Information Security Exercise

Hans Georg Schaathun
Høgskolen i Ålesund

Week 1 Autumn 2011

Task Study a few recent security incidents reported in the public press, and analyse and describe them using the established ontology.

Objective Your goal is to demonstrate an ability to use the introduced terminology unambiguously to discuss security problems.

Submission

1. The submission should be in the form of a single PDF document.
2. Name and email address must display clearly on the first page.
3. *Deadline* is Monday 29 August 2011 by 6am in Fronter.

Contents Select two recent information security incidents to analyse, using articles from the public press (www or printed press) or any other sources to get information.

Outline The document must contain (for each incident covered) the following:

Summary a brief synopsis of the incident, identifying the organisation(s) which was affected.

List of Assets enumerating all the assets relevant for the incident, with a short description of their value. For each asset you should also establish which of the security criteria (confidentiality, integrity, availability) are relevant, and why.

Impact enumerating the impacts of the incident, identifying (for each impact) which assets are affected, and which of the security criteria are broken, with reasons.

Threat and Threat Source identifying the threat source causing the incident, or if this is unknown, discussing plausible threat sources.

References listing all the sources you have used to get information

Style Remember that this is a report as any other report, and it should be made easy and motivating to read, with the language flowing naturally, linking paragraphs and sections together in a logical way.

The length of the report will depend on the complexity of the incident and the information available. Anything between 1–2 pages per incident will be normal.

Good luck