Departamento de Engenharia Informática

MEI

Engenharia de Segurança Informática

ESEGI - Assignment 3

Security and Contingency Plan

Security Plan

Author:
Daniel Dias (1181488)
Vitor Neto (1210130)

Submitted to:
Prof. Jorge Pinto Leite

June 19, 2022

Contents

List of Figures

Abstract No usable system is 100 percent secure or impenetrable. Nevertheless, there are some behaviours that may expose our systems to possible attacks that may cause considerable danger across an entire organization. Cyberspace is understood as a complex environment of values and interests, materialized in an area of collective responsibility, that results from the interaction between people, networks and information systems. This complex and heterogeneous environment offers new possibilities and opportunities but it also creates new threats and a risk environment that can lead to the occurrence of incidents with economic and social impacts that can not be underestimated. The purpose of this document is to provide a security plan for a Portuguese Health Institution. It provides instructions, recommendations, and considerations on how to create a more secure infrastructure, encompassing IT services and data. The methods and results used and obtained to develop this paper will be based on the Portuguese Council of Minister's baseline from the 41/2018 resolution. This paper has been developed by two ISEP master's degree computer engineering students in the context of the curricular unit ESEGI (Engenharia de Segurança Informática), lit. Informatics Security Engineering.

1 Introduction

1.1 Purpose

This Security Plan constitutes the "Standard Operating Procedures" in terms of guidelines, recommendations and considerations regarding the technological infrastructures of a Portuguese Health institution. More specifically, the approach in terms of the architecture of the network and the information system as well the treatment of user personal data.

For areas covered by existing processes and/or technologies, the plan briefly documents how and where this is accomplished.

1.2 Scope

This plan was developed to be applied in the technological infrastructures of a Portuguese Health institution. A Senior Manager responsible for the cybersecurity matters of the organization will be responsible to expose this document to the members of the institution as well making sure that these guidelines are being implemented.

1.3 References and Requirements

This contingency plan complies with the following baselines and requirements:

- 41/2018 resolution of the Portuguese Council of Ministers; [1]
- European Law document 32016R0679 (GDPR); [2]
- The personnel is properly trained and reminded of the existence of this document on a set timely basis;
- This document must be reviewed and updated as technology evolves and must always comply with the set latest resolutions and baselines of the Portuguese Council of Ministers, European Council and European Law;

2 Addressing People and Policy Risks

Training people to adopt security conscious behaviors and establishing policies for maintaining a secure environment go a long way toward improving an organization's overall security posture.

2.1 Cyber Security Policy

- Assign responsibility for developing, implementing, and enforcing cybersecurity policy to a Senior Manager. Ensure that the Senior Manager has the requisite authority across departments to enforce the policy.
- Define security-related roles and responsibilities.
- Define the implementation plan and enforcement mechanisms.

2.2 Personnel and Training

Insufficiently trained personnel are often the weakest security link in the organization's security perimeter and are the target of social engineering attacks. It is therefore crucial to provide adequate security awareness training to all new hires, as well as refresher training to current employees on a yearly basis.

- Establish a security-awareness program.
  - Ensure that all personnel have an understanding of sensitive information, common security risks, and basic steps to prevent security breaches. Further, ensure that personnel develop habits that would make them less susceptible to social engineering attacks.
- Train employees who have access to protected assets.
  - Ensure that employees who have electronic or physical access to critical assets know how to handle the assets securely and how to report and respond to cybersecurity incidents.
- Enforce "least privilege" access to cyber assets and periodically review access privileges.
  - Ensure that employees have only the privileges they need to perform their jobs - **Need-to-Know** Principle.

3 Addressing Process Risks

Process gaps leave the door open to an adversary. For instance, failure to conduct a vulnerability assessment of a system when introducing new functionality may allow a security weakness to go undetected. To provide another example, lack of periodic review of system logs may let a breach go undetected. Instituting and following proper security processes is vital to the security of an organization. The following checklist summarizes the various security best practices and controls that the organization should implement:

- Perform periodic risk assessment and mitigation, including threat analysis and vulnerability assessments.
- Control, monitor, and log all access to protected assets.
- Redeploy or dispose of protected assets securely.
- Define and enforce secure change control and configuration-management processes.
- Create and document incident-handling policies, plans, and procedures.
- Create and document contingency plans and procedures.
  - Ensure that the organization is prepared to act quickly and correctly to recover critical assets and continue operations after a major disruption.
  - Train employees in incident handling and contingency plans.

4 Physical Security Risks

Physical security measures aimed at protecting critical infrastructure of the smart grid are of paramount importance and form a key element of the overall security strategy. While other controls need to exist for defense in depth in case the adversary is successful in gaining physical access, physical security concerns should not be underestimated.

- Document, implement, and maintain a physical security plan.
- The organization must document and implement the technical and procedural controls for monitoring physical access at all access points at all times.
- All physical access attempts (successful or unsuccessful) should be logged to a secure central logging server. Logs should be retained for at least 90 days.
- Each physical security system must be tested at least once every three years to ensure it operates correctly.
- Testing and maintenance records must be maintained at least until the next testing cycle.

4.1 Storing Systems Redundancy

The storing systems must assure redundancy and availability, not giving a chance of existing a "single point of failure".

- The processing and storing architecture must guarantee the following properties: **redundancy**, **resilience** and **availability**;
- It should exist two types of backups (online and offsite), that should obey to the same security requirements defined for the productive systems;
  - The *offsite backups* must be saved in a localization that isn't exposed to the same external risks of the original localization, it can be part of the organization but it must geographically distinct.

5 Network and Information Systems Safety Architecture

When developing software, it's recommended to follow some guidelines on safe coding in order to reduce the possibilities of an attack. In the case of this web page, a lot of sensitive data is being transmitted from Point A to Point B, so it's important to make that our Network is prepared to handle those transmissions of data in a efficient, private and stable way.

5.1 Application development (*Web*, *Android*, *IOS*)

The information regarding COVID-19 information is accessed by a webpage, these client applications must be developed adopting proceedings of safe software development.

→**FrontEnd**

- Follow good development practices, for example, the Open Web Application Security Project (OWASP)[3], in regards to the development of safe code and the submission of that code to safety tests which respects the development of secure code and submission of that code to security tests.
- Use of secure sessions with Security protocol.
  - It is recommended to use **Transport Layer Security** (TLS), in its latest version.
- Do not store personal information in the browser, memory or disk, beyond the time of the session and only to the extent necessary.

→**Application Level** (*Backend*)

- Use of secure sessions with security protocol.
  - It is recommended to use **Transport Layer Security** (TLS), in its latest version, for the communication with the adjacent layers.
- If possible, use certificates through Application Programming Interface (API), thus not requiring the use of keywords.
- The use of plain text credentials **is not allowed**, either in the code or in the configuration files
- Embedding plain text (non-encrypted) passwords and other secrets (SSH Keys, DevOps secrets, etc.) into the source code should be avoided.
- Credentials that need to be stored in configuration files must be encoded **(HASH — minimum SHA 256)**.

→**Database Level**

- Communication with the application layer through authentication by certificate valid for a period not exceeding 2 years, in case the layers are physically or logically distinct.
  - Example: ITU-T Standard X.509 for Key Infrastructure Public (ICP).
- Predict personal information cipher (minimum 2048 bit is recommended) only if the client application has a physical and logical *DataBase* layer distinctly, preferably using technology that allows interoperability between systems.

5.2 Authentication

The capacity for authenticate and authorize every users and devices, including the control of access to systems and applications.

→**FrontEnd**

- The authentication process must always be initiated and kept in a secure session.
- It is recommended:
  1. the use of TLS, in its most recent version;
  2. use of a password, preferably in combination with another factor (Double Factor Authentication-2FA), such as:
     - Password + SMS Token
     - Password + Smartcard
     - Password + Biometrics
     - Password + graphic pattern
     - Password + Coordinate Card
     - Password + temporary random code (less than 5 minutes expiration date) sent in the form of a QR-Code.
- Personal session data excluded from Uniform Resource Locator (URL) variables or other user-visible variables.
- Login credentials passed through the **HASH** (minimum Secure Hash Algorithm-256 (SHA-256)) or use of encryption or encryption for the transmission of personal data (name, username and password in HASH and other encrypted data).

- Where applicable, the password must be at least 9 characters long (13 characters for users with privileged access) and be complex. Its composition should require the inclusion of 3 of the following 4 character sets: lowercase letters (a...z), capital letters (A...Z), numbers (0...9) and special characters [! @ # $ % &̂ ( ) _ + | ' - = [ ] : " ; ' < > ? , . /]. Alternatively, it can consist of sentences or excerpts from long text known to the user, without a "space" character.

- It is recommended that for new systems, **Double Factor Authentication** (2FA) should always be used as the authentication default.

→**Application Level** (*BackEnd*)

- The **administrators password** must be at least 13 characters long and complex. In this case, its composition should require the inclusion of are 3 of the following 4 character sets: lowercase letters (a...z), capital letters (A...Z), numbers (0...9) and special characters [! @ # $ % &̂ ( ) _ + | ' - = [ ] : " ; ' < > ? , . /]. It may, alternatively, consist of sentences or excerpts of text long known by the user, without a "space" character.

- For all administrators, **2FA** Authentication Standard must be used: Examples:
  - Password + Smartcard
  - Password + Biometrics
  - Password + certificate (eg X.509, from ITU-T for ICP, valid for a period not exceeding 2 years).

- As an information protection and security mechanism, the use of Token is recommended.

- Communication with *FrontEnd* or *Database* layers via secure session, with prior authentication if layers are physically or logically distinct.

- Embedded passwords in code should be avoided. When this is not possible, they must be encoded (HASH, minimum SHA-256).

- If possible, use certificates through API, not being necessary the use of passwords.

- Authentication of communicating elements guaranteed by validation of static information at the network level.

  Examples:

  1. Use of fixed IP + hostname + MacAddress + factors
  2. Use of certificates

→**Database Level**

- The password must be at least 13 characters long and complex. In this case, its composition must require the inclusion of 3 of the following 4 character sets: lowercase letters (a...z), uppercase letters (A...Z), numbers (0...9) and special characters [! @ # $ % &̂ ( ) _ + | ' - = [ ] : " ; ' < > ? , . /]

- Personal authentication data, transmitted through your HASH (minimum SHA-256), or using cipher or encryption to perform this transmission.

5.3 Privilege and Access

Attribution of access rights and privilege in a restrict and controlled manner.

→**FrontEnd**

- Creation of profiles with the least privileges, where each type of profile is defined according to the Type of Personal Data accessed and Action you can do on Personal Data (Create, Read, Update, Delete — CRUD), according to the **Need-to-Know** principle.
  - The **Need-to-Know** principle states that a user shall only have access to the information that their job function requires, regardless of their security clearance level or other approvals.
- Creation of access, alteration and removal logs (logs), with information on who accessed, where they accessed (IP and Port), when they accessed, what data you accessed, what action was taken on them (CRUD).

→**Application Level** *(Backend)*

- Creation of profiles with least privileges, where each type of profile is defined according to the Type of Personal Data accessed and Action you can make on the Personal Data (CRUD), in accordance with the **Need-to-Know** principle.
- Creation of access, alteration and removal logs (logs) with information about who accessed, where they accessed (IP and Port), when they accessed, what data you accessed, what action was taken on them (CRUD).

→**Database Level**

- Creation of profiles with least privileges, where each type of profile is defined according to the Type of Personal Data accessed and Action you can make on the Personal Data (CRUD), in accordance with the principle of the need to know.
- Creation of access, alteration and removal logs (logs), with information on who accessed, where they accessed (IP and Port), when they accessed, what data you accessed, what action was taken on them (CRUD).

5.4 User Access checks and regulations

Review of users access rights in regular intervals.

→**FrontEnd**

- User account renewal process according to the same security requirements as when creating the same, and should not have a life cycle greater than 180 days.
- User account life cycle management must take into account the segregation of existing roles and the access privileges that must be associated with these functions, at all times (private minimum allowances, where each type of account is defined according to the Type of Personal Data you access and Action you can take on the Personal Data (CRUD), according to the **Need-to-Know** principle.
- Alarms for user accounts with no activity recorded for a period longer than 3 months.
- A user account must be deactivated when there is no activity on the account for 3 months.

→**Application Level** *(Backend)*

- Profile validity management process is mandatory.
  - Automated profile validity management process is recommended.

- Automated process or interoperable with the systems responsible for managing the functions associated with the privileges assigned to each profile. In cases of asynchronous checking of the *function/privacy* binomial, the same must occur with a periodicity, at most bimonthly or when there is a change in the personnel map associated with this function.
- Alarms for user accounts with no activity recorded for a period longer than 3 months.

→**Database Level**

- Profile validity management process is mandatory.
  - Automated profile validity management process is recommended.
- Automated process or interoperable with the systems responsible for managing the functions associated with the privileges assigned to each profile. In cases of asynchronous checking of the *function/privacy* binomial, the same must occur with a periodicity, at most bimonthly or when there is a change in the personnel map associated with this function.
- Alarms for user accounts with no activity recorded for a period longer than 3 months.

5.5 Check Correct Use of Data by Users

Ability to make sure that users use data in a properly way.

→**FrontEnd**

- User account life cycle management must take into account the segregation of existing roles and the access privileges that must be associated with these functions, at all times (private minimum allowances, where each type of account is defined according to the Type of Personal Data you access and Action you can take on the Personal Data (CRUD), according to the **Need-to-Know** principle.
- Alarms for user accounts with no activity recorded for a period longer than 3 months.
- A user account must be deactivated when there is no activity on the account for 3 months.

→**Application Level** *(Backend)*

- For systems, network and application administrators, in case of accessing personal data, the requisites from the *FrontEnd* Layer also apply.
- User accounts validity management process is mandatory.
- Automated user accounts validity management process is mandatory.
- Automated process or interoperable with the systems responsible for managing the functions associated with the privileges assigned to each profile. In cases of asynchronous checking of the *function/privacy* binomial, the same must occur with a limited periodicity:
  1. A bimonthly period
  2. When an alteration on the personnel associated to this function is verified
- Alarms for user accounts with no activity recorded for a period longer than 3 months.

→**Database**

- For systems, network and application administrators, in case of accessing personal data, the requisites from the *FrontEnd* Layer also apply.
- User accounts validity management process is mandatory.
- Automated user accounts validity management process is mandatory.
- Alarms for user accounts with no activity recorded for a period longer than 3 months.

5.6 Profile Creation

Access restriction to the information based on the **Need-to-Know** principle, previouly mencioned, when it comes to the creation of a profile.

→**FrontEnd**

- Associate types of data to specific profiles, individuals and people associated to the function, with minimum privileges, where every type of profile is defined depending on the type of personal data that access and what action can perform on that kind of personal data (CRUD), according to the **Need-to-Know** principle.

→**Application Level** *(Backend)*

- Associate types of data to specific profiles, individuals and people associated to the function, with minimum privileges, where every type of profile is defined depending on the type of personal data that access and what action can perform on that kind of personal data (CRUD), according to the **Need-to-Know** principle.
- Registration process of the attempted logins to data outside of the privileges associated to that profile (any profile, including *admins*). Alarms for user accounts with a certain number of attempts (3 attempts for example), notifying the responsible for data protection of the organization.

→**Database**

- Associate types of data to specific profiles, individuals and people associated to the function, with minimum privileges, where every type of profile is defined depending on the type of personal data that access and what action can perform on that kind of personal data (CRUD), according to the **Need-to-Know** principle.
- Registration process of the attempted logins to data outside of the privileges associated to that profile (any profile, including *admins*). Alarms for user accounts with a certain number of attempts (3 attempts for example), notifying the responsible for data protection of the organization.

5.7 Ability to monitor, record and analyze all access activity in order to search likely threats.

- An activity record (log) of all actions that a user performs on personal data must be kept, regardless of their profile and role.
- All activity records (log) must be stored in read-only mode and, with a maximum frequency of 1 month, must be included. recorded in a single block of records and digitally signed (guarantee of integrity).
- An activity record (log) of all accesses and failed access attempts must be kept, complying with the above requirements.
- Ensure that activity records from the various subsystems (Operating Systems, applications, browsers, Database Management System Data, etc.) are unambiguously associated with their origin.
- Activity records (log) must contain, at least, the access address (IP and Port), Host, HASH of the user account that performed the action, action taken, (CRUD), Personal Data Type where the action was performed, date/time/minute/second (TimeStamp) of the action, change made to personal data.

5.8 Automatic content inspection to search for sensitive data and remote system access to from outside the organizational environment

In order to make sure that the entity responsible for the treatment of data defines and implements information protection mechanisms having in consideration it's relevance and criticality, it must be implemented:

- Threat detection by the perimeter defense of the system (for example, rules defined in the firewall, Intrusion Detection System — IDS, etc.);
- Extension of this protection desirably to all devices (including mobile) with access to personal data on the corporate systems;
- Point-to-Point cryptographic system whenever there's the need of remote access to *FrontEnd* (and only this layer), by using, for example, the Virtual Private Network (VPN) technology.

6 Personal Data Safety

The policies that guarantee the safety of the personal data must encompass:

- The prioritization and classification of the data according with the criteria of sensibility and criticality predefined
- The creation;
- The modification;
- The transmission;
- The collection of that personal data (independent from the respective process or means used to obtain);
- The destruction;
- The storing process (retention included);
- The process of searching data;

Knowledge of information assets regarding personal data must be guaranteed at all times, in order to unequivocal identify the state of the information throughout its life-cycle.

6.1 Respect the Rights of the Data Owner

The network and information systems must possess the required functionalities necessary to respect the rights of the data owner.

- The systems should have the ability to classify, prioritize, search, edit and delete personal data.
- The systems must possess the necessary controls that allow identification, authentication, access and validation of the stored personal data.

6.2 Portability and exportation of personal data

The information technologies to be implemented must allow the portability and exportation of personal data.

- The use of compatible digital formats must be guaranteed, ensuring technical and semantic interoperability within the Public Administration, in the interaction with the citizen or with the company and for the availability of content and services, adopting the technical specifications and formats defined in the National Regulation on Digital Interoperability, approved by the Resolution of the Council of Ministers no. 91/2012, or in another that will replace it.

6.3 Data Protection

Data protection against unauthorized modifications, losses, robberies and unauthorized disclosure.

→**FrontEnd**

- *FrontEnd* developed and in production according to the best safety practices, securing this layer from the most common attacks (SQLi, code injection,etc.).
- The good practices presented in Open Web Application Security Project (OWASP)[3] are recommended.
- The previous provisions concerning security of access assignation, personal data safety and the tracking of the activity carried out on the personal data, are also applied.

→**Application** *(Backend)*

- BackEnd Application layer segregated from the network or environment with visibility and/or exterior access.
- The previous provisions concerning security of access assignation, personal data safety and the tracking of the activity carried out on the personal data, are also applied.

→**Database**

- Database Application layer segregated from the network or environment with visibility and/or exterior access.
- The previous provisions concerning security of access assignation, personal data safety and the tracking of the activity carried out on the personal data, are also applied.
- Anonymization, Masking or, being necessary, encryption of the personal data transmitted or accessed.
- Stored data (including the *backups*) must be encrypted and signed digitally.
- It is recommended that, for personal data considered to be extremely critical, it's storing process must be made in a fragmented way and in physical distinct locations, while still maintaining all its uniqueness and logical integrity.

6.4 Sender/Receiver identification

Capacity of guaranteeing the correct identity of the sender and the receiver when transmitting personal data.

- The integrity of the Domain Name System (DNS) zone where the system and ecosystem are inserted must be assured. For that the good practices of DNSSec and the configuration Email Systems (for example, Sender Policy Framework - SPF, DomainKeys Identified Mail - DKIM, Domain-based Message Authentication, Reportanting and Conformance - DMARC, among others) should be applied.
- It should be used a safe communication technology (for example, VPN), with a strong authentication system (preferentially through certificates) in order that the data transmission between distinct technological environment entities is done in a safe way.

References

[1] Concelho Ministros https://dre.pt/application/conteudo/114937034

[2] UE GDPR https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A32016R0679

[3] OWASP https://owasp.org/