Annual Incident Reports 2016

Analysis of Article 13a annual incident reports in the telecom sector

JUNE 2017

About ENISA

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

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 group of experts from National Regulatory Authorities and ministries from across Europe. Listing the organizations (in no particular order): PTS (SE), FICORA (FI), Ofcom (UK), ANACOM (PT), ComReg (IE), EETT (GR), ADAE (GR), Centre for Cyber Security - CFCS (DK), RTR (AT), ANCOM (RO), CRC (BG), Ministry of Economics, Finance and Industry (FR), Bundes-netzagentur (DE), BIPT (BE), Agentschap Telecom (NL), MINETUR (ES), MPO (CZ), CTO (CZ), CERT LT (LT), Teleoff (SK), ILR (LU), PECSRS (SI), MCA (MT), Ministry of Economic Development (IT), OCECPR (CY), Nkom (NO), RIA (EE), NMHH (HU), ITSIRI (LV), OEC (PL), AKOS (SI), OFCOM (CH), and HAKOM (HR).

ISBN: 978-92-9204-222-6, DOI: 10.2824/21700

Table of Contents

Executive Summary

For the sixth year, ENISA publishes the annual report about significant outage incidents in the European electronic communications sector, which are reported to ENISA and the European Commission under Article 13a of the Framework Directive (2009/140/EC), by the National Regulatory Authorities (NRAs) of the different EU Member States.

This report covers the incidents that occurred in 2016 and it gives an aggregated analysis of the incident reports about severe outages across the EU. This report does not include details about individual countries or providers.

The aim of the incident reporting scheme is to provide transparency to society and to learn from past incidents in the electronic communications sector in order to systematically improve the security of the networks and services. This report provides an overview on an aggregated level of what services and network assets are impacted and the root causes of the incidents. Conclusions on the main patterns of incidents are drawn, contributing to discussions at policy level on strategic measures to improve the security in the electronic communications sector.

The main conclusions from this year's incident reporting are the following:

- **158 major incidents reported:** This year 24 countries, including two EFTA countries, reported 158 significant incidents that occurred in 2016, while 6 countries reported they had no significant incidents. 102 incidents were above the informal EU thresholds.
- **Mobile internet most affected service:** In 2016 most incidents affected mobile internet (48% of all reported incidents). Mobile internet and mobile telephony were the predominant affected services in the previous years also, except for 2014 where fixed telephony was the most affected.
- **System failures are the dominant root cause of incidents:** Most incidents were caused by system failures or technical failures (almost 73% of the incidents) as a root cause. This has been the dominant root cause for all the reporting years so far. In the system failures root category, software bugs and hardware failures were the most common causes affecting core network equipment.
- **System failures affected on average more user connections per incident:** In 2016 system failures was the root cause category involving most users affected per incident (around 2 million user connections on average per incident). The second place was taken by malicious actions with 1.2 million user connections on average per incident.
- **Malicious actions along with natural phenomena are not among the main root causes creating disruptions:** the total number of incidents caused by malicious actions was 5.1%; double compared to previous year (2.5% in 2015).
- **Malware caused the longest lasting incidents this year:** Incidents caused by malware (e.g. DDoS), although there were not too many of them, had most impact in terms of duration and user hours lost.
- **Emergency services are affected by incidents**: Same as last year, 20 % of the incidents affected the 112 emergency services, a considerably high percentage.
- **Mobile base stations and controllers the most affected assets:** Overall, mobile base stations and controllers and mobile switches were the network components most affected by incidents (7% and 6% respectively).

The analysis of annual incident reports the last six years has revealed specific trends and patterns of root causes, detailed causes and affected services. These assets and threats need particular attention when carrying out risk and vulnerability assessments in the electronic communications sector.

ENISA is permanently analysing the current threat environment and develops projects that address particular technical or policy related topics directly linked to the electronic communications sector. In the context of Article13a efforts, ENISA has been conducting many supporting activities in order to provide a holistic and in-depth view to providers that need to assess risks, take appropriate security measures, and report about significant security incidents.

Based on the annual summary reporting of previous years, ENISA analysed power supply dependencies[1], and issued recommendations regarding the sector's ability to withstand and act efficiently after power cuts. ENISA also studied in 2013 national roaming for increased resilience in mobile networks[2]. Last year, based on the annual summary reporting of 2012 and 2013 incidents, ENISA has issued recommendations for providers[3] about how to manage security requirements for vendors of ICT equipment and outsourced services used for core operations. Based on the 2012 and 2013 summary reporting ENISA has also studied national initiatives to reduce the number of underground cable breaks caused by mistakes[4].

ENISA has developed studies in order to facilitate NRAs as well as telco providers to incorporate these recommendations to their security activities. Recently developed a study on security measures implemented by electronic communication providers[5], and alternative indicators for measuring impact in electronic communications services[6].

Furthermore, in 2015, ENISA developed an impact evaluation of the Art. 13a provisions[7], with the purpose of assessing the changes in outcome that can directly be attributed to the article, the effects caused by this particular set of obligations within the Telecom Package.

[1] See https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/power-supply-dependencies/
[2] See http://www.enisa.europa.eu/media/press-releases/using-national-roaming-to-mitigate-mobile-network-outages201d-new-report-by-eu-cyber-security-agency-enisa
[3] See https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/requirements-ecomms-vendors
[4] See https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/protection-of-underground-infrastructure
[5] See https://www.enisa.europa.eu/publications/security-measures
[6] See https://www.enisa.europa.eu/publications/security-incidents-indicators
[7] See https://www.enisa.europa.eu/publications/impact-evaluation-article13a

1. Introduction

The current document represents the sixth iteration of the report "Annual Incident Reports", which summarises significant outage incidents in the telecom sector reported to ENISA and the European Commission (EC), under Article 13a of the Framework Directive (2009/140/EC)[8], an article introduced in the 2009 reform of the EU regulatory framework for electronic communications[9]. This year ENISA and EC received 158 incident reports from NRAs, about severe outages in the EU's electronic communication networks and/or services which occurred in 2016. This report provides an aggregate analysis of these 158 incidents.

Please note that in this document we do *not* provide details from the individual incident reports. The analysis is only an aggregation in terms of averages and percentages across the EU and EFTA countries, and it does not contain references to specific countries or specific providers. Individual incidents are discussed in more detail with the NRAs in the Article 13a Expert Group[10].

This document is structured as follows: Section 2 and Section 3 briefly summarize Article 13a and the details of the technical implementation of Article 13a, as agreed in the Article 13a Expert Group by the different NRAs of the EU Member States. Section 4 analyses the incidents from 2016 which were reported to ENISA and the Commission and provides examples of incidents. Section 5 provides the conclusions.

In the separate document of Annex (Annexes A-D) we show graphs with the trend over the years to allow for the reader to make a comparison with data from previous years. This comparison should however be done with caution, as the methodology for details in the reporting has been improved over the years and the thresholds have been lowered year by year allowing for more incidents to be reported.

[8] See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32009L0140:en:NOT

[9] See https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Copy of Regulatory Framework for Electonic Communications 2013 NO CROPS.pdf

[10] See http://resilience.enisa.europa.eu/article-13

2. Article 13a of the Framework Directive: 'Security and Integrity'

The reform of the EU regulatory framework for electronic communications[9], which was adopted in 2009 and was transposed by most EU countries around May 2011, added Article 13a to the Framework Directive[8]. Article 13a addresses the security and integrity[11] of public electronic communications networks and services. The legislation concerns National Regulatory Authorities (NRAs) and providers of public electronic communications networks and services (providers).

Article 13a states:

- Providers of public electronic communications networks and services should take measures to guarantee security and integrity of their networks.
- Providers must notify competent national authorities about breaches of security or loss of integrity that have had significant impact on the operation of networks or services.
- National Regulatory Authorities should notify ENISA and national authorities abroad when necessary, for example in case of incidents with cross-border impact.
- Annually, National Regulatory Authorities should submit a summary report to ENISA and the European Commission about the incidents.

These incident reporting flows (incident notification and annual reporting) are shown in the diagram below. This document analyses the incidents from 2015 that have been reported to ENISA (the black dashed arrow).

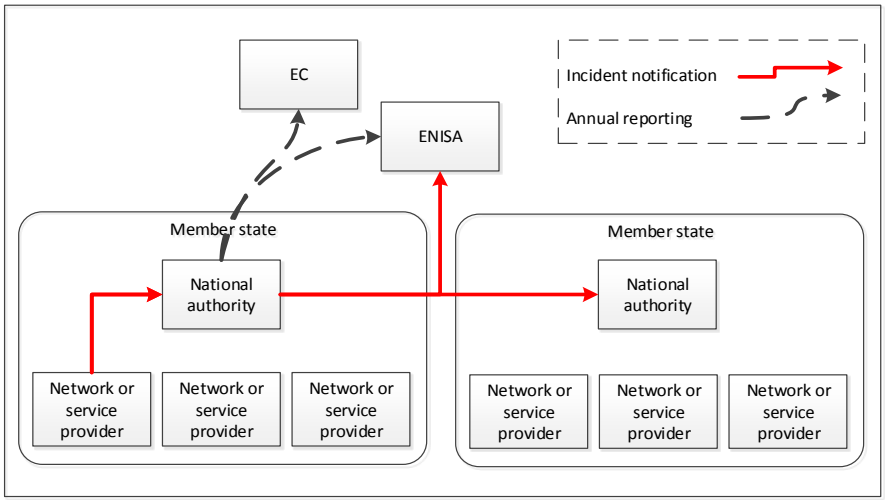

Figure 1: Incident reporting in Article 13a

In late 2015 the European Commission started the process of revising the regulatory framework on electronic communications in order to "assess the current rules and to seek views on possible adaptations to the framework in light of market and technological developments, with the objective of contributing to the Digital Single Market Strategy"[12]. A public consultation concerning the evaluation and review of the current regulatory framework was ended in December 2015. In this context, ENISA along with the Article 13a Expert Group submitted an opinion on

[11] Here integrity means network integrity, which is often called availability or continuity in information security literature.
[12] https://ec.europa.eu/digital-single-market/en/news/public-consultation-evaluation-and-review-regulatory-framework-electronic-communications

the evaluation and review of Article 13a and 13b of the Framework Directive, an area which is at the core of ENISA expertise and competence.

3. Article 13a Expert Group and Incident Reporting Procedure

In 2010, ENISA, Ministries and NRAs initiated a series of meetings (workshops, conference calls) to achieve a harmonised implementation of Article 13a of the Framework directive. In these meetings, a group of experts from NRAs, called the Article 13a Expert Group, reached agreement on two non-binding technical documents providing guidance to the NRAs in the EU Member States:

- Technical Guideline on Incident Reporting[13]
- Technical Guideline on Security Measures[14]

Later on, in 2014, the group of experts agreed on the third non-binding technical document:

- Technical Guideline on Threats and Assets[15]

The Article 13a Expert Group continues to meet several times a year to develop the technical guidelines and to discuss the implementation of Article 13a (for example, on how to supervise the electronic communications sector) and to share knowledge and exchange views about past incidents, and how to address them.

3.1 Incident reporting procedure

In spring 2012, the EC agreed with the EU Member States (in meetings of the Communications Committee, COCOM) to do the first round of annual summary reporting on the 2011 incidents impacting the continuity of supply of electronic communications services. The decision included a recommendation to use the reporting template agreed within the Article 13a Expert Group and published by ENISA. Following the COCOM meeting, ENISA implemented the technical procedure by deploying a basic electronic form based on the Article 13a Technical Guideline on Incident Reporting. There was also an agreement that in the coming years, annual reporting would be carried out by the end of February each year.

In autumn 2012, ENISA developed an online incident reporting tool (called CIRAS), which replaces the electronic forms exchanged by email. CIRAS allows NRAs to exert greater control over the data reported and provides the NRAs with better access to data about incidents reported across the EU. Since 2015 ENISA is providing the possibility for the NRAs to extract graphs from CIRAS based on their search results.

We briefly explain the main features of the incident reporting procedure, as described in the Article 13a Technical Guideline on Incident Reporting, which was developed in collaboration with the NRAs.

3.1.1 Services in scope

Although the focus of this report is still on the main 4 types of classic services, due to latest technological and legal advancements, we have decided to extend the number of services. As some of those services become more and more important in the EU digital market, and some countries already cover them through their national level regulations, their inclusion in ENISA's annual report is a must as preparatory work needs to be done to cover them in the future.

[13] See https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting
[14] See https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures
[15] See https://resilience.enisa.europa.eu/article-13/guideline_on_threats_and_assets

Besides the four main services (aka. classic services), others were added as follows:

CLASSIC SERVICES	OTHER SERVICES (SINCE 2016)
Fixed telephony	SMS
Mobile telephony	MMS
Fixed Internet access	Satellite TV
Mobile Internet access	International roaming
	RADIO broadcasting
	TV broadcasting
	Cable TV
	IPTV
	Video on demand
	Public WIFI
	Web based voice services
	Web-based messaging services
	Public email services

Table 1: Services in scope

3.1.2 Security incidents in scope

NRAs are required to report security incidents, which had a significant impact on the continuity of supply of electronic communications services. As explained, not all types of incidents are reportable under the Art. 13a provisions. Depending on the national implementation of Art. 13a, if one incident does not affect the continuity of the service (availability), although confidentiality or integrity might be affected, the incident does not need to be reported.

3.1.3 National user base

NRAs should provide estimates of the total number of users of each service in their country. The national user base is used for determining the significance of incidents, in cases where the threshold is relative to the national user base.

- For fixed telephony and Internet, NRAs should use the number of subscribers or access lines in their country.
- For mobile telephony, NRAs should use the number of active telephony SIM cards.
- For mobile Internet, NRAs should sum up[16]:
    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.
- For other types of services that are still in an experimental phase no national user base was collected at this point.

[16] Reference is made to the definition agreed in the COCOM meetings.

3.1.4 Thresholds

Art. 13a provisions state that Member States (MS) shall ensure that electronic communication providers will "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". However, the thresholds for defining significant incidents were not established through the Directive and the EC has not issued any implementing measures in this sense leaving the matter open for discussions and unrestricted for national implementation. At this point the activities of ENISA and Art. 13a expert group have proved to be very useful by defining a set of **informal and non-binding EU thresholds** to help Member States in reporting or setting up their own national level thresholds. In this respect a set of EU thresholds were adopted by the Art. 13a expert group that are known and accepted by every country, but it has remained at the discretion of each Member State to adopt its own national thresholds. All incidents reported within the annual report to ENISA and EC, and presented within this report, are based on the thresholds established at national levels, which can be above or below (in most of the cases they are below) the EU thresholds. For an analysis of incidents based on the informal EU level thresholds see Section 3.1.5.

The EU thresholds for the annual summary reporting are based on the duration and the number of users of a service affected as a percentage of the national user base of the service.

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

	1h<...<2h	2h<...<4h		4h<...<6h		6h<...<8h		>8h
1%<...< 2% of user base								
2%<...< 5% of user base								
5%<...< 10% of user base								
10%<...< 15% of user base								
> 15% of user base								

Table 2: Threshold for annual summary reporting based on a combination of duration and the percentage of the national user base.

The threshold should be understood on a "per service" basis. In other words, if an incident impacts multiple services, then for one of the services the threshold should be passed in order to trigger the reporting mechanism. NRAs have the discretion to also report incidents with impact graded below the threshold.

Since 2013, we introduced a new optional threshold for annual summary reporting, based on absolute impact, in order to allow for NRAs in large Member States to include larger incidents but that would not exceed the relative thresholds. This absolute threshold has been lowered for 2014 and has now become mandatory. NRAs should include incidents when the product of duration and number of user connections affected exceeds ***60 million user minutes, or 1 million user hours***. Note that the introduction of this mandatory and lowered absolute threshold has led to an increase in the number of reported incidents to ENISA and the Commission.

In case of the services that deviate from the four main services no thresholds were established. Member states could report incidents that they consider significant.

3.1.5 EU thresholds vs. national level thresholds

Art. 13a provisions state that member states shall ensure that electronic communication providers will "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". But the thresholds for defining significant incidents were not established through the Directive and the EC has not issued any implementing measures in this sense leaving the matter open for discussions and unrestricted as regards the national implementation. At this point the activities of ENISA and Art. 13a expert group have proved to be very useful by defining a set of **informal and non-binding EU thresholds** to help member states in reporting or setting up their own national level thresholds. In this respect a set of EU thresholds were adopted by the Art. 13a expert group that are known and accepted by every country, but it has remained at the discretion of each Member State to adopt its own national thresholds. All incidents reported within the annual report to ENISA and EC, and presented within this report, are based on the thresholds established at national levels, which can be above or below (in most of the cases they are below) the EU thresholds. This section presents a short analysis of incidents based on the informal EU level thresholds.

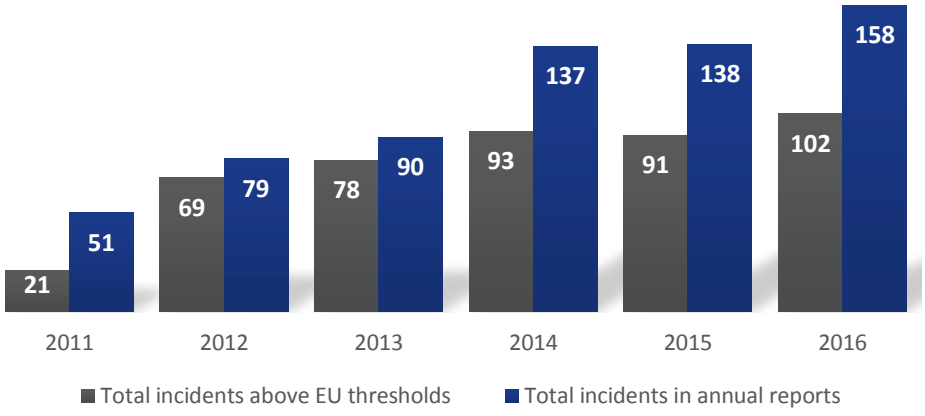

Figure 2: Total incidents in annual reports vs. Total incidents above thresholds

According to our estimations more than half of the EU member states have thresholds below the ones defined by ENISA while others use the same thresholds.

3.1.6 Root cause categories

In the incident reports four categories of root causes have been outlined plus one category that is used in conjunction with one of the other four categories.

- **Natural phenomena** – This category includes incidents caused by severe weather, earthquakes, floods, pandemic diseases, wildfires, wildlife, and so on.
- **Human errors** - This category includes incidents caused by errors committed by employees of the provider or outside the provider, during the operation of equipment or facilities, the use of tools, the execution of procedures, etc. E.g. an excavator cutting off a cable.
- **Malicious attacks** - This category includes incidents caused by a deliberate act by someone or some organisation, e.g. a Denial of Service attack disrupting the service, or a cable theft.
- **System failures** – This category includes incidents caused by technical failures of a system, for example caused by hardware failures, software bugs or flaws in manuals, procedures or policies.

- **Third party failures** – This category includes incidents caused by a failure or incident at a third party. The category is used in conjunctions with one of the other four root cause categories.

3.1.7 Detailed causes

In the incident reports, detailed causes are specified in terms of "initial cause" and "subsequent cause". "Initial cause" is the event or factor that *triggered* the incident. Often incidents involve a chain of events or factors, and by specifying a "subsequent cause" NRAs may indicate a cause that subsequently played a role in the incident. In the ENISA annual reports the initial and subsequent causes are equally presented in the graphs of the detailed causes. These detailed causes are referred to as "threats" in the Article 13a Technical Guideline on Threats and Assets[15]. In the report, which is used by the NRAs as a guide for the annual summary reporting, the causes/threats are listed and described.

3.1.8 Assets affected

Optionally NRAs may indicate what network assets were affected by the incidents, e.g. HLRs, routers and switches, underground cables etc. These assets are listed and described in the Article 13a Technical Guideline on Threats and Assets.

3.1.9 Impact evaluation on the implementation of Article 13a incident reporting scheme

As several years have passed since the publication and implementation of the Framework Directive including Art. 13a, an impact evaluation of the new article was the proper thing to do. This was done by ENISA along with the Article 13a Expert Group in 2015. The evaluation had the purpose of assessing the changes in outcome that can directly be attributed to the provision of Art. 13a, the effects caused by this particular set of obligations within the Telecom Package. The evaluation focused on 5 key areas, where we tried to identify possible outcomes:

- The new security measures implemented in the member states;
- The transparency resulting from the incident reporting process;
- The learning process resulting from incidents;
- The level of collaboration between the stakeholders;
- The harmonization of the procedures within the European Union.

The evaluation done within this project has brought to light some important outcomes that have definitely contributed to increasing the resilience and security of the telecommunications infrastructures in Europe. In a European Union which was highly diversified in terms of security measures, Art. 13a brought a certain amount of uniformity in the approach taken regarding security of telecommunication services, but more importantly contributed to strengthening the European telecom infrastructure's resilience and services availability across the EU. The role of ENISA, especially in the coordination of Art. 13a expert group, was most beneficial as it helped considerably in bringing more harmonization within the implementation process and collaboration among stakeholders (NRAs and providers). Findings and conclusions of the Impact evaluation on the implementation of Article 13a incident reporting scheme[17] have served as an input to the EU Commission in the telecom framework evaluation process.

[17] See https://www.enisa.europa.eu/publications/impact-evaluation-article13a

4. Analysis of the incidents

In total, all 28 EU Member States and 2 EFTA country participated in this process. Of these, 22 Member States and 2 EFTA countries reported in total 158 significant incidents and 6 countries reported there were no significant incidents. An increase from previous year where 21 countries reported significant incidents.

Figure 3: Countries involved in the annual summary reporting in 2015.

In this section, the 158 reported incidents are aggregated and analysed. First, the impact per service is analysed (in Section 4.1), then the impact per root cause category is analysed (Section 4.2), and in Section 4.3 detailed causes are examined. In Section 4.3.5 the impact, as a product of user connections affected and duration of the incidents, is analysed, and in Section 4.4 the components or assets affected by the incidents are considered. Throughout the text we provide anonymized descriptions (in blue italic) of actual large-scale incidents which occurred in 2015. In annex A-D we show graphs including the previous two years to allow the reader to make a comparison. This comparison should however be done with caution, see below.

Note about statistical conclusions: Readers should be cautious when drawing conclusions from the statistics in this report. In particular, they should take into account that:

1. The scope of reporting major security incidents is restricted to incidents with an impact on the *continuity* of public electronic communication services and networks. There are many other types of incidents with an impact on security of services and networks which are not in scope of annual reporting. For example, if attackers would wiretap undersea cables without causing any outages, then such a security incident would not be included in the annual reporting.
2. The scope of reporting includes major, or *significant,* incidents scoring above the agreed reporting thresholds (Table 2). Smaller incidents are not reported at EU level, meaning that the view is skewed towards the larger incidents.
3. Year by year we are in collaboration with the NRAs and in some cases the thresholds that define the significance of incidents are modified. This may cause the number of reported incidents to fluctuate. Until now the thresholds have only been lowered, causing in some years an increase in the number of incidents. This doesn't necessarily mean that the number of incidents throughout the EU is increasing.
4. We are continuously working in collaboration with the NRAs for improved quality in the incident reporting. There are still changes, more details and improvements in the way national and EU reporting is being implemented, including the lowering of reporting thresholds and refinements of parameters for reporting. Statistical conclusions about multi-annual trends should therefore ***be drawn with caution***.

5. All incidents reported within the annual report to ENISA and EC, and presented within this report, are based on the thresholds established at national levels, which can be above or below (in most of the cases they are below) the EU thresholds. For an analysis of incidents based on the informal EU level thresholds see Section 3.1.5.

4.1 Impact of incidents

First we look at the electronic communications services and compare them with each other in terms of incidents.

4.1.1 Impact per service

For third year in a row most of the reported incidents affected mobile internet. Both mobile internet and mobile telephony services had an increase on incidents compared to last year's results. In 2014 the most affected service was fixed telephony (see Annex A).

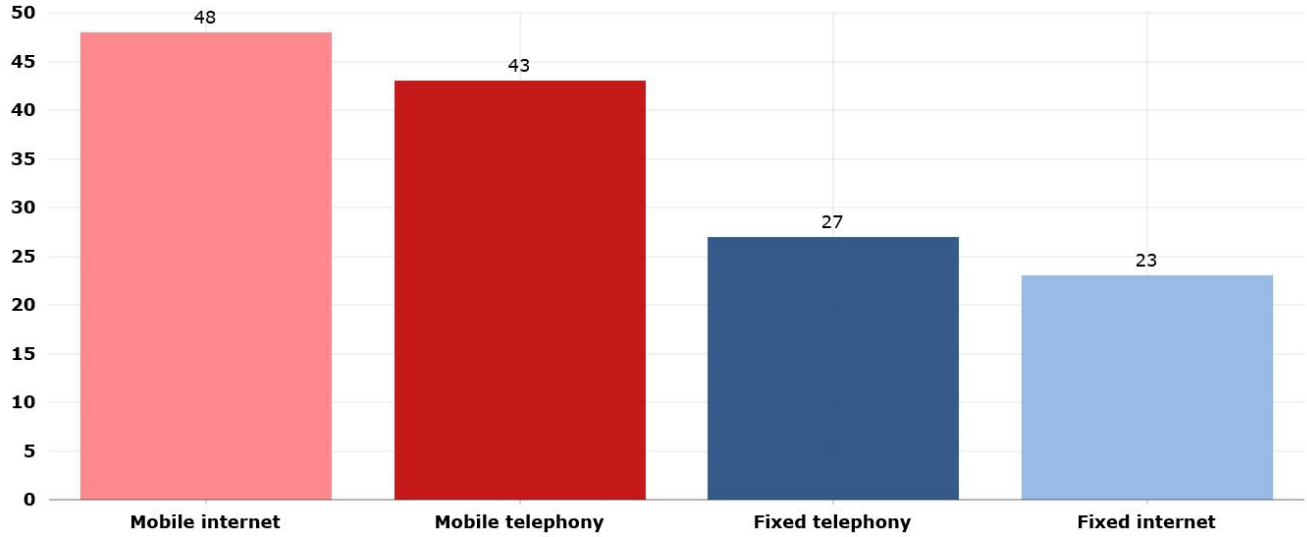

Figure 4: Incidents per classic services (percentage)

Note that most reported incidents usually have an impact on more than one service in the same incident (which is why the percentages in the chart add up to more than 100 %).

A system failure affected mobile internet to fail for millions of users (duration: hours, connections: millions, cause: software bug): *A software bug occurred in the Internal system component SDM leading to the degradation of user authorization mobile data and mobile voice. As a result end users had difficulties to access mobile services, both voice and data locally and also abroad (roaming services). Mobile switches and mobile user registerss were affected by this bug. Provider removed the obstacles in accessing the services and for the prevention of similar incidents in the future, a mitigation plan was created in collaboration with software vendors.*

Other services

Apart from the four main services, the most affected services are SMS (16,5), Cable TV (7,6%) and MMS (7%).

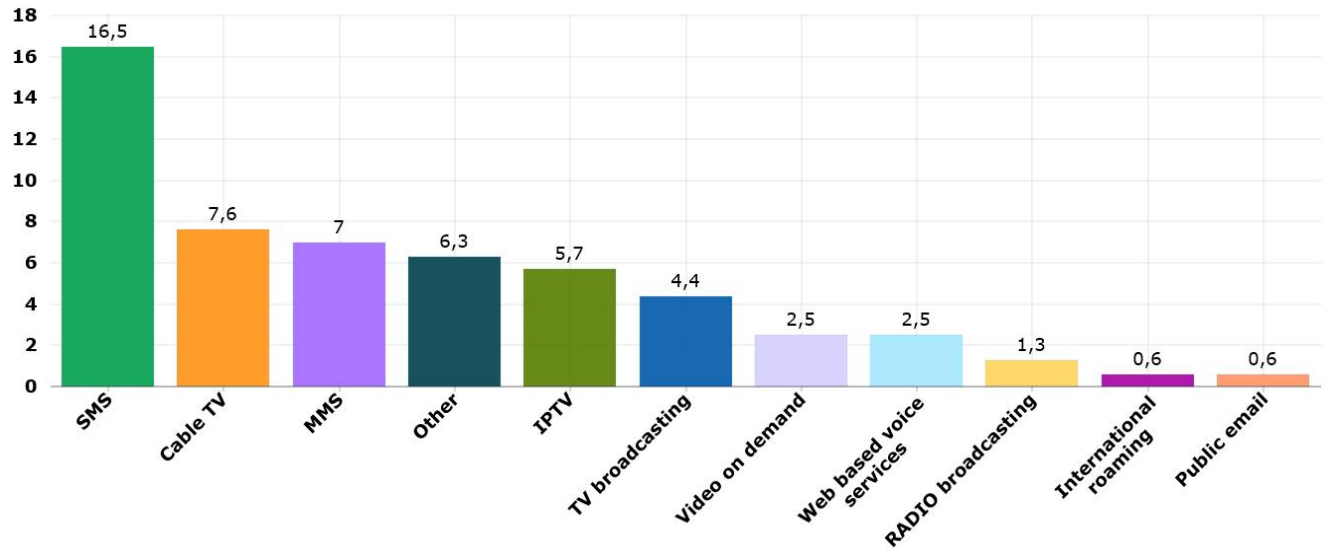

Figure 5: Incidents per other service (percentage)

4.1.2 Number of user connections affected

Mobile Internet outages affected most user connections compared to the other services, with an average of 1.3 million user connections affected per reported incident. Also in past reporting years mobile internet failures affected most user connections, and mobile telephony failures came in second place, see Annex A.

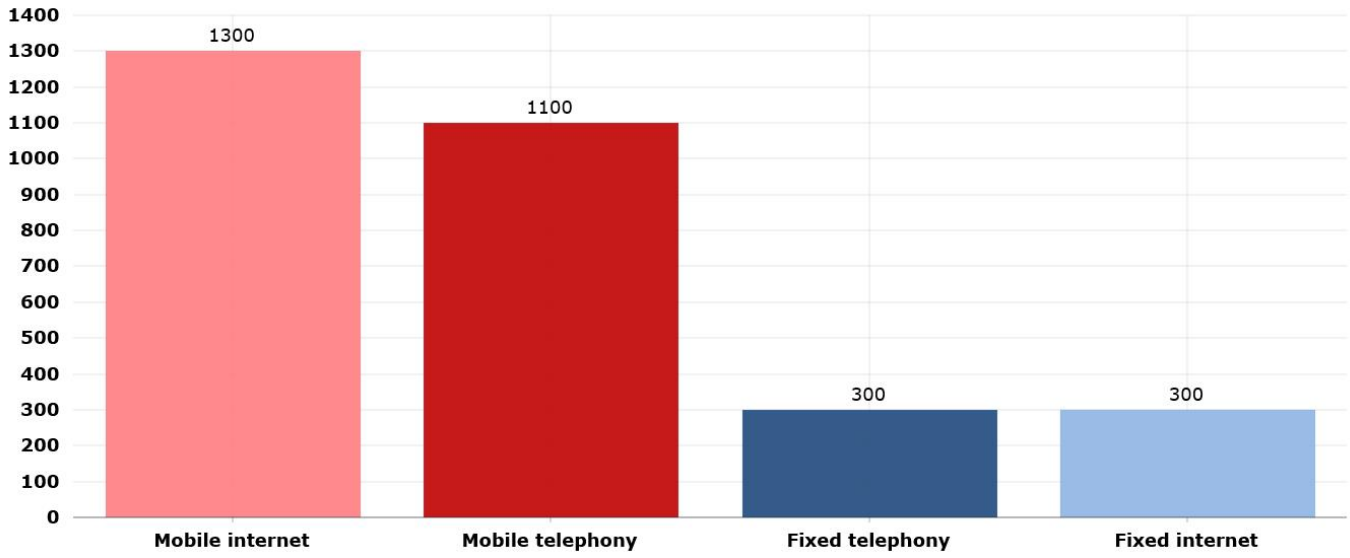

Figure 6: Average number of user connections affected per incident per classic service (1000s).

Note that the averages in these diagrams include both small and large countries, so EU averages shown in the diagram above are not necessarily representative for the size of incidents occurring nationally. The average size of

national incidents can be very different, depending on the size of the population and the national network topology. What is interesting to note is the comparison between the affected services in terms of affected user connections.

The evolution of the number of affected connections can be seen in Annex A.

Other services

The average number of connections affected for Radio broadcasting is 2 million. As for MMS (1.3 million) and SMS (1.2 million) services is in the same range as mobile telephony/mobile internet underlining the interconnection between the two.

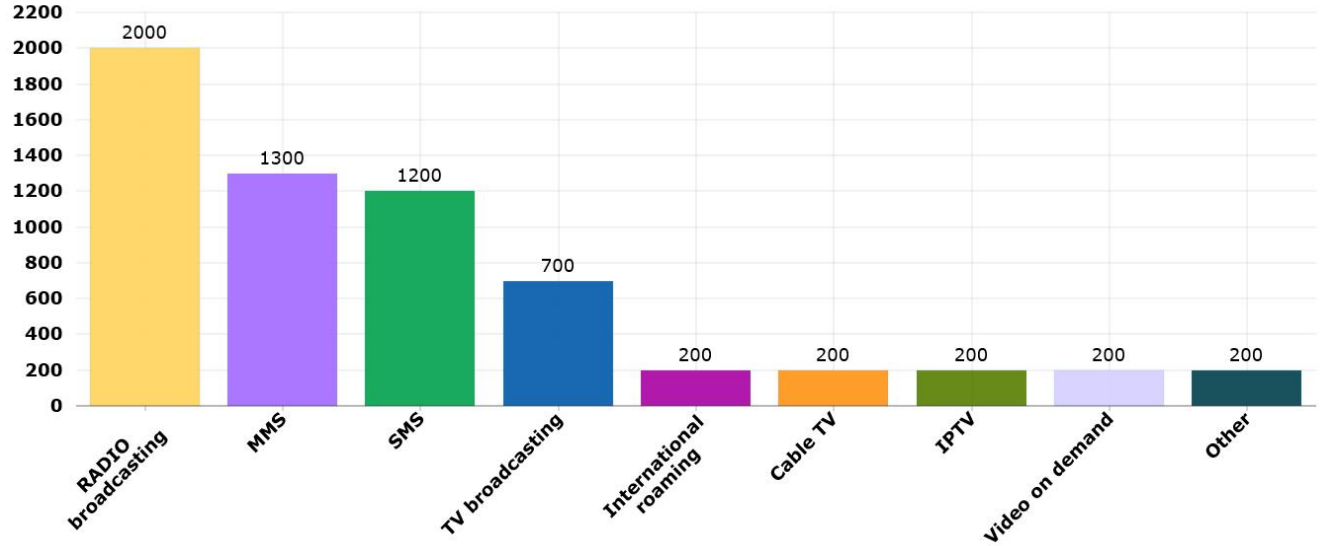

Figure 7: Average number of user connections affected (1000s) - other services

4.1.3 Percentage of the national user base affected

Mobile Internet outages impacted on average 14% of the national user base for mobile Internet user connections, which is a slight increase compared to the previous years, see annex A.3. All five years, mobile Internet has been reported to suffer the most impact in terms of percentage of its national user base compared to the other services.

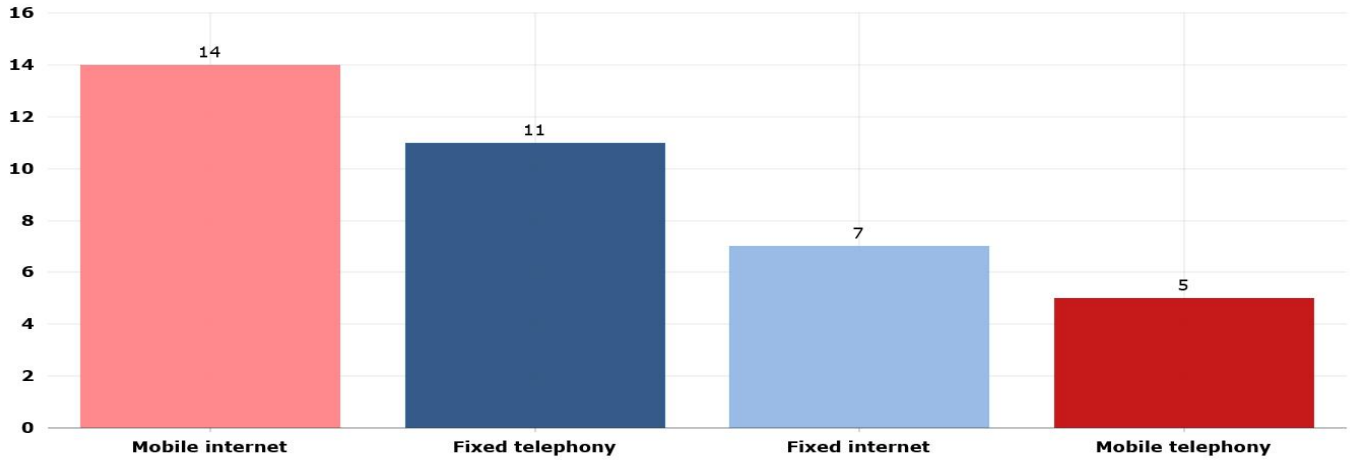

Figure 8: Percentage of national user base affected on average per incident per service.

4.1.4 Impact on emergency services

In more than 20% of incidents reported, emergency calls were impacted - i.e. the possibility for users to contact emergency call-centres using the emergency number 112.

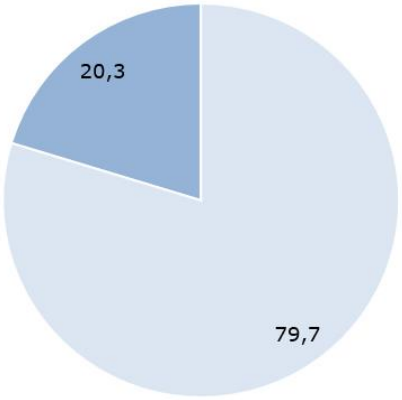

Figure 9: Impact on emergency calls.

4.1.5 Impact on interconnections

In 7 % of incidents reported there was an impact on interconnections between providers. Compared to previous year also this figure has decreased, see Annex A.

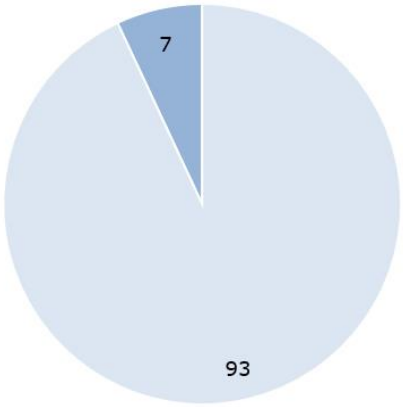

Figure 10: Impact on interconnections (percentage)

4.2 Root cause categories

In this section we look at the main root cause categories of reported incidents. For a description of the root cause categories, see section 3.1.5.

4.2.1 Incidents per root cause category

This year, almost 73% of the reported incidents were caused by system failures or technical failures, a ratio which is consistent compared to all the previous years, see Annex B. For all reporting years, system failures has been the most common root cause category. In second place, for this year is root cause of human errors 11,4% of the reported incidents, also consistent with previous years. Malicious actions and natural phenomena caused the least of the incidents (both with 5,1%).

Figure 11: Incidents per root cause category (percentage).

System failure caused disruption in all classic services and SMS/ MMS services affecting millions of users (duration: hours, connections: millions, cause: *hardware failure): System failure caused outage of network components using technology for DSL in the subscriber access network. Provider raised the capacities of network components in order to provide electronic communications service. As a next step a software upgrade of several selected network components was applied.*

4.2.2 Third party failures

About 22.5% of the incidents reported were categorized as third party failures, a significant increase compared to the previous year (14.8%), see Annex B.

Figure 12: Third party failures and non-third party failures of all incidents (percentages).

4.2.3 Root cause categories per service

In this section we look at the root causes for each of the four services separately: fixed telephony, fixed Internet access, mobile telephony and mobile Internet access.

As in 2015, also in 2016, system failures was the dominant root cause for all services, scoring more than half of the incidents reported per service. For mobile telephony and mobile internet, this was the case also in the previous years, whereas the dominant root cause for fixed telephony and fixed internet oscillated in the previous years between natural phenomena and system failures, see Annex B.

4.2.3.1 Fixed Telephony

Figure 13: Root cause categories for fixed telephony (percentage).

4.2.3.2 Fixed Internet

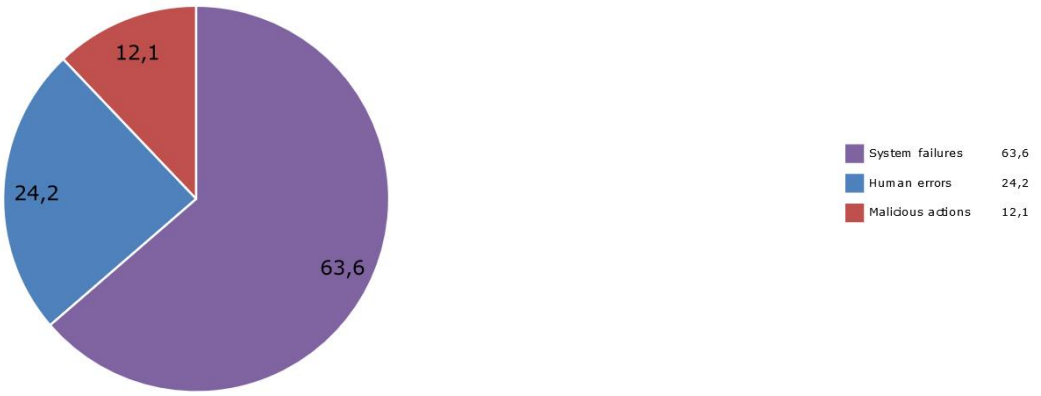

Figure 14: Root cause categories for fixed Internet (percentage).

4.2.3.3 Mobile telephony

Figure 15: Root cause categories for mobile telephony (percentage).

4.2.3.4 Mobile internet

Figure 16: Root cause categories for mobile Internet (percentage).

4.2.3.5 Other services

System failures is also the main root cause for other services besides the classic services, with a percentage of approximately 71%.

Figure 17: Root cause categories for other services (percentage).

4.2.4 Average number of user connections affected per root cause category

Also this year, system failures affected most user connections, on average about 2.0 million user connections per incident. In the previous year, system failures affected on average 1.6 million user connections.

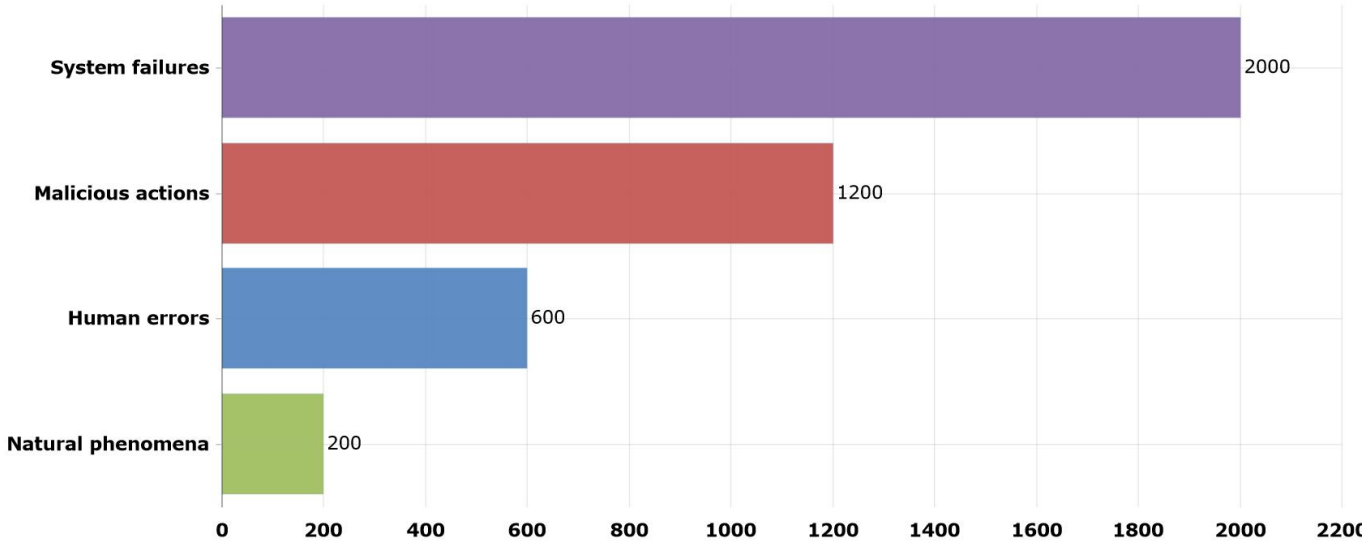

Figure 18: Average number of user connections affected per incident per root cause (1000s)

4.2.5 Average duration of incidents per root cause category

The reported incidents caused by natural phenomena had the longest recovery time on average per incident (400 hours). Excluding last year's result where malicious action was the root cause with the longest incidents on average, natural phenomena tend to cause the longest incidents in terms of duration. For the evolution in time of the average duration pls. check Annex B.

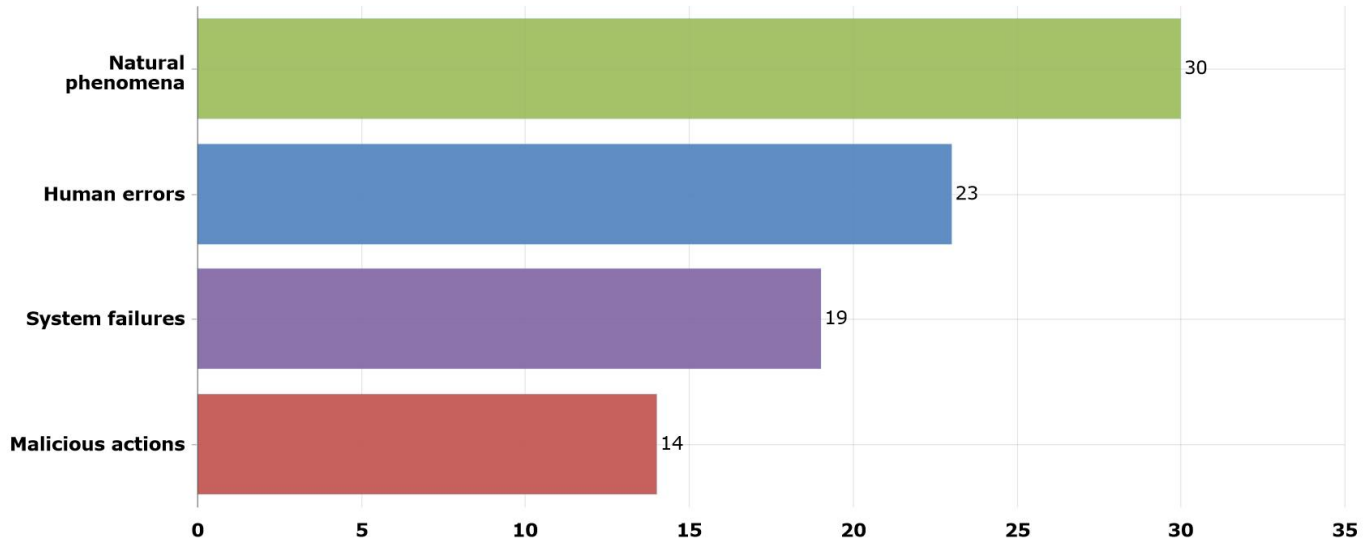

Figure 19: Average duration of incidents per root cause category (hours).

4.2.6 User hours lost per root cause category

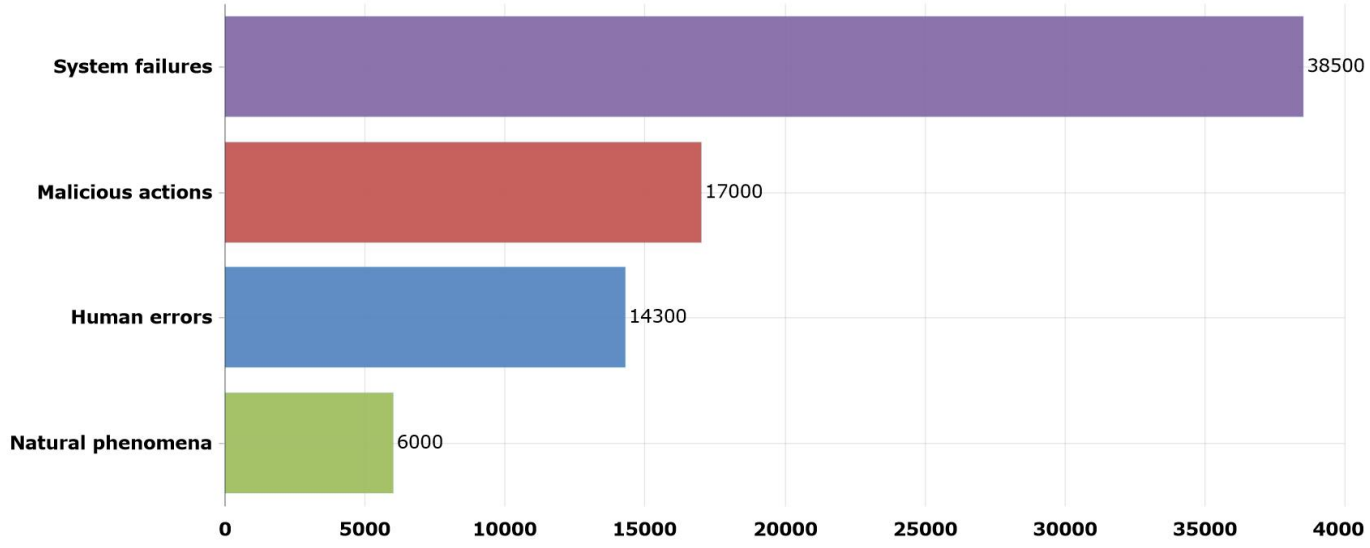

Figure 20: User hours lost per root cause category (hours).

4.3 Detailed causes

Root cause categories are rather broad but give a good summary of the most common types of incidents. In this section we break down the root cause categories in predefined detailed causes of incidents.

An incident is often not only triggered by one cause but often by multiple causes and a chain of causes. For instance, an incident may initially be triggered by heavy winds, which tear down power supply infrastructure causing a power cut, which in turn leads to an outage. For this incident both heavy winds and power cut are detailed causes. These detailed causes are equally represented in the statistics, because both causes may be addressed by the provider in terms of security measures.

4.3.1 Detailed causes of all incidents

In 2016, the most common causes of incidents were hardware failures and software bugs. This can now be considered a trend as this has been the case all the previous years, with the first position being occupied by one or the other. Also power cuts and cable cuts seem to slightly decrease and leave their place from the top four causes of the last four years. Many detailed causes of incidents reports do not fall under a specific category and form the category of "Other" which has a significant position in the overall chart. However, analysing further these detailed causes we see that most of them describe a cause that resulted to a system failure. Even though most of the causes in Other category in generic terms fall either under Software bug or Faulty software change/update, we detail some that seem interesting: billing platform failure, connectivity failure, maintenance, scheduled work failure, STP error, redundancy failure, etc.

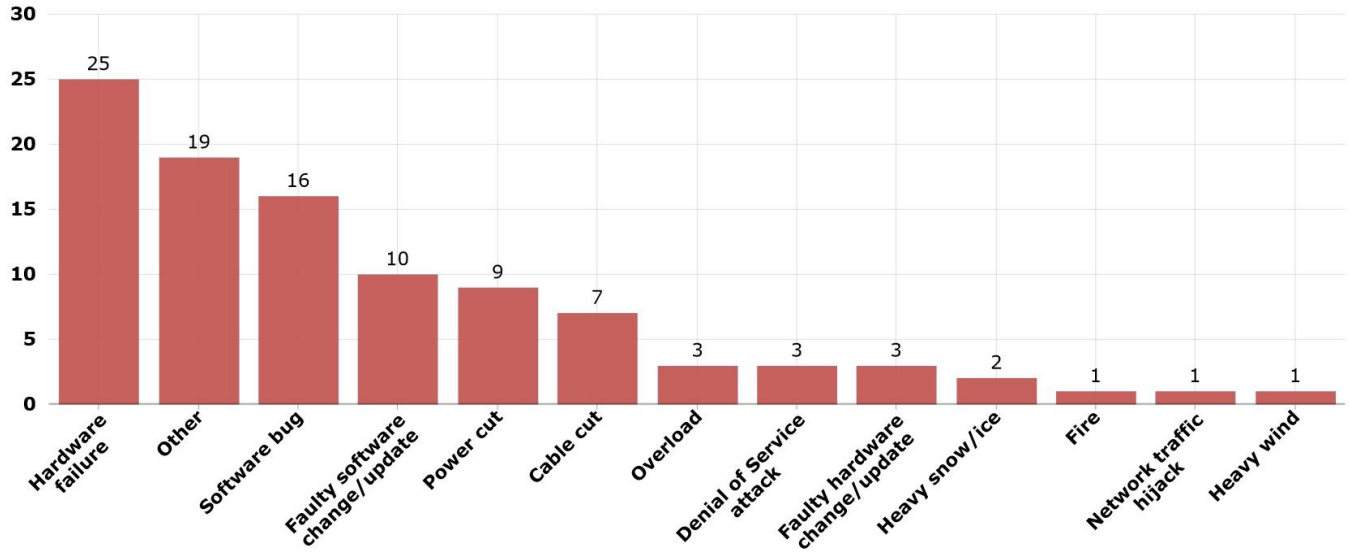

Figure 21: Detailed causes of reported incidents (percentage)

***Hardware failure resulted in unavailability of services for more than a million users (duration: hours, connections: millions, causes**: **system failure):** Outage of network components using technology for DSL in the subscriber access network resulted to disruption of all classic services as well as SMS and MMS services.*
Provider responded to the incident by raising the capacities of network components in order to provide elelctronic communications service. Followed a software upgrade of several selected network components to resolve the issue completely.

4.3.2 Detailed causes per service

In this section we show the detailed causes of incidents for each of the main four services (fixed telephony, fixed Internet, mobile telephony and mobile Internet) and for the other services. As in the previous year, also this year, Hardware failures were the most common causes for failures in all the main four services and for the other services as well.

4.3.2.1 Fixed Telephony

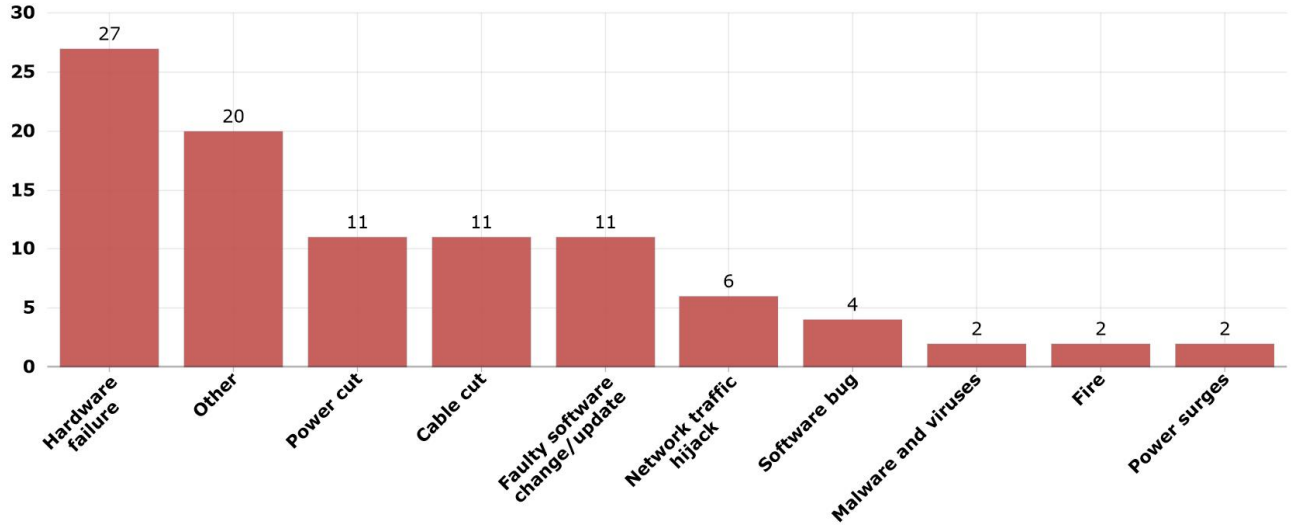

Figure 22: Detailed causes for fixed telephony (percentage).

4.3.2.2 Fixed Internet

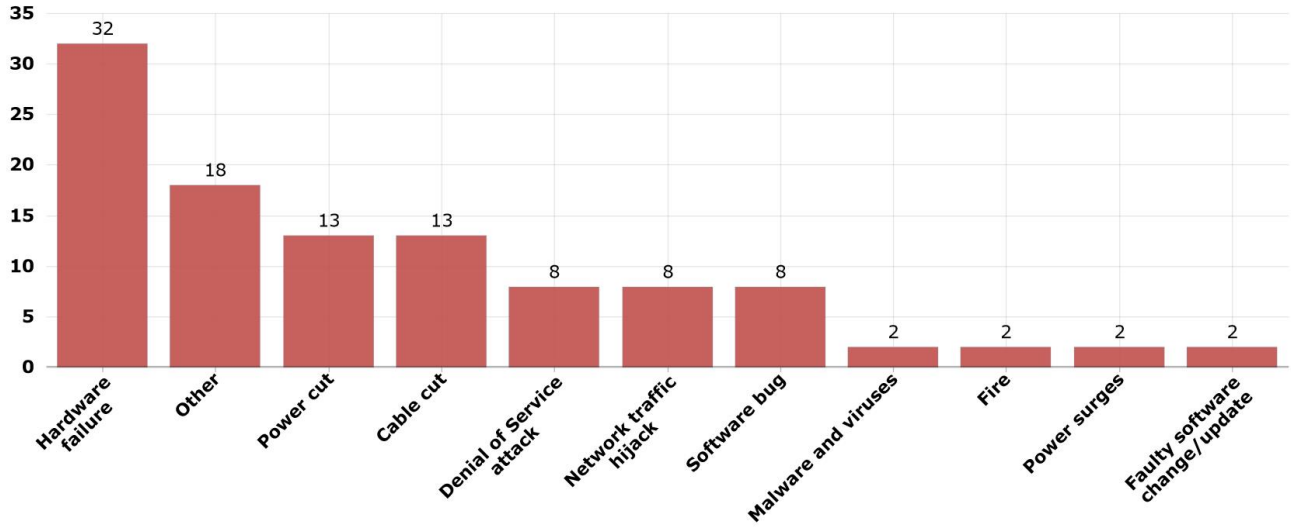

Figure 23: Detailed causes for fixed Internet (percentage).

4.3.2.3 Mobile Telephony

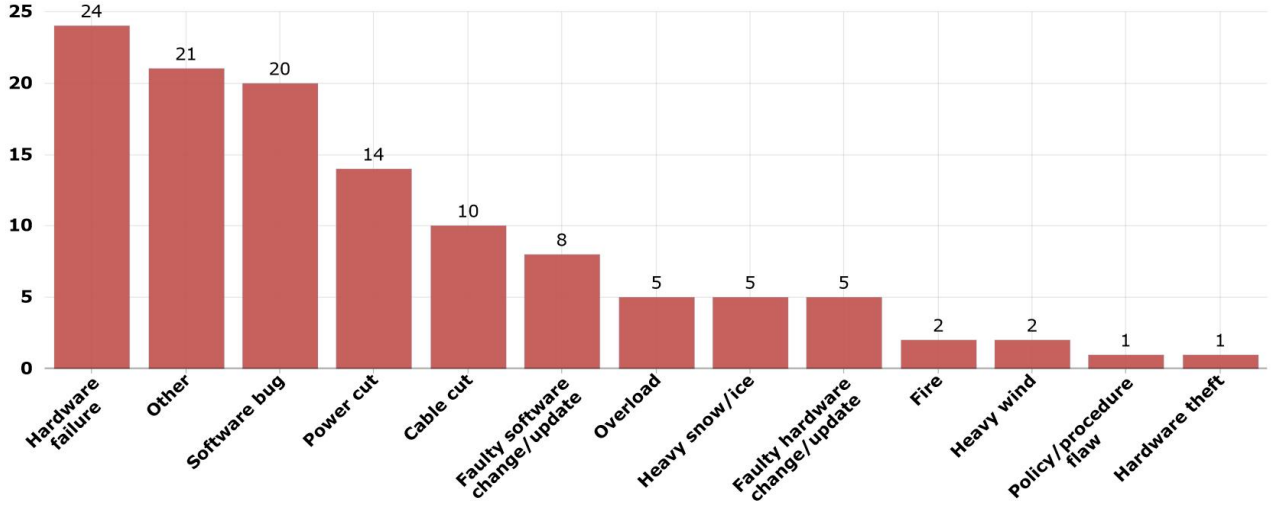

Figure 24: Detailed causes for mobile telephony (percentage).

4.3.2.4 Mobile Internet

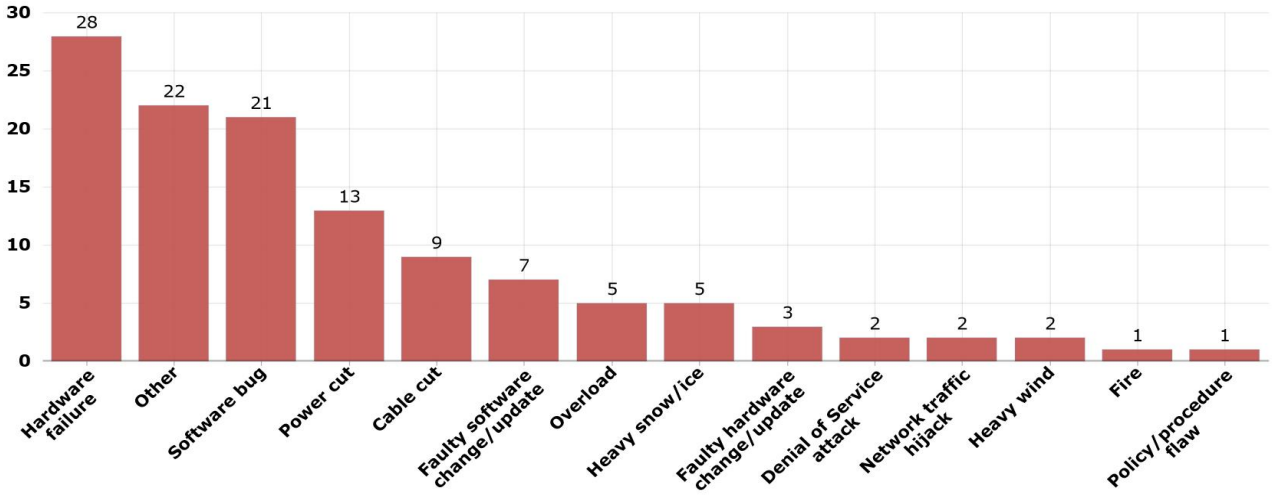

Figure 25: Detailed causes for mobile Internet (percentage).

4.3.2.5 Other services

More than 50% of the incidents affecting other services, except the four main services, were caused by Hardware failures, Power cuts and Cable cuts, with 26%, 16% and 12% respectively. Cable cuts and Software bugs had the same percentage in this case.

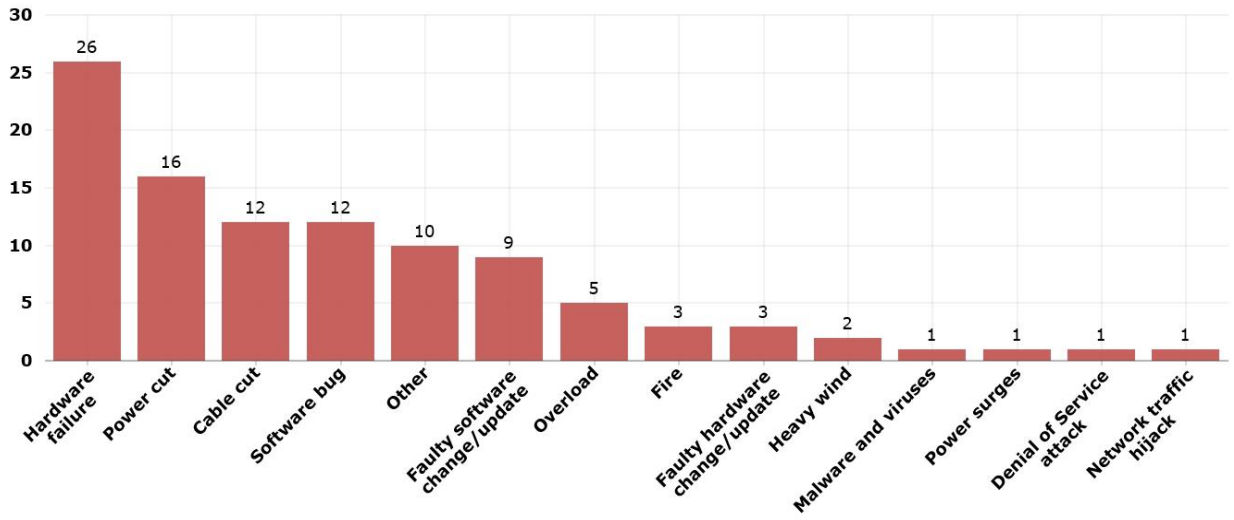

Figure 26: Detailed causes for other services (percentage).

4.3.2.6 Average number of user connections affected per detailed cause category

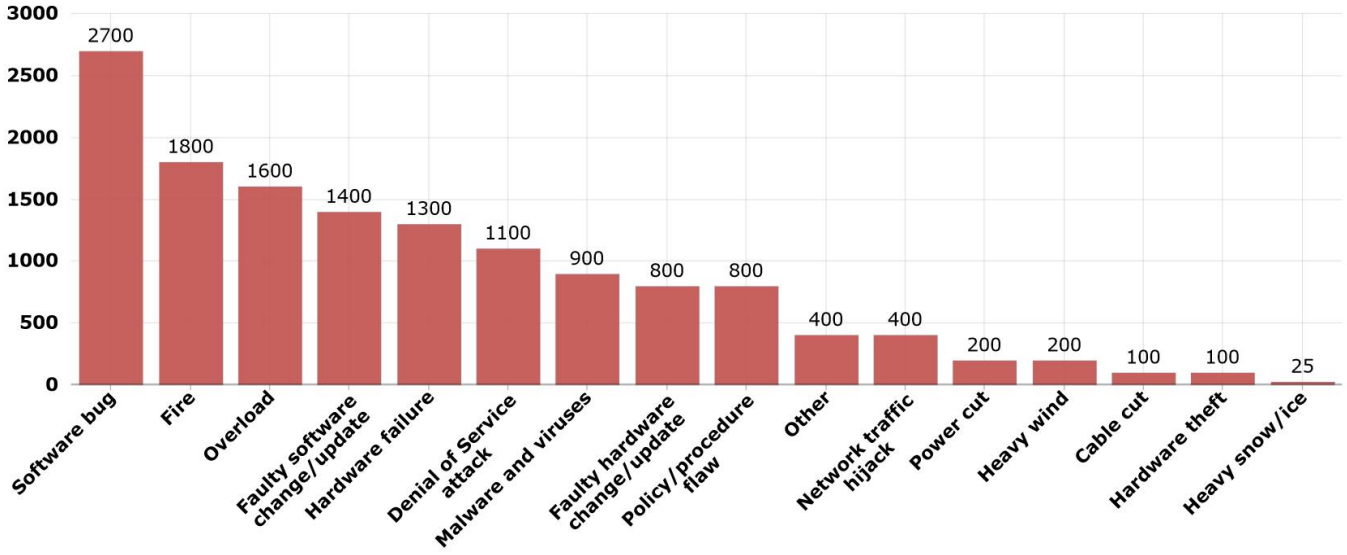

Figure 27: Average number of user connections affected per detailed cause (hours).

4.3.3 Average duration of incidents per detailed cause category

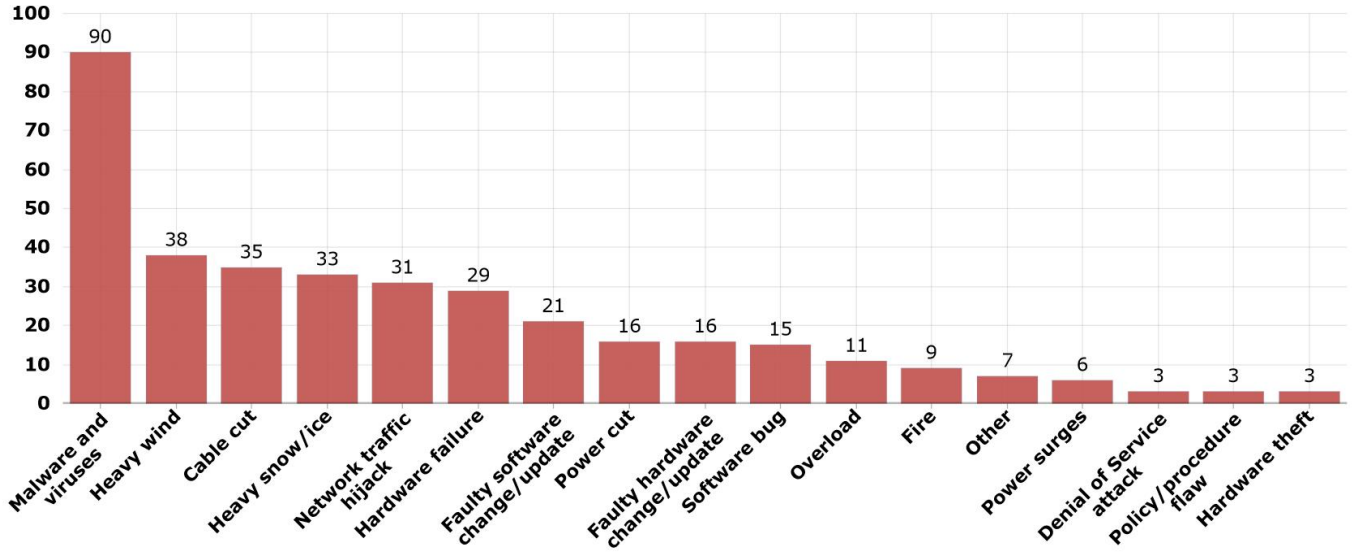

Figure 28: Average duration of incidents per detailed cause category (hours).

4.3.4 User hours lost per detailed cause

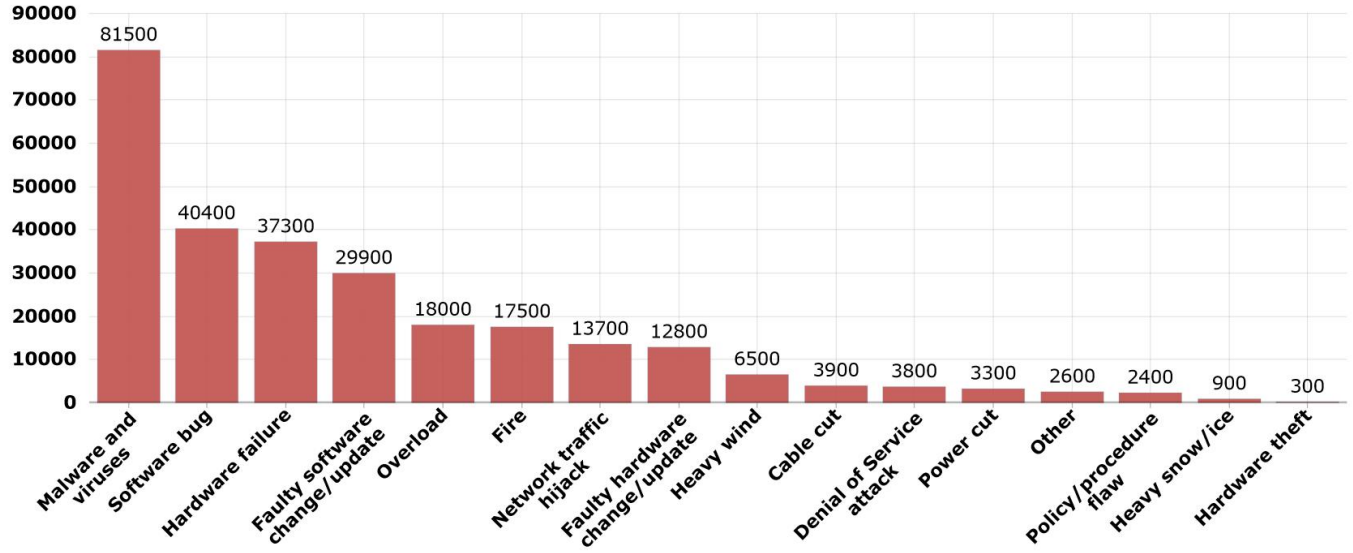

Figure 29: User hours lost per detailed cause (hours).

An attempt at malware infection coming from a malicious action caused outage on fixed internet, fixed telephony, IPTV and DNS services for more than three days: (duration: days, connections: thousands, cause: Malicious action): A worldwide attack of a botnet attempted to infect maintenance interfaces of customer premises equipments with a malware. This attempt failed but caused a restricted access to electronic communications services. Provider mitigated this attack by implementing filtering measures in order to prevent further malicious attacks of this kind. Provider updated remotely the firmware in customer premises equipments (CPEs) and asked affected customers to disconnect CPEs from the power supply, and switch them on in order to finalise the update.

4.4 Analysis of arising cybersecurity trends/issues

For the reporting years 2012-2016, annual reports included in total 614 incident reports with 425 incident reports (69% of total incident reports) coming from system failures. On the other side, only 34 incident reports (5,5% of total incident reports) are a result of malicious actions. Approximately 76,5% of the malicious actions consist of cybersecurity attacks, namely Denial of Service attacks, malware / viruses and network hijacks, while the rest concern deliberate damages to physical infrastructure. During all the reporting years only 3 reported incidents were caused by malware. The proportion of malicious actions (especially cybersecurity related incidents) among the total number of incidents reported remains low due to the focus of the current regulation on the "availability" of services and networks, meaning mostly disruptions.

Considering the above we may conclude that malicious actions (especially cyber-attacks) are not necessarily focused on creating disruptions in Telecom, a conclusion that has already been presented in previous versions of this report. But, what we also can conclude is that, under the current form of Art. 13a within the Electronic Telecommunication Framework Directive, we do not have a very good overview of the cyber-attacks affecting the telecommunication infrastructure in EU. Although the present incident reporting scheme currently does not allow us to see the whole picture, external sources (public reports, statistics, online articles etc.) on Telecom incidents confirm an increasing trend as regards cyber-attacks. According to PwC's Global State of Information Security, 2016 [18], IT security incidents in the telecom sector increased 45% in 2015 compared to the year before.

However, for the first time in the six year analysis of annual incident reports we see malware as the detailed cause, with the most impact in terms of average duration and user hours lost. Interestingly, the same terms of impact were trending in last year's report but for root cause of malicious actions. It is of high importance to underline that cybersecurity related detailed causes appeared to result the most user hours lost for both years of 2015 and 2016.

According to Gartner, 8.4 billion connected things will be in use worldwide in 2017, an increase of 31 percent compared to 2016, and it is estimated that connected devices will reach 20.4 billion by 2020. The increasing spread of digital technologies, the burst of emerging technologies, such as Software Defined Networks (SDN), Network Function Virtualization (NFV) and IoT can lead to a growth in the number of cybersecurity attacks. The DSM strategy [19] recognizes the importance of the paradigm shifts the digital sector is undergoing and aims to tackle regulatory fragmentation and build a more effective regulatory institutional framework.

In the light of the DSM strategy for Europe and based on the objective of ensuring a high-level of security of networks and services in telecommunication, the European Commission has drafted a new Proposal for the European Electronic Communications Code (EECC)[20]. The new proposal of EECC will extend the incident reporting mechanism and will cover the entire threat landscape of telecommunications in EU by introducing:

a) a comprehensive definition of security in telecom. The revised definition of security puts in scope, apart from the availability, also the confidentiality, integrity and authenticity of services and networks.

[18] See http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html
[19] See https://ec.europa.eu/digital-single-market/en/news/digital-single-market-commission-calls-swift-adoption-key-proposals-and-maps-out-challenges
[20] See http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52016PC0590&from=EN

b) a wider scope to include also number-independent interpersonal communications services,also called Over-The-Top (OTTs), and

c) new parameters for measuring significance of incidents. Parameters to determine significant incidents, expand from user connections affected by the breach and duration of the breach, also to geographical spread, the extent to which the functioning service is disrupted, and to societal and economic impact.

The new EECC is expected to be adopted in 2018.

Additionally, regulations with substantial improvements on security that facilitate the coverage of the entire spectrum of the rapidly changing digital society have been adopted recently.

The NIS Directive and GDPR will affect the regulatory obligations in the Telecom sector, requiring new procedures and more dimensions of information security compliance. The NIS Directive will introduce new requirements in the area of security measures and incident notification for Digital Service Providers (DSP) and Essential Services Operators (ESO). The NIS Directive and the new EECC converge on the incident reporting as many cloud services of DSPs and digital infrastructure of ESOs share common resources coming from telecom providers.

The ePrivacy Directive and the GDPR, which provide together the legal framework to ensure digital privacy for EU citizens, will also affect the electronic communications sector.

The harmonisation level between all relevant security related EU level regulations has certainly increased in recent years. The providers will have to consider all these three legal acts when building their cyber security and compliance policies.

4.5 Assets affected

Also this year we received reports from NRAs about which components or assets of the electronic communications networks were affected by the incidents. This provides some more information about the nature of the outages and what assets of the infrastructure that were primarily involved in them.

4.5.1 Assets affected overall

In 2016, mobile base stations and controllers, mobile switches and switches and routers were the assets most affected by incidents. For more details on the timeline of assets affected please see Annex D.

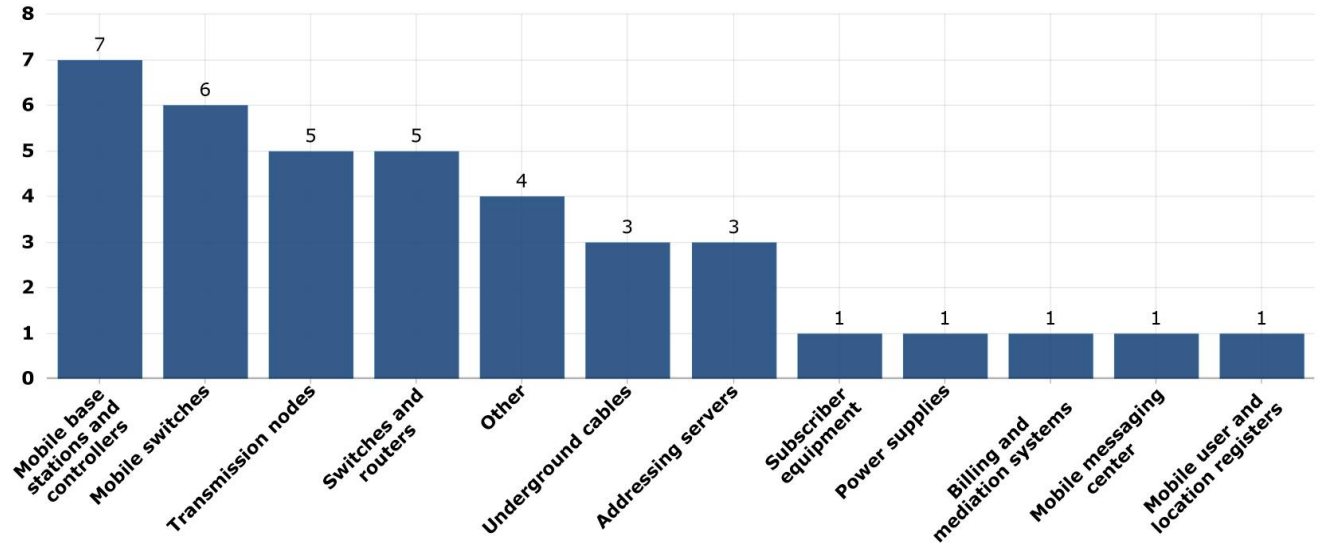

Figure 30: Assets affected by the incidents (percentage).

4.5.2 Affected assets in system failures

As for all previous reporting years, system failures (or technical failures), was the most common root cause category in 2016. In these system failures, the most common assets that failed were mobile switches, switches and routers and other uncategorised assets. Also the previous year mobile switches, and switches and routers were the most common assets to fail in this root cause category.

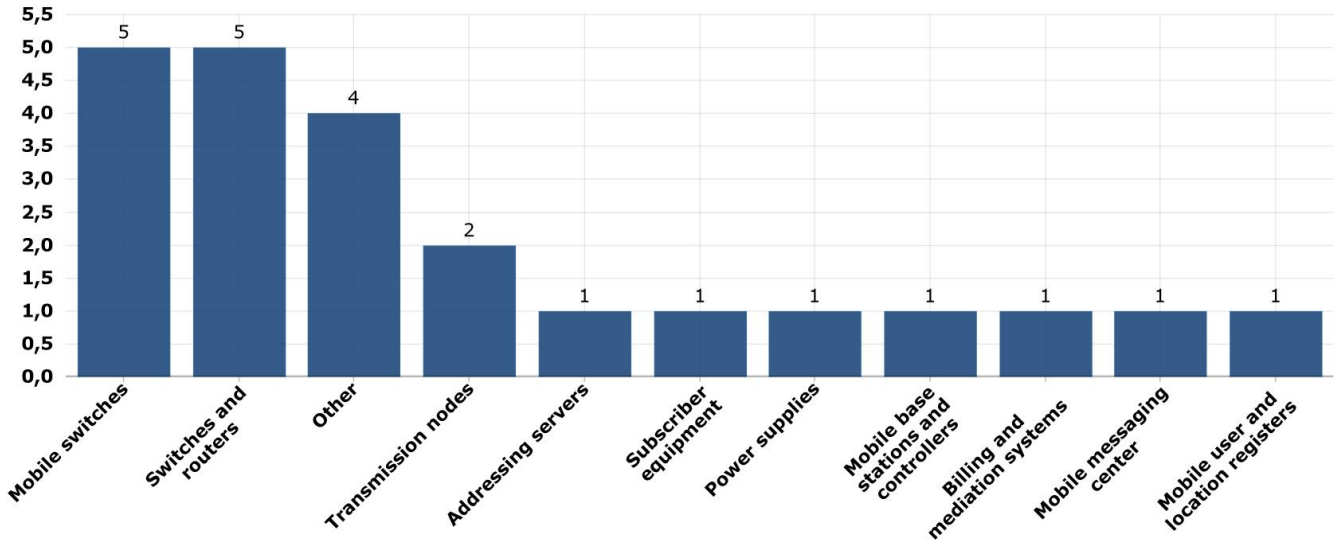

Figure 31: Assets affected by system failures (percentages).

5. Conclusions

In this report ENISA summarized and analysed the outage incidents that were sent by the National Regulatory Authorities (NRAs) from member states and EFTA countries to ENISA and the European Commission in 2017 concerning incidents in 2016, as mandated by Article 13a of the Framework Directive (2009/140/EC)[8].

In 2016, analysing the **158 significant** incidents reported to ENISA and the EU Commission, the following conclusions can be drawn, first looking at services and network assets affected and then at the causes of the incidents.

- **Mobile internet remains the most affected service:** In 2016 most incidents affected mobile internet (48% of all reported incidents). Mobile internet and mobile telephony were the predominant affected services in the previous years also, except for 2014 where fixed telephony was the most affected.
- **Mobile services outages have affected in average more users than other:** Incidents affecting mobile Internet or mobile telephony affected most users (around 1.3 million users and 1.1 million users respectively per incident). On average 14% of national user base was affected by incidents on mobile internet services.
- **System failures are the dominant root cause of incidents affecting availability:** Most incidents were caused by system failures or technical failures (more than 70 % of the incidents) as a root cause. This has been the dominant root cause for all the reporting years so far. System failures was also the most common root cause for all the main services when looking at them separately and also the main root cause for all services, both classic and other services. In the system failures category, software bugs and hardware failures were the most common causes. The assets most often affected by system failures were switches and routers, and mobile base stations.
- **Third party failures continue to affect a considerable part of the total number of incidents**: 21.5% of all incidents were caused by third party failures, a significant increase from last year (15,2%). Third party failure incidents are of high importance as they represent incidents completely out of the control of the provider. Therefore, such kind of incidents are complex and difficult to tackle. System failures followed by human errors were the most common cause category for third party failures also.
- **Malware is causing increasingly long lasting incidents:** In last year's analysis incidents caused by malicious actions (e.g. malware and DDoS), although we didn't have too many of them, had most impact in terms of duration. This year, a single incident of malware caused the most impact in terms of average duration and user-hours lost. This change is strongly related to large DDoS attacks of last year. Last 2 years of reporting have certainly showed that cyber-attacks can also aim at creating long lasting disruptions in Telecom.

As the legal landscape affecting the Telecom industry has undergone recent updates, it is our opinion that the new improvements will certainly contribute to a more secured and harmonised telecommunications environment across Europe[21]. Covering a wider range of threats and types of incidents that can affect telecommunications can be key in better understanding the challenges within the sector, and dealing with their main causes. The electronic telecommunication industry has reached a certain level of maturity among other IT related sectors, but the threat level is still high, maintained by the importance of the sector, as an infrastructure provider for the digital economy.

[21] https://www.dotmagazine.online/issues/connecting-the-world-whats-it-worth/challenges-in-eu-telecom-security

ENISA, in the context of the Article 13a Expert Group[10], will continue discussing specific incidents in more detail with the NRAs, and if needed, discuss and agree on mitigating measures. ENISA will also continue to give support to other sectors that are developing network and information security incident reporting schemes.

ENISA would like to take this opportunity to thank the NRAs, Ministries and the European Commission for a fruitful collaboration and we look forward to leveraging this kind of reporting to further improve the security and resilience of the electronic communications sector in the EU and more generally for supervision of security also in other critical sectors.

References

Related ENISA papers

- ENISA's reports about the 2011, 2012, 2013, 2014, 2015 incidents, reported under Article 13a: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports
- ENISA's study "Impact evaluation on the implementation of Article 13a incident reporting scheme within EU": https://www.enisa.europa.eu/publications/impact-evaluation-article13a
- The Article 13a Expert Group technical guidelines on incident reporting, security measures, and threats and assets respectively: https://resilience.enisa.europa.eu/article-13
- ENISA's study 2013 on Power Supply Dependencies in the Electronic Communications Sector: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/power-supply-dependencies
- ENISA's study 2013 on National Roaming for Resilience: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/national-roaming-for-resilience
- ENISA's study and guide 2014 to Electronic Communications Providers when procuring ICT products and outsourced services for core operations: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/requirements-ecomms-vendors
- ENISA's study 2014 on information sharing systems for announcing civil works in order to protect underground communications infrastructure from cable cuts: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/protection-of-underground-infrastructure
- ENISA's whitepaper from 2012 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 6 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

EU legislation

- Article 13a of the Framework directive of the EU regulatory framework for electronic communications: http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32009L0140
- The EU regulatory framework for electronic communications (incorporating the Framework Directive including Article 13a): https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Copy%20of%20Regulatory%20Framework%20for%20Electonic%20Communications%202013%20NO%20CROPS.pdf
- The NIS directive, that also contains incident notification provisions for essential (ESPs) and digital service providers (DSPs): http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

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

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

TP-AD-17-001-EN-N

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

ISBN: 978-92-9204-222-6
DOI: 10.2824/21700