SOTER

Training Handbook:
INCIDENT HANDLING

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833923

Autohrs: Eliseo Venegas Mayoral, Paul Rabel, Martin Griesbacher and Nora Schreier
Design and Layout: Matthew Reilly and Ekaterina Kyulyumova

Published in January 2022 (Graz/Dublin/Madrid)

ISBN: 978-3-903374-14-0
DOI: 10.25364/978-3-903374-14-0

Table of contents

1. SOTER Training Handbooks Introduction 1

2. Introduction to Incident Handling 2

3. Threats and Risks 4

4. Incident handling: Best practices for securing SOTER 8

5. Best practice for mitigation 12

6. Compliance and Regulation 15

5.1. How important bodies in the EU collect threats? Best practice 16

SOTER Training Handbooks Introduction

The financial sector is experiencing a real digital revolution in recent years, in which traditional entities are becoming providers of digital services in order to remain competitive. Although it is clear that this new era implies many advantages for businesses and citizens, in addition, the release of new digital services and connections imply the appearance of new threats and risks in terms of cybersecurity, data privacy and the use of digital identities.

These threats must be tackled under a holistic approach and pointing at their different origins, including the human factor.

Furthermore, the current regulations to be met, apart from involving a technological and mind-set challenge and increasing the number of entities with which to interact with, also aim to create or improve tools to prevent fraud and reduce cyber vulnerabilities as much as possible.

SOTER takes the challenge, considering both technological and non-technological (human factor and governance within organizations) aspects and providing innovative solutions that will act as a transformative process of the finance sector, helping their players to increase their cybersecurity level, improving the fight against present and future cyber attacks and vulnerabilities and, to summarise, increasing their cyber-resilience.

SOTER addresses two main challenges. The first will be how to improve the digital onboarding process. This will involve researching and developing a digital onboarding technology platform that will incorporate biometric identification and authentication technology. And the second will be how to implement a state-of-the-art cybersecurity culture. This will be done with a user training methodology and a manual to improve cybersecurity resilience in organisations.

This handbook summarises the results of SOTER's work on incident management. It is based on the various regulations of European and national bodies, and on specific regulations for incident handling. The following sections present what incident management is and what are the good practices to be carried out in SOTER.

1

Introduction to Incident Handling

A security incident is an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system manages, that constitutes a violation or imminent threat of violation of a security policy or procedure.

According to ENISA[1], the typical cost of a security incident in the EU usually ranging from 213 000 to 300 000 EUR.

An incident may cause heavy losses to organizations, from economic losses, or data breaches to reputational harms. Also incidents, may lead intro law infringement. That is why organizations should protect their information systems from them.

For this purpose, incident handling procedures are carefully defined, taking into account the specific context of each organization and considering their systems, business processes and regulatory framework.

[1] https://www.enisa.europa.eu/news/enisa-news/cybersecurity-spending-an-analysis-of-investment-dynamics-within-the-eu

2

Threats and Risks

For the effective management of threats and risks financial organisations currently don’t need to follow a specific threat taxonomy. As mentioned in ISO 27005, there is no single taxonomy to follow. One of the most prominent European approach is ENISA's taxonomy of threats. However, it should be noted that, according to ENISA, "the complexity of the financial sector makes it difficult to interpret the threat landscape, as different domains within financial services and banking may face completely different cyber risks and threats".

However, according to ENISA, the following threats (ranked by prevalence) have seen a significant increase in incidents in the financial sector over the past year:

1. Attacks on web applications: These attacks include SQL injection and cross-site scripting (XSS) attacks, exploiting weaknesses in web applications and services.

2. Insider threat (unintentional abuse): The most common insider threat pattern occurs when the attacker collaborates with an insider actor, often by providing monetary incentives to convince the insider. However, it is often difficult to distinguish between legitimate, malicious, and erroneous actions of insiders.

3. Malware: Malware is perhaps the most well-known cyber-attack next to phishing emails. It comes in all shapes and sizes, from viruses, worms, spyware to ransomware. Common targets of a malware attack are information or identity theft and service disruption.

4. Data theft (data breach): In a data breach, sensitive and sometimes confidential information is accessed without proper authorisation, usually by a malicious actor. It is usually the result of a previously conducted cybersecurity attack, such as a phishing attack.

This taxonomy defines the main security incidents identified in the European context for the financial sector:

Abusive content: Attacks aimed at damaging the organisation's image or using its electronic means for other illegal uses (such as advertising, extortion or, in general, cybercrime).

Malicious code: Software that is intentionally included or inserted into a system for a harmful purpose. It usually requires user interaction to activate the code.

Information harvesting: Attacks aimed at gathering critical information to progress to more sophisticated attacks, through social engineering or vulnerability identification.

Intrusion attempts: Attacks aimed at exploiting vulnerabilities in the design, operation, or configuration of different technologies, in order to break into the organisation's systems.

Intrusions: A successful compromise of a system or application (service). It can be caused remotely, through a known or newvulnerability, orthrough unauthorised local access. It also includes being part of a botnet.

Availability: This type of attack causes the system to crash due to the large number of packets it receives, resulting in a delay in operations or a system crash.

Information content security: In addition to local abuse of data and systems, information security can be compromised by a successful account or application compromise. In addition, attacks can intercept and access information during transmission (eavesdropping, spoofing, or hijacking). Human, configuration, or software errors can also be the cause.

Fraud: Incidents related to fraudulent actions arising from identity theft, in all its variants.

Vulnerabilities: Open resolvers, global read-only printers, out-of-date virus signatures, etc.

Another threat reference taxonomy that has been used is the Common Attack Pattern Enumeration and Classification (CAPEC™) catalogue. CAPEC™ is a "publicly available catalogue of common attack patterns that helps users understand how adversaries exploit weaknesses in applications and other cyber capabilities". The catalogue provides an overview of "attack patterns" along with an associated description. It aims to provide an up-to-date community resource of common attack methods.

According to ENISA's research, the financial sector is complex and hard to interpret, therefore it is almost impossible to define an accurate threat landscape. This is because different domains with financial services may face entirely different cyber risks and threats.

However, the most common attacks in the financial sector proposed by ENISA are:

- **Web application attacks**
- **Insider threat (unintentional abuse)**
- **Malware**
- **Data theft**

According to the European Central Bank (ECB)[1], the most common attacks are presented in the graph below. Also, the ECB detected a new highly sophisticated cyberattack in which a widely used monitoring software was manipulated, making organisations download a malware during the usual update process.

[1] https://www.bankingsupervision.europa.eu/press/publications/newsletter/2021/html/ssm.nl210818_3.en.html

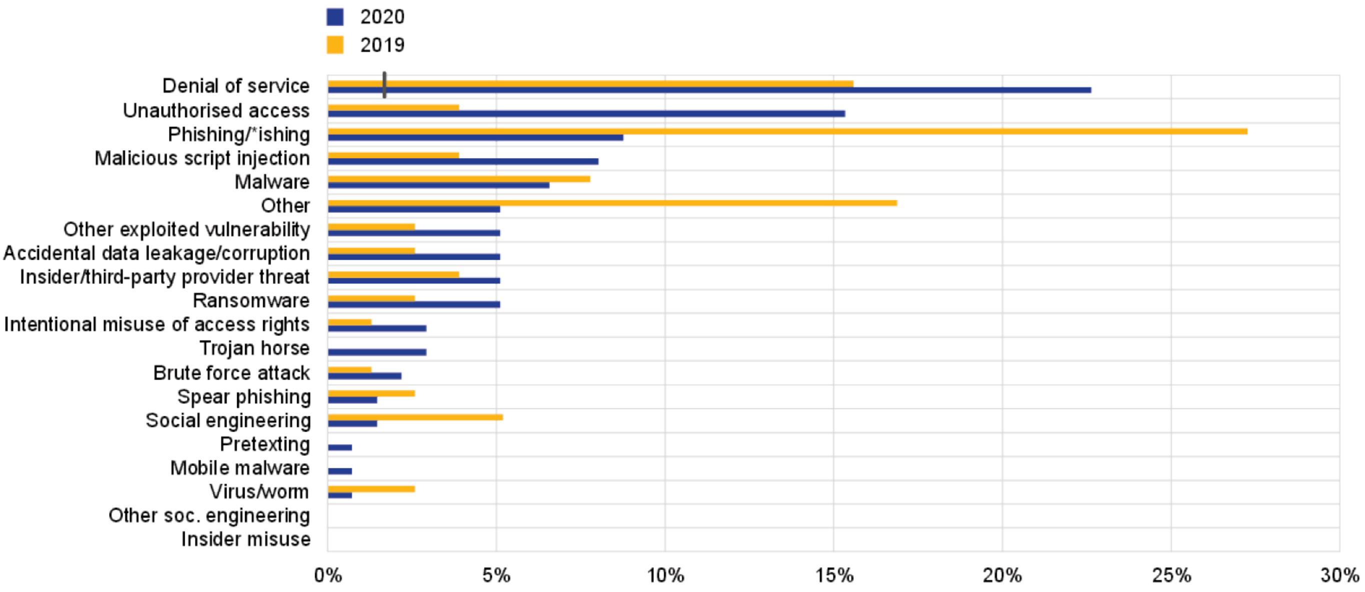

Figure 1. Most common attacks in financial sector.

- The central bank's hacking of the SWIFT payment terminal in Bangladesh in 2016, which led to fraudulent payment messages and the theft of $81 million (financial theft)[2].

- The data leak at Equifax in 2017[3]. This resulted in an estimated 143 million US records containing customer information stolen by hackers. This included social security numbers, dates of birth and credit card details (violation / theft of data)

- The hacking of the Cosmos Bank ATM server in India in 2018[4], which resulted in the theft of $13.5 million through fraudulent credit and debit card transactions (financial theft)

- The Banco de Chile network incident[5], which resulted in a loss of $10 million (financial theft)

- The incident that affected the interbank payment system of the Bank of Mexico, SPEI[6], resulting in a loss of $15 million (financial theft).

- Edenred, a payment solution provider, reported that it was infected by a malware that affected several computers in the organisation[7]. It operates in 46 countries and handled over 2.5 billion payment transactions two years ago. The company confirmed that they set up the measures to prevent future infections as soon as the incident was detected.

- Hackers used PayPal user's accounts to make unauthorised purchases, with a value of 10 thousand euros, by exploiting PayPal's Google Pay integration[8]. Most of the victims were German PayPal users.

- The following sections relate these threats and risks to the good practices to be carried out with the main challenges on which the digital handbook focuses.

[2] https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/
[3] https://techcrunch.com/2017/09/07/equifax-data-leak-could-involve-143-million-consumers/
[4] https://www.reuters.com/article/cyber-heist-india-idUSL4N1V551G
[5] https://www.bankinfosecurity.com/banco-de-chile-loses-10-million-in-swift-related-attack-a-11075
[6] https://www.bloomberg.com/news/articles/2018-04-28/mexican-banks-are-said-to-have-been-targeted-in-cyber-attack
[7] https://www.bleepingcomputer.com/news/security/edenred-payment-solutions-giant-announces-malware-incident/
[8] https://www.zdnet.com/article/paypal-accounts-are-getting-abused-en-masse-for-unauthorized-payments/

3

Incident handling: Best practices for securing SOTER

The following standards and methodologies may be viewed as a set of best practices and procedures regarding incidence handling.

ISO/IEC 27035:2016 (Incident Management)[1]

- This standard covers the processes for managing information security events, incidents, and vulnerabilities.
- The standard extends the information security incident management section of ISO/IEC 27002. It cross-references this section and explains its relationship with the ISO27k eForensics standards. The 5 steps to follow according to the standard are:

1. Definition of a plan and preparation to deal with incidents *e.g.,* prepare an incident management policy, and establish a competent team to deal with incidents.
2. Identifying and reporting information security incidents.

- Analysing incidents and making decisions about how they are to be addressed *e.g.,* patching things up and getting back to business quickly, or collecting forensic evidence even if it delays resolving the issues.

3. Responding to incidents *i.e.,* containing them, investigating them and resolving them.
4. Learning the lessons - more than simply identifying the things that might have been done better, this stage involves actually making changes that improve the processes.
5.

NIST SP 800-61 Incident Management[2]

- According to this standard, these functions should be performed concurrently and continuously to form an operational culture that addresses the dynamic cybersecurity risk:
- **Preparation**: The first step when facing security incidents is to establish incident response capabilities and to prevent security incidents by securing the systems. The organisation should define some mechanism for preparing against security incidents, like communication procedures, security in the facilities, analysis of hardware and software, analysis of resources and mitigation software. Also, the organisation should deploy some preventing measures, like periodic risk assessments or malware prevention.
- **Detection and Analysis:** The next step is the detection and analysis of possible security incidents. The attack vectors, sings of incidents and precursors of incidents have to be clearly identified by establishing procedures and software like IDPSs or SIEMs.Also, an effective incident analysis has to be carried out for resolving it quickly and accurately. The incident has to be documented, prioritised and reported to the relevant authorities.
- **Containment, Eradication, and Recovery:** First it is necessary to contain the incident for avoiding further propagation. It is also necessary to gather some evidence of the security incident and to identify the attacking host. Then, it is time to eradicate the incident and restore the systems back to normal operation.
- **Post-Incident Activity:** This is the most often omitted part of the incident response, learning, and improving. It is important to use the experience for improving the response procedure and systems

Digital Single Market Strategy (DSM)[3]

Another relevant security set of best practices is the Digital Single Market Strategy for Europe of 2015 (DSM). This is one of the most relevant strategic goals of European Union. This strategic

[1] https://www.iso.org/standard/60803.html
[2] https://www.nist.gov/privacy-framework/nist-sp-800-61
[3] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192

decision is enforced and driven by the already mentioned European Cybersecurity Strategy and the opportunities created by H2020.

The Digital Single Market Strategy will be built on three pillars:

- Better access for consumers and businesses to online goods and services across Europe – this requires the rapid removal of key differences between the online and offline worlds to break down barriers to cross-border online activity.
- Creating the right conditions for digital networks and services to flourish – this requires high-speed, secure and trustworthy infrastructures and content services, supported by the right regulatory conditions for innovation, investment, fair competition and a level playing field.
- Maximising the growth potential of our European Digital Economy – this requires investment in ICT infrastructures and technologies such as Cloud computing and Big Data, and research and innovation to boost industrial competitiveness as well as better public services, inclusiveness and skills.

ENISA (European Network and Information Security Agency) Incident Management Guide[4]

- ENISA provides best practice guidance and practical information for the management of network and information security incidents. The main focus of the guide is the incident management process, which involves incident detection and logging, followed by triage (classification, prioritisation, and assignment of incidents), incident resolution, closure, and subsequent analysis.
- The guide also includes a formal framework for CERTs, covering roles, workflows, basic policies, cooperation, outsourcing and reporting to management.

Payment Card Industry Data Security Standard (PCI DSS)[5]

- The Payment Card Industry Data Security Standard (PCI DSS) is a payment media standard issued by credit card companies to protect the credit card data of customers making transactions from any source.
- PCI DSS is organised into six different domains, including security incident management in domain 6. Maintain an information security policy:

1. Building and maintaining a secure network and secure systems.
2. Protecting cardholder data
3. Maintaining a vulnerability management programme
4. Implementing strong access control measures
5. Regularly monitoring and testing networks.
6. Maintaining an information security policy

EU Cybersecurity Act (Regulation (EU) 2019/881)[6]

The EU Cybersecurity Act defines a continued and strengthened authority for ENISA, as the European Cybersecurity Agency, and also specifies a structure for the European Union to be used for the development of cybersecurity certification for Information and Communications Technology (ICT) products, including IoT devices, processes, and services to be recognised in all EU Member States.

[4] https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management
[5] https://www.pcisecuritystandards.org/document_library
[6] https://eur-lex.europa.eu/eli/reg/2019/881/oj

EU Blueprint[7]

- The EU Blueprint is used for the Coordinated Response to Large-Scale Cyber Incidents. It offers cross-border response procedures, the taxonomy of cyber incidents as well as rapid and effective cooperation and preparedness.

Applying these facilitates the planning of activities to improve security in applications, processes, and controls, requiring mapping business priorities with security priorities, assessing current state using the maturity model safety program and setting the maturity model state target. For each case, procedures and processes collect internationally accepted best practices for managing incident.

[7] https://www.enisa.europa.eu/events/artificial-intelligence-an-opportunity-for-the-eu-cyber-crisis-management/workshop-presentations/20190603-ec-blueprint.pdf

4

Best practice for mitigation

ISO/IEC 27035:2016

Efficient incident management involves detective and corrective controls designed to recognise and respond to security incidents, minimise adverse impacts, gather forensic evidence, and 'learn lessons' in terms of driving improvements to the ISMS, typically by improving detection mechanisms, preventive controls, or other risk treatments[1].

Information security incidents often involve the exploitation of previously unrecognised and/or uncontrolled vulnerabilities, so vulnerability management (e.g., applying relevant security patches to IT systems and addressing various control weaknesses in operational and management procedures) is partly preventive and partly corrective action[2].

This standard covers the processes of managing information security events, incidents, and vulnerabilities.

NIST 800-61 SECTION 3.4.2

It is important to document how all evidence of the incident, including compromised systems, has been preserved. Evidence should be collected in accordance with procedures that comply with all applicable laws and regulations that have been developed with appropriate legal personnel and law enforcement agencies. In addition, evidence should be accounted for at all times; whenever evidence is transferred from one person to another, chain of custody forms should detail the transfer and include the signature of each party. A detailed record of all evidence should be kept, including the following:

- Identifying information (e.g., location, serial number, model number, host name, media access control (MAC) addresses, and IP addresses of a computer).
- Name, title and telephone number of each person who collected or handled the evidence during the investigation.
- Time and date (including time zone) of each handling of the evidence.
- Locations where the evidence was stored.

Another good practice is to hold a "lessons learned" meeting with all parties involved after a major incident. It is also advisable to hold regular meetings after minor incidents as it can be useful to improve security measures and the incident management process itself.

Digital Single Market Strategy (DSM)

Another relevant security set of best practices is the Digital Single Market Strategy for Europe of 2015 (DSM).[3] The adoption of the Network and Information Security Directive, currently in the legislative process, should mark an important step forward. One of the key priorities of the European Cybersecurity Strategy is to develop industrial and technological resources for cybersecurity. A more joined-up approach is therefore needed to step up the supply of more secure solutions by EU industry and to stimulate their take-up by enterprises, public authorities, and citizens. In addition, an effective law enforcement response to online criminal activity is necessary.

The General Data Protection Regulation will increase trust in digital services, as it should protect individuals with respect to processing of personal data by all companies that offer their

[1] ISO 27035:2012, p.2

[2] ISO 27035:2012, p.3

[3] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC ANDSOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A Digital Single Market Strategy for Europe, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52015DC0192

services on the European market. Special rules apply to electronic communications services which may need to be reassessed once the general EU rules on data protection are agreed, particularly since most of the articles of the current e-Privacy Directive apply only to providers of electronic communications services, i.e., traditional telecoms companies.

ENISA (European Network and Information Security Agency) Incident Management Guide

ENISA also provides a good practices and practical information guideline for the management of network and information security incidents[4]. The main focus of the guide is the incident handling process, which involves the detection and registration of incidents, followed by triage (classifying, prioritising, and assigning incidents), incident resolution, closing and post-analysis.

Payment Card Industry Data Security Standard

Payment Card Industry Data Security Standard[5] (PCI DSS) is a payment media standard issued by credit card companies to protect the credit card data of customers making transactions from any source.

Some good practices that are included in the PCI DSS include:

- Monitoring of security controls.
- Ensuring that all security control failures are detected and responded to in a timely manner.
- Reviewing changes in the environment.
- Changes in organisational structure resulting in a formal review of the impact on the scope.
- Conducting periodic reviews and communications.
- Reviewing hardware and software technologies at least annually.

EU Cybersecurity Act (Regulation (EU) 2019/881)

The EU Cybersecurity Act[6] defines a continual and reinforced authority for ENISA, as the European Cybersecurity Agency, and also specifies a structure for the European Union that will be used for the development of the cybersecurity certification for Information and Communications Technology (ICT) products, including IoT devices, processes and services that will be recognised in all EU Member States.

EU Blueprint

The EU Blueprint is used for the Coordinated Response to Large-Scale Cyber Incidents[7]. Applying this facilitates the planning of activities to improve security in applications, processes, and controls, requiring mapping business priorities with security priorities, assessing current state using the maturity model safety program and setting the maturity model state target. For each case, procedures and processes collect internationally accepted best practices for managing incidents.

[4] ENISA Good Practice Guide for Incident Management, available at: https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management

[5] Payment Card Infrastructure Data Security Standard, available at: https://www.pcisecuritystandards.org/document_library

[6] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance), https://eur-lex.europa.eu/eli/reg/2019/881/oj

[7] Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises, https://eur-lex.europa.eu/eli/reco/2017/1584/oj

5

Compliance and Regulation

There are different regulations from European and national bodies, and in specific regulations for incident management. The most important European bodies that regulate and propose recommendations for incident management are EBA, ECB and ENISA, and the national bodies are BaFIN, INCIBE, IE-NCSC and UK-NCSC. The specific regulations that are recommended to be followed are NIS D, PSD2, GDPR and eIDAS.

5.1. How important bodies in the EU collect threats? Best practice

5.1.1. European bodies

EBA

The European Banking Authority (EBA) is a European authority whose mandate is to ensure effective finance and banking sector regulation and supervision exists throughout the European Union.[1] The objective of the EBA is to contribute to the stability and efficiency of the financial system, for the Union economy, its citizens, and businesses. The EBA provides regulatory guidelines and recommendations to the industry and provides information and guidance on IT risk management, risk management and risk mitigation strategies. One of the key pieces of regulation for the industry is the second Payment Services Directive.[2]

ECB

The European Central Bank (ECB) is the entity responsible for administrating the monetary policy of European Union member countries which have adopted the euro currency. The principal goal of the ECB is to maintain price stability in the euro area, thus preserving the purchasing power of the euro. The ECB works with the central banks of the EU Member States to ensure that national central banks, as well as the entire EU banking system, are protected against cyber-attacks, limiting damage in the event of a data breach and ensuring the continuity of work carried out in financial institutions and banks. The EU Computer Emergency Response Team - or CERT-EU for short - warns its members of new threats, conducts tests, and provides advisory services. It also supports its members in responding to cyber-attacks and exchanges information with Member States' national or governmental CERTs or CSIRTs on cybersecurity threats, vulnerabilities and incidents, possible countermeasures and to improve the protection of their ICT infrastructures.

ENISA

The European Union Agency for Cybersecurity was established to contribute to the development of a European Union policy in the field of network security.[3] ENISA has published an Incident Reporting Framework for incident reporting under Article 19 of the eIDAS Regulation. ENISA has also provided guidance and recommendation to the finance sector[4], amongst others, and continues to be the central research agency for the European Commission in regard to cybersecurity.

5.1.2. National bodies

BaFIN

BaFIN is the acronym for the Federal Financial Supervisory Authority in Germany. In November 2017, the BaFIN published the Circular on Supervisory Requirements for IT in Financial Institutions.[5]

[1] Art 1 (5) Regulation (EU) 1093/2010.

[2] https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2

[3] https://www.enisa.europa.eu/about-enisa

[4] https://www.enisa.europa.eu/publications/EU_Cybersecurity_Initiatives_in_the_Finance_Sector

[5] Circular 10/2017 (BA): Supervisory Requirements for IT in Financial Institutions, published on 6th November 2017 (in the version of 14th September 2018) https://www.bafin.de/SharedDocs/Downloads/EN/Rundschreiben/dl_rs_1710_ba_BAIT_

INCIBE

The INCIBE is the Spanish National Cybersecurity Institute[6], a body responsible for the development of cybersecurity and digital trust. Its activity is based on research, the provision of services and coordination with the agents with competences in the field, contributing to building cybersecurity at a national and international level.

INCIBE's activity is founded on three fundamental pillars[7]:

- Services: INCIBE works for the user's protection and privacy, promoting mechanisms for the prevention of and reaction to data security incidents, minimising their impact where they occur, and promoting training and raising awareness.
- Research: INCIBE has at its disposal a great ability to address a range of complex projects of an innovative nature, guiding this approach as a researcher.
- Coordination: INCIBE participates in partnership networks, and therefore the coordination and collaboration with other national and international entities is an essential element of INCIBE's activity.

INCIBE-CERT[8] is the security incident response centre of reference for citizens and private law entities in Spain. It is one of the reference incident response teams that coordinates with other national and international teams to improve the effectiveness of the response to crimes involving networks and information systems, reducing their impact on public security.

IE-NCSC

The National Cyber Security Centre (IE-NCSC) of Ireland[9] is the main governmental body responsible for the execution of Ireland's National Cyber Security Strategy (2019-2024)[10]. The NCSC is given the governmental responsibility to:

- Advise and inform relevant bodies, government departments, and the sector in general.
- Ensure that national and critical infrastructure are suitably protected and informed.
- Understand and communicate the current cybersecurity climate.

UK-NCSC

The United Kingdom also has a National Cyber Security Centre[11] (UK-NCSC), whose role is to:

- Provide guidance on cybersecurity topics available to all.
- Respond to formal cybersecurity incidents within the United Kingdom.
- Nurture the UK's cybersecurity capability through specific events, guidance, and training.
- Actively secure public and private sector networks.

5.1.3. Specific regulations

NIS D

Member States have to also lay down notification procedures for OES (Operators of Essential

en.html

[6] https://www.incibe.es/en/what-is-incibe

[7] https://www.incibe.es/en/what-is-incibe/what-we-do

[8] https://www.incibe-cert.es/en/what-incibe-cert

[9] https://www.ncsc.gov.ie/

[10] https://www.ncsc.gov.ie/pdfs/National_Cyber_Security_Strategy.pdf

[11] https://www.ncsc.gov.uk/section/about-ncsc/what-we-do

Services) to the competent authority or CSIRT, including a determination of the significance of the impact of an incident[12], which is relevant for follow-up cross-border reporting of the respective incident if there is a significant impact on the continuity of essential services in other Member States.[13]

PSD2

The incident reporting framework established by the PSD2 obliges the payment service provider to notify the competent authority of its home Member State. This authority will then promptly provide details of the incident to the European Banking Authority (EBA) and the European Central Bank (ECB)[14].

EBA and the ECB shall, in cooperation with the competent authority of the home Member State, assess the relevance of the incident to other relevant Union and national authorities and shall notify them accordingly. The ECB shall notify the members of the European System of Central Banks on issues relevant to the payment system. On the basis of that notification, the competent authorities shall, where appropriate, take all of the necessary measures to protect the immediate safety of the financial system.

GDPR

For the purpose of incident handling, GDPR contains in Articles 33 and 34 a requirement to notify and communicate personal data breaches to the supervisory authority, also regulating the procedure for handling a security incident involving personal data. The notification of a personal data breach must contain, as a minimum, the following information:

- Nature of personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned.
- Name and contact details of the data protection officer or other contact point where more information can be obtained.
- Description of the likely consequences of the personal data breach.
- Description of the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects[15].

eIDAS

eIDAS is an EU regulation on a set of standards for electronic identification and trust services for electronic transactions in the European Single Market. According to Article 10 of the eIDAS regulation, security breaches of notified electronic identification schemes have to be suspended or revoked, without delay, by the notifying Member State and other Member States as well as the Commission have to be informed[16]. In order to regain availability of the cross-border authentication scheme, the authentication shall be re-established as soon as possible after the breach or compromise has been remedied and other Member States and the Commission shall be informed accordingly. As a last resort, the electronic authentication scheme is to be withdrawn by the Member States, if the breach or compromise is not remedied within three months of suspension or revocation.

[12] Art 14 (3) and (4) Directive (EU) 2016/1148
[13] Art 14 (5) Directive (EU) 2016/1148
[14] Art 96 Directive (EU) 2015/2366
[15] Art 33 (3) Regulation (EU) 2016/679
[16] Art 10 (1) Regulation (EU) 910/2014