Technical Guideline on Incident Reporting

Technical guidance on the incident reporting in Article 13a

Version 2.0, January 2013

About ENISA

The European Network and Information Security Agency (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. Marnix Dekker, Christoffer Karsberg

Contact

For contacting the authors, please use resilience@enisa.europa.eu.

For media enquires about this paper, please use press@enisa.europa.eu.

Acknowledgements

For the completion of this report ENISA has worked closely with a working group of experts from national regulatory authorities and ministries from across Europe:

PTS (SE), Agentschap Telecom (NL), FICORA (FI), Ofcom (UK), ANACOM (PT), ComReg (IE), EETT (GR), Ministry of Defence (DK), RTR (AT), ANCOM (RO), EA "ECNIS" (BG), CCED (FR), Bundesnetzagentur (DE), BIPT (BE), MITYC (ES), MPO (CZ), CERT LT (LT), MFSR(SK), ILR (LU), APEK (SI), MCA (MT), Ministry of Economic Development (IT), OCECPR (CY), PT (NO).

We are grateful for their valuable input and comments.

Preface

The 2009 reform of the EU legislative framework for electronic communications (EU Directive 2009/140/EC) introduces Article 13a into the Framework directive (Directive 2002/21/EC as amended by Directive 2009/140/EC). The reform, was transposed by most EU Member States halfway 2011.

Article 13a concerns security and integrity of electronic communication networks and services. The first part of Article 13a requires that providers of networks and services manage security risks and take appropriate security measures to guarantee the security (paragraph 1) and integrity (paragraph 2) of these networks and services. The second part of Article 13a (paragraph 3) requires providers to report about significant security breaches and losses of integrity to competent national authorities, who should report about these security incidents to ENISA and the European Commission (EC) annually.

In 2010, ENISA, the European Commission (EC), Ministries and Telecommunication National Regulatory Authorities (NRAs), initiated a series of meetings (workshops, conference calls) to achieve an efficient and harmonised implementation of Article 13a across the EU. The Article 13a working group now comprises experts from NRAs of most EU countries, and several EFTA and EU candidate countries. Meetings (telephonic or physical) are organized and chaired by technical experts from ENISA. The European Commission acts as an observer in these meetings.

The Article 13a Working Group reached consensus on two non-binding technical guidelines for NRAs: the “Technical Guideline on Minimum Security Measures” and the “Technical Guideline on Incident Reporting” (this document).

This document, the Technical Guideline for Incident Reporting, provides guidance to NRAs about the technical implementation of paragraph 3 of Article 13a: incident reporting to ENISA, the EC and between NRAs. In spring 2012 NRAs, from all EU countries and some EFTA and EU candidate countries, implemented the first annual summary reporting about the 2011 incidents. An aggregate analysis of the reported incidents can be found in a public report.

Table of Contents

1 Introduction

In this document, we provide guidance to National Regulatory Authorities (NRAs) about paragraph 3 of Article 13a of the Framework directive (Directive 2002/21/EC as amended by Directive 2009/140/EC). It focusses on how to report incidents with ENISA and the EC and between NRAs.

This document is drafted by a working group comprising experts from NRAs and representatives of the EC, supported by technical experts from ENISA (see Preface): the Article 13a Working Group.

1.1 Target audience

This document is addressed to national ministries and NRAs in European Member States, the authorities tasked with the implementation of Article 13a.

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 NRA's about the technical implementation of the incident reporting described in paragraph 3 of Article 13a.

1.3 Updates

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

Version 2.0 (this document) is an update of Version 1.0 of the Guideline on Incident Reporting. Besides many smaller changes, simplifications and (most importantly) clarifications, the main changes are:

- Simplified thresholds for annual incident reporting.
- Examples of approaches for national incident reporting.
- More detail about incident impact and incident causes.

1.4 Structure of this document

In Section 2 we introduce Article 13a. In Section 3 we explain the scope and definitions used in this document. In Section 4 we show different approaches to national incident reporting. In Section 5 we describe ad-hoc reporting and in Section 6 we describe how NRAs should implement annual summary reporting to ENISA and the EC. In Section 7 we describe a incident report template fields, which should be used by NRAs for ad-hoc reporting and annual summary reporting.

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 font.

2 EU policy context and ENISA's role and objectives

In this section we discuss ENISA's role and objectives and we summarize the EU policy context.

2.1 EU policy context

This guideline concerns Article 13a of the Framework directive (Directive 2002/21/EC as amended by Directive 2009/140/EC). Besides Article 13a there are a number of other initiatives (legal or otherwise) addressing the security of public electronic communications networks and services:

- In 2006, the EC issued a strategy for a secure information society – dialogue, partnership and empowerment (COM (2006) 251), which was endorsed the next year by the European Council (Council Resolution 2007/068/01). One of the main actions of the strategy is a multi-stakeholder dialogue on the security and resilience of networks and information systems: the European Programme for Critical Infrastructure Protection (EPCIP).
- In 2009, the EC adopted, in March 2009, a communications and action plan on Critical Information Infrastructure Protection (CIIP), called *Protecting Europe from Large Scale Cyber-Attacks and Disruptions: Enhancing Preparedness, Security and Resilience* (COM (2009) 149). This communication focuses on *"prevention, preparedness, and awareness"* and defines an immediate action plan to strengthen the security and resilience of CIIs.
- The Council Conclusion on CIIP issued on May 2011, taking stock of the results achieved since the adoption of the CIIP action plan in 2009, was launched to strengthen the security and resilience of vital Information and Communication Technology Infrastructures.

The European Commission is also developing a European Cyber Security Strategy. The roadmap for the strategy and speeches from the EC contain explicit references to Article 13a and they mention the possibility of extending Article 13a to other business sectors (see also References).

For an overview of several security articles, which address security measures and incident reporting, we refer to the ENISA paper Cyber incident reporting in the EU which summarizes and compares Article 13a of the Framework directive, Article 4 of the e-Privacy directive, Article 15 of the proposed e-Trust/e-ID regulation and the reporting requirements in the proposed data protection reform.

2.2 ENISA's role and objectives

We briefly describe ENISA's role and objectives in the implementation of the Framework directive (2002/21/EC as amended by 2009/140/EC) and Article 13a in particular.

ENISA is mentioned in the preambles of the Framework directive:

- In preamble 44 of the Framework directive ENISA is asked to contribute to enhancing the level of security of electronic communications by, among other things, *"providing expertise and advice, and promoting the exchange of best practice"*.
- In preamble 44 of the Framework directive also mentions that ENISA should have the means to carry out the relevant duties and the powers to obtain sufficient information to assess the level of security of networks and services.
- In preamble 46 of the Framework directive ENISA is asked to contribute to the harmonisation of security measures by providing expert advice.

ENISA is also mentioned in Article 13a of the Framework directive:

- Paragraph 3 of Article 13a requires NRAs to, when appropriate, inform NRAs in other Member States and ENISA.
- Paragraph 3 of Article 13a requires NRAs to submit annual summary reports of the incidents to both the European commission and ENISA.
- Article 13a mentions that the European commission may decide to adopt technical implementing measures with a view to harmonisation of the implementation of paragraphs 1, 2, and 3 of Article 13a. Article 13a mentions that in this case the European commission will take into account the opinion of ENISA.

ENISA's primary objective is to implement the incident reporting mandated in Article 13a, 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 NRAs 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. ENISA published such an aggregate analysis for the first time in 2012, in the first annual report.
- To facilitate the exchange of experiences and lessons learned among NRAs, to allow them to better understand and address security incidents.
- Issue recommendations and guidance for NRAs, 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 NRAs 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.

3 Incident reporting in Article 13a

In this section we introduce paragraph 3 of Article 13a and the scope of this guideline.

3.1 Paragraph 3 of Article 13a

For the sake of reference, we reproduce the text of paragraph 3 of Article 13a here.

"3. Member States shall ensure that undertakings providing public communications networks or publicly available electronic communications services notify the competent national regulatory authority of a breach of security or loss of integrity that has had a significant impact on the operation of networks or services.

Where appropriate, the national regulatory authority concerned shall inform the national regulatory authorities in other Member States and the European Network and Information Security Agency (ENISA). The national regulatory authority concerned may inform the public or require the undertakings to do so, where it determines that disclosure of the breach is in the public interest.

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

Hence Article 13a introduces three types of incident reporting: 1) National incident reporting from providers to NRAs, 2) Ad-hoc incident reporting between NRAs and ENISA, and 3) Annual summary reporting from NRAs to the EC and ENISA. The different types of reporting are shown in Figure 1. This guideline focusses on the latter two.

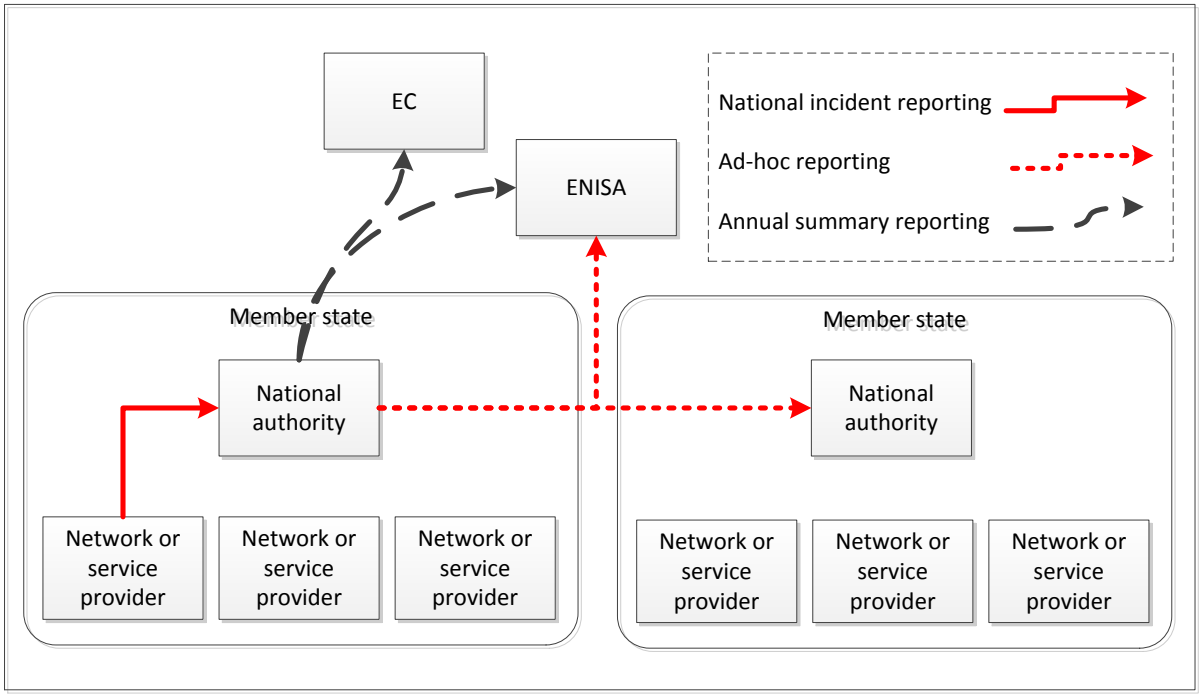

Figure 1. Three types of incident reporting in Article 13a

3.2 Electronic communication services

This guideline focuses on the following communication services and networks.

- Fixed telephony
- Mobile telephony
- Fixed internet access
- Mobile internet access

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

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

3.3 Security incidents

Article 13a mentions 'security incidents', 'security breaches' and 'integrity losses':

- Paragraph 1 requires "*that measures shall be taken to prevent and minimise the impact of security incidents on users and interconnected networks"*
- Paragraph 2 requires providers to *"take all appropriate steps to guarantee integrity of their networks, and thus ensure the continuity of supply of services"*.
- *Paragraph 3 requires "to notify the competent national regulatory authority of a breach of security or loss of integrity that has had a significant impact on the operation of networks or services"*

The use of the term integrity in the article text may be confusing to some readers. We refer to the definition in technical literature about networks and network interconnections[1], which defines integrity *"as the ability of the system to retain its specified attributes in terms of performance and functionality"*. Integrity of networks would be called availability or continuity in most information security literature[2].

In this guideline we call these types of incidents simply 'security incidents' and we use the following definition in this document.

Security incident: A breach of security or a loss of integrity that could have an impact on the operation of electronic telecommunications networks and services.

[1] *Ward, K, 1995, 'The Impact of Network Interconnection on Network Integrity'. British Telecommunications Engineering, 13:296–303.*

[2] *In information security literature the term 'integrity' usually refers to the property that data or communications cannot be altered or tampered with.*

3.4 Significant impact

Article 13a requires that providers report about a breach of security or a loss of integrity that has had a *significant impact* on the operation of networks or services to the NRAs. Annually NRAs should send summary reports about these security incidents to ENISA and the EC.

Note that it is at the discretion of the NRA to determine what is *significant*. This ultimately depends on national circumstances. For example, a security incident affecting just a small number of users in a specific area could already be considered significant by an NRA.

A security incident can have different types of impact on the operation of services.

- Impact on the continuity of supply of services.
- Impact on the security of users and interconnected networks

When there is an impact on the continuity of supply of services over the network the incident is often called 'outage' or 'disruption'. An outage or disruption can be complete (for instance 'network completely down') or partial ('50% of phone calls dropped in the last 15 minutes', 50% of internet bandwidth lost').

It is good to note here that security incidents sometimes lead to personal data breaches. If this is the case such a security incident would become relevant also in the context of Article 4 of the e-Privacy directive.

4 National incident reporting

Article 13a requires providers to report significant security incidents to the NRA. We call this national incident reporting in this document. 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 NRAs implementing Article 13a.

We would like to stress that this section is *not* intended as guidance, but rather as an illustration of the range of different implementations of national reporting across the EU, and to highlight the difference between national reporting and EU level reporting, between NRAs, ENISA and the EC.

Example: Country A

In country A the NRA is only required to keep track of large outages. The NRA is not interested in smaller outages, or in other types of security incidents. The NRA sets thresholds for national reporting relatively high.

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

The NRA allows providers to report incidents using email (unformatted), fax, phone or paper mail. The NRA provides guidance on the data that should be reported, but no specific template. Incident reports, once collected, are archived manually. The NRA 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 NRA does not play an active role in improving the security of networks and services. The NRA only intervenes when there have been very large incidents, or when there is a repetition of serious incidents involving a particular provider, service or network. The NRA works based on the assumption that providers will address security of the networks and services without support or incentives from the NRA. The coarse grained incident reporting allows the NRA to supervise to some extent the security of networks and services.

Example: Country B

In country B the NRA is required to keep track of major security incidents and to intervene whenever network and service providers fail to improve on security issues. National incident reporting includes large security incidents and smaller security incidents.

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

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

The NRA 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 NRA 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 NRA supervises the security of networks and services. The NRA 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 NRA is required to monitor the security of networks and services, and to work with network and service providers to improve security. The NRA 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 NRA 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 NRA 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 NRA sets up specific working groups to address the frequent and high-impact incidents. In other words, the NRA 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.

5 Ad-hoc incident reporting

In this section we describe the procedure for ad-hoc incident reporting to other NRAs and ENISA.

5.1 Goal

The goal of ad-hoc reporting is to inform NRAs abroad and ENISA about recent or on-going incidents, which may be relevant for other NRAs abroad. The purpose of ad-hoc reporting is not incident response or crisis management.

5.2 Reporting criteria

The NRA should assess whether or not an incident is relevant for NRAs in other countries and in this case make an ad-hoc report. It is at the discretion of an NRA to determine if an incident is relevant for other NRAs and ENISA[3].

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

5.3 Incident report data

Ad-hoc reporting is at the discretion of NRAs and NRAs should determine which information about the incident is relevant for sharing in ad-hoc reporting.

NRAs may use the incident report template fields for annual summary reporting (see Section 7).

5.4 Reporting modality

ENISA maintains a contact list of email addresses and telephone numbers of contact points at NRAs to enable ad-hoc incident reporting. The contact list is provided to NRAs upon request (resilience@enisa.europa.eu). The contact list is updated when needed. In this case the NRAs will receive a change notice.

Additionally ENISA provides an online tool to support ad-hoc incident reporting – access to the tool is provided to NRAs upon request (resilience@enisa.europa.eu).

[3] *Whether or not these incidents should be included in annual reporting depends on the impact of the incident.*

6 Annual summary reporting

In this section we define scope and thresholds for annual summary reporting.

We stress that this section should not be understood as a recommendation about which incidents are significant nor about which incidents should be reported nationally. NRAs should use a wider scope and stricter thresholds, where relevant, taking into account national circumstances and requirements.

6.1 Goal

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

- to get feedback from NRAs 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. ENISA published such an aggregate analysis for the first time in 2012, in the first annual report.
- to facilitate the exchange of experiences and lessons learned among NRAs, 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 NRAs, the private sector and policy makers, about security measures.

6.2 Scope

For the initial period, the scope of annual reporting to ENISA and the EC is restricted to losses of integrity, i.e. the security incidents with an impact on the continuity of supply of electronic communication services.

6.3 National user base

To allow for aggregation at an EU level (one of the goals of annual summary reporting) NRAs should provide ENISA and the EC with *estimates* of the total number of users of each service in their country. NRAs may (optionally) use the following metrics as estimates:

- For fixed telephony and fixed internet, NRAs may use the number of subscriber or access lines in their country.
- For mobile telephony, NRAs may use the number of active telephony SIM cards.
- For mobile internet, NRAs may sum up[4]:
  1. The number of standard mobile subscriptions, which offer both telephony 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.

[4] *Here we follow the definition agreed in the COCOM meetings. In some countries other metrics are used.*

6.4 Thresholds for annual reporting

In this section we define the thresholds for annual summary reporting to ENISA and the EC.

6.4.1 Combination of duration and user percentage

The threshold for annual summary reporting is based on the duration (see Section 7.1.3) and the number of users of a service affected (see Section 7.1.2) as a percentage of the national user base of the service (see Section 6.3).

NRAs should send an incident report, 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%.

	1h-2h	2h-4h	4h-6h	6h-8h	>8h
1% - 2%					
2% - 5%					
5% - 10%					
10% - 15%					
> 15%					

Figure 2. Threshold based on a combination of duration and the percentage of the national user base.

The threshold should be understood *per service* (see Section 3.2). In other words, even if an incident involves impact on multiple services, for one service alone the number of users affected and the duration should surpass the threshold.

6.4.2 User minutes

We are aware of the fact that the above-mentioned relative threshold excludes many large incidents occurring in larger countries. For example, in a country with 50 million citizens, even a day-long outage of a large city (say 500.000 inhabitants) would not exceed the (above-mentioned) relative threshold. To provide guidance to NRAs about reporting below the relative threshold we also introduce an optional threshold based on absolute impact.

NRAs may (optionally) include incidents in annual summary reporting when the product of duration and number of users affected exceeds: 180 Million user minutes, or 3 Million user hours.

For example, when 1 million users are affected for 3 hours, then the incident may be included in annual summary reporting.

7 Incident report template

In this section we describe incident report fields which should be used by NRAs when submitting incident reports to ENISA and the EC, as part of annual summary reporting.

7.1 Incident impact

7.1.1 Service affected

In the field "service affected" NRAs should provide information about which electronic communication services where affected, for example, by indicating a selection of one or more from

- fixed telephony,
- mobile telephony,
- fixed internet access,
- mobile internet access.

Or alternatively, NRAs may indicate that another type of service was affected. Optionally NRAs may provide further information about the 'technology' or 'platform' 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.

7.1.2 Number of users

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

- For fixed telephony and fixed internet, NRAs should report the number of subscriber or access lines impacted.
- For mobile telephony and mobile internet, NRAs should report an estimate, taking into account the normal usage of the affected facilities.

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.

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 NRAs 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 NRAs should report estimates.

7.1.3 Duration

In the field "duration" NRAs 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 telephony 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.

7.1.4 Impact on emergency calls

In the field "impact on emergency calls" NRAs should indicate if there was an impact on the possibility to call the emergency services, such as ambulances or fire brigades via emergency telephone numbers (112 in many countries).

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 had an impact on emergency calls.

7.1.5 Impact on interconnections

In the field "Impact on interconnections" NRAs should indicate if there was impact on the national or international interconnections between providers.

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 had on impact on interconnections.

7.2 Incident cause

7.2.1 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" NRAs should indicate the category of the root cause of the incident. There are 5 root cause categories[5]:

7.2.1.1 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'.

7.2.1.2 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'.

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

7.2.1.3 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'.

7.2.1.4 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.

7.2.1.5 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 may be used stand-alone when the root cause of the incident is unknown. In all other cases, 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'.

7.2.2 Initial cause

In the field "initial cause" NRAs may indicate the initial cause of the incident, i.e. the event or factor that *triggered* the incident.

For example, initial causes could be software failure, bad change, back-up fuel exhaustion, overload, power cuts, cyber-attack, and so on.

Note that these detailed causes may fit different root cause categories, depending on the specifics of the setting. For example, a cable cut may be caused by a human error or by a flaw in a procedure.

7.2.3 Subsequent cause

Often incidents involve a chain of events or factors. In the field "subsequent cause" NRAs may indicate a cause 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'.

7.2.4 Assets affected

NRAs may 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.

7.3 Incident description and follow-up

7.3.1 Incident description

In the field “incident description” the NRA should provide a description of the incident, and how it initially developed.

7.3.2 Incident response actions

In the field “incident response actions” the NRA may provide a description of actions taken by the provider to mitigate the impact of the incident.

7.3.3 Post-incident actions taken

In the field “post-incident actions” the NRA may provide a description of actions taken by the provider to reduce the likelihood or impact of similar incidents.

7.3.4 Lessons learnt

In the field “description of lessons learnt” the NRA may provide a description of lessons learnt from the incidents or measures which will be implemented on the long-term, by the NRA or providers.

8 References

In this section we provide references to related ENISA papers, and relevant EU legislation.

8.1 Related ENISA papers

- The first public annual report of incidents, concerning the 2011 incidents, is available at: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2011/
- This guideline and the Article 13a WG minimum security measures are available at: https://resilience.enisa.europa.eu/article-13
- ENISA's whitepaper on cyber incident reporting in the EU shows Article 13a and how it compares to some other security articles mandating incident reporting and security measures: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/cyber-incident-reporting-in-the-eu
- For the interested reader, ENISA's 2009 paper on incident reporting shows an overview of the situation in the EU 3 years ago: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/good-practice-guide-on-incident-reporting/good-practice-guide-on-incident-reporting-1

8.2 EU Legislation

- 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
- The electronic communications regulatory framework (incorporating the telecom reform): http://ec.europa.eu/information_society/policy/ecomm/doc/library/regframeforec_dec2009.pdf
- An overview of the main elements of the 2009 reform: http://ec.europa.eu/information_society/policy/ecomm/tomorrow/reform/index_en.htm
- The cyber security strategy has been announced in a roadmap and Commissioner Kroes highlighted 5 strands in a speech.

P.O. Box 1309, 71001 Heraklion, Greece
www.enisa.europa.eu