2. Exercise sheet
Hand in solutions until Wednesday, 13 November 2013, 23:59

Exercise 2.1 (“IT-Grundschutz”).
(20 points)

At

https://www.bsi.bund.de/EN/Publications/BSIStandards/standards.html

you find the BSI documents about IT-Grundschutz [basic protection for IT]. Say, you are the Security Officer responsible for setting up a computing centre for a new cloud for a government-secure voice phone service. (Speculate where additional information is needed.)

(i) Consider the threats catalogue and name at least one example of a threat that

(a) is a natural disaster.
(b) maybe seen as a random attack.
(c) is a human factor.
(d) is an intentional attack.
(e) is an internal attack.
(f) is an availability issue.

Now we turn to BSI 100-2.

(ii) What are your first steps for the security process?  

(iii) Illustrate the security risks and effects of security incidents.  

(iv) Illustrate the processing of a phone call: which data has to be handled, classify in short-term and long-term data? Which long-term data must be available? When is short-term data it created, stored, modified, deleted?

(v) Sketch a security policy. (At most half a page.)
Exercise 2.2 (DDoS). (8+4 points)


(i) Where does the data come from?

(ii) Does an attack’s source country indicate the location of the attacker?

Find the attack with the largest peak data rate observed during the last two month.

(iii) When did it occur and how long did it endure?

(iv) What type of attack was it?

(v) What has been its target?

(vi) Which port(s) were attacked?

(vii) Are these port(s) registered? For which application?

(viii) Was it an attack?

And finally:

(ix) What can individual sites do to protect themselves from DDoS attacks?