EUROPEAN UNION AGENCY
FOR CYBERSECURITY

TECHNICAL GUIDELINE ON INCIDENT REPORTING UNDER THE EECC

MARCH 2021

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. For more information, visit www.enisa.europa.eu.

CONTACT

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

AUTHORS

Marnix Dekker, Eleni Vytogianni - European Union Agency for Cybersecurity

ACKNOWLEDGEMENTS

For the completion of this guideline ENISA has worked closely with a working group of experts from national authorities, the ECASEC Expert Group (formerly known as the Article 13a Expert Group). We are grateful for their valuable input, comments and support in the process of developing of this document.

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN: 978-92-9204-471-8 – DOI: 10.2824/633879

EXECUTIVE SUMMARY

In December 2018, the new set of telecom rules called the European Electronic Communications Code[1] (abbreviated as EECC) was published and it entered into force. The EECC updates the EU telecom package of 2009[2] and paves the way for the roll out of fibre, very high capacity networks and next generation mobile networks (5G). EU countries have to transpose this EU directive into national law by the end of 2020.

An important part of the EECC is consumer protection and security of electronic communications. More services are in scope and the terms security and security incidents are now defined. Article 40 of the EECC contain detailed security requirements for electronic communication providers and article 41 empowers the competent authority with respect to the implementation and enforcement of these requirements.

More specifically, Article 40 requires that providers of public electronic communications networks or services manage security risks posed to the security of networks and services and take security measures including encryption where appropriate. It also requires providers to report about significant incidents to competent national authorities, who should report about these security incidents to ENISA and the European Commission (EC) annually.

This document describes the formats and procedures for cross border reporting and annual summary reporting under Article 40 of the EECC. Paragraph 2 of Article 40 describes three types of incident reporting: 1) National incident reporting from providers to CAs, 2) Ad-hoc incident reporting between CAs and ENISA, and 3) Annual summary reporting from CAs to the EC and ENISA. The focus of this guideline is on the 2nd and 3rd type of reporting: ad-hoc reporting and annual summary reporting.

Article 40 and 41 of the EECC replace Article 13a and b of the Telecoms Framework directive. This document replaces the Article 13a incident reporting guideline that was developed by the ECASEC group (formerly the Article 13a Expert Group), under the old legal framework. The ECASEC Expert Group is a group of competent authorities on telecom security, set up in 2010 to develop a common EU-wide approach to the implementation of Article 13a.

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1972&from=EN
[2] The EECC replaces four EU directives: a) The Framework Directive, which is based on the Framework Directive 2002/21/EC as amended by Directive 2009/140/EC. b)The Access Directive, which is based on the Access Directive 2002/19/EC and amended by Directive 2009/140/EC. c) The Authorisation Directive is based on the Authorisation Directive 2002/20/EC and amended by Directive 2009/140/EC. d) The Universal Service Directive is based on the Universal Service Directive 2002/22/EC and the Citizens' Rights Directive 2009/136/EC.

TABLE OF CONTENTS

1. INTRODUCTION

In this document, we provide guidance to national authorities supervising security in the electronic communications and other Competent Authorities, about implementing paragraph 2 of Article 40 of the European Electronic Communications Code (EECC). This document focuses on when and how to report security incidents to ENISA the EC and between CAs.

This document is drafted and published by ENISA and validated and adopted by the ECASEC group.

1.1 TARGET AUDIENCE

This document is addressed to national ministries, NRAs, and Competent Authorities (CAs) in the EU Member States, the authorities tasked with the implementation of Article 40.

This document may be useful also for experts working in the EU's electronic communications sector and for experts working in the information security field.

1.2 GOAL

This document is published by ENISA to provide guidance to CAs about the technical implementation of the incident reporting described in paragraph 2 of Article 40 of the EECC.

1.3 UPDATES

ENISA updates this guideline periodically, when necessary and in agreement with the CAs.

This version (V. 2.2) is an update of Version 2.1 of the Guideline on Incident Reporting. The overall structure has remained largely unchanged. The main changes are:

- Updated definitions of security and security incidents and alignment of the text and terminology used with the provisions of the EECC
- Broader scope in terms of services and incidents
- New thresholds for the annual incident reporting
- Updated incident report template
- Examples of security breaches which are in scope of the EECC

1.4 STRUCTURE OF THIS DOCUMENT

In Article 40 of the EECC we introduce Article 40. In Incident reporting flows 3 we explain the scope and definitions used in this document. In National thresholds versus annual summary reporting thresholdswe show different approaches to national incident reporting. In Crossborder criteria we describe cross border information sharing and ad-hoc reporting and in Section 6, we describe how CAs should implement annual summary reporting to ENISA and the EC. In Annex A we describe the incident report template fields, which should be used by CAs for ad-hoc reporting and annual summary reporting. In Annex B we list some examples of security breaches under the EECC.

Throughout this text we use as in IETF RFC2119 the terms 'should' (or 'recommended') for recommended items, and 'may' (or 'optional') for optional items. For the sake of explanation, we provide some (non-binding) examples using a *blue italic font*.

2. EU POLICY CONTEXT

In this section, we give an overview of the policy context, the basis for this guideline, related policy, and ENISA's role and objectives and we summarize the wider EU policy context.

2.1 ARTICLE 40 OF THE EECC

This guideline concerns Article 40 of the European Electronic Communications Code (abbreviated as EECC) which provides the obligation to incident reporting in the case of a security incident. For the sake of reference, the relevant legal text is reproduced below.

*"**Article 40 Security of networks and services***

2. Member States shall ensure that providers of public electronic communications networks or of publicly available electronic communications services notify without undue delay the competent authority of a security incident that has had a significant impact on the operation of networks or services.

In order to determine the significance of the impact of a security incident, where available the following parameters shall, in particular, be taken into account:

(a) the number of users affected by the security incident;
(b) the duration of the security incident;
(c) the geographical spread of the area affected by the security incident;
(d) the extent to which the functioning of the network or service is affected;
(e) the extent of impact on economic and societal activities.

Where appropriate, the competent authority concerned shall inform the competent authorities in other Member States and ENISA. The competent authority concerned may inform the public or require the providers to do so, where it determines that disclosure of the security incident is in the public interest.

Once a year, the competent authority concerned shall submit a summary report to the Commission and to ENISA on the notifications received and the action taken in accordance with this paragraph.."

Below we cite the definitions of the terms "security" and "security incident" in the EECC.

Article 2
….
(21)'security of networks and services' means the ability of electronic communications networks and services to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of those networks and services, of stored or transmitted or processed data, or of the related services offered by, or accessible via, those electronic communications networks or service

….
(42)'security incident' means an event having an actual adverse effect on the security of electronic communications networks or services

2.2 EU CONTEXT

Besides Article 40, there are a number of other initiatives (legal or otherwise) related to the security of public electronic communications networks and services:

- The NIS Directive (EU 2016/1148)3 is the first piece of EU-wide cybersecurity legislation aiming to enhance cybersecurity across the EU. It was adopted in 2016 and member states had to transpose it to their national legislation by May 2018. The NIS Directive has several parts:
  - National capabilities i.e. Member states must designate national authorities for supervising cybersecurity in the sectors, have a national CSIRT, perform cyber exercises, etc.
  - Cross-border collaboration between EU countries e.g. operational EU CSIRT network, the strategic NIS cooperation group and
  - National supervision of critical sectors; EU Member states have to supervise the cybersecurity of critical market operators in their country: Ex-ante supervision in critical sectors (energy, transport, water, health, digital infrastructure and finance sector), ex-post supervision for critical digital service providers (online market places, cloud and online search engines). The sector digital infrastructure covers TLD, DNS, IXP, and is closely related to the EU telecom sector. For example, DNS resolution is often a service provided by telecom providers.
- The ePrivacy Directive 2002/58/EC (as amended by Directive 2006/24/EC and Directive 2009/136/E) concerns the processing of personal data and the protection of privacy in the electronic communication. The Commission has proposed a regulation to repeal this directive and make the provisions lex-specialis under the GDPR. But the discussions about this change are still ongoing.

2.3 ENISA'S ROLE AND OBJECTIVES

We briefly describe ENISA's role and objectives in the implementation of article 40 of the EECC.

ENISA is mentioned in the preamble (98):

"*..The European Union Agency for Network and Information Security ('ENISA') should contribute to an enhanced level of security of electronic communications by, inter alia, providing expertise and advice, and promoting the exchange of best practices…*"

Article 40 par.1 of the EECC asks ENISA to **facilitate harmonization** on the security aspects.

"The European Union Agency for Network and Information Security ('ENISA') shall facilitate, in accordance with Regulation (EU) No 526/2013 of the European Parliament and of the Council (4), the coordination of Member States to avoid diverging national requirements that may create security risks and barriers to the internal market.".

Article 40 par.2 requires that CAs:

a) when appropriate, inform CAs in other Member States and ENISA about significant incidents
b) submit annual summary reports of the incidents to both the European Commission and ENISA.

[3] DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (currently under revision).
https://eur-lex.europa.eu/eli/dir/2016/1148/oj

[4] Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004 (OJ L 165, 18.6.2013, p. 41).

ENISA's primary objective is to implement the incident reporting mandated in Article 40, i.e. to agree with the Member States on an efficient implementation of ad-hoc incident reporting and annual summary reporting.

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

- To give feedback to CAs about
  - security incidents that have had significant impact,
  - 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 security incidents across the EU[5]. ENISA has been publishing such aggregated analyses (annual reports) since 2012.
- To facilitate the exchange of experiences and lessons learned among CAs, to allow them to better understand and address security incidents.
- Issue recommendations and guidance for CAs, 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 CAs with the implementation of national incident reporting schemes and in this way support efficient and harmonized incident reporting schemes across the EU. Harmonized implementation of legislation creates a level playing field and makes it easier for providers and users to operate across different EU countries.

[5]ENISA offers an online visual tool for the analysis of the incidents, detailed causes and multiannual trends. https://www.enisa.europa.eu/topics/incident-reporting/cybersecurity-incident-report-and-analysis-system-visual-analysis/visual-tool

3. INCIDENT REPORTING UNDER THE EECC

In this section we introduce the incident reporting framework in the EECC and set the scope for the rest of the guideline. We describe:

- Incident reporting flows
- Services in scope
- Security incidents in scope (what is “significant impact”)

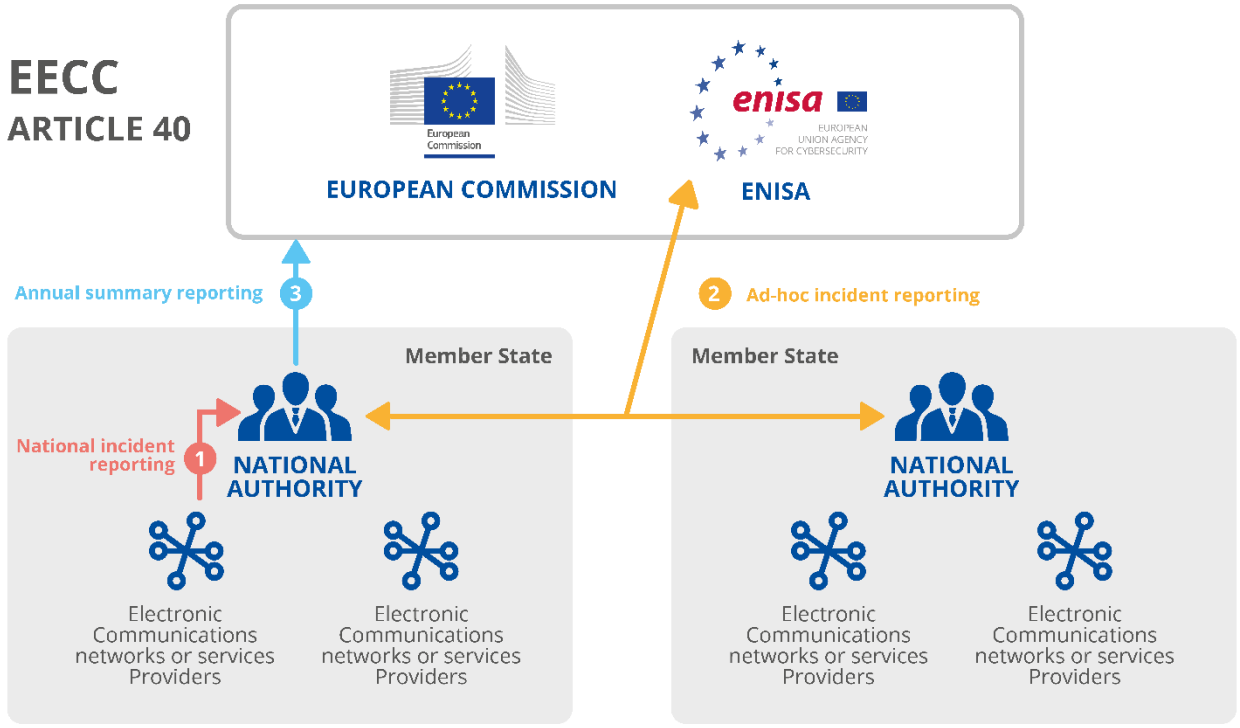
3.1 INCIDENT REPORTING FLOWS

Article 40 introduces three types of incident reporting:

1. National incident reporting from providers to CAs,
2. Ad-hoc incident reporting between CAs and ENISA, and
3. Annual summary reporting from CAs to the EC and ENISA.

The different types of reporting are shown in Figure 1: **Three types of incident reporting in Article 40**.

Figure 1: Three types of incident reporting in Article 40



The implementation of the national incident reporting (type 1 reporting as depicted in *Figure* 1) is at the discretion of EU member states and different member states are taking different approaches. We describe some national implementations in Section 4.

This guideline focusses mostly on the ad-hoc incident reporting between CAs and ENISA, and annual summary reporting from CAs to the EC and ENISA (type 2 and type 3 reporting as depicted in the above *Figure* 1).

3.2 ELECTRONIC COMMUNICATION SERVICES

The EECC (article 2) defines three categories of electronic communications services:

- internet access service,
- interpersonal communications service and
- services consisting wholly or mainly in the conveyance of signals such as transmission services used for the provision of machine-to-machine services and for broadcasting.

We quote the legal definition below for ease of reference:

Article 2 Definitions

(4) 'electronic communications service' means a service normally provided for remuneration via electronic communications networks, which encompasses, with the exception of services providing, or exercising editorial control over, content transmitted using electronic communications networks and services, the following types of services:

(a)'internet access service' as defined in point (2) of the second paragraph of Article 2 of Regulation (EU) 2015/2120;

(b) interpersonal communications service; and

(c)services consisting wholly or mainly in the conveyance of signals such as transmission services used for the provision of machine-to-machine services and for broadcasting

(5) 'interpersonal communications service' means a service normally provided for remuneration that enables direct interpersonal and interactive exchange of information via electronic communications networks between a finite number of persons, whereby the persons initiating or participating in the communication determine its recipient(s) and does not include services which enable interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service;

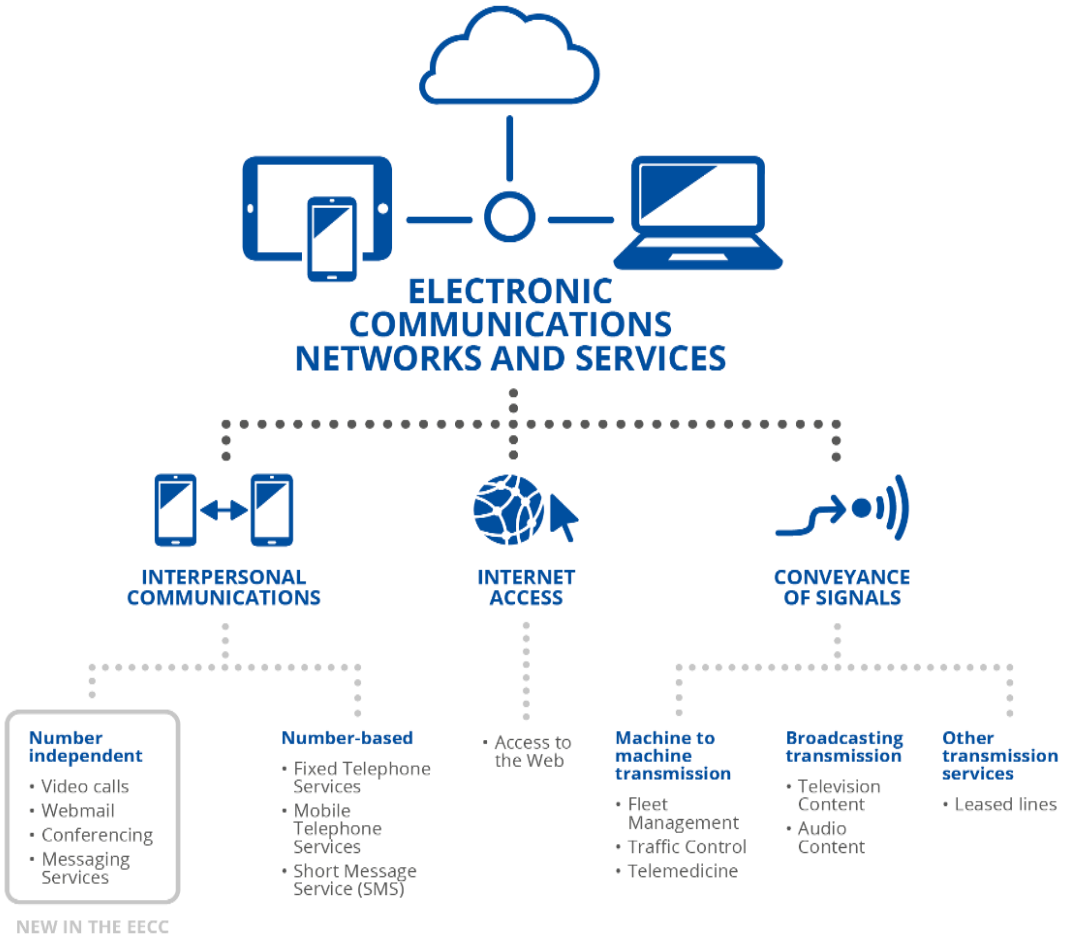
(6)'number-based interpersonal communications service' means an interpersonal communications service which connects with publicly assigned numbering resources, namely, a number or numbers in national or international numbering plans, or which enables communication with a number or numbers in national or international numbering plans;

(7)'number-independent interpersonal communications service' means an interpersonal communications service which does not connect with publicly assigned numbering resources, namely, a number or numbers in national or international numbering plans, or which does not enable communication with a number or numbers in national or international numbering plans;

(8)'public electronic communications network' means an electronic communications network used wholly or mainly for the provision of publicly available electronic communications services which support the transfer of information between network termination points

The services in scope of the EECC are depicted in the following Figure 2: **Services in scope of EECC**.

Figure 2: Services in scope of EECC



Interpersonal communications services are sub-divided into "number-based" interpersonal communication services which connect to the public switched telephone network and "number-independent" interpersonal communication services which do not connect with publicly assigned numbering resources.

- The number-based interpersonal communications services are the "traditional" fixed and mobile services, which use and connect with numbers from the national or international numbering plan.
- The number-independent interpersonal communications services are provided over internet connections, on top of more traditional networks.

The acronym 'NI ICS' is used in this document to denote 'Number-Independent Interpersonal Communications Service' and "NB ICS" to denote the "Number-Based" ones.

3.2.1 Services in scope of annual reporting

Services in scope of this reporting guideline are:

- Number-based interpersonal communication services over:
  - fixed networks (PSTN, ISDN, VoIP, ...)
  - mobile networks (SMS, 2G, 3G, 4G, 5G, ...)
- Number-independent interpersonal communications services (NI ICS) (such as messaging, chat, video calls,..)
- Internet access services over:
  - fixed networks (DSL, DOCSIS, FTTx, GPON)
  - wireless networks (GPRS, 3G, 4G, 5G, Satellite...)

- Machine to machine (transmission) (5G URLCC, MTC)
- Broadcasting (transmission) (television, radio)
- Emergency services

These services can be provided free or paid, for consumers or business.

We stress that this is *neither* an exhaustive list of electronic communication services defined in the EECC nor an exhaustive list of services that are being regulated by CAs.

Other services are not discussed explicitly in this guideline, but many of the concepts in this guideline should apply to other types of electronic communication services as well.

3.3 SECURITY INCIDENTS

EECC includes definition of the security and security incident. For ease of reference, we reproduce these definitions below:

Article 2 Definitions

(21) 'security of networks and services' means the ability of electronic communications networks and services to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of those networks and services, of stored or transmitted or processed data, or of the related services offered by, or accessible via, those electronic communications networks or services;

(42) 'security incident' means an event having an actual adverse effect on the security of electronic communications networks or services.

Moreover, article 40, par. 1 requires:

"In particular, measures, including encryption where appropriate, shall be taken to prevent and minimise the impact of security incidents on users and on other networks and services"

In the scope of the reporting are any incidents, which ***affect*** *the* **confidentiality, authenticity, integrity and availability** of the following ***assets***:

- the networks
- services
- the stored or transmitted or processed data
- other services offered or accessed via those e-communications networks or services

So, in the scope are incidents which have

a) impact on the availability[6]; when the incident affects the continuity of supply of services, degrades the performance of the service, the network or service is "completely" or "partially" down. This is often called 'outage' or 'disruption'. e.g. *50% of phone calls dropped in the last 15 minutes' or 50% of internet bandwidth lost, customers experiencing service degradation to the point where the customer feels the service is not fit for purpose*

b) impact on the confidentiality[7]; when the confidentiality of communications, communications data or metadata has been compromised. *e.g. encryption does not work and content of communication is hacked, private messages and exchanged*

[6] Availability is typically defined as a property of *being accessible and usable on demand by an authorized entity* (ISO/IEC 27000:2018)
[7] Confidentiality is typically defined as a *property that information is not made available or disclosed to unauthorized individuals, entities, or processes* (ISO/IEC 27000:2018)

content have been accessible by attackers, IMSI catchers, provider's database with communications logs has been compromised, emails are forwarded to unknown recipients, configuration files or routing files have been accessible by attackers and have been disclosed;.

c) Impact on the integrity[8]; when there is a compromise of the integrity of the communications data or metadata. *e.g. IP address and caller id spoof, log files have been tampered; configuration files or routing files have been found altered (integrity of files); malware or unauthorised software has been found installed into a server capable to identify and alter data from various files (violation of integrity of the systems software that then causes violation of the integrity of retained information)*

d) Impact on the authenticity[9]; when there is a compromise of user's identity (identity fraud). e.g. *man-in-the-middle attacks or eavesdropping on applications lead to theft and misuse of authentication credentials, user accounts become accessible and taken over by attackers*.

It should be noted that these examples are indicative. In practice, when an incident happens multiple security properties may be affected. For example, in the case of the Mirai botnet attack, the integrity of 1M home routers was compromised by an attacker using the default password. The result of this attack was also an outage, and it could have resulted in a breach of confidentiality (like in a pharming attack).

Events, which reduce the redundancy of a network or service, such as for instance when one of two redundant submarine cables breaks, could fall under the definition of an incident because they reduce the ability of the system to protect itself.

Newly discovered security vulnerabilities may become security incidents, if there is an actual effect on the security of the networks and services. It does not mean that all such vulnerabilities fall under mandatory breach reporting, which requires to be a significant impact on the networks or services.

Several examples of security incidents covered by this definition in the EECC are provided in Annex B.

3.4 SIGNIFICANT IMPACT

Article 40 requires that providers notify CAs, of any security incidents, which have had a *significant impact* on the operation of networks or services. Annually, CAs should send summary reports about these security incidents to ENISA and the EC.

The EECC specifies parameters that, where available, should be taken into account when determining the significance of a security incident:

(a) the number of users affected by the security incident;
(b) the duration of the security incident;
(c) the geographical spread of the area affected by the security incident;
(d) the extent to which the functioning of the network or service is affected;
(e) the extent of impact on economic and societal activities.

Note that it is at the discretion of the CAs to determine what is *significant*. This ultimately depends on national circumstances.

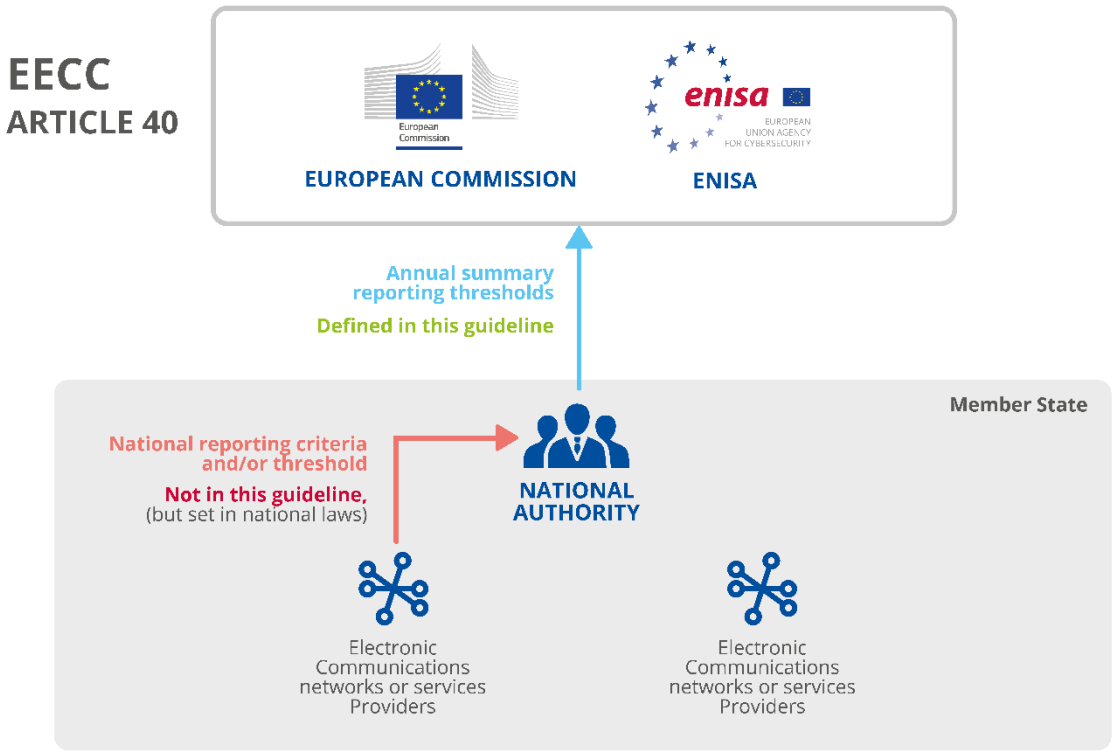
[8] Integrity is typically defined as a *property of accuracy and completeness* (ISO/IEC 27000:2018)
[9] Authenticity is typically defined as a *property that an entity is what it claims to be* (ISO/IEC 27000:2018)

There are different approaches in the different EU countries when it comes to defining what are the significant incidents to be notified to the national authority. In some countries the national regulation defines specific quantitative thresholds based on technical parameters, while other countries set qualitative criteria. See for examples Section 4 about national incident reporting.

3.5 NATIONAL THRESHOLDS VERSUS ANNUAL SUMMARY REPORTING THRESHOLDS

This guideline does not define thresholds for incident reporting at national level. The thresholds and criteria are define by each MS at national level, and apply to the reporting by the providers to the CAs, while the EU level only apply to the annual summary reporting process that takes place at the start of each calendar year, between EU Member States, ENISA and the Commission. See the diagram below.

Figure 3: National Thresholds Vs European Thresholds



This means that while a country may receive many incident notifications from providers, the annual summary report contains summary information about a subset of these notified incidents.

4. NATIONAL APPROACHES TO INCIDENT REPORTING

Article 40 requires providers to report significant security incidents to the CA. We call this step "national incident reporting" and it is the type 1) reporting depicted in Figure 1. It is important to distinguish the national reporting from the reporting to ENISA. The implementation of national incident reporting is at the discretion of EU member states and different member states are taking different approaches. In this section, we briefly describe three approaches, based on input from the CAs implementing Article 40.

We would like to stress that this section is not intended as guidance, but rather as an illustration of the range of different national reporting schemes across the EU and to underline the difference between national reporting and the annual summary reporting at an EU level (between CAs, ENISA and the EC).

Example: Country A

In country A the CA focuses on the larger outages, and less on smaller outages. The CA sets thresholds for national reporting relatively high.

The CA receives incident reports days after the incident has been resolved. The reporting is independent from crisis management and other national incident response teams.

The CA allows providers to report incidents using email (unformatted), fax, phone or paper mail. The CA provides guidance on the data that should be reported, but no specific template. Incident reports, once collected, are archived manually. The CA keeps an eye on the number of incidents per provider, but does not feed data into a database for improved search or statistical analysis.

The CA mostly works ex-post and intervenes following large incidents, or when there is a repetition of serious incidents involving a particular provider, service or network. The CA works based on the assumption that providers will pro-actively improve the security of the networks and services without support or incentives from the CA.

Example: Country B

In country B the CA keeps track of major security incidents and intervenes whenever network and service providers fail to improve on security issues. National incident reporting includes large security incidents but also smaller security incidents.

The CA receives reports in two steps:

A brief report is sent within hours, describing only basic information about the incident and impact. If needed, the brief report is updated whenever there are significant developments.

A full report is sent within weeks after the incident is resolved, describing full impact, root causes, actions taken, lessons learnt, et cetera.

The reporting is independent from crisis management and other incident response teams, but the CA receives notifications from crisis management and, vice versa, notifies crisis management, in case of large incidents. The CA requires the brief report not for crisis management purposes, but to be able to brief other government authorities (ministries, or parliament, e.g.).

The CA requires the provider to inform customers, emergency services, whenever relevant and plays no role in this.

The CA requires incident reporting via email or an electronic (online e.g.) form. Emailed reports must be structured according to a specific template to allow for automated collection and structured storage of incident reports. The CA performs subsequent analysis on the reports, not only to understand which providers are underperforming, but also, for example, to understand common root causes, vulnerable networks, et cetera.

The CA supervises the security of networks and services. The CA only intervenes when network and service providers fail to improve on security issues– for example, because there are few economic incentives or because these issues require national agreements.

Example: Country C

In country C the CA is required to monitor the security of networks and services, and to work with network and service providers to improve security. The CA is expected to intervene when smaller providers are underperforming and putting their customers at risk. National incident reporting includes relatively small security incidents and incidents affecting critical infrastructure even if there was no actual outage.

Technically incident reporting is implemented similar to country B (in two steps, structured, electronic). The CA performs statistical analysis on the received incidents, analysing common root causes, frequency and impact. Anonimised statistical data about incident reports is shared with providers in industry working groups.

The CA implements fine-grained incident reporting, to be able to supervise providers, but also to be able to help providers in improving security of services and networks. For instance the CA sets up specific working groups to address the frequent and high-impact incidents. In other words, the CA not only intervenes when needed, but also works pro-actively with the providers to improve where possible security of networks and services. Fine-grained incident reporting is used to provide feedback on the effectiveness of security measures and to get feedback about improvements, in the market as a whole or at single providers.

Examples of thresholds

At national level there are many different approaches to define criteria and thresholds for notification of incidents to the CA. Below we give some examples:

- *Over the year country A has received 211 incident notifications. A subset of these incidents are above the threshold for annual summary reporting to ENISA and the Commission. The summary information about the subset of incidents is entered in the annual report using the annual reporting template. In the annual summary report the CA also give general information about the overall year, trends, and observations.*

- *In country B the legislation does not contain detailed quantitative thresholds, but only high-level criteria for incident reporting. These high-level criteria were mapped to the internal incident classification levels used already by the telecom providers. In the annual summary report, the CA provides a summary of the notified incidents which*

pass the quantitative and qualitative annual summary thresholds in Section 6 of this Guideline.

- *Country C has set the national threshold for confidentiality incidents at 0,1% of the service userbase. The national userbase of mobile telephony in the country is 5.000.000 users and therefore providers need to report such incidents if they affect more than 5000 users. The annual summary reporting thresholds (see Section 6 of this guideline) is set at 1% of the national userbase.). This means that some of these incidents do not have to be included in the annual summary report to ENISA and the Commission.*

5. CROSSBORDER INFORMATION SHARING

In this section, we describe step 2 in the incident framework (see *Figure 1*), the procedure for cross border information sharing between CAs.

5.1 CROSSBORDER CRITERIA

The goal of crossborder reporting is to inform CAs abroad (and ENISA) about recent or on-going incidents, which may be relevant for CAs abroad. This is mentioned in Article 40 of the EECC . Note that this reporting flow is for CAs supervision purposes, not crisis management.

The CA should assess whether or not an incident is relevant for CAs in other countries and in this case make a crossborder report. It is at the discretion of a CA to determine if an incident is relevant for other CAs and ENISA[10] .

For example, relevant incidents might be:

- *Incidents affecting networks and services in other countries*
- *Incidents affecting equipment in use in other countries as well*
- *Incidents involving infrastructure in other countries, such as international interconnections.*
- *Natural phenomena, such as storms or earthquakes which span across borders*
- *Large-scale power cuts spanning across borders*
- *Incidents requiring actions which extend across the border, such as international agreements*
- *Incidents affecting large number of users in roaming*
- *Incidents involving compromise of databases mirrored in other country*

5.2 INCIDENT REPORT DATA

Crossborder reporting is at the discretion of CAs and CAs should determine which information about the incident is relevant for sharing in this case.

CAs may follow the incident report template fields for annual summary reporting (see Annex A). ENISA provides an online tool (CIRAS) to support crossborder incident reporting; access to the tool is provided to CAs upon request (resilience@enisa.europa.eu).

5.3 PROCEDURES AND TOOLS

ENISA offers a number of tools to allow CAs to exchange information

- CIRAS[11] (for incidents with a cross border impact)
- Mailing list (for non-sensitive but interesting information)
- Issue tracker (for jointly working on common issues or cases that are not incidents)

[10] Whether or not these incidents should be included in annual reporting depends on the impact of the incident.
[11] CIRAS is also used for the annual reporting to ENISA and EC.

ENISA also maintains and distributes contact a list of email addresses and telephone numbers of contact points at CAs to enable ad-hoc contact between authorities across borders. This contact list is also accessible via the CIRAS tool[12] . The contact list is kept updated by the individual CAs.

[12] See: https://resilience.enisa.europa.eu/ciras/contact-details?article=article13a

6. ANNUAL SUMMARY REPORTING

In this section, we define scope and thresholds for annual summary reporting by CAs to ENISA and the EC. This is the step 3 in the diagram in Figure 1.

We stress that this section should not be understood as a recommendation about which incidents are (nationally) significant nor about which incidents should be reported nationally. In practice CAs may use a wider scope and less or more stricter thresholds, where relevant, taking into account national circumstances and requirements.

6.1 GOAL OF ANNUAL SUMMARY REPORTING

The goal of annual summary reporting to ENISA and the EC is:

- to get feedback from CAs about security incidents that have had significant impact, incident trends, root causes of security incidents
- to provide policy makers, the public and the industry with aggregate (statistical) analysis of incidents which explain the overall frequency and impact of security incidents across the EU.
- to facilitate the exchange of experiences and lessons learned among CAs, to allow them to better understand and address specific types of security incidents or vulnerabilities.
- to evaluate the effectiveness of security measures in place, and to issue recommendations and guidance for CAs, the private sector and policy makers, about security measures.

6.2 THRESHOLDS FOR ANNUAL SUMMARY REPORTING

In this section, we define the thresholds for annual summary reporting by CAs to ENISA and the EC. We define two types of thresholds.

(a) **Quantitative thresholds**[13]**:** Assessing the impact according to quantitative parameters: the number of the users affected and the duration of the incident (see below).

(b) **Qualitative thresholds**: Assessing the impact according to qualitative parameters: Geographical spread, impact on economy and society, extent to which the functioning of the network or service is affected;

Quantitative thresholds are clear and easy to understand, but they do not always apply to all situations. The total size of the incident, the number of users, or hours, is not always the main significance factor. Sometimes a small incident, in terms of users, or hours, can be very significant. Therefore, qualitative thresholds are needed in addition to the quantitative thresholds. Overall, all thresholds should be applied.

[13] Geographical spread may be measured by the size of the area affected by the incident. However, there are also qualitative aspects of the geographical spread and therefore we categorise this parameter under the qualitative ones.

In practice, CAs should apply the thresholds for annual summary reporting as follows:

Step 1: Does the impact exceed the quantitative thresholds?
- Yes: The incident should be included in the annual report
- No: Go to step 2

Step 2: Does the impact exceed the qualitative thresholds?
- Yes: The incident should be included in the annual report
- No: The incident may be included in the annual report

6.2.1 National user base

The thresholds defined below are based on national user base. CAs should estimate the total number of users of each service in their country. CAs may (optionally) use the following metrics as estimates:

- For fixed voice communications service and fixed internet access, CAs should use the number of subscriber or access lines in their country.
- For mobile communications service, CAs should use the number of active telephony SIM cards.
- For mobile internet access, CAs should sum up14:
  1. The number of standard mobile subscriptions, which offer both voice service and internet access, and which have been used for internet access recently (e.g. in the past 3 months).
  2. The number of subscriptions dedicated for mobile internet access, which are purchased separately, either standalone or on top of an existing voice subscription.
- For NI ICS CAs may sum up the number of active users of the services in the end of a period. These could be measured as the active users (MAU), where an 'active user' can, for example, be defined as the user who has used the service at least once in the respective time period.

6.2.2 Quantitative thresholds: Relative plus absolute

The quantitative thresholds consist of two parts; a relative threshold based on the userbase and an absolute threshold.

6.2.2.1 Relative threshold

The relative threshold for annual summary reporting is based on the **percentage of the national user base**. Number of users affected are expressed as a percentage (%) of the national user base of that service (see **Error! Reference source not found.**).

(a) Relative threshold for security incident which have an **impact on the availability**[15].

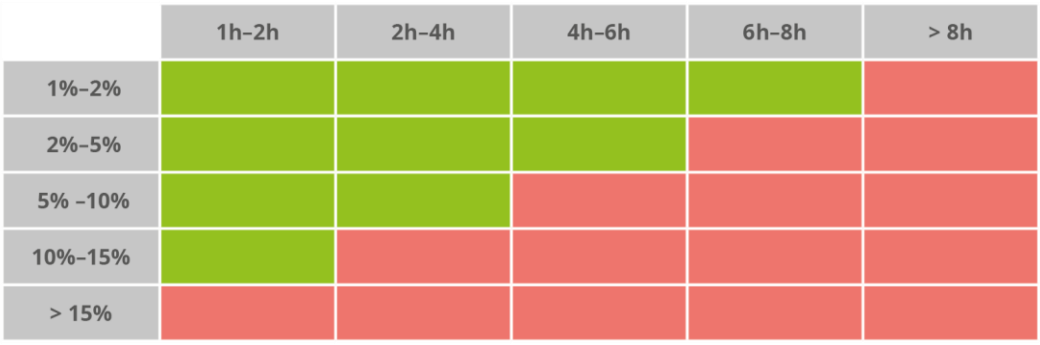
In this case the impact is assessed based on the users affected expressed as % of the national user base and the duration of the incident.

CAs should report incidents, as part of the annual summary reporting, if the incident

- lasts more than an hour, and the percentage of users affected is more than 15%,
- lasts more than 2 hours, and the percentage of users affected is more than 10%,
- lasts more than 4 hours, and the percentage of users affected is more than 5%,
- lasts more than 6 hours, and the percentage of users affected is more than 2%, or if it
- lasts more than 8 hours, and the percentage of users affected is more than 1%.

[14] Here we follow the definition agreed in the COCOM meetings. In some countries other metrics are used.
[15] Impact on the availability i.e. impact on the availability of networks, services, the stored or transmitted or processed data and other services offered or accessed via those e-communications networks or services

Figure 4: Relative threshold based on the duration and the percentage of the national user base



(b) Relative threshold for security incident which have an **impact on the confidentiality, authenticity and integrity**[16].

CAs should report incidents, as part of the annual summary reporting, if the **number of users affected is more than 1% of the national user base of that service.**

6.2.2.2 Quantitative parameters - Absolute threshold

The absolute threshold for annual summary reporting is applied on the product of the duration and the number of users affected – for a particular service, inside the country[17] (see Annex A)

This threshold is applied for security incident which have an impact **on the availability**.

CAs should include incidents in the annual summary reporting if the product of the duration of the incident and the number of users affected is equal or exceeds: **60 Million user minutes, or 1 Million user hours**. This threshold is applied for assessing the impact on the availability.

Excluded are very small incidents, which affect less than 25.000 user connections, as well as very short incidents, which last less than 1 hour.

For example, when half a million users are affected for 2 hours, then the incident should be included in annual summary reporting.

6.2.3 Qualitative thresholds

The following qualitative thresholds should be considered to assess the impact for the security incidents:

a) Geographical spread: This applies to incidents affecting the availability of the services provided in specific regions/areas as defined in national legislation, such as:
- when there is a cross-border impact
- large (areas larger than xx km2), remote or rural areas, islands, affected
- capital or critical region affected
  interconnections are affected (or number of international interconnections affected)

b) Impact on economy and society, or on users: it refers to security incidents which
- affect the access to 112 or national emergency numbers
- have impact on public warning systems
- create high risk to public safety, public security or of loss of life create high costs and high material damage (reputational damage, impact on morale, data loss for consumers, productivity impact)
- have media coverage (evening news)

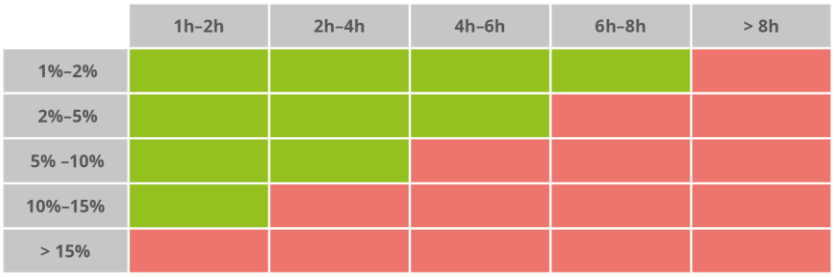
[16] Impact on the confidentiality, authenticity, integrity of networks, services, the stored or transmitted or processed data and other services offered or accessed via those e-communications networks or services
[17] This means that cross-border providers of NI ICS should assess the impact of incidents within the national borders.

- have impact on the continuity of essential services or critical sectors/operator
- have impact on especially critical days, such as election or referendum days.
- have impact on critical functions to the society (e.g. ministry, gov. bodies, etc.)
- “high profile” users have been affected (e.g. prime minister, political person)

6.2.4 Annual summary reporting threshold overview

We give an overview of the qualitative and quantitative annual summary reporting thresholds in the table below.

Figure 5: Annual summary reporting threshold overview

<table>
<tr><th colspan="3">Annual incident reporting thresholds</th></tr>
<tr><td rowspan="2">Quantitative Parameters</td><td>Availability</td><td>1: Relative threshold based on the percentage of the user base (nationally) and the duration (nationally)
 

2: Absolute threshold of > 1M user hours (nationally)</td></tr>
<tr><td>Confidentiality, Integrity, Authenticity</td><td>3: Relative threshold based on the percentage of the user base of the service (nationally)

Number of users affected > 1% of the user base of the service (nationally)</td></tr>
<tr><td rowspan="2">Qualitative Parameters</td><td>Availability</td><td rowspan="2">4: Significant due to the geographical spread of the incident. i.e. cross-border, or if large remote/rural areas, or a capital/critical region affected etc.

5: Significant due to the impact on economy and society, or on users i.e. lack of access to 112, national emergency numbers, impact on public warning systems, high costs, high material damage, high risks to public safety, public security or of loss of life , media coverage (evening news), impact on the continuity of essential services or critical sectors/operators, impact on especially critical days, such as election or referendum days.</td></tr>
<tr><td>Confidentiality, Integrity, Authenticity</td></tr>
</table>

A ANNEX: INCIDENT REPORT TEMPLATE

In this section, we describe the incident report template to be used in annual summary reporting.

The template starts with an incident type selector and contains 3 parts:

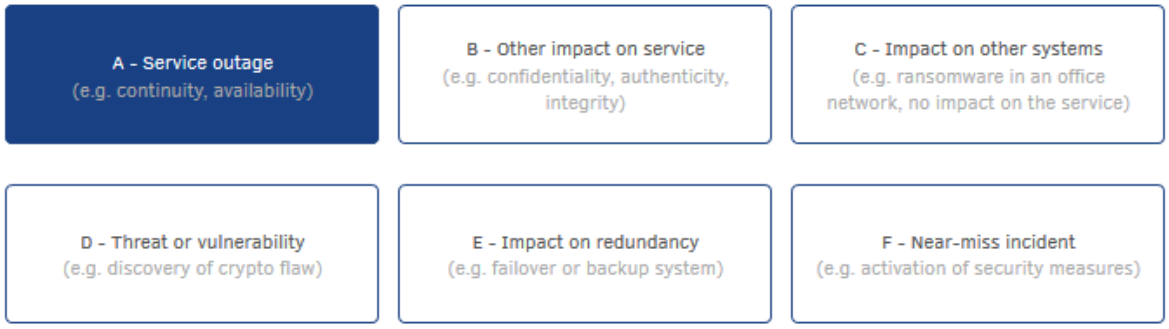
1. **Impact of the incident** - which communication services are impacted and how much)
2. **Nature of the incident** - what caused the incident
3. **Details about the incident** – detailed information about the incident, a short description, the types of network, the types of assets, the severity level etc.

We go over the template fields one by one.

Type of incident

The incident type selector is used to adapt the template to the type of incident. The selector has 6 types, but most of the notified incidents are typically of type A or B.

Figure 6: Type of incident overview



- Type A: Service outage (e.g. continuity, availability)

  *For example, an outage caused by a cable cut caused by a mistake by the operator of an excavation machine used for building a new road would be categorised as a **type A** incident.*

- Type B: Other impact on service (e.g. confidentiality, authenticity, integrity)

  *For example, a popular collaboration tool has not encrypted the content of the media channels which are being established when a session is started, between the endpoints participating in the shared session. This leads to the interception of the media (voice, pictures, video, files, etc.) through a man-in-the-middle attack. This incident would be categorised as a **type B** incident.*

- Type C: Impact on other systems (e.g. ransomware in an office network, no impact on the service)

  *For example, a malware has been detected on several workstations and servers of the office network of a telecom provider. This incident would be categorised as a **type C** incident.*

- Type D: Threat or vulnerability (e.g. discovery of crypto flaw)

  *For instance, the discovery of a cryptographic weakness would be categorised as a **type D** incident.*

- Type E: Impact on redundancy (e.g. failover or backup system)

  *For example, when one of two redundant submarine cables breaks would be categorised as a **type E** incident.*

- Type F: Near-miss incident (e.g. activation of security measures)

  *For instance, a malicious attempt that ends up to the honeypot network of a telecom provider would be categorised as a **type F** incident.*

Depending on the type selected, some fields in the template are deactivated. For example, in the case of a Type A incident the fields "threat severity factors" and "severity of threat" are not active.

PART 1: IMPACT OF THE INCIDENT

Service impacted

In the field "services impacted" CAs should provide information about the affected electronic communication services by indicating one or more from the following

- fixed telephony (i.e. fixed voice communications service),
- mobile telephony (i.e. mobile voice communications service),
- fixed internet access,
- mobile internet access,
- OTT (i.e. NI ICSs),
- machine to machine (transmission),
- broadcasting (transmission)

Alternatively, CAs may specify "other" type of service (such as emergency service).

Number of users

In the field "number of users" CAs should indicate the total number of users affected.

- For fixed voice communications service and fixed internet access, CAs should report the number of subscriber or access lines impacted.
- For mobile voice communications service and mobile internet access, CAs should report an estimate, taking into account the normal usage of the affected facilities
- For NI IC services, CAs should report an estimate, taking into account the active users under normal operating conditions at the time of the incident in a jurisdiction

For example, if a base station, which serves 1000 users per hour on average, is offline for an hour, then the impact of such an incident should be estimated to 1000 users.

For example, by collecting data on the number of active users under normal operating conditions, at different periods of the day and different days of the week, it will be possible to define the statistical baseline in a jurisdiction. This could be used to estimate the number of users affected in case there is a degradation or loss of an NI IC service.

Note that in many incidents multiple services are affected at the same time, and that the number of users affected could be different per service. In these cases, CAs should provide separate numbers per service.

Note also that providers do not always have an exact notion of the number of users affected, because they deliver services to other providers (often called resellers, or intermediate users). The provider, in that case, does not always know the exact number of users (or 'clients' as referred to in the Directive) of the latter and consequently may not know the exact number of users affected by an incident. In these cases, CAs should report estimates.

Duration

In the field "duration" CAs should indicate the length of time (in hours) there was significant impact on the operation of the services.

For example, suppose that a storm causes a power outage from midnight to 6 o clock in the morning, and suppose that the mobile communications service is affected from 4 o'clock at night (when backup power runs out) until 7 o'clock in the morning. In this case the duration of the incident is 3 hours.

PART 2: NATURE OF THE INCIDENT

Root cause category

The root cause of an incident is the initial cause of an incident, in other words, the event or factor that *triggered* the incident. In the field "root cause category", CAs should indicate the category of the root cause of the incident. There are 5 root cause categories[18]:

Human errors

The category "human errors" should be used for incidents caused by human errors during the operation of equipment or facilities, the use of tools, the execution of procedures, et cetera.

For example, suppose an employee of a provider made an error in following prescribed equipment maintenance procedures, which causes an outage. In this case the incident would be in the root cause category 'Human errors'.

System failures

The category "system failures" should be used for incidents caused by failures of a system, for example hardware failures, software failures or flaws in manuals, procedures or policies.

For example, suppose the provider operates a full maintenance program for its equipment, that diesel generators are not included on this program, and that a generator fails because of lack of maintenance. In this case the root cause of the incident would be in the root cause category 'System failures'.

Natural phenomena

The category "natural phenomena" should be used for incidents caused by severe weather, earthquakes, floods, pandemic diseases, wildfires, wildlife, and so on.

For example, suppose squirrels caused a cable cut, causing an outage, then the incident would be in the root cause category 'natural phenomena'.

Malicious actions

The category "malicious actions" should be used for incidents caused by a deliberate act by someone or some organisation.

For example, incidents which have a root cause like a fire started by employees as an act of sabotage, the poisoning of the provider's DNS systems by criminals, the hacking of the provider's computer systems, vandalism directed at street cabinets, and so on.

Third party failures

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.

This category should be used in conjunction with one of the other root cause categories.

For example, an outage caused by a cable cut caused by a mistake by the operator of an excavation machine used for a building a new road, would be categorized in the root cause category 'human error' and *'third-party failure'.*

PART 3: DETAILS ABOUT THIS INCIDENT

Summary

[18] The root cause categories were derived from secondary legislation issued by FICORA and CESG, the UK National Technical Authority for Information Assurance.

In this field, CAs should provide a description of the incident. CAs may also describe incident response actions, i.e. actions taken by the provider to mitigate the impact of the incident, and lessons learned from the incidents or measures, which will be implemented on the long-term, by the CA or providers.

Service technology

In this field, CAs should provide further information about the 'technology' that was affected.

> *For instance, if a storm takes down a set of mobile base stations, causing network outage, the service affected in this incident would be mobile telephony and mobile internet, and specifically GSM, GPRS/EDGE, UMTS, to explain the type of technology or platform affected.*

Technical causes

In the field "Technical causes" CAs should provide information about the initial cause of the incident, i.e. the event or factor that triggered the incident in combination with any other detailed causes that subsequently played a role in the incident.

> *For example, if a storm causes a powercut, which causes an outage, then in this case the initial cause would be 'storm' and the subsequent cause would be 'powercut'.*

Technical assets affected

CAs should indicate the assets which were first affected in the incident.

> *For example, assets affected could be mobile base stations, street cabinets, location register, switches, international backbone, area network, and so on.*

Significance factors

This field contains factors that CAs may want to take into consideration when assessing the scale of impact:

- Number of users affected
- Duration of the incident
- Geographical spread (cross-border, interconnections, large remote area, islands/critical region, ...)
    - *For these incidents what it counts is the specific area which has been impacted regardless the number of the affected users. CAs may have set national thersholds such as a list of islands or rural areas or set a thresholds of xx km2. When an incident has affected these areas for more than, XX mins, it has to be reported.*
    - *For example, an optical cable was cut affecting all services offered by a company throughout the territory of an island for a duration of more than 20 minutes. This incident has an impact on the whole island and therefore is categorised as an **incident with geographical spread.***
    - *For example, suppose a large internet exchange point is affected by a power cut, causing large-scale internet connection issues. In this case the incident has an impact on interconnections and it is categorised as **an incident with geographical spread**.*
- Extent of impact on functioning (severe degradation, important functions failing, ...)
- Impact on economy and society (112, costs, damage, high safety risks, media coverage, ...)
    - *For example, suppose that the datacentre of a telecom operator has a blackout, which prevents large areas of the country to connect to 112. In this case, the incident has an impact on emergency calls and it is categorised as an incident with **impact on economy and society.***
    - *For example, Illegal tapping of more than 100 mobile phones on the XX network belonging mostly to members the government and top-ranking civil servants it is categorised as an incident with **impact on economy and society.***

Scale of impact

The scale of impact can be “no”, “minor”, “large”, “very large” [19] impact. Based on the input provided in the other fields (duration, number of users, significance factors) the system suggests the scale of impact of the incident[20]. CAs may indicate a different value than the suggested one.

Threat severity factors

This field contains factors that CAs may want to take in consideration when assessing the severity of the threat[21]:

- Mitigation costs
- Potential damage (criticality)
- Rate of spreading of the threat (aggressiveness)
- Likelihood of exposure (attacks-in-the-wild)
- Criticality of systems potentially affected (e.g. SCADA systems)
- Lack of good solutions to mitigate the threat

Severity of threat

The severity of the threat is used to indicate, from a technical perspective, the potential impact, the risk associated with the threat.

- High – High severity, potential impact is high.
- Medium – Medium severity, potential impact is medium.
- Low – Low severity, potential impact is low.

For instance, the severity is high if a software vulnerability is easily exploited and present in many different systems.

[19] The system suggests the scale of impact of the incident according to the following algorithm:

For type A incidents:

- If (users*duration) <= 100.000 then the algorithm checks
  - If none of the significance factors have been selected then the impact is **Minor**
  - If at least one of the significance factors have been selected then the impact is **Large**
- If users*duration are between 100.000 and 1.000.000 then the impact is **Large**
- If (users*duration) >= 1.000.000 then the impact is **Very large**.

For type B incidents:

- If users <= 100.000 then the algorithm checks
  - If none of the significance factors have been selected then the impact is **Minor**
  - If at least one of the significance factors have been selected then the impact is **Large**
- If users are between 100.000 and 1.000.000 then the impact is **Large**
- If users >= 1.000.000 then the impact is **Very large**.

[20] The system suggestion applies only to type A and type B incidents.
[21] Threat severity factors and Severity of threat are according to the EU Cybersecurity Incident taxonomy CG Publication 04/2018

B ANNEX: EXAMPLES OF INCIDENTS

In this annex we give examples of incidents which would be in scope of the EECC reporting provisions. For each incident we indicate which of the security properties mentioned in the EECC (C confidentiality, I integrity, A availability, Au Authenticity) would be affected.

ID	Security property	Description
1	C	Cyber-attack on core routers of a provider, metadata (call logs) about thousands of customer communications were exfiltrated. No outage occurred.
2	C	Cyber-attack on a database containing records of hundreds of thousands of customers. The database contains phone numbers and IMSI numbers and call logs which are leaked.
3	C I	Hundreds of base stations are found to be vulnerable to exploit, some base stations have been hacked, exposing communications of using these base stations.
4	C I	Vulnerabilities are found in the 3G network protocol, which allows intercepting mobile phones. Evidence that the vulnerabilities are being exploited already.
5	C	Thousands of voice mailboxes have standard passwords. Journalists accessed voice mails of politicians.
6	A	Employee makes an operational error configuring BGP routes, leading to traffic diversion. Thousands of users have experienced availability issues.
7	A	A wrong/ buggy update pushed by the ISP to customer-premise equipment results in loss of service for thousands of customers.
8	C I A Au	Provider discovers thousands of VOIP gateways sold to customers, are hacked exposing customers to eavesdropping, dialer fraud, et cetera.
9	C	Wi-Fi hotspots were found to allow attackers to eavesdrop on traffic.
10	C	Messaging application vulnerability has been exploited and information stored in users mobile devices was compromised
11	CI	Attackers exploited a feature in a chat application code to gain access to user accounts and potentially take control of them.
12	C I A Au	Cybersecurity attacks on any part of the network over which the OTT service provider has direct control, such as • breach in the server farm that exposes personal identifiable information of users or other data such as password files. • packet sniffing of unencrypted data. • man-in-the-middle attacks causing communication exchange between OTT users to be manipulated or altered.

13	A	An issue in the NI ICS providers' supporting infrastructure which impacts a number of customers in a given region such as: • failure to authenticate due to RADIUS failure • or denial of service due to issues with billing systems or • failure of portal access to payments methods such as direct debits from a particular bank or payments from PayPal. This caused outages for a significant group of customers.
14	C I	Attackers corrupted the user device app to gain access to user's devices and data. Devices and data were compromised.
15	C I	Application tampering – An attacker exploits code modification via malicious versions of the application in third-party or unauthorized app stores. The attacker may also trick the user into installing a rogue application version through phishing attacks.
16	A	Due to denial of service attacks on the authentication server people are unable to authenticate and use the OTT platform.
17	C	Due to successful attack on the authentication server, credentials were misused
18	C I	An attack where the application fails to protect the media streams – either by not providing encryption or by leaking information from the application prior to encryption. The attacker gains access to information, voice/video sessions, or other sensitive information by exploiting a problem with the application.
19	Au	The application failure to ensure that the process of authentication is protected from outside, unauthorized access. Man-in-the-middle attacks or eavesdropping on the NB ICS application lead to the theft and misuse of authentication credentials.
20	C I Au	Identity fraud – The application fails to protect against the use of identity and security credentials stolen from exploits outside the application itself. For example, the application fails to protect against password changes being made by individuals who are not authorized to make the changes.
21	A	Configuration –cloud and virtualized services are not properly configured for traffic management. High volumes of traffic to the cloud (or, from the cloud) render the OTT platform unavailable.
22	CI	Data theft – An attacker uses an unprotected network (for instance, an Wi-Fi connection unprotected by encryption) to intercept, store and analyse traffic without the knowledge of the victim. The result of the data theft are stolen credentials, stolen data, inappropriate access to voice and video media streams and other sensitive data.
23	A	Congestion – At attacker makes the OTT platform unavailable by overwhelming the client side device with malicious traffic. In this case the congestion at the client or the Internet access point makes connection to the Internet (and, thus, the OTT platform) impossible.
24	C	The pin for gaining access a shared session of a collaboration tool was configured to be a six-digit number. Attackers gained unauthorized access to a video conference protected by that PIN
25	C I	Data stored on servers in the OTT platform was not encrypted and were exploited
26	C I	Due to an app vulnerability, the application was found to be taking advantage of an iOS feature that allowed any application installed on the phone to have read and write access to the phone's clipboard. App was discovered to be constantly reading users' clipboards. The exploit by this app affected the confidentiality and integrity of other services.
27	C I	Provider, during an inspection of its systems, detected unauthorized export of file from the company's system with call details, without name, The file export was the result of a cyber-attack. This file contained data, without name, of the calls made or received by mobile subscribers on five days and specifically: telephone number, day and time of the call and its duration, device type, IMSI 1, age, gender, base station coordinates.

TP-02-21-228-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN: 978-92-9204-471-8
DOI: 10.2824/633879