Jan Rehwaldt, 2012-03-11, University of Tartu

Exercise 5, Principles of Secure Software Design

Scenario: University of Tartu wants to check their security against social engineering. Develop any two cases using social engineering techniques to leak the confidential information. Explain the countermeasures to avoid these attacks in future.

Scenario 1

An ERASMUS student goes to the Dean's office for issuing a signature under its Learning Agreement. When the signature is provided he further asks for a scanned copy and whether the Dean's office could possibly copy it onto his USB stick, which is prepared with malware software.

In order to make those attacks impossible no scan jobs should be performed or scan submission may only be issued to the student's UT mail address. This additionally proves that a certain person is a real student (at least has access to this address, which could also be gained by social engineering). Additionally all USB ports at office computers may be abandoned, except those required for mouse, keyboard or printer operation.

Scenario 2

A person pretending to be from IT department writes a fake email Friday morning from IT staff's address that the computers need to be security-checked during the lunch break. Just before lunch starts he enters the office and kindly asks for computer access. The office worker is asked to login (stay logged in) and allowed to have lunch. After the worker left full access to computer systems is granted for around 30 minutes.

Countermeasures could be the checking of an ID card before trusting random IT staff, but this may be easily faked. Before issuing system access any employee should call a pre-specified number within IT department to verify that the IT task is issued by them.