Proposal for Article 19 Incident reporting

Proposal for an Incident reporting framework for eIDAS Article 19

www.enisa.europa.eu European Union Agency For Network And Information Security

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation, and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Authors

Dr. Konstantinos Moulinos, Christoffer Karsberg, Dr. M.A.C. Dekker.

Contact

For contacting the authors please use konstantinos.moulinos@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

Acknowledgements

For the completion of this guideline ENISA has worked closely with a working group of experts from national regulatory authorities and ministries from across Europe: the Article 19 Expert Group. We are grateful for their valuable input and comments.

Last but not least, ENISA would like to acknowledge the contributions by Andrea Servida and Marco Fernandez-Gonzalez from European Commission.

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

ISBN 978-92-9204-143-4 doi: 10.2824/014673

Table of Contents

Preface

The new regulation for electronic identification and trust services (Regulation (EU) No 910/2014[1], referred to as eIDAS), adopted on 23 July 2014, contains Article 19 which requires, among other requirements, that providers of trust services 1) assess risks, 2) take appropriate security measures to mitigate the risks, and 3) notify the supervisory body[2] about significant incidents/breaches. This triangle is also present in Article 13a of the Telecommunications Framework directive, which applies to the telecom sector, and Article 14 of the proposed Network and Information Security (NIS) directive, which applies to operators of critical infrastructures.

Article 19 also addresses various types of incident reporting to other different stakeholders (e.g. users, data protection authorities, competent national bodies for information security, ENISA etc.) involved in its application. Member States should efficiently analyse and then implement these notification flows in order to comply with the incident notification requirements of the eIDAS regulation.

In 2014, after eIDAS was adopted, ENISA initiated contacts with experts from ministries agencies, supervisory bodies, authorities, et cetera, who are (or might become) involved with the application of Article 19. For the sake of brevity these are referenced as competent authorities[3]. The goal of these contacts has been to discuss and agree the technical application of Article 19 by Member States. ENISA formed an expert group, to work together with experts from competent authorities on the application of Article 19 and, more generally, security incidents in the trust services.

The focus of this document is the implementation of incident reporting and it aims at supporting the supervisory bodies in being aligned with obligations set out in Article 19. The proposal has been prepared in consultation with the members of the expert group and reviewed by the private sector and the Forum of European Supervisory Authorities for Electronic Signatures (FESA) as well. Based on this document, ENISA will facilitate a pilot incident reporting framework which is expected to be finalised and adopted by the Member States in spring 2016. This piece of work falls under Work Package 3.2, Deliverable no 5 on ‘Guidelines on Incident Reporting Scheme for Article 19’ of the ENISA Work Programme 2015[4].

It has to be noted that article 19(4) of the eIDAS regulation foresees an implementing act on “formats and procedures, including deadlines ...”. Guidelines, described in this document, are a soft and flexible approach to address supervisory bodies’ (SB) needs. The Commission may issue implementing acts in the future if

[1] Regulation (EU) No 910/2014 of the European Parliament and of the Council, of 23 July 2014, on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[2] Article 20 of the same regulation mentions that EU Member States supervise the qualified trust service providers (QTSPs) that they conform to the requirements laid down by the Regulation.

[3] Although especially in the first years this work involves also experts from ministries and authorities who are not yet formally appointed as supervisory bodies to implement Article 19.

[4] https://www.enisa.europa.eu/publications/programmes-reports/enisa-work-programme-2015

deemed necessary / appropriate building upon the guidelines (and the results of their operational implementation).

Introduction

This document describes a framework for security incident reporting based on the requirements set by article 19 of the eIDAS regulation. It is being developed on a consensus basis between the experts of the working group formed by ENISA and it is reviewed by various relevant stakeholders from both the private and the public sector. The final report includes the consensual contributions and modifications of all stakeholders involved in its development and as such it is not a binding guideline.

Target audience

This document is primarily for the supervisory bodies (SBs) responsible for the application and enforcement of Article 19 in European Member States.

Scope

The scope of this document is the security incident reporting obligations contained in paragraphs 2 and 3 of Article 19 of the eIDAS regulation. It has to be noted that the scope of reporting within MS could be broader than article 19 as defined by national legislation related to supervision.

Goal

This document is published by ENISA to provide support to supervisory bodies responsible for the technical application of Article 19. In particular, the incident reporting set out in paragraphs 2 and 3 of Article 19. However the report might prove useful also to other entities such as trust service providers, TSL scheme operators, conformity assessment bodies etc.

1. Article 19 and the wider policy context

This document regards the incident reporting obligations in Article 19 of the eIDAS regulation, called "Security requirements applicable to trust service providers". For the sake of completeness, and for the convenience of the reader, the full text of Article 19 is quoted below. Incident reporting is addressed in paragraphs 2 and 3, and briefly touched on in the last sentence of paragraph 1. The reader can also find an overview of related EU policy initiatives and legislation.

1.1 Full text of Article 19

"1. Qualified and non-qualified trust service providers shall take appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide. Having regard to the latest technological developments, those measures shall ensure that the level of security is commensurate to the degree of risk. In particular, measures shall be taken to prevent and minimise the impact of security incidents and inform stakeholders of the adverse effects of any such incidents.

2. Qualified and non-qualified trust service providers shall, without undue delay but in any event within 24 hours after having become aware of it, notify the supervisory body and, where applicable, other relevant bodies, such as the competent national body for information security or the data protection authority, of any breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein. Where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the trusted service has been provided, the trust service provider shall also notify the natural or legal person of the breach of security or loss of integrity without undue delay.

Where appropriate, in particular if a breach of security or loss of integrity concerns two or more Member States, the notified supervisory body shall inform the supervisory bodies in other Member States concerned and ENISA.

The notified supervisory body shall inform the public or require the trust service provider to do so, where it determines that disclosure of the breach of security or loss of integrity is in the public interest.

3. The supervisory body shall provide ENISA once a year with a summary of notifications of breach of security and loss of integrity received from trust service providers."[5]

1.2 Policy context

In the following paragraphs, there is an overview of related EU legislation.

[5] According to article 17 (6) supervisory bodies have to notify Commission too. 'By 31 March each year, each supervisory body shall submit to the Commission a report on its previous calendar year's main activities together with a summary of breach notifications received from trust service providers in accordance with Article 19(2)'.

Article 13a of the Framework directive: *"Security and Integrity"*

The Telecommunications reform[6] package which was adopted in 2009, adds Article 13a to the Telecommunications Framework directive, regarding security and integrity of public electronic communication networks and services. Article 13a states that providers of public communication networks and services should take measures to guarantee security and integrity (i.e. availability) of their networks and that they must report to competent national authorities about significant security breaches. In addition, the Directive imposes obligations to national regulatory authorities to inform ENISA and authorities abroad when necessary, for example in case of incidents with impact across borders, and report to ENISA and to the Commission the summary incident reports annually. Article 13a also says that the Commission may issue more detailed implementation requirements if needed, taking into account ENISA's opinion.

The Commission, ENISA, and national regulators have since collaborated on implementing Article 13a and, in particular, to agree on a single set of security measures for the European electronic communications sector and a model for reporting on security breaches in the electronic communications sector to authorities abroad, to ENISA and the Commission.

While incident reporting is implemented differently at national level, with different procedures, thresholds, et cetera, nearly all national regulators use a common procedure, a common template and common thresholds for reporting to the Commission and ENISA.

In May 2012, ENISA received the first set of annual reports from EU Member States, concerning incidents that occurred in 2011. Every year ENISA receives incident reports from EU Member States and consolidates/aggregates these reports in a single public report.

Collected information is analysed in order to identify the root causes of incidents and then issue recommendations to further improve the resilience and security of EU communication networks. The guidelines together with the aggregated annual reports are public and one can find them at the ENISA website[7]. However, anonymised national reports are only available to the national authorities. National reports according to Article 13a of the Framework Directive are also shared voluntarily with operators who agree to provide information about their own incidents.

Article 4 of the e-Privacy directive: "Security of processing"

The Telecommunications reform package also amended the e-Privacy Directive[8], which addresses data protection and privacy related to the provision of public electronic communication networks or services.

[6] Available at: https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Copy%20of%20Regulatory%20Framework%20for%20Electonic%20Communications%202013%20NO%20CROPS.pdf

[7] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports

[8] Directive 2002/58/EC of the European Parliament and of the Council, of 12 July 2002, Concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

Article 4 of the e-Privacy directive requires providers of public communication networks and services to notify personal data breaches to the competent authority[9] and subscribers concerned, without undue delay. According to this article, providers are obliged to notify personal data breaches to the competent national authority and the subscribers or individuals concerned, when the personal data breach is likely to adversely affect their privacy. In addition, they should take appropriate technical and organisational measures to ensure security of services and keep an inventory of personal data breaches, including the facts surrounding the breaches, the impact and the remedial actions taken.

Article 4 also says that the Commission may issue technical implementing measures regarding the notification formats and procedures, in consultation with the Article 29 Working Party, the European Data Protection Supervisor (EDPS) and ENISA.

In 2011, ENISA started an expert group, including experts from national data protection authorities, industry, and EDPS, to draft recommendations for the technical implementation of Article 4. In 2013, the Commission started an expert group with experts from national competent authorities, to meet and discuss issues concerning e-Privacy.

Data protection reform

The European Commission has proposed to reform the current European data protection framework (Directive 95/46/EC), and has proposed an EU regulation on data protection, which covers those organisations that are processing personal data, regardless of the business sector in which the organisation operates. Security measures and personal data breach notifications are addressed in Articles 30, 31 and 32:

- Organisations processing personal data must take appropriate technical and organisational security measures to ensure security appropriate to the risks presented by the processing.
- For all business sectors, the obligation to notify personal data breaches becomes mandatory[10].
- Personal data breaches must be notified to a competent national authority without undue delay and, where feasible, within 24 hours, or else a justification should be provided.
- Personal data breaches must be notified to individuals if it is likely there will be an impact on their privacy. If the breached data was unintelligible[11], notification is not required.
- Discussions about this proposal are still underway.

Network and information security (NIS) directive

The European Commission also published a European Cyber Security Strategy and proposed a directive on network and information security (NIS). The strategy and the directive explicitly refer to Article 13a as an

[9] In a number of countries, the competent body for notification about personal data breaches related to electronic communications networks and services is not the telecom regulator, but a data protection authority or other agency.

[10] This provision extends personal data breach notifications beyond the electronic communications sector.

[11] In the recommendation for the technical implementation of Article 4, unintelligible data is described as data that has either been encrypted (asymmetric or symmetric), or hashed.

example, and the proposed directive basically extends Article 13a to other critical sectors. In particular, Article 14 of the proposed NIS directive contains the following provisions:

- Market operators and public administrations should take appropriate security measures to protect their core services.
- Market operators and public administrations should report incidents to competent national authorities.
- Competent authorities should collaborate and share summaries of incident reports amongst the network of competent authorities.

In the preamble of the NIS directive, ENISA is tasked with acting as a bridge between the different types of authorities, including data protection authorities, national telecommunications regulators, and others, and to develop a single reporting template. The promulgation of the NIS directive has yet to be finalised.

ENISA's role and objectives

ENISA's role is mentioned in preamble 39 of the eIDAS regulation; *"To enable the Commission and the Member States to assess the effectiveness of the breach notification mechanism introduced by this Regulation, supervisory bodies should be requested to provide summary information to the Commission and to European Union Agency for Network and Information Security (ENISA)."*

Furthermore, article 19 (2), requires the 'notified supervisory body, where appropriate, in particular if a breach of security or loss of integrity concerns two or more Member States, to inform the supervisory bodies in other Member States concerned and ENISA'. Finally, article 19 (3), requires the supervisory body to provide ENISA once a year with a summary of notifications of breach of security and loss of integrity received from trust service providers.

ENISA's primary objective is to implement the incident reporting mandated in Article 19, i.e. to agree with the Member States on an efficient implementation of ad-hoc cross border incident and annual summary reporting.

Secondly, ENISA aims to use annual summary reporting for the following purposes:

- To provide feedback to supervisory bodies about:
  - security incidents that have significant impact on trust services and the personal data contained therein,
  - root causes of security incidents,
  - lessons learned from security incidents; and
  - incident trends.
- To provide aggregate (statistical) analysis of incidents for policy makers, the public and the industry, describing overall frequency and impact of trust service security incidents across the EU.
- To facilitate the exchange of experiences and lessons learned among supervisory bodies, to allow them to better understand and address security incidents.
- Issue recommendations and guidance for supervisory bodies, the private sector and policy makers.
- Evaluate the effectiveness of security measures in place.
- Develop more realistic incident scenarios for pan-European exercises.

Thirdly, ENISA aims to support supervisory bodies with the implementation of national incident notification schemes and in this way support efficient and harmonized incident notification schemes across the EU. Harmonized implementation of legislation creates a level playing field and makes it easier for trust service providers (TSPs) and users to operate across different EU countries.

2. Security Incident notification in Article 19

In this section the basic article 19 terms and concepts are presented together with some abbreviations that are used later on in this document.

2.1 Security incidents

Paragraph 1 of Article 19 asks providers to assess risks for the security of the trust services they provide, and take commensurate security measures to mitigate the impact.

Security incidents: Any breach of security or loss of integrity that has an impact on the security of the trust service provided. i.e. an **all-hazard approach** is foreseen– any incident that would have an impact on the security of the trust service.

Reportable security incidents: Any breach of security or loss of integrity that has a significant impact on the trust service provided[12] or on the personal data maintained therein.

Thresholds for trust service providers to notify (i.e. what is significant) the national supervisory bodies depend on national circumstances: different countries will adopt a different approach to setting national reporting thresholds, depending on national details, including: the type of providers in the sector, the population of the country, national legislation, etc. The objective of this document is to agree upon indicators and thresholds[13] which can be used as a basis for the annual summary reports submitted by the supervisory bodies to ENISA and the European Commission; they can also be used as guidance to supervisory bodies when setting national thresholds. The following non-exhaustive list[14] provides several sample incidents:

- Private key storage: e.g. unauthorized access to
  - Root CA private keys,
  - Subordinate CA private keys,
  - Private keys for signing certificates, CRLs, OCSP responses,
  - Keys for the operation of the qualified trust service,
  - Unauthorised access to end users’ private keys due to TSP’s unsuitable security measures,

[12] It has to be noted that the TSP shall only be responsible for reporting breaches on systems or processes that are under the TSP’s control. In case core functions are subcontracted, the TSP remains liable for notifying security incidents that occur in the sub-contractor's systems.

[13] A threshold is considered as a triad of an indicator accompanied by specific values and measurement unit description.

[14] ETSI EN 319 411 could be used as a useful source of inspiration for scenarios which undermine the security requirements for TSPs described therein.

  - Unauthorised request using key belonging to a third party for the issuance or the renewal of a certificate; and
  - Unrecoverable destruction of private keys.

- Issuing of certificates: Stolen certificates (Diginotar scenario)[15,16]
- Identity theft[15, 16]: Attacker makes a false identity claim, obtains a number of certificates for a different identity.
- Revocation of trust claim: Software bug or Hardware crash causes an outage of the revocation response service.

  - Failure of the TSP to accept or to process revocation requests; and
  - Failure to provide information on the validity or revocation status of qualified certificates (unavailability of CRL/OCSP service).

- Security breach leading to personal data breach, of customers and of other parties, such as, but not only, TSP employees or consultants.
- Unavailability of Public Key Infrastructure Repository (Root and Sub CA certificates)[16].
- Unavailability of Timestamp service[16].
- Issuance of qualified certificates without using trustworthy systems in accordance with Article 24(2) and (5).
- Degraded or unavailable trust service e.g. where signing servers or network/centralized key- storage is used[16].
- Unauthorized access to, deletion of, or changes to personal data of customers of the provider.
- Security incidents which lead to a breach of communications security, leading to privacy breaches: Diginotar scenario.

2.2 Services in scope

Services in scope are those defined in article 3 of the eIDAS regulation, namely:

'trust service' means an electronic service normally provided for remuneration which consists of:

- *the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or*
- *the creation, verification and validation of certificates for website authentication; or*
- *the preservation of electronic signatures, seals or certificates related to those services*

Examples of business processes following under each service follow. The list of examples is only indicative.

[15] The incident is not relevant in case that the breach is caused by insufficient security controls at the owner of the certificate.

[16] This failure should only require incident reporting if it exceeds the SLA communicated to the relying parties.

2.2.1 Electronic signature service

2.2.1.1 Certification services (issuing certificates for electronic signatures)

- Creation
    - Registration and identification
        - Subject device provisioning
        - Certificate delivery to subject
        - Registration data and management (e.g. Subjects' certificates, RA private key destruction)
        - Subject certificate dissemination
        - Subject certificate renewal, rekey and update
    - Certificate creation data and management (e.g. Key pair generation, CA private key destruction)
    - CA Certificate dissemination
    - Certificate requester identity verification
- Verification and validation
    - Key pair generation of Validation Authority (VA)
    - VA certificate creation data and management (e.g. Key pair generation)
    - CA private key destruction
    - Validation assets (e.g. CRLs, OCSP servers) management
    - Revocation data (e.g. CRLs) management and dissemination
    - TSP providing verification and validation services identity verification

2.2.1.2 Signature services (signature as a service)

- Creation
- Registration and identification
    - Subject device provisioning
    - Signature delivery to subject
    - Registration data and management (e.g. Subject's signature, subject's certificate, RA private key destruction)
    - Subject signature renewal, rekey and update
- Signature Creation data and management (e.g. Key pair generation, CA private key destruction)
- Certificate requester identity verification

- Verification and validation
    - Key pair generation of Validation Authority (VA)
    - VA certificate creation data and management (e.g. Key pair generation,)
    - CA private key destruction
    - Validation assets management

    - Revocation data management and dissemination
    - TSP providing verification and validation services identity verification

2.2.2 Electronic seal service

2.2.2.1 Certification services (issuing certificates for electronic seals)

- Creation
    - Registration and identification
        - Subject device provisioning
        - Electronic seal delivery to subject
        - Registration data and management (e.g. subject's electronic seal, RA private key destruction)
        - Subject electronic seal renewal, rekey and update
    - Certificate creation data and management (e.g. Key pair generation, CA private key destruction)
    - CA Certificate dissemination
    - Certificate requester identity verification
- Verification and validation
    - Key pair generation of Validation Authority (VA)
    - VA certificate creation data and management (e.g. Key pair generation)
    - CA private key destruction
    - Validation assets (e.g. CRLs, OCSP servers) management
    - TSP providing verification and validation services identity verification

2.2.2.2 Seal services (seal as a service)

- Creation
    - Registration and identification
        - Subject device provisioning
        - Seal delivery to subject
        - Registration data and management (e.g. Subject's signature, subject's certificate, RA private key destruction)
        - Subject seal renewal, rekey and update
    - Seal creation data and management (e.g. Key pair generation, CA private key destruction)
    - Certificate requester identity verification
- Verification and validation
    - Key pair generation of Validation Authority (VA)
    - VA certificate creation data and management (e.g. Key pair generation)

    - CA private key destruction
    - Validation assets management
    - Revocation data management and dissemination
    - TSP providing verification and validation services identity verification

2.2.3 Electronic time stamping service

- Creation

    - Registration and identification
    - Registration data and management (e.g. subject's digital certificate)
    - Certificate creation data and management (e.g. TSA key pair generation, TSA private key destruction)

- TSA Certificate dissemination
- Verification and validation

    - Key pair generation of Validation Authority (VA)
    - VA certificate creation data and management (e.g. Key pair generation)
    - TSA private key destruction
    - Validation assets (e.g. CRLs, OCSP servers) management

2.2.4 Registered delivery service[17]

- Creation: what relates to signing / sealing key creation, certificate generation and distribution, signing / sealing process, control over the transmission path, acceptance of a delivered item by the recipient's delivery system, delivery receipt generation and transmission to the sender,
- Verification and validation

    - what relates to the transmission path
    - what relates to verifying all signatures/seals.

2.2.5 Website authentication certificate service

- Creation

    - Registration and identification

        - Subject device provisioning
        - Certificate delivery to subject
        - Registration data and management (e.g. Subjects' certificates, RA private key destruction)
        - Subject certificate dissemination

[17] For both public and private documents

    - Subject certificate renewal, rekey and update
  - Certificate creation data and management (e.g. Key pair generation, CA private key destruction)
  - CA Certificate dissemination

- Verification and validation

  - Key pair generation of Validation Authority (VA)
  - VA certificate creation data and management (e.g. Key pair generation)
  - CA private key destruction
  - Validation assets (e.g. CRLs, OCSP servers) management
  - Revocation data (e.g. CRLs) management and dissemination

2.2.6 Preservation services

- Key pair storage, backup and recovery
- RA/CA/VA/TSA private key pair destruction
- Adding information for extended long-term and archival signatures

2.3 Incident reporting flows

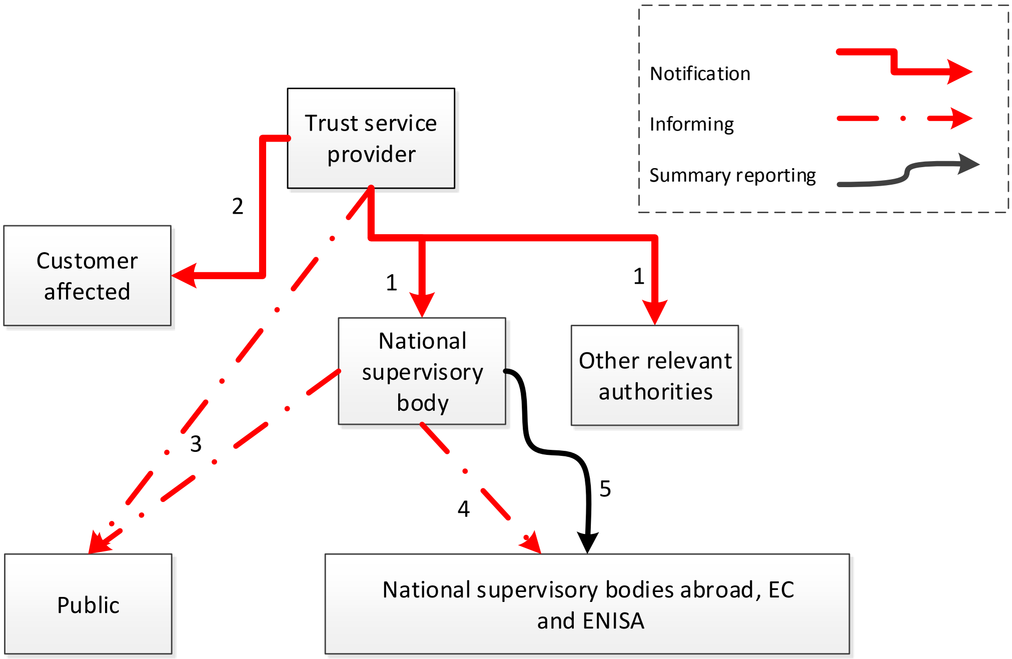
Article 19 addresses different types of reporting:

1. Notification about a security incident, that has a significant impact on the trust service provided or on the personal data maintained therein, within 24 hours after the trust service provider is becoming aware of it[18], to the supervisory body and, where applicable, other relevant bodies (e.g. DPA, national competent authority for information security, etc.).
2. Notification of the natural or legal person to whom the trust service was provided, who was affected by the security incident, without undue delay. In this document and in the diagram below, this abbreviates to 'the customer affected'
3. Informing the public (or requiring the provider to do so)
4. Informing relevant supervisory bodies abroad and ENISA, where a security incident involves two or more Member States.
5. Annual summary reporting to ENISA.

The diagram below shows the different incident reporting flows, numbered as above.

[18] By the provider or by the NRA or by an external party.

Figure 1: Overview of reporting flows in Article 19


Notification
Informing
Summary reporting
Trust service provider
Customer affected
National supervisory body
Other relevant authorities
Public
National supervisory bodies abroad, EC and ENISA
1
1
2
3
4
5

Actors are explained in more detail, by referring to the legal text of Article 19[19]:

- Trust service provider: the "Qualified and non-qualified trust service providers" where the security breach is detected.
- Customer affected: the "natural or legal person to whom the trust service has been provided" who is affected by the security breach.
- Supervisory body: the body established in Member State territory or, upon mutual agreement with another Member State, a body established in that other Member State which is responsible for supervisory tasks in the designating Member State.
- Other relevant authorities: any other relevant bodies, depending on the national setting, such as the competent national body for information security or the data protection authority.

The diagram shows a number of reporting flows such as **annual summary reporting** (flow 5), **cross-border notification** (flows 2[20], 4) and **national incident notification** (flows 1, 2, 3). The next sections give more details for each reporting flow.

[19] A relying party is considered as part of the public.

[20] Flow no 2, might be either national or cross border because article 17 (1) of the Regulation foresees that Member States shall designate a supervisory body established in their territory or, upon mutual agreement with another Member State, a supervisory body established in that other Member State.

3. Annual summary reporting

The following are the key elements of annual summary reporting: the reporting template (what is reported), the reporting thresholds (when it is reported) and the means to submit the report (how the report is submitted).

Remark about information sharing: The annual summary reporting is not the only information sharing that happens between supervisory bodies and ENISA. Supervisory bodies have to be informed about cross-border incidents and severe security incidents which may also be discussed in meetings of this group – on a case by case basis.

3.1 Annual summary reporting template

This section defines the reporting template. This will be implemented as a form for authorities to use when reporting to ENISA. Information to be collected, might at least include:

3.1.1 Trust service concerned

- QTSP/N-QTSP: Qualified or non-Qualified trust service provider
- A (multiple) choice of one or more service(s) impacted by the incident. See Section 2.2

3.1.2 Impact of security incident

- Severity of the incident: significant or severe impact or disastrous (see section 3.2)
- Personal data impacted
- Type of personal data impacted
- Number of users affected
- Cross-border impact

3.1.3 General description of the security incident

Free text description

3.1.4 Root cause category

Choose one of: human error, external or internal malicious actions, natural disaster, system failure, third party[21].

[21] The category “third party failure” should be used for incidents where the root cause is outside the direct control of the provider, for example, when the root cause occurred at a contractor used for outsourcing, or at an organization somewhere along the supply chain.

3.1.5 Detailed causes

Detailed description of causes and the course of the security incident.

3.1.6 Assets affected

Detailed description of the assets affected.

3.1.7 Mitigating security measures

Description of mitigating security measures taken to address the security incident (in the response phase).

3.1.8 Notifications and information

- Other authorities notified, nationally
- Other authorities notified, abroad
- Customers affected notified
- Public informed
- Information disclosure by supervisory body under freedom of information legislation

3.1.9 Total duration of the security incident and/or the recovery time

The length of time the security incident lasted, including the time it took to rectify.

3.1.10 Improvements and lessons learned

Describe what measures have been taken or are planned to prevent similar incidents from occurring.

3.2 Indicators for annual summary reporting

Providing a framework for determining the importance of a TSP’s reportable incident is fundamental to the effectiveness of the overall reporting scheme. Paragraph 2 of Article 19 says that security incidents with a “*significant impact”* should be reported. Thus, Article 19 will be most effective if a framework is put in place that allows for consistency and clarity in weighing an incident's significance. Member states can take different approaches to defining reporting thresholds (see 2.1), thus it is important to set notification indicators and thresholds which are the same for all Member States.

A previous ENISA study[22] has indicated that the **number of users** affected, by a reportable incident under Article 19, would seem to provide information about the incident's nature, and the **duration of the incident** may indicate the TSP’s ability to recognize and solve the problem, which also is a factor that could be considered in weighing the importance of a reportable incident affecting a TSP. As ENISA’s interaction with

[22] ENISA, Implementation of article 15 of the draft regulation on electronic identification and trusted services for electronic transactions in the internal market’, 2012, available at https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/implementation-of-article-15.

the stakeholders has shown, the following indicators, or combinations of them, might also be used to assess the significance of an incident in the context of article 19:

a. The service affected by the incident (one of the services in section 2.2).
b. The asset(s) involved in the provision of the service and affected by the incident (see Annex B: for a list of assets).
c. The security concept affected by the incident: one or more out of Confidentiality, Integrity, Availability and Accountability[23].
d. Duration of the unavailability of the service (one of the services in section 2.2) affected by the incident.
e. Number of users affected by the incident.

In this section, only the indicators, for annual summary reporting from national authorities to ENISA, are discussed. A balance must be struck between ensuring that sufficient and timely information flows between SBs, ENISA and Commission so as to promote Article 19's objectives, and not burdening them with unnecessary work and information overload. There should be clarity surrounding what indicators should trigger a trust service provider's reporting requirement and mechanism.

The topic of notification thresholds was explored with regard to notifying ENISA and other countries' competent authorities in '*Technical Guideline on Reporting Incidents report for Article 13a implementation*' by ENISA. As a baseline matter, the standard for reporting an incident to ENISA was determined to be "every time the impact is equal to, or higher than, a set of predefined thresholds agreed between ENISA and the NRAs." It explained that the thresholds should serve as a minimum entry level for required notification, and every competent authority can then "impose stricter and more granular thresholds to trigger the reporting at national level," but that these thresholds should then also be used to trigger the process of reporting to ENISA[22].

From the discussions with stakeholders it seems that the two most favourable approaches for impact assessment or loss of integrity of a trust service under article 19 are:

- Security scenarios/examples combined with indicators.
- Combinations of indicators

3.2.1 Security scenarios/examples

This approach is based on the classification of incidents in different impact levels. The severity of security incidents is rated on a scale from 1 to 5:

1. No impact

[23] '*Loss of accountability of actions: In case of an incident, existing logs, as well as their protection again manipulation, are an important tool to be able to determine the nature and source of the incident. Lack of an appropriate level of logging, loss of existing logs or lack of protection of logs can lead to the impossibility to determine user actions.*', 'Risk assessment Guidelines for trust services providers – Part 2', ENISA, 2013 available at https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/tsp2-risk/at_download/fullReport

2. **Insignificant impact: provider assets were affected but no impact on core services**
3. **Significant impact: part of the customers/services is affected**
4. **Severe impact: large part of the customers/services is affected**
5. **Disastrous: the entire organisation, all services, all certificates are affected**

Only incidents of severity level 3 and beyond are reportable. Below there is a list of examples of incident scenarios which is not exhaustive.

Examples for level 1

- **A zero-day vulnerability has been found. This means a number of servers are at risk. Provider acts quickly to patch within several hours of the disclosure.**
- **Unsuccessful attacks and attempts for penetration.**

Example for level 2

- **Server got infected with a virus but services were not impacted.**
- **Phishing attacks.**
- **Data breach of basic identification (i.e. name and surname) data**

Examples for level 3.

- **A number of certificates are provided to the wrong natural or legal person (e.g. identity theft).**
- **A number of qualified certificates issued without using trustworthy systems in accordance with Article 24(2) and (5)A number of unauthorized certificates are issued (e.g. stolen certificates, with false data, Diginotar e.g.).**
- **CRL/OCSP service is unavailable provided that unavailability is beyond the communicated SLA and imposes security risks beyond responsibilities communicated to relying parties.**
- **Unavailability of Timestamp service provided that unavailability is beyond the communicated SLA and imposes security risks beyond responsibilities communicated to relying parties.**
- **Unavailability of Public Key Infrastructure Repository (Root & Sub CA certificates)–Webpage hacked, in case that unavailability of the repository impedes validation of certificates.**

- **Trust list is unavailable provided that unavailability is beyond the communicated SLA and imposes security risks beyond responsibilities communicated to relying parties[24].**
- **Loss of exclusive control on private key by end user(s) as far as the TSP is responsible for this.**
- **Security incidents affecting Registration service actually affecting user's registration.**
- **Breach of personal data other than the basic identification.**

Examples for level 4

- **Certificate issuance /renewal is unavailable, for more than 24 hours, provided that unavailability is beyond the communicated SLA and imposes security risks beyond responsibilities communicated to relying parties.**
- **Unavailability of Timestamp service for more than 24 hours, provided that unavailability is beyond the communicated SLA and imposes security risks beyond responsibilities communicated to relying parties.**
- **CRL/OCSP service is unavailable for more than 24 hours, provided that unavailability is beyond the communicated SLA and imposes security risks beyond responsibilities communicated to relying parties.**

Examples for level 5

- **Root, or issuing CA or intermediate CA certificate is revoked (e.g. general compromise of issuance/signing operations) unexpectedly or unplanned.**
- **Permanent unavailability of CA HSM private key.**
- **Natural disaster permanently affecting the CA HSM availability.**

The SB can use the aforementioned examples as a good practice guideline to decide if they should include an incident to the annual summary report or not. While straightforward, this approach leaves sufficient space for different national interpretations of what is reportable or not among different SBs. Therefore, the stakeholders have proposed to use this list of examples in combination with specific indicators and more specifically with thresholds based on the **duration of the unavailability of the service** and/or the **number of users** affected by the incident.

[24] The incident is reportable only if the service is provided by a TSP.

3.2.2 Combinations of indicators

For each type of trust services (see section 2.2) all possible combinations of the asset(s) involved in the provision of this service and the security concept affected by the incident (indicators b and c in the list cited at section 3.2), for that particular asset, will be rated by using specific qualitative values (low, medium, high). Personal data is considered as an asset of the service. Only medium and high impact combinations will be reported to ENISA and European Commission. The '*Risk assessment Guidelines for trust services providers – Part 2*'Error! Bookmark not defined. report by ENISA describes a detailed list of assets for TSPs.

3.3 ENISA annual incidents report

From January to February of each year, the Member States submit their annual reports to ENISA. Then, ENISA aggregates, via secure communication channels, the Member State annual summary reports and analyses the data. ENISA's resulting public report will provide an aggregated and anonymized overview of security incidents affecting trusted services across the EU; omitting details on individual incidents.

Remark about single point of notification: *Note that the article asks trust service providers to notify the supervisory body and other relevant authorities. In some settings this may be confusing for providers, causing double work and delays in compiling different incident notification templates and forms. To simplify notification procedure, Member States have two options:*

Set up a single-point-of-contact[25] for notification of incidents. In such a setting, the single-point-of-contact would relay or forward the notification to other relevant authorities. This single point of contact might or might not be the supervisory body. However, in some cases this might be cumbersome because:

- *communication channels between different national authorities are set by national administrative laws which are difficult and time consuming to change;*
- *it might add delays to the incident reporting production line because of the extra time needed by the intermediate body which first receives and then evaluates the notification information before forwarding it to the competent authority; and*
- *different authorities need access to different data subsets of the reported information. This means that the receiving authority should be empowered to take decisions on this matter which sometimes might be proved difficult especially in cases that personal data are involved the decision making.*
- *TSPs have to be considering laws and industrial standards which are might not be known to the single point of contact entity.*

Develop a single template[26] that is sent to different recipients by the TSP.

[25] For more details on the single-point-of-contact principle under eIDAS one can access http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2015.053.01.0014.01.ENG.

[26] An example of such a template is described in to ISO/IEC 27035:2011 Annex D.4.

4. Cross-border notification

Article 19 also requires the supervisory body to *inform* the supervisory bodies in other EU Member States (cross-border notification). Article 19 states: *"Where appropriate, in particular if a breach of security or loss of integrity concerns two or more Member States, the notified supervisory body shall inform the supervisory bodies in other Member States concerned and ENISA."*

The goal of cross-border information is to inform supervisory bodies abroad, about recent and/or ongoing incidents[27], which may be relevant for them.

The key elements of annual summary reporting are: the reporting template (what is reported), the criteria for reporting (when it is reported) and the means to submit the report (how the report is submitted).

Remark about incident response: Note that not every supervisory body has a 24/7 or crisis management role, which means that authorities in some Member States may not be able to notify or receive notifications outside office hours. Therefore this cross-border information sharing might not be used for incident response or crisis management purposes, see below. In all EU countries there are national CERTs, which are part of a worldwide network of CERTs for 24/7 communication and response to security incidents.

4.1 Cross-border notification template

Cross-border notification is an informal, ad hoc process, which happens largely at the discretion of supervisory bodies. Depending on the setting, supervisory bodies may use a template, for example, the template for annual summary reporting (see 3.1).

4.2 Criteria for cross-border notifications

The legal text of Article 19 implies two criteria for informing supervisory bodies in other Member States:

- Customers affected: Authorities should inform authorities in other Member States only when customers (i.e. natural or legal persons) in that other member state are affected.
- Appropriate: Authorities should only inform when it is appropriate.

The interpretation of the first criterion has to be seen on a case-by-case basis. Here are some examples:

No need to notify other MS supervisory bodies

- *A breach of security of a TSP in country X impacts a trust service only used by the citizen of country X living in country Y to interact with country X authorities.*

Need to notify other MS supervisory bodies

[27] In order to achieve this, a two steps reporting approach (see 5.2) might needed.

- *One may consider that a breach of security occurring to a trust service provider providing trust services only at national level might have a cross-border impact if the customers are using such trust services to carry out cross-border transactions (with public authorities in another MS for example).*
- *Unavailability of TSL (CRL/OSP) will affect validation services of other EU countries, fake certificate could be used in systems of all EU countries as well. The TSP in country X, where the security breach took place, should assess and then determine on a case-by-case basis to notify the supervisory bodies in other MS as indeed a significant security breach affecting a validation service might potentially concern other MS.*

The following is a non-exhaustive list of examples of cases that it would be appropriate to undertake cross-border notification.

- *Incidents affecting services or websites or legal persons based in other EU countries*
- *Incidents involving equipment or services that are also in use in other EU countries*
- *Incidents with causes affecting other EU countries such as large scale DDoS attacks.*
- *Incidents requiring actions by the supervisory body abroad.*
- *Incidents affecting governmental affairs in other EU countries*

4.3 Cross-border notification process

ENISA maintains a contact list of email addresses and telephone numbers of contact points at supervisory bodies to enable cross-border information sharing. The contact list contains:

- Information about the supervisory body (name, street address, general phone number, URL)
- Information about two contact points (name, phone number, email, contact availability)
- Other remarks (any relevant information for the contacting body, such as X.509 certificates, PGP keys, or response times, shifts, etc.).

The contact list is provided to supervisory bodies upon request (resilience@enisa.europa.eu). The contact list is updated by the bodies when needed. The contact list is maintained and updated at a designated URL.

5. National incident notification

This section does not contain any guidance for Member States because national circumstances are different: in each country, the relevant authorities are different, with different resources, different responsibilities, and so on. The reader can find two fictitious examples of how Member States could set up a framework for notifying supervisory bodies and informing the public about national incidents under the eIDAS regulation as well as with a template for national notifications.

5.1 National notification framework examples

Example Country A:

Certification service providers have to notify the supervisory body immediately of all circumstances which do not allow to provide the certification services in accordance with the policy documents. Changes of the policy documents must be reported to the supervisory body before they become effective. Termination of services must be reported to the supervisory body three weeks in advance. Failure of both the primary and the secondary system for directory and revocation services must be notified to the supervisory authority within one calendar day.

There is no standard form for notification because of the very different nature of this kind of incidents. Formally, there is no two-step approach for the notification. But every incident notification of a Certificate Service Provider (CSP) leads to an investigation by the supervisory body where the CSP has to answer questions until the circumstances of the incident are sufficiently clear to the supervisory body.

Granting qualified status to CSPs contain, among others, the following notification requirements:

- **System failure, in particular regarding directory and revocation services, has to be reported unless it has been resolved within 24 hours.**
- **Shortage of qualified staff has to be reported if it is impossible to operate in accordance with the provider's role model.**
- **Suspect of compromise of TSP’s signature-creation data has to be reported in any case.**
- **Deficiencies detected in the course of internal audits have to be reported unless they do not constitute the breach of minimal prescribed requirements or they have been resolved within three working days.**

Example Country B:

Listing of non-qualified providers, thresholds for reporting, 24/7 point of contact for regulator, CERT and DPA, two-step approach (notify first, report later).

5.2 National notification template example

When it comes to notifying authorities, it is very common that the providers of a service adopt a two phase approach. According to this, the provider submits an initial and short description of the incident to the supervisory body and then, at a later stage, when details of the incident have been identified, he/she provides a more detailed and descriptive notification[28]. Information collected from an incident notification might include:

First incident notification

- Date and time the security incident detected (or started if known already)
- Contact details: contact details for questions about this security incident
- Provider concerned: name of the company
- Trust service(s) impacted (or potentially impacted): description of the service(s)
- Personal data impacted (or potentially impacted): description of the personal data impacted
- Short description of the security incident:
- Measures taken or planned: summarize what measures are taken or planned
- Cross-border impact

Final incident notification

- Date and time the security incident started
- Date and time the security incident detected by the TSP
- Contact details: contact details for questions about this security incident
- Provider concerned: name of the company
- Trust service(s) impacted: description of the service(s)
- Security feature(s) affected: confidentiality, integrity, availability etc.
- Personal data impacted: description of the personal data impacted
- Number of customers affected
- Duration of the incident
- Root cause category: One of human errors, malicious actions, natural disaster or system failure.
- Detailed cause of the security breach
- Detailed assets affected
- General description of the security incident: For example affected IT-systems, how was the incident detected, how long the incident was active, is there a vulnerability in a software which involves a third party etc.

[28] In order to follow development of long lasting incidents the supervisory body might require a regular reporting scheme. E.g. by adding a field to the incident notification for expected next report or by requiring one report at regular intervals during the lifetime of the incident.

- Cost estimation
- Measures taken: summarize what measures were taken to mitigate the incident
- long term measures, taken or plan, to avoid similar incidents from happening in the future
- Cross-border impact
- Other authorities notified
- Customers affected notified
- Public informed

Annex A: Threats and assets

This annex contains a dictionary of terms for threats and causes. The main use of this dictionary/vocabulary is to use them in reporting forms.

A.1 Terminology

A threat is defined as follows[29].

Threat: A threat is an event or a circumstance that could cause a security incident

This definition is based on the definition of a security incident that is common in international standards (such as ISO standards).

The word “cause” is used to speak about a threat when it has already caused an incident (in the past).

A.2 Root cause categories

Five different root cause categories are identified. Root cause categories are very broad categories that describe the underlying problem. This categorization is often subjective and a matter of judgement.

A.2.1 Human error

The category “human error” includes incidents caused by human error during the operation of equipment or facilities, the use of tools, the execution of procedures, etc.

A.2.2 System failures

The category “system failures” includes incidents caused by failures of a system, for example, hardware failures, software failures or errors in procedures or policies.

A.2.3 Natural disaster

The category “natural phenomena” includes incidents caused by severe weather, earthquakes, floods, wildfires, and so on.

A.2.4 Malicious actions

The category “malicious actions” includes incidents caused by a deliberate act by someone or some organisation.

[29] This definition is similar to the definition in ISO27K5, which defines a threat as the cause of an incident.

A.2.5 Third party failures

The category “third party failure” includes incidents where the cause was not under direct control of the provider, but some third-party.

A.3 Detailed threats and causes

A non-exhaustive list of more detailed threats and causes follows.

A.3.1 Denial of service attack

A Denial of Service (DoS) attack aims to overload systems with traffic; such attacks can have an impact on the continuity of trust services.

A.3.2 Malware and viruses

Malware can affect databases, servers, etc., which could have an impact on the security of trust services.

A.3.3 Theft or loss of equipment

Hardware theft could have an impact on trust services, for example, where theft damage systems, in particular, multi-purpose IT equipment, or valuable items, such as HSM or large batteries, are valuable and portable.

A.3.4 Theft or loss of data

Theft of data may have an impact on the well-functioning of trust services and on the privacy of the customers’ personal data as well.

A.3.5 Power cut

Power cuts of the (public) power grid, can have an impact on infrastructure that relies on power.

A.3.6 Hardware failure

Hardware failures (when physical hardware breaks) could affect physical infrastructure such as servers, routers, HSMs, etc. and impact trust services.

A.3.7 Software bug

Software bugs[30] could have an impact on ICT systems, such as routers, servers, databases, et cetera, and in this way impact trust services.

[30] Zero day threats are also included.

A.3.8 Faulty hardware change/update

A change or update of hardware, for example, for maintenance, replacement, or renewal, could go wrong and have a negative impact on trust services.

A.3.9 Faulty software change/update

Software changes or updates, for example, the installation of new software or software patches, could go wrong and have a negative impact on trust services. Note: this threat includes software such as ‘configuration files’.

A.3.10 Tampering of personal data

Tampering of personal data has an impact on the well-functioning of trust services and on the privacy of the customers’ personal data as well.

A.3.11 Eavesdropping

Eavesdropping may have an impact on the confidentiality of the data and on the privacy of the customers’ personal data as well.

A.3.12 Cryptanalysis

Cryptanalysis may have an impact on the confidentiality of the data and on the privacy of the customers’ personal data as well.

A.3.13 Overload

Overload of traffic and usage (e.g. too many CRL requests) could impact trust services.

A.3.14 Policy or procedure flaw

A flaw in a policy or procedure, or the absence of a policy or a procedure, could have a negative impact on trust services.

A.3.15 Security shutdown

Security risks could force a provider to shut down a service, for example, in order to have the time to patch software vulnerability.

Annex B: Assets

This annex will contain a dictionary of terms for assets. The main use of this dictionary/vocabulary is to use them in reporting forms

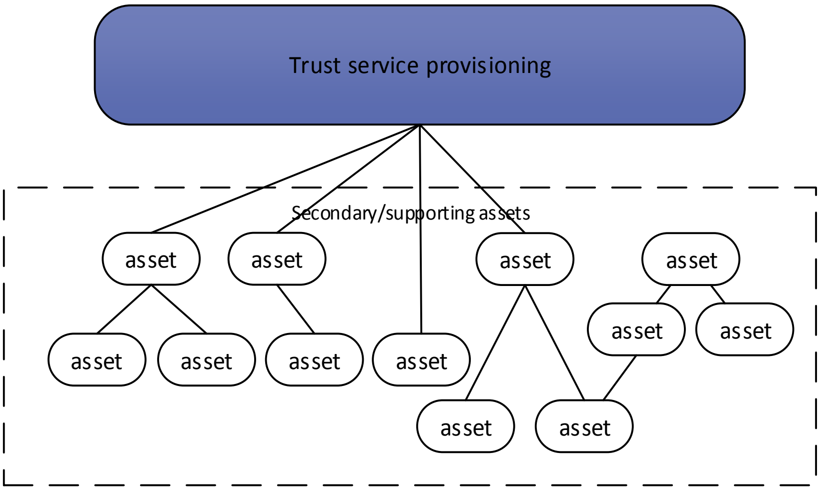
B.1 Terminology

An asset is basically anything of value. Assets could be abstract assets e.g. processes or reputation, virtual assets e.g. data, physical assets e.g. cables or a piece of equipment, human resources, money, etc. In this section, the focus is on the following assets:

Scope: The assets in scope are those assets that support the provision of trust services.

This means that abstract assets like 'money' or 'reputation' are out of scope. Similarly, suppose a provider has an online store for selling smartphones and subscriptions. The shopping cart system is an asset, but it is out of scope of this guideline because it does not directly support the provisioning of network and communication services.

Figure 2: Assets in scope of Article 19



B.2 Asset types

In this section different asset types are listed as a means to provide a vocabulary for authorities to use when reporting security incidents[31]:

- Private key storage
- Signing servers
- Webservers
- Facilities and physical security systems
- Logical security systems
- Hardware Security Modules (HSMs)
- Private keys
- Audit logs
- Backup copies
- RA information
- Revocation information
- Timestamp Servers
- Repository and Users Database Servers
- Personal data
- Card/payment data
- Procedures
- Human resources
- Hardware
- Software

[31] The ENISA report on "Risk assessment Guidelines for trust services providers – Part 2", contains a comprehensive and detailed list of assets in a Trusted Service Provider (TSP). The report is available at http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/tsp2-risk.

Annex C: Informing the public and/or victims

Article 19 imposes an obligation to TSPs to notify customers affected to whom the trusted service has been provided and the public in case that disclosure of the breach of security or loss of integrity is in the public interest. Each TSP must be prepared to respond to a possible breach of security of the services it provides. Apart from the technical skills, the TSP should have the right communication capabilities in order to inform the involved, in the breach of security, parties. For this reason it must prepare a communication plan emphasizing on: a) internal communications, b) communication with supervisory bodies and law enforcement authorities where relevant and c) the affected individuals. The aim of this communication plan is to minimize the impact of the breach on the individuals and on the reputation of the organization. The TSP should exercise the effectiveness of its communication plan from time to time and keep it up to date.

C.1 Informing customers affected

It is particularly relevant to assess the consequences of security incidents on the customers affected to determine whether or not the breach of security should be notified to individuals. The harm that an individual may suffer as a result of the breach of security has to be first determined by the TSP and then he has to send a notification to the individuals affected. ENISA has published a report which provides with useful tips when notifying individuals[32] in case of a data breach. In addition, the Article 29 Working Party has issued an opinion which provides guidance to controllers (the TSPs) in order to help them to decide whether to notify data subjects (individuals) in case of a “personal data breach”[33]. TSPs might get inspiration from these documents when it comes to notify the customers affected by a security breach.

C.2 Informing the public

TSPs will likely provide this notification in the form of a press release to appropriate information security media outlets. Like individual notice, this media notification should be provided without unreasonable delay and might include the same information required for the individual notice (see previous paragraph).

Spokesperson(s) need to be prepared to respond to media inquiries. The plan should anticipate the need to provide access to services and information to help those impacted. In addition to email, written correspondence, and web site postings, companies should monitor the use of social networking sites such as Facebook, Twitter and blogs for consumer sentiment. Companies may consider using them for controlled, scripted and moderated postings, but need to be prepared for a debate or dialog, which may follow.

[32] ENISA report on ‘Recommendations on technical implementation guidelines of Article 4[32]’, pp. 28-36, available at https://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/dbn/art4_tech

[33] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

The TSP might also consider to create a set of pre-approved web pages and templates staged, phone scripts prepared and frequently asked questions (FAQs) drafted and ready for posting. TSP personel needs to anticipate call volumes and steps to minimize hold times following a significant breach of security and to consider the need of multi-lingual support.

Annex D: Informing other authorities

Notification to other national authorities is an informal, ad hoc process, which happens largely at the discretion of supervisory bodies. Depending on the setting, supervisory bodies may use a template, for example, the template for annual summary reporting (see 3.1).

References

Legislation

[1] Article 13a of the Framework directive of the EU legislative framework on electronic communications: http://ec.europa.eu/information_society/policy/ecomm/doc/140framework.pdf

[2] Article 4 of the e-Privacy directive, part of the EU legislative framework on electronic communications: http://ec.europa.eu/information_society/policy/ecomm/doc/24eprivacy.pdf

[3] The electronic communications regulatory framework (incorporating the telecom reform): http://ec.europa.eu/information_society/policy/ecomm/doc/library/regframeforec_dec2009.pdf

[4] Article 15 of the Regulation on electronic identification and trust services for electronic transactions in the internal market: http://ec.europa.eu/information_society/policy/esignature/eu_legislation/regulation/index_en.htm

[5] Article 30, 31 and 32 of the proposed Data Protection regulation: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf The regulation is part of a wider reform of the data protection framework: http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

[6] Roadmap for a proposal on a European strategy for internet security: http://ec.europa.eu/governance/impact/planned_ia/docs/2012_infso_003_european_internet_security_strategy_en.pdf

[7] The speech of EU Commissioner Neelie Kroes on the EU strategy for internet security: http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/204&format=HTML&aged=0&language=EN&guiLanguage=en

[8] The speech of EU Commissioner Cecilia Malmström on the EU Cyber security strategy: http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/315

Related ENISA papers

[1] ENISA's Article 13a Guidelines on Incident reporting and Minimum security measures.

[2] ENISA's Recommendations for the technical implementation of Article 4.

[3] ENISA's 2009 paper on incident reporting shows an overview of the situation 3 years ago.

[4] ENISA's 2011 paper on data breach reporting across the EU shows an overview of the different national approaches to personal data breach notifications.

[5] ENISA's paper on National Cyber Security Strategies shows commonalities and differences between national cyber security strategies across the EU Legislation.

[6] ENISA's report on Security framework - Guidelines for trust services providers – Part 1.

[7] ENISA’s report on TSP Risk assessment - Guidelines for trust services providers – Part 2.[8] ENISA’s report on Mitigating the impact of security incidents - Guidelines for trust services providers – Part 3.

ENISA
European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

Catalogue Number (IF APPLICABLE)

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-143-4

DOI: 10.2824/014673