Systems and Information Security
SEGSI

TP06

Security Plan

Pinto Leite, Jorge (jpl@isep.ipp.pt)

Departamento de ENGENHARIA INFORMÁTICA
Instituto Superior de Engenharia do Porto

Security Plan - background

- European Union published on 2016 a directive concerning the measures to assure a high level of security of systems and information systems on all EU
- As a directive, its application in not immediate on all EU members, but need to be translated and incorporated on each country legal system
- In Portugal, that was done by Law 46/2018 of 13 August
- That Law, however, refers to complementary (Portuguese) legislation to frame additional or define mandatory requirements of the EU directive
- Finally, Decree-Law 65/2021 was published on 30 June 2021, clarifying and complementing all the undefined aspects
- On next slide this Decree-Law will be referred as 65/2021

Security Plan - background

- As stated on Article 7 of 65/2021, all entities must elaborate and keep updated a Security Plan, properly documented e signed by the Chief Information Security Officer (CISO)
  - That document is exclusively internal of the entity and does not need to be turned public nor provided to the country authority
- A Security Plan is a structured document that describes how the entity addresses all its needs under information security
- Those needs are expected to change dynamically, implying that the plan itself is also dynamic

Security Plan - background

- The required information on the plan can be grouped on the following components

Security Plan

Adopted measures

Security responsible

Permanent contact point

Security Plan - background

- Security Plan
  - Includes security policy itself, including the description of the organizational measures and human resources training
- Adopted measures
  - Description of all adopted measures in terms of security requirements e incident notification
- Security responsible (CISO)
  - Nominal identification – it cannot be an organization, needs to be a specific person
- Permanent contact point
  - Identification of contact(s)
  - Needs to be nominal, however can be more than one person as long as the contact is the same
    - In case of need, the national security team will get in touch with an email or phone number without the need to know the schedule of organization team and who is on duty

Security Plan - background

- Each country authority might define their own suggestions for the Security Plan, so we are going to adopt suggestions of the Portuguese one (Centro Nacional de Cibersegurança, CNCS, https://cncs.gov.pt)

Security Plan

- Description of actual state of information security with plans of future improvement for the entity, taking into consideration the following aspects
  - General Security Policy
  - Description of all adopted measures in terms of security requirements and incidents notification
    - These measures must include, at least, Incident Management, Business Continuity e Human Resources Management
  - Human resources training
  - Responsibilities and calendar
  - Identification of the responsible for security and permanent contact point
  - Validity and plan revision

General Security Policy

- The General Security Policy can be seen as a high level declaration of the purpose and intention of the entity regarding information security
- It must include driven lines for a specific intention for all people, on all hierarchical levels

Description of adopted measures

- The Security Plan should specifically cover Cybersecurity and the organizational measures needed to safeguard physical and virtual assets, business or activity information, as well as personal data
- Those measure should address important areas like the Incident Management, Business Continuity, Disaster Recovery, Human Resources Management, to ensure that in the occurrence of a disruptive event the entity is able to adequate and sufficient response to safeguard information and operations through a consistent approach
- Taking in consideration the Incident Management, the term *Incident* should be clearly defined

Description of adopted measures

- Within the scope of Human Resources Management, it should contemplate Cybersecurity on RH processes, at least:
  - Categorize functions (roles, scope, responsibilities and risk)
  - Carry out hiring screening, based on the perceived risk of the position
  - Implement processes for assigning and reviewing physical and logical access to networks and information systems and facilities (for example, Identity Management)
  - Trigger disciplinary proceedings in the event of non-compliance

Human resources training

- Entity should establish training plans on Cybersecurity and Information security (also infrastructure security for the applicable people), as well as define the necessary processes and procedures to ensure their correct implementation
- The success level of the trainings should be measured
- As so, the entity must therefore create, disseminate and update:
  - A plan for information security training actions
  - Formal processes and procedures that simplify the implementation of actions
  - Measure the success of the training actions carried out by interviewing the trainees
  - Keep a record of training sessions, their contents and participants

Responsibilities and calendar

- Must include a time plan detailing how and when the elements of the plan are realized
- These dates also provide the targets to be achieved, which serve as a benchmark for management to management to monitor the progress of their implementation
- Associated with the time plan, the people responsible for implementing the security requirements
  - This documentation is essential for those responsible for coordinating the individual tasks together with the individual tasks together with the safety experts, making it explicit who is (or can be) the person responsible for ensuring the proper implementation of requirements or the response to detected vulnerabilities

Identification of the responsible for security and permanent contact point

- The names and two (at least) contact methods (like email and phone number) for each of them are mandatory components of the document

Security responsible	Permanent contact point
Name: Email Phone number:	Name: Email Phone number:

Validity and plan revision

- The Security Plan must be reviewed periodically
- Other factors such as the evolution of technology, changing vulnerabilities and attacks, the obsolescence of solutions or changes in the legal or regulatory framework, that require a review of the organization's existing information security management system should be part of the validity

Points to keep in mind

- A Security Plan must be created and updated
- The Security Plan must be signed by the CISO
- National Laws might provide a timeline to create it
- Ensure that the elaboration of the Security Plan contains all the needed information and is always updated
- It is a mandatory, yet, internal document