## UC: Network Security

## TP1 Report – Simplified Risk Analysis /Análise de Risco simplificada

## Students (Nº / Name):

**António Lourenço (68452)**

**Jorge Ribeiro (60027)**

**Pedro Alves (61893)**

## Introduction

Information security has 3 requirements/constraints:

- **C**onfidentiality
- **I**ntegrity
- **A**vailability

Information Security is an engineering problem, concepts to solve it:

- Vulnerability: bug that allows to violate one of the constraints.
- Exploit: way to use vulnerabilities to accomplish an objective that violates the constraints.
- Asset: what is valuable for an organization (E.g. hardware, software, data, reputation).
- Threat: potential violation of the constraints.
- Risk: statistical and economical evaluation of the exposure to damage because of the presence of vulnerabilities and threats.

RISK = ASSETS x VULNERABILITIES x THREATS


| Threats / Ameaças | Attacks / Ataques | Vulnerabilities / Vulnerabilidades |
|---|---|---|
| **Denial of service** | DdoS Attack | -Inability to identify traffic as illegitimate and block it |
| **Identity theft** | Password guessing/snooping | -Single-factor authentication<br>-Not forcing the user to change the password from time to time<br>-Abnormal for humans to keep secrets |
| **Data Leak** | SQL injection<br>Disclosure | - user input incorrectly filtered<br>- Human factor; wrong assumptions about thrust and boundaries |

**Critical resource / Recurso crítico: (justified / justificado)**

Estonia is the most advanced digital society in the world, every task that can be done with a digital service, is done that way. Some examples are e-voting and that almost all of the country's tax returns are made on-line, taking users an average of five minutes to fill in the parts that hadn't been automatically completed by the link between the tax office and local banks. Besides, they have a free Wi-Fi network that covers most of the populated areas and huge amounts of fiber-optic cabling.

This is very positive, but also means that a lot of information is on-line, which causes the risk to be much higher and the critical resources to be many. We consider that perhaps the most critical resource is one's identity. If someone's identity gets stolen, very serious damage can be done.

Reference for the first paragraph:
http://www.wired.co.uk/magazine/archive/2015/07/features/estonia-e-resident

**Security control / Controlo de segurança: (justified / justificado)**

To protect one's identity, from the authentication's point of view, the most effective thing to do is to create multi-factor authentication. Authentication (providing proof for identity), can be done through (one or a combination of more than one) 3 different factors. Being those factors something the entity knows, something the entity has or something the entity is (To know, to have or to be). Combining more than one of these factors will make the authentication's security more effective, even though it will have a cost in matters of usability.