Departamento de Engenharia Informática

MEI

Engenharia de Segurança Informática

ESEGI - Assignment 3

Security and Contingency Plan

Contingency Plan

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

Submitted to:
Prof. Jorge Pinto Leite

June 19, 2022

Abstract The purpose of this document is to provide a risk management that provides instructions, recommendations, and considerations for a(n) company/organization/infrastructure/entity, in this case, a Portuguese Health Institution, on how to recover their IT services and data in the event of a security breach, disaster, or system disruption, as no infrastructure or software is 100% secure. 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 as well as the European Commision's GDPR. Other excerpts may be taken from similar documents such as the NIST framework's guide to improving critical infrastructure cybersecurity. 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.

Contents

List of Figures

1 Introduction

1.1 Purpose

This document's purpose is to provide a way for the Portuguese Health Institution to deal with and recover from a data breach or any sort of misconduct or disaster related to the events of compromising data related to natural persons involved in the institution's operations or the IT infrastructure that accommodates the network involved in the cyberspace of the institute's work environment. The cause's root may be centered around an individual, a group of individuals, an organization, a natural disaster or an eventual data theft involving artificial intelligence. 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. These information technology security incidents may not only impact the cyberspace environment, but can also extend its reach to physical infrastructures that support critical or essential services which support the daily functioning of our society.[5]

The following objectives have been established for this plan:

- Maximize the effectiveness of contingency operations through an established plan that consists of the following phases [4]:
  - Notification/Activation phase to detect and assess damage and to activate the plan;
  - Recovery phase to restore temporary IT operations and recover damage done to the original system;
  - Reconstitution phase to restore IT system-processing capabilities to normal operations.
- Identify the activities, resources, and procedures needed to carry out system name processing requirements during prolonged interruptions to normal operations.
- Assign responsibilities to designated Organization name personnel and provide guidance for recovering system name during prolonged periods of interruption to normal operations.
- Ensure coordination with other Organization name staff who will participate in the contingency planning strategies. Ensure coordination with external points of contact and vendors who will participate in the contingency planning strategies.

1.2 Applicability

This contingency plan applies to the functions, operations, and resources necessary to restore and resume the Institution's operations as it is installed. The contingency plan applies to Portuguese Health Institution and all other persons associated with the website as identified under section 2.2, ***Responsibilities and Line of Succession***. This plan is supported by the existing baseline of the 41/2018 resolution of the Portuguese Council of Ministers [1] as well as the European Union's law document **32016R0679** of the European Union's 2016/679 regulation of the European Parliament and Council, of the 27th of April 2016, relative to the protection of singular, natural persons in which the treatment of personal data and the free circulation of this data respects and which repealing previous directive **95/46/CE** of the European Council. [2]

1.3 Scope

In order to follow the correct guideline before taking any action, the scope of the current security breach must be defined, identifying the institution's high level goals and priorities. Based on this scope, the institution will decide which measures must be taken based on the universe of systems and assets that support the critical activity of the institution. [5] Risk analysis will also be taken into account, which will also decide which measures must be taken based on the different levels of risk tolerance.

1.3.1 Planning Principles

If the primary site of operations for the website is inaccessible, there must be a secondary site that allows for the operation of the website as if it was being operated with the same privileges as in the main site. This also means there must be an offline backup (such as a nightly run), that allows this kind of fast accessibility and recovery from the secondary site with all the available information and IT resources to allow for the recovery and processing throughout the period of disruption, until the return to normal operations.

If the main site is still operable but any equipment has been irreversibly damaged, the secondary site's backups may be required and possibly even brought to the main site to try and continue normal operations until the return to normal.

There may also be a cloud backup that stores all the critical information with all the base security assumptions already applied to the storing of this data.

These principles are based and required by the Portuguese Council of Ministers' 41/2018 resolution, on the table **Arquitetura de segurança das redes e sistemas de informação** annexed to this document. This requirement is evidenced on the 4th to last row of the table, which says that the storage systems must guarantee redundancy and availability, without any "single point of failure". The process architecture and storage must guarantee the redundancy, resilience and availability. There must be two types of backups, online and offsite, which must also obey the same security requirements evidenced in the applicable documents. The offsite backups must be stored in a location that is not exposed to the same exterior risks of the original location. These may belong to the same organization, but must be geographically separated. [1]

Os sistemas de armazenamento devem garantir redundância e disponibilidade, não devendo existir nenhum «single point of failure».	A arquitetura de processamento e armazenamento deve garantir as propriedades da redundância, resiliência e disponibilidade.	Obrigatório.
	Devem existir dois tipos de *backups* (*online* e *offsite*), que devem obedecer aos mesmos requisitos de segurança definidos para os sistemas produtivos.	Obrigatório.
	Os *backups offsite* devem ser guardados numa localização que não esteja exposta aos mesmos riscos exteriores da localização original, podendo ser da organização mas geograficamente distinta e/ou afastada.	Obrigatório.

Figure 1: Table evidenced by the 41/2018 resolution of the Portuguese Council of Ministers [1]

1.4 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;
- The institution's infrastructure is properly designed and implemented in such a way that allows for the proper execution of any contingency measures that must be taken;
- The institution must have its Security Plan developed, it must comply with the applicable baselines and requirements and must be properly reviewed and validated.
- The line of succession for the responsibilities relative to the activation of this Contingency Plan must be taken into account, as well as the enforcement of the previously mentioned Security Plan, unless the next in line of succession for this matter is the main suspect of an inside attack, in which case the next in line of succession is responsible for the activation and enforcement of the matters hereby discussed.

2 Concept of Operations

The operations behind the application of the methods defined within the scope of this document will be discussed here. The activation of this plan may occur due to the following contemplated types of risks:

Natural Disaster
Any natural disaster that may strike the institution's critical infrastructure and make it so the normal operations of the same cannot continue normally. Natural disasters that may damage critical infrastructure required by the normal operations of the institution include, but are not limited to:

- **Earthquakes** that damage the institution's property that directly hosts and/or influences the normal operations;
- **Floods/Tsunami** that destroy or make inoperable any of the previously mentioned property;
- **Wild Fires** which may burn and/or destroy the required equipment or otherwise raise the temperature in the building that no longer permit the correct level of cooling of the equipment;
- **Landslides** that compromise the safety of said equipment;
- **Volcano eruptions** that destroy the building used to store said equipment;
- **Hurricanes, tornadoes and severe storms** that may destroy the equipment or otherwise make it inoperable through power shortages;
- **Avalanche/Severe Hail** that may cause equipment permafrost, destruction and/or inoperable due to power shortages;
- **Severe lightning** that may cause fires or otherwise make the equipment inoperable due to power shortages, short circuits and/or power surges.

Inside threats
Can be very hard to identify and are usually one of the must dangerous possible kinds of attackers as they have a lot of information related to their victim as they usually are workers within the institution;

Phishing attacks
The most common type of attack as it is very easy to lead humans into pressing embedded links, often by exploiting their curiosity;

DoS (Denial of Service) attacks
Attempt to crash the victim's server, rendering them inoperable, by flooding the system with requests and traffic;

SQL/Code injections
Is the insertion of malicious code into the software's source code that may compromise the entire database;

Ransomware attacks
As the name indicates, is the request for a ransom to be paid in order to unlock the victim's personal data;

Password attacks
Have many variations, such as brute force, key logging, illegally listening to communication channels, etc. These attacks include phishing attacks, which also include session hijacking;

Sensitive Data Exposure
Involves the inclusion, for example, in the software's source code, of data that shouldn't be there, such as plain text passwords, sensitive code, IP/MAC addresses, etc.;

Software vulnerabilities
Include all other attacks that are related to software such as sensitive data exposure, SQL injections, ransomware attacks, etc.;

Hardware malfunctions May render the system inoperable;

Scalability Related Issues
Occur when the infrastructure no longer provides the necessary power to handle all the traffic derived from the use of the software that is being supported by it.

2.1 Risk Management

Risk management is the act of analysing the threat and deciding upon the risks it may bring to the institution. An impact analysis may be done to try and predict the consequences of treating a threat in a certain way. Proper risk analysis should be made before any action is taken to decide upon the best measures to be taken. The people responsible for this are mainly the stakeholders, which include investors, the board of management, including people like the CEO. These contingency measures must be balanced between the cost of containing them to a certain extent, and the value of the information/assets that are at risk.

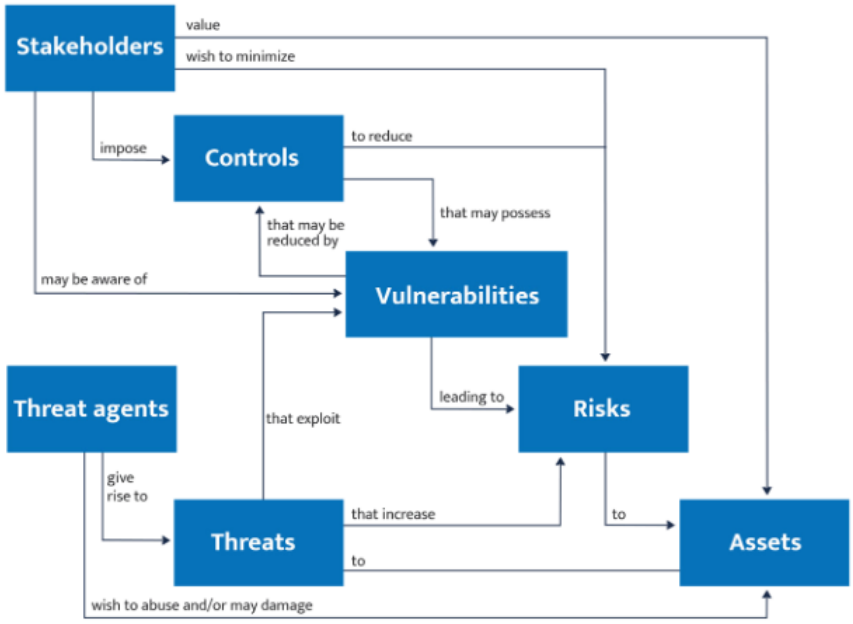

Figure 2: Basic Concepts and high level relationships [5]

2.2 Responsibilities and Line of Succession

The main person responsible for the activation of this contingency plan is the CIO (Chief Information Officer), which is ultimately the one responsible for assuring the data withing the scope of his work is being handled ethically and safely. If the CIO is unavailable or is the main suspect of an internal threat, the CISO (Chief Information Security Officer) is the next one in line of succession as he is responsible for assuring each team's work within software and hardware security is being properly done. If the CIO wishes, he may appoint another person to be next in line of succession if he believes he is not capable of handling the occurrence, as long as this decision is backed and approved by the institution's board of management as well as the CEO (Chief Executive Officer).

The board of management or the CEO may, at any time, appoint whoever they believe is more suitable for being the primary responsible of activating this plan, as long as it is backed and approved unanimously by the board and the CEO.

In the worst case scenario, where chaos has been installed and neither the board of management nor the CEO are able to activate this plan, the highest competent rank in charge will be the responsible for this action.

3 Notification and Activation Phase

This section addresses what should happen in case this plan is activated and what procedures must be taken into account according to each event. For all events, a set of rules is applicable. These include: [5]

- The response plan (this document) is executed during or after the incident and is put into effect as soon as the incident is detected;
  - Technical Implementation: Incident handling platform.
  - Process implementation: The organization's responsible for the document should define escalation procedures, ensure that scope, applicability, rigor and results from the incident response activities are consistent and transversal across the organization.
  - The incident must be well documented and properly logged.
- The personnel know their respective roles and order of operations when a response is needed;
  - The institution's organigram must be previously very well defined.
- The incidents are reported to the stakeholders of that system and the specific affected software accordingly. This implicates an established communication platform. This platform is Outlook's email provider;
- The information is propagated throughout the institution as fast as possible to reduce the response time as much as possible through the previously mentioned communication channel;
- Stakeholder communication must occur as fast as possible in case any outsource funding is required if the institution isn't monetarily capable of handling the situation;
- Detection system logs implemented according to the security plan must be analyzed and properly reported and documented;
- The impact of the incident is well understood by both the responsible for the activation of this plan and the stakeholders;
- Forensics must be performed, allowing the people responsible for the analysis of the incident to collect raw data from disc, memory and network traffic. These raw data logs must be available according to the 8th to last row of the annexed Portuguese Council of Ministers' 41/2018 resolution document table **Arquitetura de segurança das redes e sistemas de informação**, where the following requirement is specified as obligatory: "Capacity to monitor, register and analyze all access activity in order to procure probable threat sources." [1]
- Incidents are categorized in 2, **Concept of Operations**.
- These processes and this document may be activated to respond to vulnerabilities disclosed to the institution from internal as well as from external sources.
- Incidents are contained and mitigated.
- New vulnerabilities are mitigated and documented and may possibly be documented as newly accepted risks which leads to the requirement of having this document up to date at all times.

- This document has a lessons learned section where everything that was acknowledged as new information must be reported in order to improve the processes presented in this document in future possible occurrences.
- The contingency plan is declared closed whenever normal operations may continue, assuming everything has been well documented and reported for future knowledge.

3.1 Natural Disaster

3.1.1 Identifying disaster

Whenever a natural disaster occurs that directly affects the institution's infrastructures, this natural disaster should be identified as one of the mentioned in 2, **Natural Disasters**. It is assumed the institution has complied with the security plan's rule of inventorying all of the equipment that compliments the normal operations of the institution, including hardware, software as well as a list of all human resources that are in any way involved with the institution.

3.1.2 Damage Assessment

Before anything happens whatsoever, the responsible must make sure that above all, no member of the institution has been hurt in any way by the disaster and must call the responsible entities if anyone is in a complex situation that may put their life or the others in threat. Depending upon the type of natural disaster the responsible is dealing with, several infrastructure pieces and hardware integrity must be checked:

- **Earthquake and landslides**: in case the entire building falls to ruins, everything must be obviously checked. If not, the most affected rooms must be defined and the inventory must be checked to see if any equipment was damaged and properly replaced.
- **Floods/Tsunami and other water damage**: in case of floods, the equipment on the floors that suffered the most must also be counted and tested to make sure they are all properly working.
- **Wild Fires**: in case of wild fires, besides the normal equipment check on the affected rooms, an assessment to verify if any equipment suffered from overheat due to the temperature and smoke must all be done on any affected room.
- **Volcano eruptions**: usually render entire buildings inoperable for which an entire inventory check must be performed.
- **Hurricanes and storms**: usually in case of storms and strong winds, there are power outages. If this occurs, and the assumed to be installed generator that should last at least a couple of hours also runs out of fuel, on the last 30 minutes of power, there should be a notification to all the affected people as well as a graceful shutdown of all the equipment.
- **Avalanche and Hail**: similar to storms, this may render power outages, so the procedures are similar to the storms.
- **Lightning**: there must be a lightning rod installed in the building to prevent lightning to hit the power lines, but, if this occurs, the procedures are the same as for storms. In the occurrence of any power spikes and eventual short circuits there must be a check for fires.

3.2 Hardware malfunction

3.2.1 Identifying malfunction

Hardware malfunctions include the overheat of any equipment present on the critical infrastructure of the institution, the damage by any animal or plant, any possible defect that may spontaneously occur due to the device's normal way of operations or due to hardware old age. Another type of hardware malfunction may derive from sabotage which will be treated on 3.3, **Inside Threats**.

3.2.2 Damage Assessment

Usually, this kind of malfunction should not harness many negative consequences as it is assumed redundancy has been taken into account setting up the infrastructure. Still, if all redundant equipment is also damage, there must be an assessment on what is being affected by the malfunction of said equipment. For example, if the institution's web server is damage, connection to the internet will not be possible and the entire website will be down until this is fixed. If the file server is damaged and all related redundant equipment is also damaged, there may be harsher consequences, as the institution's client's data are stored in this server, such as the vaccines taken by each client, etc. If this happens, the institution becomes dependent either on the offsite backups or the cloud backups which should be performed on a nightly basis, based on what has been defined on the security plan. If the authentication server is damaged and all redundant equipment as well, users will not be able to login or register their accounts. A report must be generated on the status of the equipment on the exact moment of the occurrence. A log assessment, assuming logging has been implemented according to what is mandatory by the Portuguese Council of Ministers' 41/2018 resolution [1] (**Arquitetura de segurança das redes e sistemas de informação**'s table 8th to last row), must also be performed by the damage assessment team, to try and determine what was the root cause of the failure and to check if it was a software cause or a physical cause.

3.3 Inside Threats

3.3.1 Identifying type of attack

Inside threats involve many types of attacks, from hardware sabotage, unauthorized sensitive information disclosure, espionage, terrorism, corruption and intentional or unintentional loss or degradation of departmental resources or capabilities. [6]

3.3.2 Identifying attack

Identifying the type of attack is crucial to trace back to who was the root cause of this attack, their motivations and also how to fix the problem caused by this threat. These attacks can be [6]:

- **Violence**: this action includes the threat of violence as well as other threatening behaviors that create intimidation and hostile environments. The attacker may use this kind of attack to obtain confidential information from an insider.
- **Espionage**: is the covert or illicit practice of spying on the institution's direct or indirect way of operations to obtain confidential information for military, political, strategic or financial advantage.
- **Sabotage**: deliberately taking actions to harm the organization's physical or virtual infrastructure, including noncompliance with maintenance or IT procedures, contamination of clean spaces, physically damaging facilities, or deleting code to prevent regular operations.
- **Theft**: it's the act of stealing, either money, equipment or intellectual property.
- **Cyber**: Digital threat includes theft, espionage, violence, and sabotage of anything related to technology, virtual reality, computers, devices, or the internet.

Insider threats may also be unintentional, when someone who works at the institution accidentally does not comply with some rule, if that person is being blackmailed or manipulated in any kind into performing actions that can potentially harm the institution's normal way of operations. This kind of threat can be very difficult to identify, and this is why user activity logging, constant employee training and workshops about cybersecurity are crucial to prevent this kind of threats.

3.3.3 Identifying attacker

Identifying the attacker may or may not be easy. One way to do this is to check user logging, which is mandatory by the Portuguese Council of Ministers' 41/2018 resolution [1] (**Arquitetura de segurança das redes e sistemas de informação**'s table 8th to last row). By accessing the user log history, it can be possible to trace which user commit the act that lead to the exploitation and/or abuse.

3.3.4 Damage Assessment

The performance of a damage assessment must also be performed at this level in order to realize just how much of the hardware/software and possibly human resources was involved in this attack, as the people who were possibly corrupted may have to be laid off and, people who have been blackmailed/threatened/abused may require psychological help. First, the assessment must be made at the origin of the problem, which is at the human resources level, and only then should if be made at hardware and software levels, with possible hints given by the involved. An inventorying may also be required if any equipment is noticed to be missing.

3.4 Phishing Attacks

3.4.1 Identifying attack

Phishing attacks, although common, most often are easily identified. The authors of phishing attacks often target compromised lists of emails leaked in online sources, which are then added to send-lists which the attackers use to mass send these phishing emails, often targeting entire enterprises. These emails are identified by lack of good grammar, flashing images, suspicious hyperlinks, fishy emails and promises or notices that often do not make any sense. Enquiries must be routinely made to the possible victims, in this case, the employees, on a set basis, in this case, monthly. A channel to report these kind of attacks must be available at all times for the victims to be able to report such cases.

3.4.2 Identifying attacker

Once an attack or attempt of attack of this kind has been detected and reported by someone, the next step is to identify the attacker, blacklist their email and report them to the responsible entities, in this case, PSP (Polícia de Segurança Pública) and GNR (Guarda Nacional Republicana).

3.4.3 Damage Assessment

The first step in damage assessing this kind of attack is to question all involved whether they have clicked any links or performed any action required by the sender of the malicious email. If the answer is yes, then further actions must be taken to contain this problem, which will be discussed in 4, **Recovery Operations**. Else, only the steps identified in 3.4.2, **Identifying Attacker**, shall be taken.

3.5 DoS Attacks

3.5.1 Identifying attack

A Denial-of-Service attack can be identified by a massive wave of requests to try to crash and stop a machine and/or network. Considering the fact that there are firewalls installed in the network, which is mandatory according to the Portuguese Council of Ministers' 41/2018 resolution [1], supervising the network should not be a hard task in order to detect these kinds of attacks. Monitoring and analyzing network traffic on a regular basis is mandatory and should be taken very seriously as these kinds of attacks can bring the access to the institution's website to a halt for a potentially damaging amount of time.

3.5.2 Identifying attacker

The first step after identifying the attack should be to identify the attacker and verify if they left any traces of their original IP address, if they are using VPN, law enforcement may help by requiring the VPN service their logs to trace back the attacker.

3.5.3 Damage Assessment

When a DoS attack occurs, not only the file, web and authentication servers need to potentially be restarted, the proxy servers, which are required to be installed by the Portuguese Council of Minister's 41/2018 resolution [1], also need to be rebooted as well as the hardware and web firewalls. The damage

assessment of this type of attack is going to be heavily dependent on the amount of time the servers and the service has been down as well as the required time to reboot the servers. To calculate this, it is required that an impact analysis is performed to calculate the losses due to inactivity, the losses to detect and fix the issue as well as the impact the attack has on the clients' trust on the service.

3.6 Ransomware Attacks

3.6.1 Identifying attack

Ransomware attacks can be detected through various ways, but, are sometimes not that easy to detect:

- Weird file changes that haven't been performed by any expected procedures from inside the institution's normal operations;
- Files that have been deleted or moved without a rationale.
- Inaccessible files that would otherwise be normally accessed by the required personnel;
- Unauthorised network access.

Any of these triggers may indicate that an attack like this has been performed on the institution's premises before any kind of contact asking for ransom is received. After any contact asking for a ransom is performed, it is obviously a ransom attack.

3.6.2 Identifying attacker

As is required by the Portuguese Council of Minister's 41/2018 resolution [1], network logging is mandatory to identify every activity that happens within the institution. As long as this required is fulfilled, the perpetrator can be traced back by their activity in the network log. By tracking their activity, their IP address can be fast obtained and reported to the authorities, which, if using a VPN, will redirect the authorities to the VPN entities responsible for obfuscating their IP.

3.6.3 Damage Assessment

Proper damage assessment must be calculated just like previously. But this time, information may have been compromised. All information data files within the institution must be inventoried and a proper inventory check must be performed to understand which files have been stolen, corrupted, deleted and accessed without permission. After the files that have been compromised have been identified, the costs of losing those files, and possibly having to rework them, should be taken into account. A former impact analysis must be performed if any of the compromised files contain critical information containing data that can possibly damage any individual.

3.7 Password Attacks

3.7.1 Identifying attack

There can be several types of password attacks, of which a phishing attack can be considered one, but, will not be reviews here as it is referenced in 3.4, **Phishing Attacks**. One of the most common types of attacks is the man in the middle attack, which consists of a perpetrator listening to public connections on the network. Since there are no intentions of implementing private channels for these type of communications, the public channels should never be used to exchange messages that may contain sensitive data or, if it is really necessary, there must be encryption of these types of messages. The way to identify this type of attack is through the unusual interception of messages that is detected in the network. Brute force attacks are easily identified by implementing a time limit penalty if someone tries to access the service an unusual amount of times, usually in the hundreds or even thousands. Another way to identify these types of attacks, is by identifying an unusual program running in the background that logs the user's keys inputs. This detection is usually a red flag.

3.7.2 Identifying attacker

To identify the attacker, similar log checking should be performed just like described in 3.6.2, **Ransomware attacker identification**, where the network logging should be checked to try and trace the IP of the perpetrators.

3.7.3 Damage Assessment

To assess the kind of damage a password theft may cause, first, a traceability between what potential data may be compromised because of said password theft must be done, by identifying what privileges the account or software which password was stolen have, to really understand what type of data may be at risk, according to the level of access that account/software has. If the access password to the file server has been breached, the entire database may be at risk and further damage assessment may be necessary by tracking down the perpetrator and querying said perpetrator to confess what data they have gotten their hands on.

3.8 Cloud Service Provider Attack

3.8.1 Identifying attack

This kind of attack may not be directly detected by the institution but rather by the cloud service provider, which is required to publicly report any known vulnerabilities or breaches that may occur within their software and/or infrastructure. These attacks may also be reported by the institution if any unusual activity is detected related to the data that is stored within the cloud service being used. This should be reported through the support channel by opening a ticket on the cloud service provider's website.

3.8.2 Identifying attacker

This is usually a task by the service provider but, if the institution was the one reporting the issue, they may be asked by the provider to provide network logging in order to trace back the perpetrator.

3.8.3 Damage Assessment

According to what has been reported by the cloud service provider, the damage assessment need to be performed on the entirety of the files that may be compromised by the types of services that are being used by the institution that have been breached.

3.9 Software Attacks

3.9.1 Types of software attacks and vulnerabilities

- **DNS spoofing** is an attack that uses altered Domain Name records to redirect traffic to a fraudulent site. This is often called DNS cache poisoning.
- **SQL injection** is a server-side vulnerability that involves trying to illegally manipulate database records from inputting SQL queries in the website's text inputs;
- **XSS scripting** similar to SQL injection but on the client side, involves manipulating the source code of the website, for example, to try and hook the user's browser or to display fake login pages;
- **Session hijacking** is the theft of a user's session cookie from another user to be able to use their session as if it was theirs, having access to the victim's web page as if was the victim using it;
- **Code and malware injection** involves manipulating the source code of the website other than the Javascript, such as, for example if the website is developed in Python, manipulating that source code;

- **Sensitive data exposure** happens when developers forget to remove sensitive data such as plain text passwords from the production code, leaving it exposed to anyone curious about the website's source code to explore. This can very easily happen, for example, on the HTML code of a website, and should not be forgotten to be removed.

3.9.2 Identifying type of attack and attack

To identify these types of attacks, one must be attentive to fishy code inside the source code of the website and infrastructure production code. By doing these, it can be often be evidenced before an attack occurs that there may be sensitive code in production. This leads to the necessity of changing the sensitive piece of data that was exposed in order to avoid anyone with bad intentions to get their hands on that info in an unauthorised fashion. Other ways to identify these types of attacks is to keep an eye on the database records, where there may be fishy entries of failed SQL injections that shouldn't even be there, such as "a' 1 OR 1", which is obviously a failed SQL injection attack. The same applies to XSS attacks inside source code and database records as well. To detect session hijacking and DNS spoofing, one can detect suspicious access from an IP address that isn't usually that specific user's normal point of access to their account, and a trigger should be made to activate the 2FA of that specific account as well as the report that that specific occurrence has happened. A sudden rise in DNS activity on a single domain from a single source suggests a possible DNS cache poisoning attack. A single-source increase in DNS operation that queries several domain names may also be indicative of this type of attack by analyzing logged DNS activity.

3.9.3 Identifying attacker

The same rationale that has been taken on other types of attacks will be taken on this type, to try and trace back the attacker's IP address and report it to the authorities.

3.9.4 Damage Assessment

Assessing just how much damage some of these attacks may have caused can prove to be difficult. Some of the damage assessment is directly related to if the attacker is tracked down and just how much information he stole. The best way to assess the kind of damage caused by these types of attacks is to assume that every possible kind of information was stolen and assume new passwords for every server needs to be reset.

3.10 Notification

The stakeholders must always be notified when a significant kind of these types of attack occur, as they are ultimately the ones who keep the institution up and running. The cybersecurity team, including the damage assessment and impact analysis team including finance must also be notified to calculate the possible losses and expenses the attack and its respective fix will cause. Besides this, the entire team responsible for the data that has been compromised must also be informed. At last, if the attack has the possibility to have compromised clients' private data and/or passwords, a public announcement must also take part for the ones who this notification may concern, such as affected users. This kind of notification can be done through email, from the institution's website, directly to the team via Microsoft Teams on the development and cybersecurity side, and, if the occurrence has affected enough users, and depending on the gravity of the situation, a television/radio news broadcast may also be considered on local and national news channels, such as RTP, Sic and CMTV.

4 Recovery Operations

The recovery plan is executed during or after the incident. This plan is executed by putting in practice the following steps [5]:

- Backup and restore solution;
- Implement incident recovery process;

- Ensure that the rigor, scope, applicability and results from recovery activities are consistent and transversal to the whole organization and for all incidents;
- Evaluate and prioritize the set of incident recovery activities, considering other plans such as business continuity plan.

Evidences generated from the handling of these operations include the support document for incident handling and the reports from past incident recovery activities as well as the updating of the lessons learned document with what has been learnt from this experience that hadn't yer been learnt from past similar or not experiences. This document and process must be regularly updated to accommodate new disasters that hadn't previously been thought of. Public relations must be held by those responsible.

4.1 Natural Disaster

4.1.1 Repairing the flaw and mitigating future flaws

The goal of this repair is to fix all possible damage caused by the disaster. Depending upon the type of disaster that has occurred, it may be necessary to recur to the offsite backups to get the system up and running if the damage of the original infrastructure is too bad and will not be operable for at least 48 hours [5]. If the disaster is simply a storm or lightning that may have cut the power, the official responsible entities with taking care of getting the energy to get back up and running should be contacted, in this case, EDP <EDP's contact>. It may be necessary to rebuild the entirety of the original infrastructure and buildings if the damage caused by the disaster is too bad. This can be significantly accelerated by using then backups from the cloud services and from the offsite backups.

4.1.2 Testing Reparation

After being sure no more repercussions of the event will happen and that the fixes have all been implemented, it is imperative to test the website, as well as the servers involved, such as the database server, authentication server and web server. It is also important to make sure all of the proxy servers, firewalls and web firewalls are up and running to prevent any exploits by attackers who know the fragility of the situation and may take advantage of the event to attack.

4.2 Hardware malfunction

4.2.1 Repairing the flaw and mitigating future flaws

The objective of this repair is to get the defective hardware up and running again. The hardware piece should be rebooted and, if damaged, should be repaired on site or offsite if the piece is not confidential and requires external maintenance.

4.2.2 Testing Reparation

- The specific hardware piece that has malfunctioned should be tested to make sure it is working.
- Endurance tests should be performed to test the limits of the new or fixed hardware.
- Normal and regular maintenance should be performed.

4.3 Inside Threats

4.3.1 Repairing the flaw and mitigating future flaws

The goal of this repair is to fix all vulnerabilities and threats as well as to eliminate all potential individuals who may pose a threat to the normal way of operations. If the suspect is found they should be reported to the responsible entity and properly prosecuted as well as fired if they are an employee. Once the previous step has been completed, to contain the spread of this individual's damage, the proper repairs to their attack should be performed based on which of the attacks they have performed, which may be one of the attacks in 4, **Recovery Operations**, and the related repair procedure

should be partaken, or, if it is a new unseen attack, research must be performed, asking for help to a cybersecurity agency, such as Cybers3c to know exactly what the procedures are. Employee training should take place regularly to reduced the insider threat as well as the treating of employees with respect so they don't turn against their employer.

4.3.2 Testing Reparation

- The testing procedures related to the attack should be performed according to the performed attack, foreseen in 4, **Recovery Operations**.
- Occasional fake phishing emails should be sent to the institution's employees to test if they fall for the trap.

4.4 Phishing Attacks

4.4.1 Repairing the flaw and mitigating future flaws

The goal of this repair is to train the employees to never press any suspicious links from unknown email senders as well as to recover compromised passwords or information. Creating a blacklist with past emails from these kind of attackers and applying it to the enterprise's email environment is essential to try and prevent as much emails like these to be sent to the employees.

To fix the issue, the employee should change all their passwords as soon as possible. That specific employee's related data should be contained and analyzed for any data breaches. If possible, the network log and the sender's email should be checked and reported to the responsible entity to try and find the perpetrators so they can be prosecuted. Regular training should be made to teach the employees just how devastating these kinds of attacks can really be as well as the sending of phishing emails to the employees to test if they fall for it.

4.4.2 Testing Reparation

- An email from one of the blacklist's emails should be sent using an alias to try and see if the employee still receives the email.
- The employee should test their new password to make sure the exchange worked properly.
- Occasional fake phishing emails should be sent to the institution's employees to test if they fall for the trap.

4.5 DoS Attacks

4.5.1 Repairing the flaw and mitigating future flaws

The goal of this repair is to try to get the services back available while making sure that the possible damage caused won't affect the normal functioning in the future. DDoS (Distributed Denial of Service) attacks are typically fast (90% are less than 3 hours in duration). It is usual for attacks to occur in burst, once the first attack is ceased, it is recommend to wait until it's absolutely sure the attacker won't return before rolling back any modifications that have being made to the service. Finally, once the service has fully recovered, the impact of the assault, the possibility of recurrence and the readiness instructions should be examined to determine what, if any, modifications are required to prevent future problems.

4.5.2 Testing Reparation

- Simulating attacks: By simulating *DoS* attacks, we are testing our system in various factors:
  - How many packets are dropped by the mitigation solution;
  - How the mitigation solution functions in a real attack;
  - What level of service it can provide under attack;
  - How people and processes react to and withstand an attack.

- Regular Audits: Regular network security audits are also recommended. A network security audit will:
  - Determine how vulnerable the company's network is to intrusion;
  - Verify the strength of passwords;
  - Who has access to what data;
  - Whether software is up to date or not.
- Continuous monitoring of network traffic: Continuous monitoring (CM) analyzes traffic in real time and detects evidence of *DoS* activity.

4.6 Ransomware Attacks

4.6.1 Repairing the flaw and mitigating future flaws

The goal of this repair is to try and recover the lost files/data and to repair the infected machines. The first rule of ransomware is to never pay the attacker's for the recovery of those files. The files should be considered lost forever, recovery is a bonus. The first step is to quarantine the machine as the attacker will most likely try to spread the attack to other machines in the network. The next step is to make a backup and try to decrypt the ransomware's targeted files to try and recover the items. When the files are considered recovered or lost forever, the victim machine should be cleaned and restored from a safe backup, so that it is clean of all malware.

4.6.2 Testing Reparation

- To test the repair pen-testing should be performed by a third party to ensure the system is threatened by the least vulnerabilities possible.
- First, the planning of the attack must be performed, as well as the scope being defined.
- Second, the pen-tester should execute the tests trying to exploit known possible vulnerabilities.
- At last, a report should be made by the pen-tester to acknowledge the types of threats posed by the known vulnerabilities on the scope of the test.

4.7 Password Attacks

4.7.1 Repairing the flaw and mitigating future flaws

The goal of this repair is to recover and change compromised passwords as well as to educate users on how to choose and reinforce their passwords. If a password has been compromised, the first step is to inform the user(s) and recommend that they immediately change their passwords. The second step is to acknowledge that the data linked to that user's account may have been compromised and try to prosecute the attacker to understand just what other information has been stolen. At last, a strict password policy should be enforced, such as making users choose only strong passwords with a set mandatory number of characters, special characters and digits. Mandating that users use a 2FA medium is also recommended, such as:

- Biometric;
- Authenticator apps;
- Email verifications;
- SMS;
- Authentication matrices;
- Security keywords;
- Smart card;
- Graphic pattern.

4.7.2 Testing Reparation

- To test the previous mitigation activities are being enforced, users should be prompted to change their password on a set timely basis;
- They should also be forced to use passwords with at least 9 characters for normal users or 12 characters for privileged access users, and 3 of the 4 following groups of characters: capital letters [A-Z], lower case letters [a-z], digits [0-9] and special characters [! @ # $ % & ( ) _ + | ‘ - = [ ] : “ ; ‘ < > ? , . /] [1]
- 2FA activation should be recommended regularly.

4.8 Cloud Service Provider Attack

4.8.1 Repairing the flaw and mitigating future flaws

The goal of this repair is to ensure no data has been compromised and that no machine has been infected with malware. The responsible with maintaining the cloud services should remain in contact with the provider to be informed in a timely manner on what attacks may be currently be putting the institution's information at risk. If the provider reports an attack, the service that suffered the attack should be provided and contained. After this step, the only remaining thing to do is to wait and maintain in contact with the service provider helping them in any way possible as may be requested by them.

4.8.2 Testing Reparation

The repair team should keep in touch with the cloud service provider to collaborate and know exactly what to do in these types of situations as well as what data could possibly have been leaked or compromised.

4.9 Software Attacks

4.9.1 Repairing the flaw and mitigating future flaws

The objective of this repair is to clean any code that may contain flaws as well as reinforcing existing code to be more sturdy and enduring as well as making sure the network is being well protected by proxy servers as well as firewalls and web firewalls. Coding guidelines should be established as well as secure coding training. At the end of the day the developers are the ones responsible for allowing these vulnerabilities loose and the best way to prevent them is to properly train them and developing guidelines for them to follow. Backing up every version that is released is imperative so that rollbacks can occur whenever necessary to a more stable version if any version is ever compromised. The vulnerable code shall be contained as soon as possible and repaired by the person responsible for it whenever possible. If any information is breached because of this vulnerability, users should be notified and the attacker must be prosecuted whenever possible to find out the range of information that may have been compromised.

4.9.2 Testing Reparation

- To test the repair pen-testing should be performed by a third party to ensure the system is threatened by the least vulnerabilities possible.
- First, the planning of the attack must be performed, as well as the scope being defined.
- Second, the pen-tester should execute the tests trying to exploit known possible vulnerabilities.
- At last, a report should be made by the pen-tester to acknowledge the types of threats posed by the known vulnerabilities on the scope of the test.
- Static code analysis as well as code reviews must also be performed within the development teams.

- Development code should always be tested before being released.
- Regular tests should be performed, such as nightly runs, on production code and a given minimum coverage should be maintained.
- Firewalls and proxy servers should always be working whenever the network is up.
- Audits should be regularly made, specially to the user logs as well as to how the development is being made to make sure all processes are being thoroughly followed from design to production.

5 Return to Normal Operations

This section discusses the activities of restoring the normal operations before the attack took place at the original or new site of operations. The goal is to provide a seamless transition of operations from the alternate site to the computer center. If the original site is unscathed, then the return of operations should be seamless, possibly without the insider threats, which may be required to be replaced by someone else. If the return is given at a new site, then the employees should receive normal training, for example as to where exits and fire extinguishers are, etc.

This kind of operation should also be as seamless as possible although that is sometimes hard because of the different installations and buildings. Returning to operations should be understood by the managers as a period of vulnerability and possibly less efficiency as workers may need time to accustom to the new site.

5.1 Plan Deactivation

Whenever the security flaws have been contained, fixed, mitigated to prevent future occurrences, and all the learnt lessons and required documents have been generated, the responsible for activating this plan must deactivate it, triggering the return to normal operations.

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] NIST https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[4] Template https://wdr.doleta.gov/directives/attach/UIPL/UIPL26-09a1.pdf

[5] Centro cyber portugal https://www.cncs.gov.pt/docs/qnrcs-web-eng.pdf

[6] Inside Threats https://www.cisa.gov/defining-insider-threats