéphane Adamiste

GAISF Global Association of International Sports Federations

ELCA

Agenda

1 — Information security in a nutshell

2 — Threat modelling

3 — Case study

4 — Tools

About the speaker

Stéphane Adamiste
Information Security Consultant

- 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)

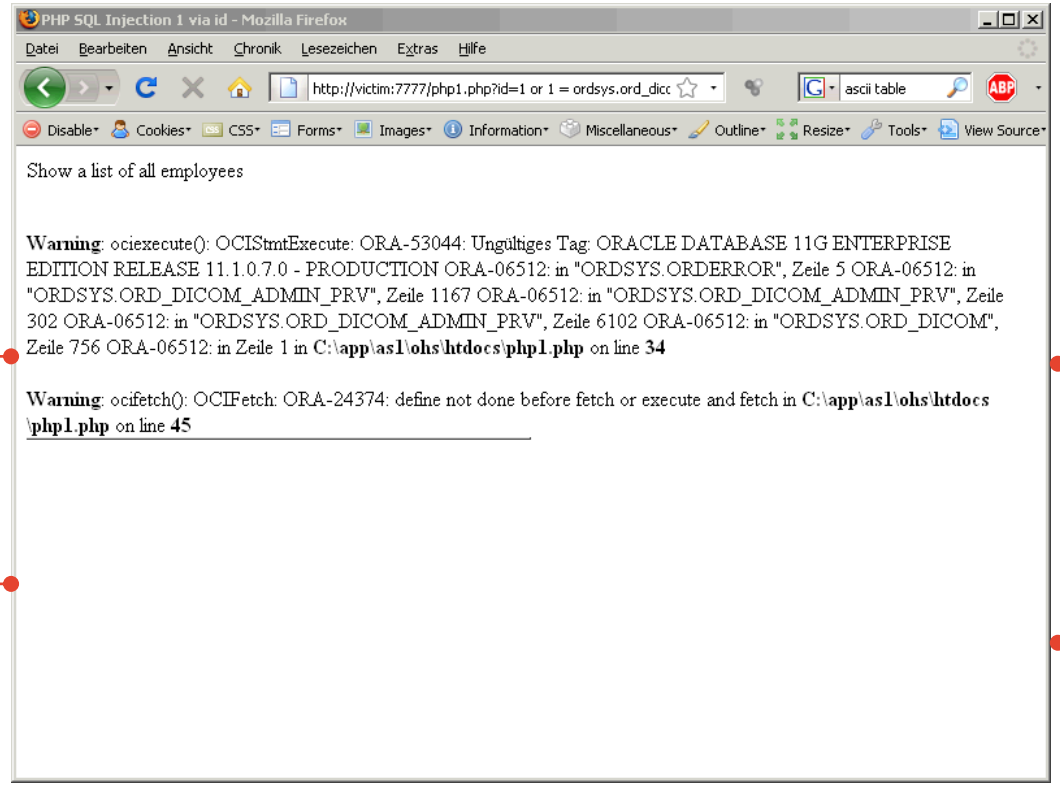
Information security in a nutshell

- 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

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

Security features

Security assurance

- Organisational security controls
  - Human resources security
  - Data breach management
  - Etc.

Threat modelling

Threat modelling: Definition / characteristics

a process to identify and document threats to a particular system and their most appropriate countermeasures

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

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

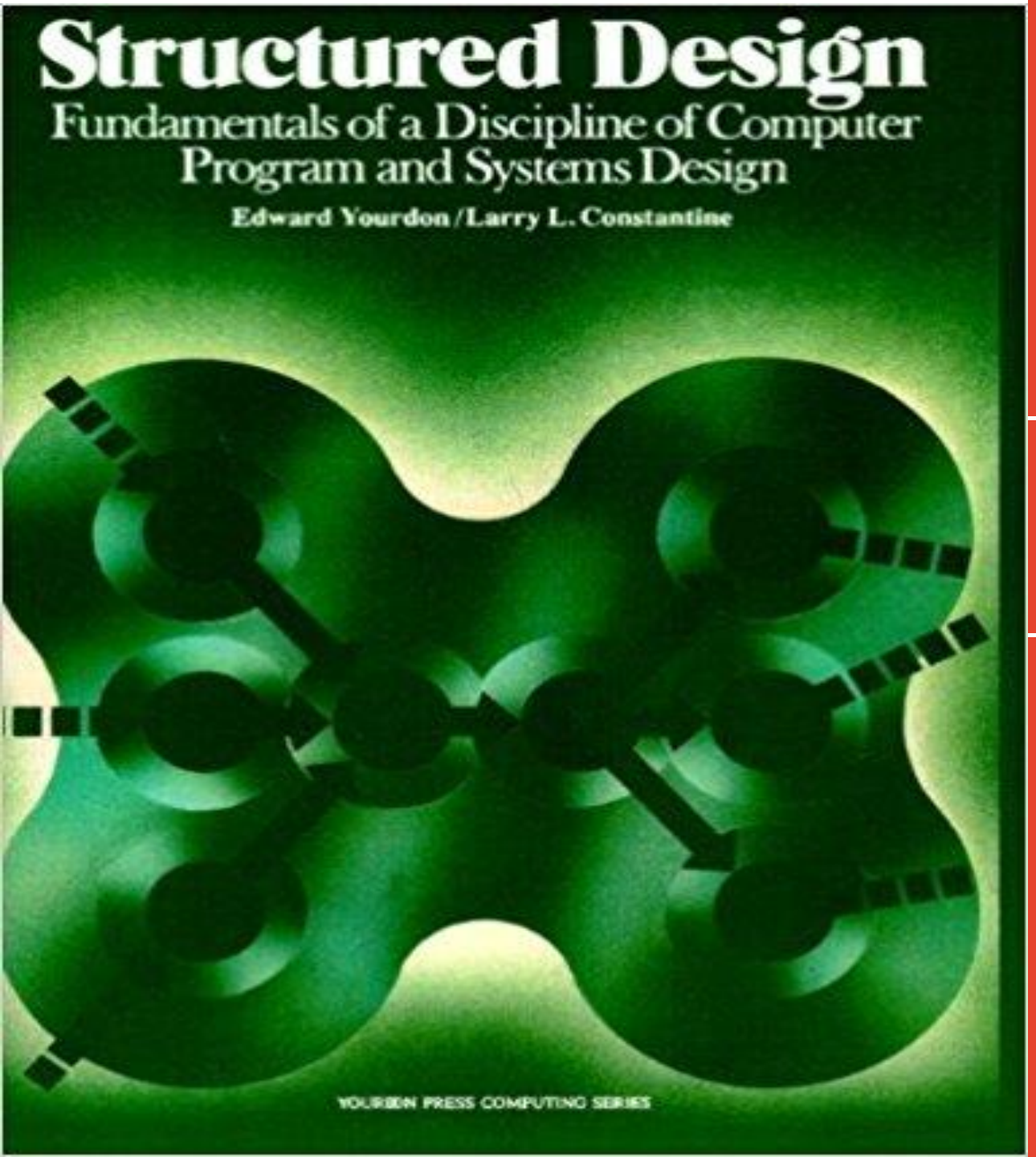
- Identify types of “profiles” likely to threaten the system
- E.g. script kiddie vs state
- E.g. Human unintentional / human intentional (insider, outsider), natural (flood, fire, lightning, etc.)
- Subjectivity / projection

Software-centric

- Focus on the system being built
- Based on a graphical representation of the system
- More objective / systematic

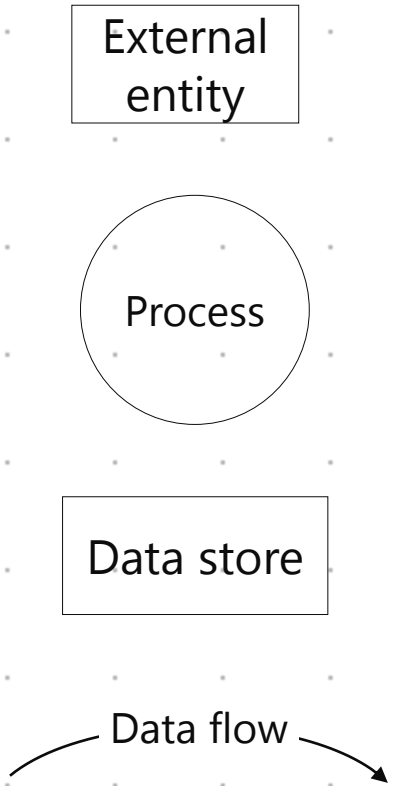
Prerequisites for threat modelling

- 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*



Data Flow diagrams symbols (Yourdon/De Marco)

- **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.

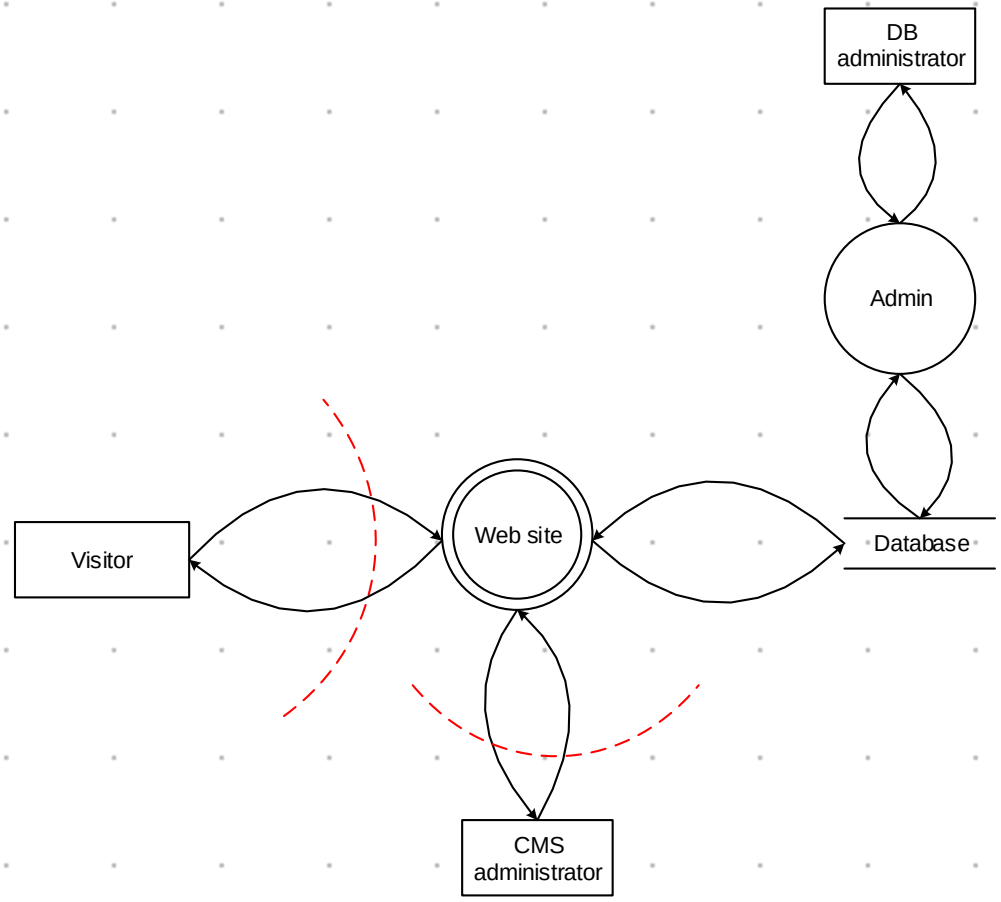
Case study

Application functionalities

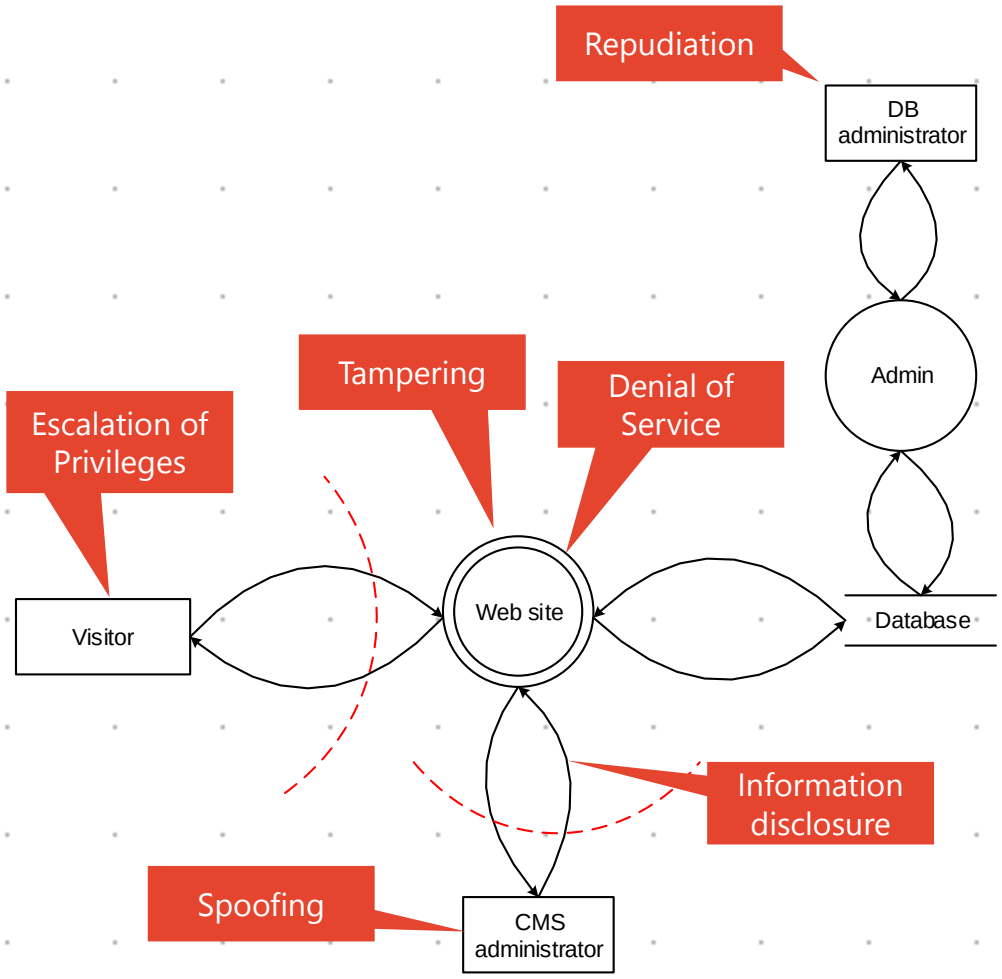
https://gaisf.org/

— Purely informative site

Application features



- Purely informative site



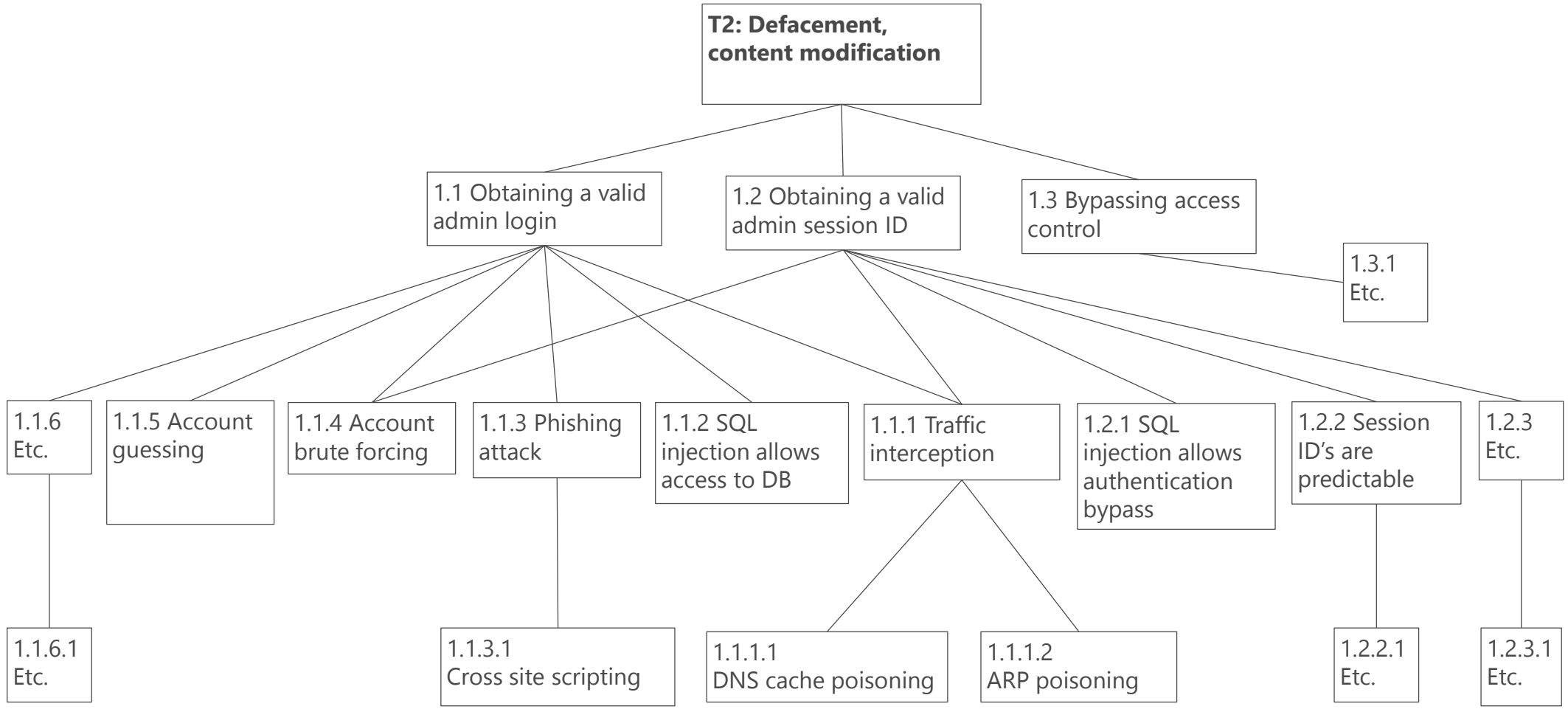
Information assets

Information asset	C	I	A
Website content		X	X
Connection logs	X		X
Admin credentials	X	X	X

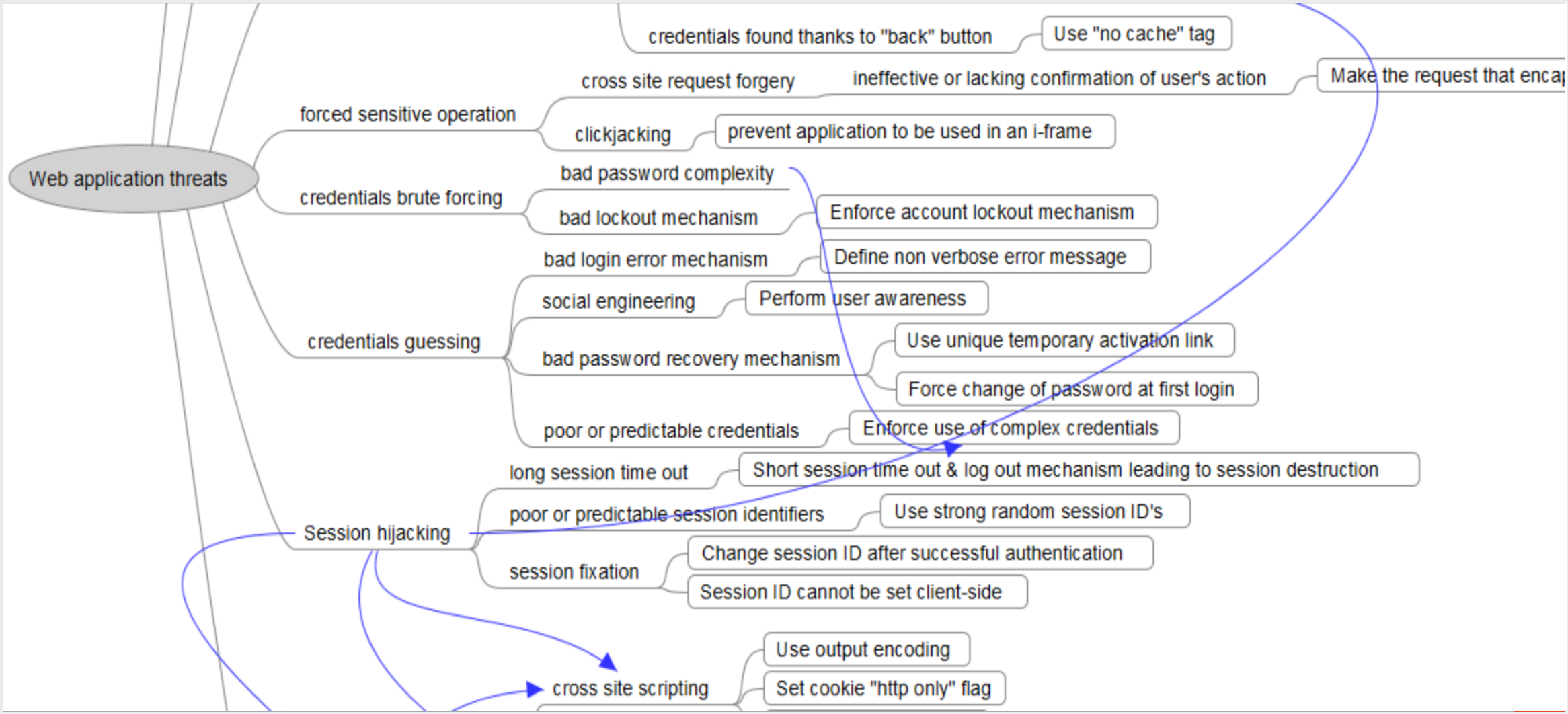
Threat scenarios

#	Scenario	Threat agent
T1	Denial of service	Internet hacker
T2	Defacement	Internet hacker
T3	Impersonation	Internet hacker
T4	Insertion of malicious code	Insider, Internet hacker

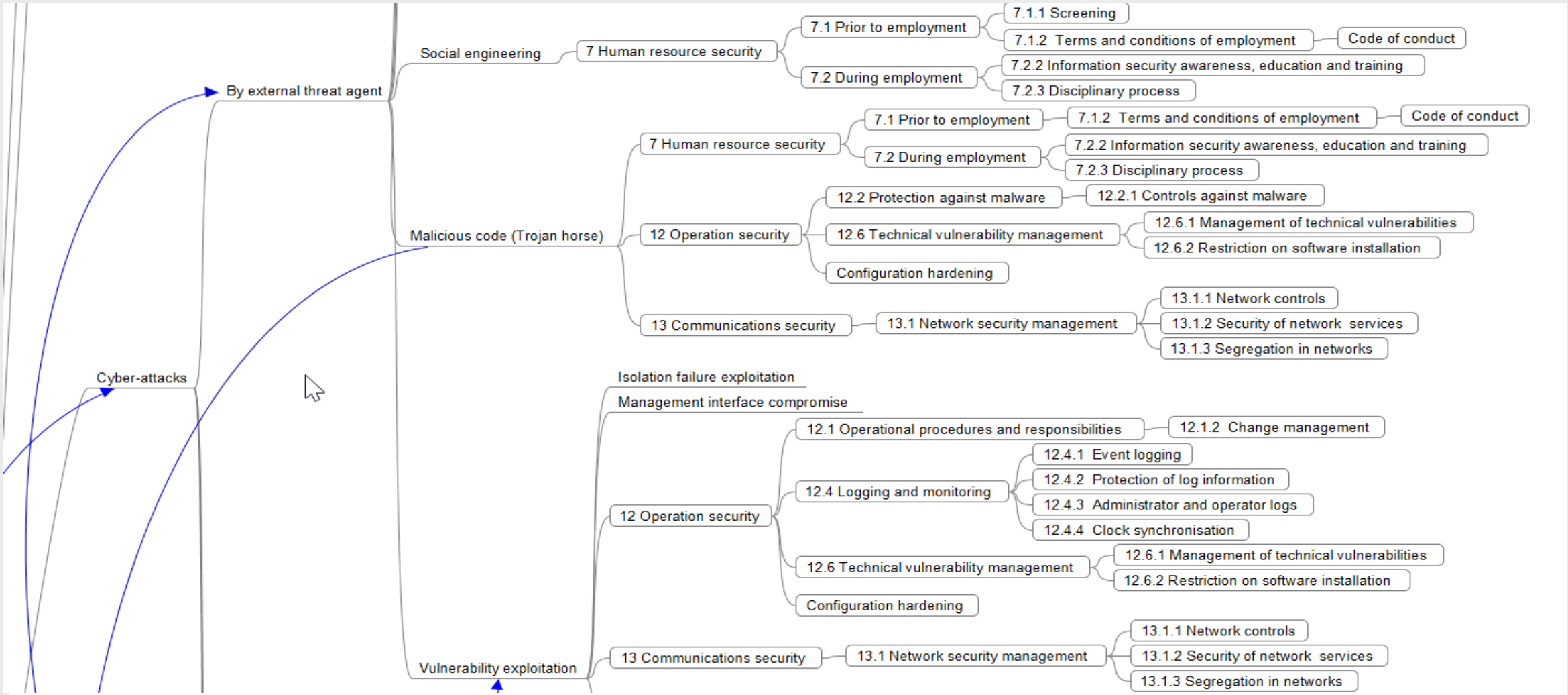
Threat trees



Generic threat trees



Corporate risks & mitigation controls



Tools