Annual Report Telecom Security Incidents 2017

AUGUST 2018

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 the EU and EFTA countries. 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: 978-92-9204-257-8, DOI: 10.2824/017314

Table of Contents

Executive Summary

Electronic communication providers in the EU have to notify significant security incidents to the national telecom regulatory authorities (NRAs) in each EU member state. Every year the NRAs report summaries about a selection of these notified incidents, the most significant incidents, based on a set of agreed thresholds. This document, the Annual Report on Telecom Security Incidents 2017, aggregates the incident reported in 2017, and provides a single EU-wide overview of telecom security incidents in the EU.

Mandatory breach reporting has been part of the EU's telecom regulatory framework since the 2009 reform of the telecom package: Article 13a of the Framework directive (2009/140/EC) came into force in 2011. The breach reporting in Article 13a focuses on security incidents causing significant outages. The Commission recently proposed an update of the telecom rules. The new breach reporting requirements in Article 40 of the Electronic Communications Code[1] [2] have a broader scope, including not only incidents causing outages, but also confidentiality breaches. Security breach reporting is also mandatory for trust service providers in the EU (under Article 19 of the EIDAS regulation), for Operators of Essential Services in the EU (under Article 14 of the NIS directive) and for Digital Service Providers (under Article 16 of the NIS directive) in the EU.

Key statistics from the 2017 reporting

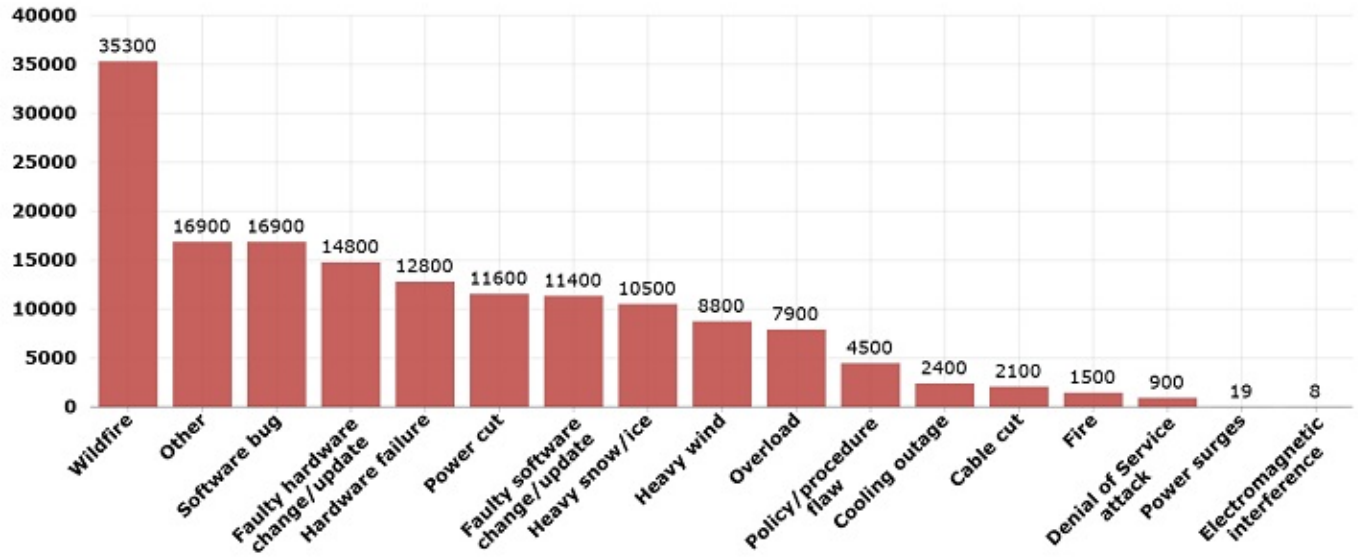
This year's annual incident report covers 169 incidents, reported by the NRAs across the EU. The reports come from the 28 EU countries and additionally 2 EFTA countries participated. 6 EU countries reported no incidents with significant impact, submitting so-called empty reports. We highlight some of the statistics:

- **Most incidents have an impact on mobile telephony and internet:** In 2017 most incidents affected mobile telephony (51% of all reported incidents). Mobile internet and mobile telephony were the predominant affected services in the previous years also, except for 2014 when fixed telephony was the most affected.
- **Incidents with mobile telephony and mobile internet impact, on average, most users:** Incidents affecting mobile internet or mobile telephony affected most users, on average around half a million users per reported incident, around 8% of the national user base. Over the past years we observe is a downward trend, meaning that the average size of reported incidents is decreasing. This could be due to the fact that many EU countries are adopting lower reporting thresholds.
- **System failures are the dominant root cause of reported incidents:** Most incidents reported were caused by system failures (62% of the incidents) as a root cause. Often these are hardware failures or software bugs.

[1] http://europa.eu/rapid/press-release_IP-18-4070_en.htm
[2] http://www.consilium.europa.eu/en/policies/electronic-communications-code/

- **Human errors affect (on average) a high number of user connections:** In 2017 human errors was the root cause category involving most users affected per incident (around 1.2 million user connections on average).

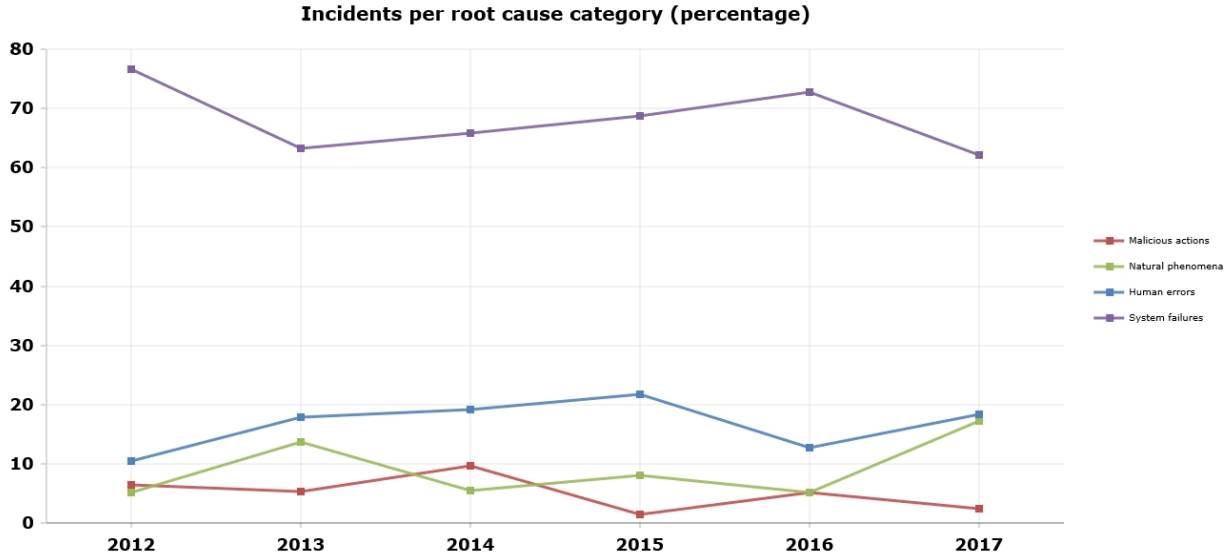
- **Incidents caused by malicious actions are rare:** Only a small percentage of reported incidents (2.5% in 2017) was categorized as caused by malicious actions. This percentage reduced by half compared to the previous year (5.1% in 2016).
- **System failures are the dominant root cause:** In 2017 most incidents were caused by system failures, i.e. more than 62 % had system failure as a root cause. This is in line with previous years (always between 60% and 80%). In the category system failures, software bugs and hardware failures were the most common causes. The assets failing in these cases are most often switches, routers, and power supplies.
- **Natural phenomena are causing more incidents:** In 2017 a larger number of incidents (18%) were caused by natural phenomena, such as heavy snow/ice, storms and wild fires. This is significantly higher than 2016, 2015, and 2014 when natural phenomena accounted for around 5% of the incidents. Natural phenomena also cause the highest number of user hours lost, on average, per incident, with 56800 user hours. Natural phenomena will continue to be a concern for telecom providers across the EU, with extreme weather becoming more common due to climate change.
- **A fifth of the incidents are third party failures**: Almost a fifth of the incidents (18%) are third party failures. This is similar to last year (22%). Third party failure incidents are interesting for NRAs to investigate further because often third-party failures involve other sectors, and are complex and costly to tackle for providers. Most of the incidents categorized as a third party failures are also categorized as caused by natural phenomena. A common incident scenario is when a natural disaster, like a storm or wildfire, disrupts the power grid infrastructure, which then impacts the mobile network infrastructure.
- **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 (9% and 8% respectively).
- **Wild fires cause, on average, most impact in user hours:** A good measure for the total impact is to multiply the number of users and the number of hours outage: this gives a total number of user hours. The diagram below shows the total number of user hours lost, per detailed cause, for the incidents reported in 2017.



Trends in 7 years of reporting

Mandatory security incident reporting was introduced in the 2009 reform which came into force in 2011. ENISA has been collecting and aggregating incident reports since 2012. Looking back at the 7 years of annual incident reports, we can observe a number of multi-annual trends.

- **System failures dominate:** Every year system failures are the most common root cause of reported incident, responsible for about 60-70% of the major outages.
- **Natural phenomena trending upwards:** There is an upward trend in the impact of natural phenomena on telecom services. Heavy storms, heavy floods, or wildfires cause by extreme drought, can severely impact the telecom infrastructure. Extreme weather is likely to increase due to climate change and this means that natural phenomena will continue to be a concern for the EU telecom sector.



Follow-up by NRAs and ENISA

The NRAs are responsible for supervision the security telecom sector in each EU member state. ENISA supports the NRAs with common guidelines and collecting good practices. Incident reporting is a key pillar of this supervision. Article 13a and incident reporting are key in allowing the NRAs to understand trends and to work with the sector to address issues. This positive impact was confirmed also in an independent impact assessment analysing the impact of EU legislation on telecom security[3].

As a follow up to the incident reporting, at the EU level, ENISA works with the NRAs and the private sector to analyse and address EU-wide issues and trends:

- Power cuts are a common cause of outages. In 2013 ENISA analysed power supply dependencies[4], and issued recommendations regarding the sector's ability to withstand and act efficiently after power cuts.
- ENISA published an overview of good practices regarding to national roaming for increased resilience in mobile networks[5]. A number of EU Member States have implemented such national roaming frameworks.

[3] See https://www.enisa.europa.eu/publications/impact-evaluation-article13a
[4] See https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/power-supply-dependencies/
[5] 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

- Issues with ICT equipment were a major source of outages in 2012 and 2013. In 2014, ENISA published recommendations for providers[6] about how to address security requirements when dealing with ICT equipment vendors and suppliers of outsourced services for core operations.
- Cable cuts (due to civil works) were a prominent cause of incidents in the 2012 and 2013 annual incident reporting. In 2014, ENISA worked with NRAs to publish an overview of good practices and frameworks to reduce underground cable cuts[7].
- In 2016, ENISA assessed, EU-wide, which security measures are implemented by telecom providers[8].
- In 2018, ENISA published an EU state of play report on legacy protocols used for interconnections.[9]

[6] See https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/requirements-ecomms-vendors
[7] See https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/protection-of-underground-infrastructure
[8] See https://www.enisa.europa.eu/publications/security-measures
[9] See https://www.enisa.europa.eu/news/enisa-news/legacy-technologies-as-a-threat-to-eu2019s-telecommunications-infrastructure

1. Introduction

Electronic communication providers in the EU have to notify security incidents, with a *significant* impact on the continuity of electronic communication services, to the national telecom regulatory authorities (NRAs) in each EU member state. Every year the NRAs report a summary to ENISA, covering a selection of these incidents, i.e. the most significant incidents, based on a set of agreed EU-wide thresholds. This document, the Annual Security Incidents Report 2017, aggregates the incident reports reported in 2017, and gives a single EU-wide overview of telecom security incidents in the EU.

This is the 7th time ENISA publishes an annual incident report for the telecom sector. ENISA started publishing such annual reports in 2012. Mandatory breach reporting has been part of the EU's telecom regulatory framework since the 2009 reform of the telecom package: Article 13a of the Framework directive (2009/140/EC) came into force in 2011. The breach reporting in Article 13a focuses on security incidents causing significant outages. For example, consider an attack in which attackers wiretap undersea cables; if this attack causes no outages, then the security incident does not fall under the breach reporting requirements of Article 13a. The Commission recently proposed an update of the telecom rules. The new breach reporting requirements in (Article 40 of) the Electronic Communications Code[10] have a broader scope, including not only incidents causing outages, but also significant confidentiality breaches for example.

Note that this document does *not* contain details about individual countries or individual incident reports and it does not contain any references to regions, countries or specific providers.

This document is structured as follows: Section 2 and Section 3 briefly summarize Article 13a and the technical details of the implementation of the annual summary reporting, as agreed by the experts in the Article 13a Expert Group which involves different NRAs from different EU Member States and EFTA countries. Section 4 contains the statistical analysis of the incidents from 2017 and contains examples of incidents and Section 5 contains the conclusions.

[10] http://www.consilium.europa.eu/en/policies/electronic-communications-code/

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

The reform of the EU regulatory framework for electronic communications[Error! Bookmark not defined.], which was adopted in 2009 and transposed by most EU countries in 2011, added Article 13a to the Framework Directive[Error! Bookmark not defined.]. 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 that:

- 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 2017 that have been reported to ENISA (the black dashed arrow).

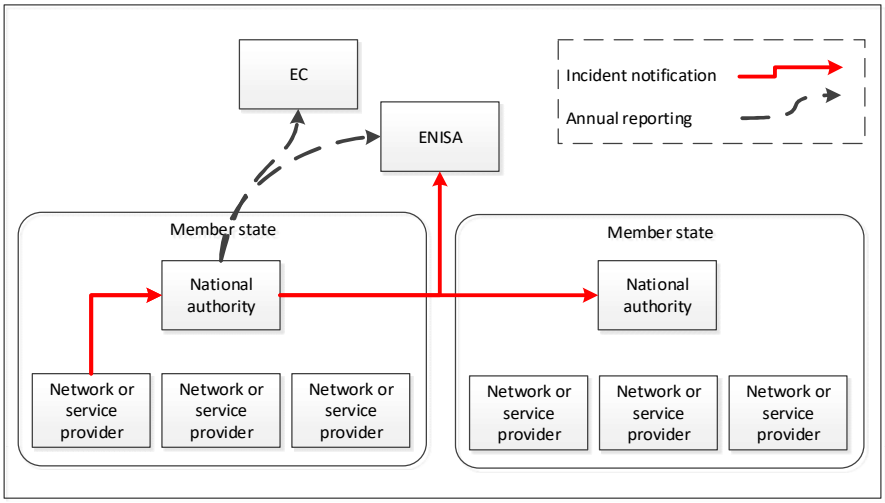


Figure 1: Incident reporting in Article 13a

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 ended in December 2015. In this context, ENISA along with the Article 13a Expert Group submitted an opinion on 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.

[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

3. Article 13a Expert Group and Annual Incident Reporting Procedure

3.1.1 Article 13a Expert group

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 the following years, during these meetings, a group of experts from NRAs, now referred to as the Article 13a Expert Group, reached agreement on three non-binding technical guidelines:

- Technical Guideline on Incident Reporting[13]
- Technical Guideline on Security Measures[14]
- Technical Guideline on Threats and Assets[15]

The Article 13a Expert Group continues to meet 3 times per 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.

3.1.2 Annual summary reporting by NRAs to ENISA

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 replaced 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.

3.1.3 Services and incidents in scope of reporting

There are four main services (aka classic services) in scope:

- Fixed telephony
- Mobile telephony
- Fixed Internet access
- Mobile Internet access

Additionally NRAs can report about other services, such as SMS, MMS, Satellite TV, International roaming, RADIO broadcasting, TV broadcasting , Cable TV, IPTV, Video on demand, Public WIFI, Web based voice services, Web-based messaging services, and Public email services.

[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

Providers are required to notify security incidents to NRAs, if there is a significant impact on the continuity of supply of electronic communications services. As mentioned, the mandatory reporting requirements in Article 13a focus on the continuity of the service.

3.1.4 Thresholds for annual summary reporting

To facilitate an efficient and effective process of annual summary reporting from NRAs to ENISA, the NRAs agreed on a set of EU wide thresholds, based on the duration of an incident and the relative number of customers affected.

Relative thresholds

The relative threshold 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 include incidents in 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 1: Threshold for annual summary reporting based on a combination of duration and the percentage of the national user base

Absolute thresholds

Complementing the relative threshold, there is an absolute threshold: Incidents should be included in annual summary reporting if the product of duration and number of user connections affected exceeds ***60 million user minutes, or 1 million user hours***.

3.1.5 Annual summary reporting template

The annual summary reporting template for annual summary reporting contains fields for the services affected, the number of customers affected and the duration of the incident.

The annual summary reporting template distinguishes 5 root cause 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 conjunction with one of the other four root cause categories.

Optionally the template allows NRAs to indicate:

- **Detailed causes** triggering the incident, either as “initial cause” or as “subsequent cause”, because incidents often involve a chain of events. For example, often a storm, leads to a power cut.
- **Assets affected** by the incident, 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.

4. Analysis of the incidents

In total, all 28 EU Member States and 2 EFTA countries participated in this process. Of these, 22 Member States and 2 EFTA countries reported in total 169 significant incidents and 6 countries reported there were no significant incidents. This is a small increase from the previous year where the same number of countries reported 158 significant incidents.

Figure 3: Countries involved in the annual summary reporting in 2017.

Examples of incidents

We give some specific examples of incidents to give an idea of the kind of incidents that are notified to NRAs and then included in the annual summary reporting to ENISA:

- ***A system failure caused a mobile internet outage for millions of users (duration: hours, connections: millions, cause: software bug):*** *A software bug occurred in the Internal system component Software Deployment Manager (SDM) leading to the degradation of user authorization for mobile data and mobile voice. As a result end users had difficulties to access mobile services, both voice and data. Also customers abroad were affected (roaming services). Mobile switches and mobile user registers were affected by this bug. The 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.*
- ***System failure caused disruption in, both mobile and fixed, telephony and internet services as well SMS/ MMS services, affecting millions of users (duration: hours, connections: millions, cause:*** *hardware failure): Outage of several network components used for delivering DSL in the subscriber access network resulted in the disruption of mobile and fixed telephony and internet access. The provider responded by raising the capacity of the remaining network components. A subsequent software upgrade resolved the issue completely.*
- ***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 premise equipments with malware. This attempt failed but the attack impacted a large number of fixed internet connections. The provider mitigated this attack by implementing filtering measures in order to prevent further attacks of this kind. Later the provider updated the firmware of the customer premises equipments (CPEs) and asked affected customers to disconnect their CPEs from the power supply, and switch them on again, in order to finalise the update.

The rest of this section contains statistical information.

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:

- 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 under the current telecom framework 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 this process of annual reporting. The new breach reporting requirements in (Article 40 of) the Electronic Communications Code[16] have a broader scope, including not only incidents causing outages, but also confidentiality breaches for example.

The scope of reporting includes major, or *significant,* incidents scoring above the agreed reporting thresholds (Table 1: Threshold for annual summary reporting based on a combination of duration and the percentage of the national user base

-). Smaller incidents are not reported at EU level, meaning that the view is skewed towards the larger incidents. Common incidents that get resolved quickly stay below the radar, so to speak.
- National reporting thresholds are different across the EU. Every country has a different size. Thresholds have also been adapted over the years. Many countries started with relatively high thresholds, lowering them later on. For instance there is an increase in the number of reported incidents. This does not mean, for instance, that the telecom sector is getting less secure, or that the total number of incidents is increasing. In fact, over the years we have seen more incidents getting reported which are on average smaller in size.

4.1 Impact of the incidents

First, we look at which services are impacted by the reported incidents.

4.1.1 Impact per service

For the 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.

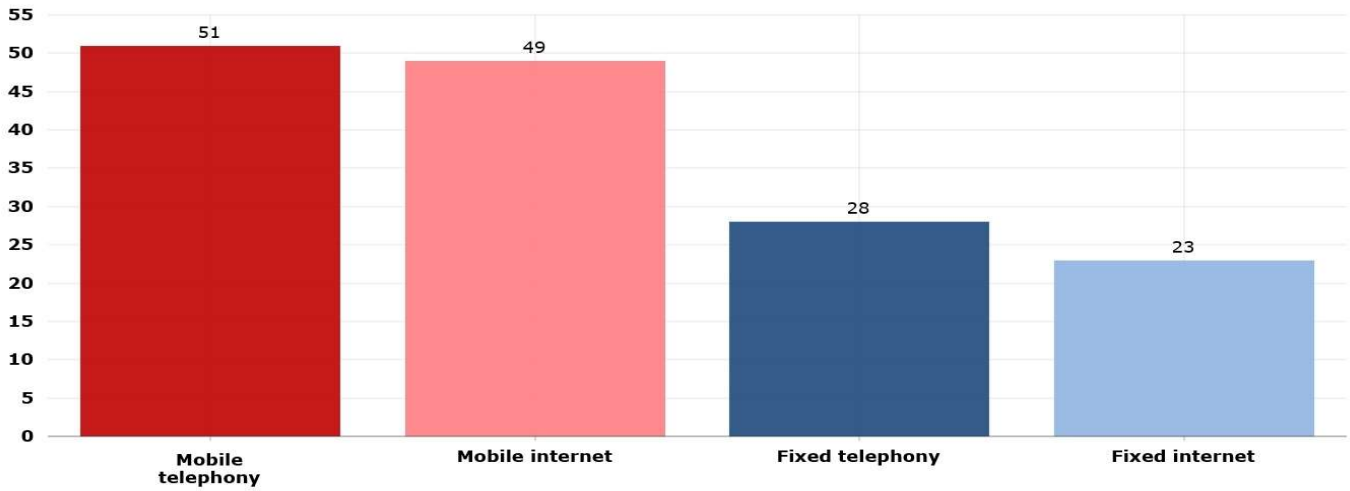


Figure 4: Impact on classic services (percentage)

[16] http://www.consilium.europa.eu/en/policies/electronic-communications-code/

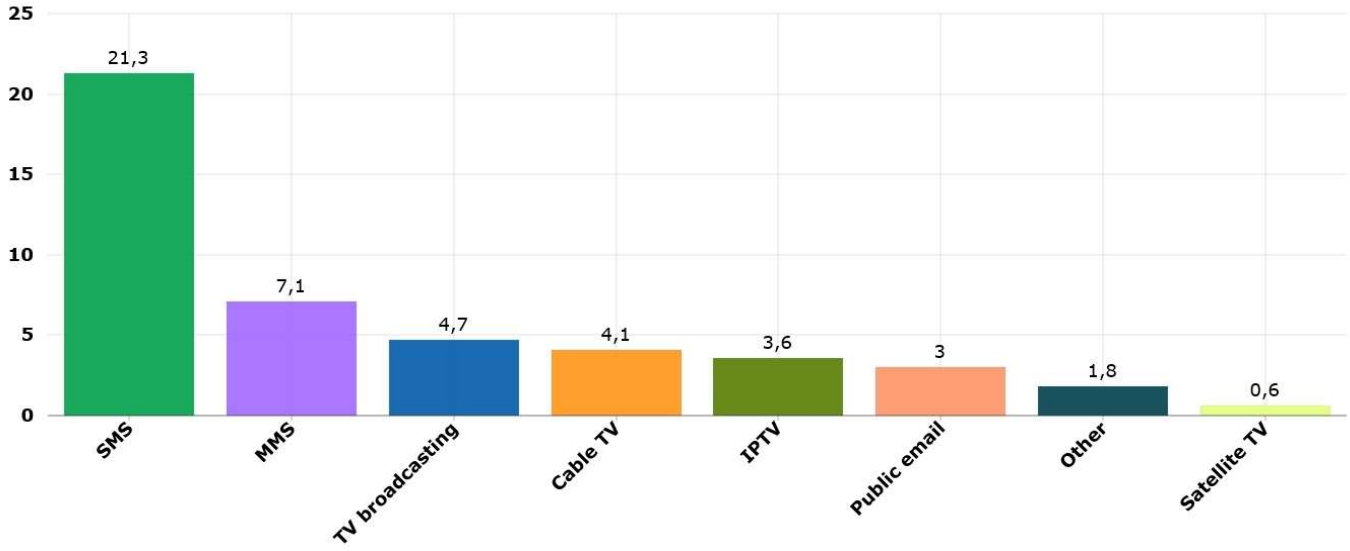


Figure 5: Impact on other services (percentage)

Note that each incident can have an impact on more than one service (which is why the percentages in the chart add up to more than 100 %).

4.1.2 Number of user connections affected

Mobile internet outages affect most user connections s, with an average of 600 thousand user connections affected per reported incident. Compared to the previous years this is a 50% decrease, which is significant.

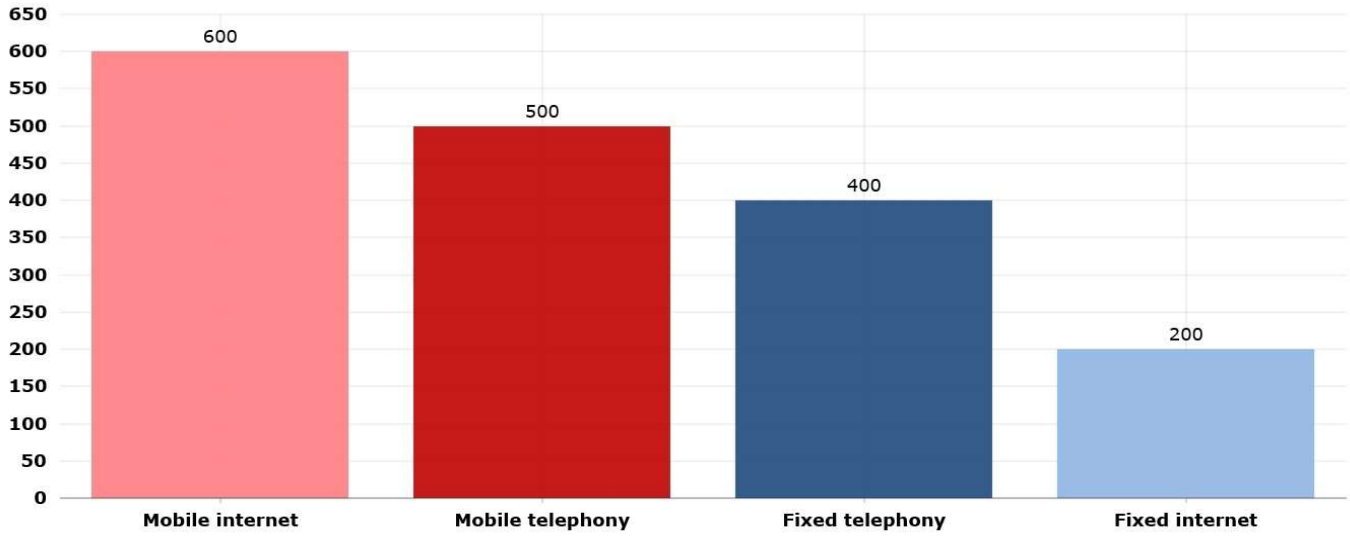


Figure 6: Average number of user connections affected per incident per classic service (1000s).

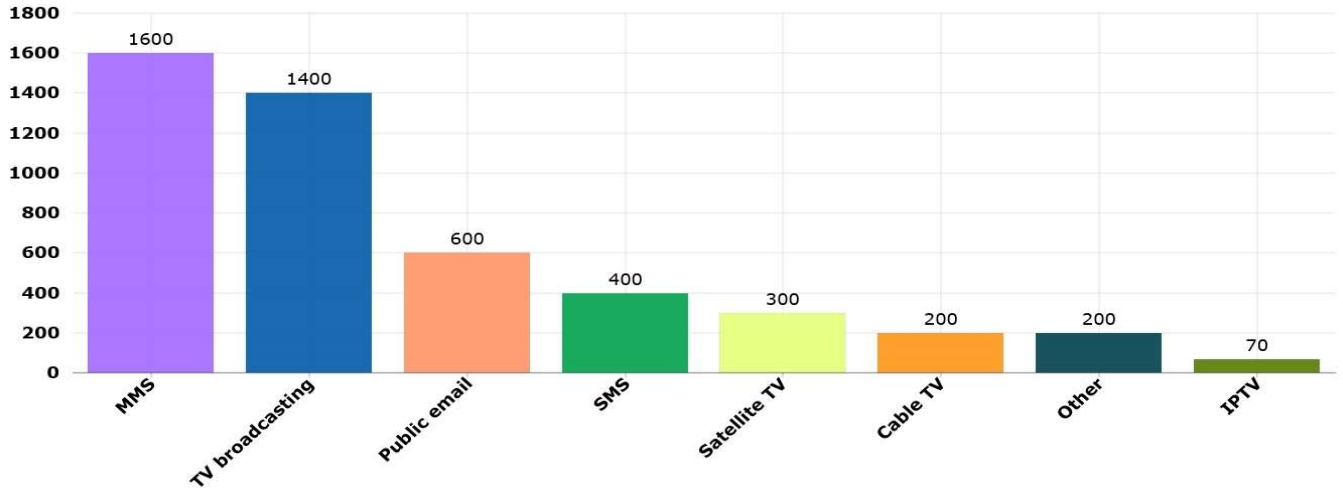


Figure 7: Average number of user connections affected (1000s) - other services

Note that the averages in these diagrams include both small and large countries. These EU-wide averages, are not necessarily representative for the size of incidents occurring nationally.

4.1.3 Percentage of the national user base affected

Mobile internet outages impact on average 8% of the national user base (a 14% decrease compared to 2016).

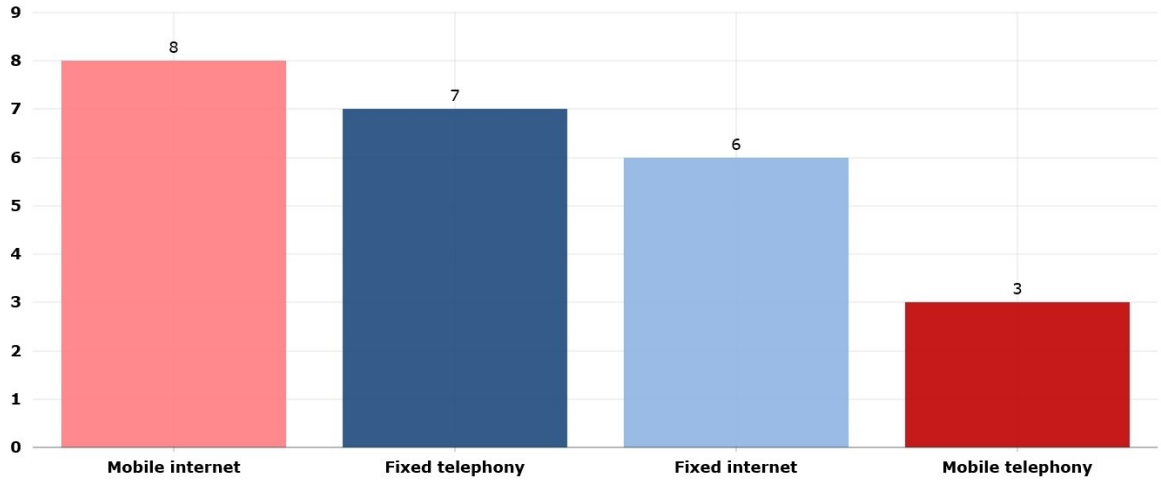


Figure 8: Percentage of national user base affected on average per incident per service.

4.1.4 Impact on emergency services

A third of the reported incidents had an impact on the reachability of emergency call-centres, i.e. 112.

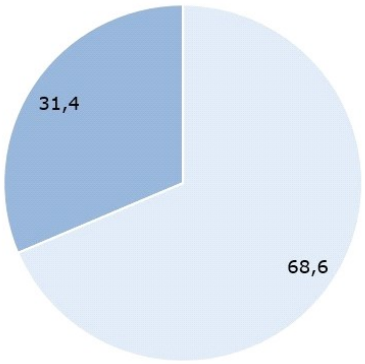


Figure 9: Impact on emergency calls.

4.1.5 Impact on interconnections

In 7 % of incidents reported there was an impact on interconnections between providers. Compared to 2016 this figure is stable.

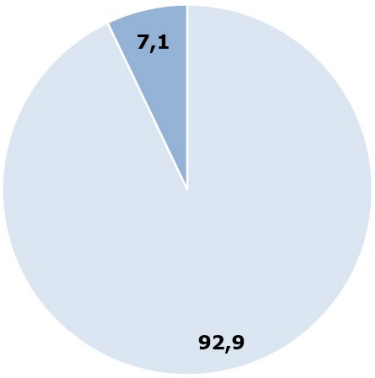


Figure 10: Impact on interconnections (percentage)

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, 62% of the reported incidents were caused by system failures or technical failures. 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 (18,3% of the reported incidents), a small increase compared with previous years. Natural phenomena as expected due to the wildfires consist of 17%.

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

4.2.2 Third party failures

Around 18% of the incidents reported were categorized as third party failures, a slight decrease compared to the previous year (22.5%).

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 the services separately. As in 2016, also in 2017, 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. Wildfires caused a significant increase in the number of incidents categorized under natural phenomena.

4.2.3.1 Fixed Telephony

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

4.2.3.2 Fixed Internet

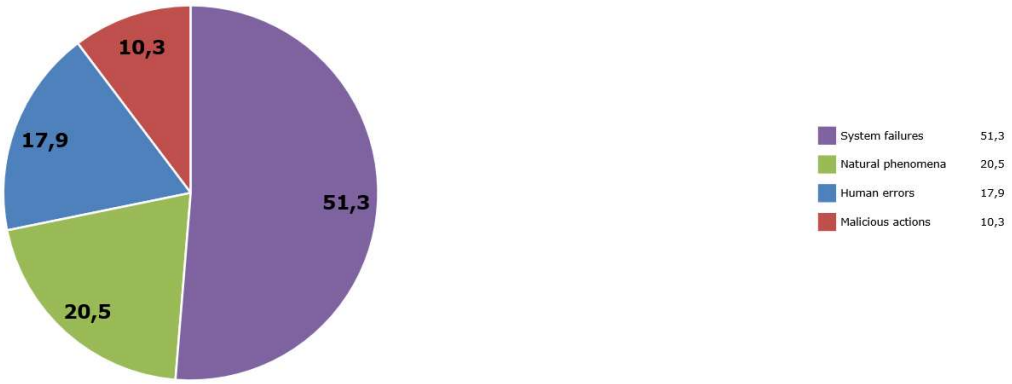


Figure 14: Root cause categories for fixed Internet (percentage).

4.2.3.3 Mobile telephony

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

4.2.3.4 Mobile internet

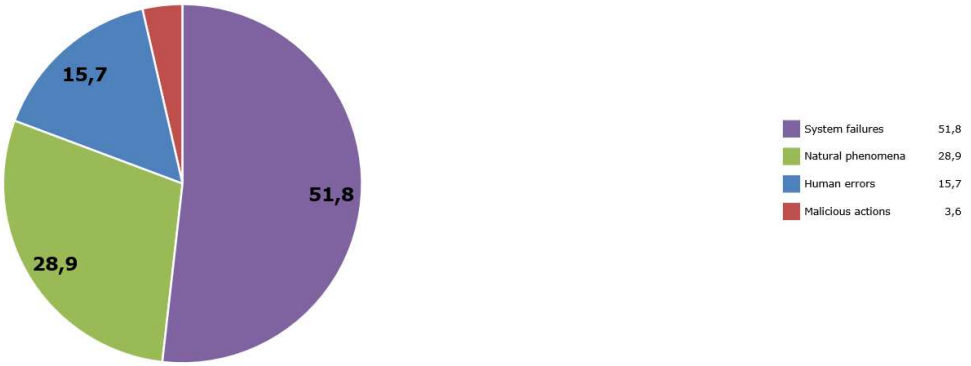


Figure 16: Root cause categories for mobile Internet (percentage).

4.2.3.5 Other services

System failures is also the main root cause for the other services besides the classic services, with a percentage of approximately 53%.

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

4.2.4 Average number of user connections affected per root cause category

This year, human errors affected most user connections, on average about 1.2 million user connections per incident, which is a significant increase, compared to the previous year. A significant decrease was noted on malicious actions

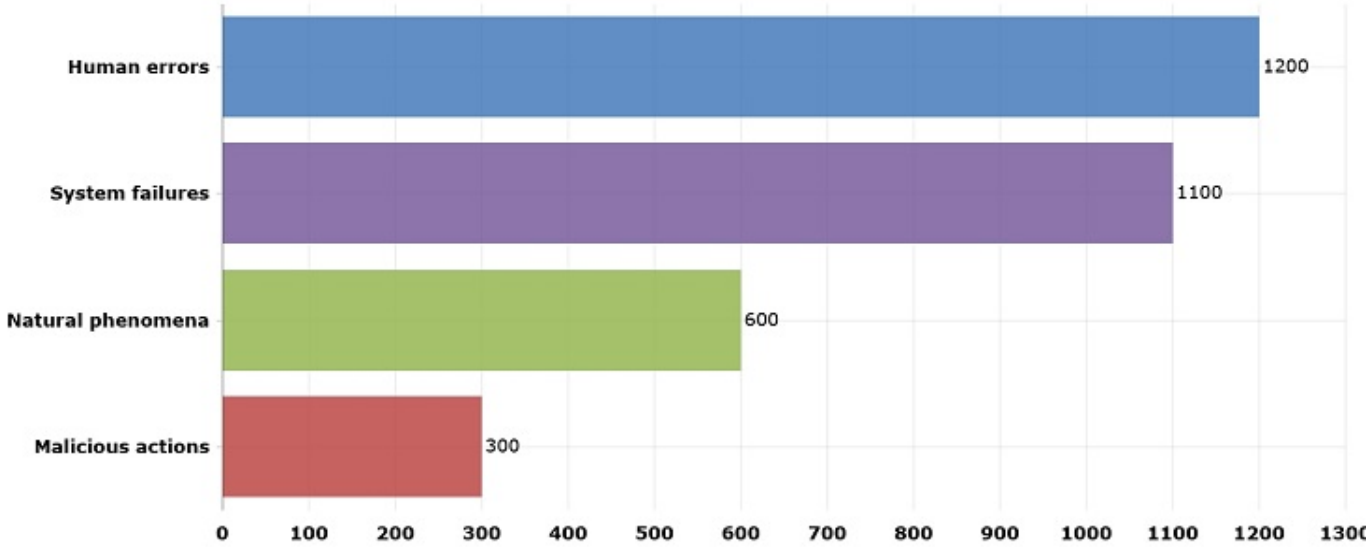


Figure 18: Average number of user connections affected per incident per root cause (1000s)

4.2.5 Average duration of incidents per root cause category

The reported incidents caused by natural phenomena had by far the longest recovery time on average per incident with a tremendous increase compared to last year. However, this extraordinary result is an exception due to the last year's wildfires.

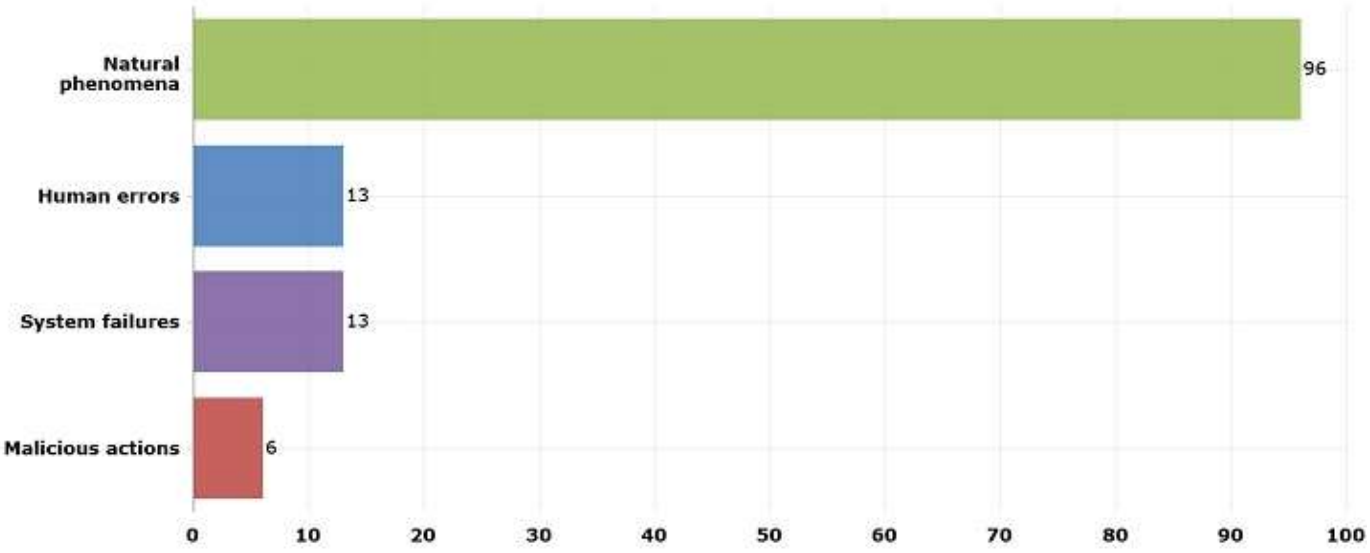


Figure 19: Average duration of incidents per root cause category (hours).

4.2.6 User hours lost per root cause category

Natural phenomena also cause the highest number of user hours lost, on average, per incident, with 56800 user hours.

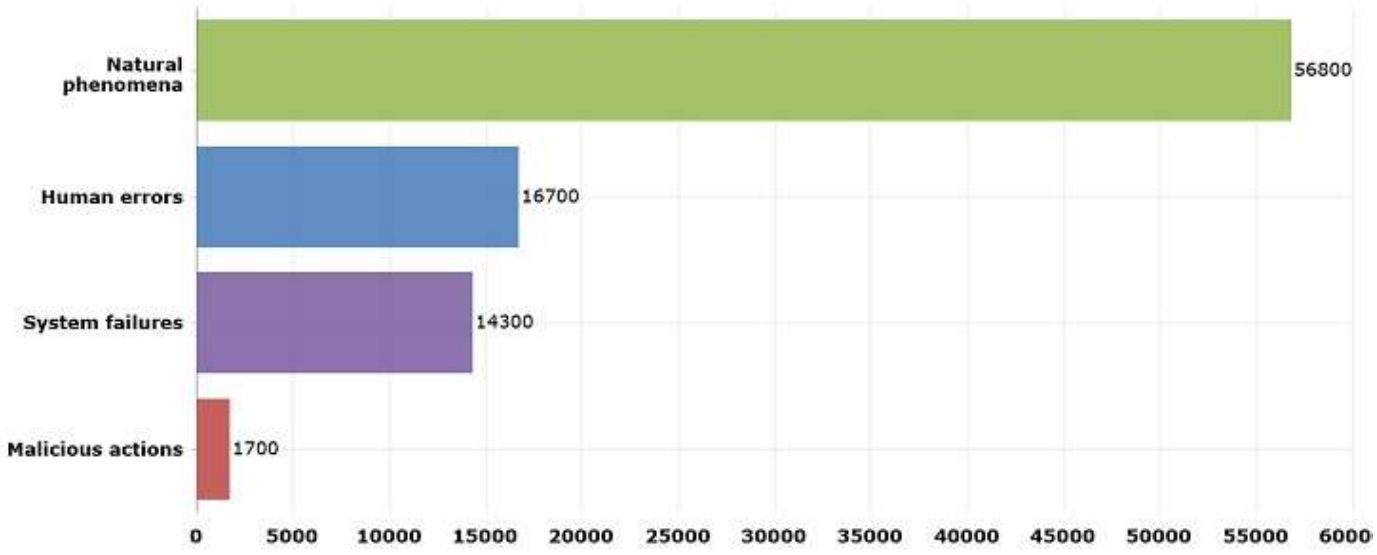


Figure 20: User hours lost per root cause category (hours).

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 a set of more detailed causes.

An incident is often a chain of events and failures, involving multiple causes. For instance, an incident may be triggered by storm, heavy winds, which tear down power supply infrastructure, then cause a power cut, which in turn leads to an outage because base stations are without power. For this incident both heavy winds and power cuts are listed as detailed causes. In the annual summary reporting we keep track of these detailed causes.

4.3.1 Detailed causes of all incidents

In 2017, the most common cause was hardware failure. This is part of a multi-year trend, because in previous years, hardware failure is always either the first or the second most common cause. Despite last year's decrease, power cuts and cable cuts are again in the top four of most frequent causes. The cause "Other" saw an increase this year. A more in-depth analysis showed that these incidents are different types of system failures.

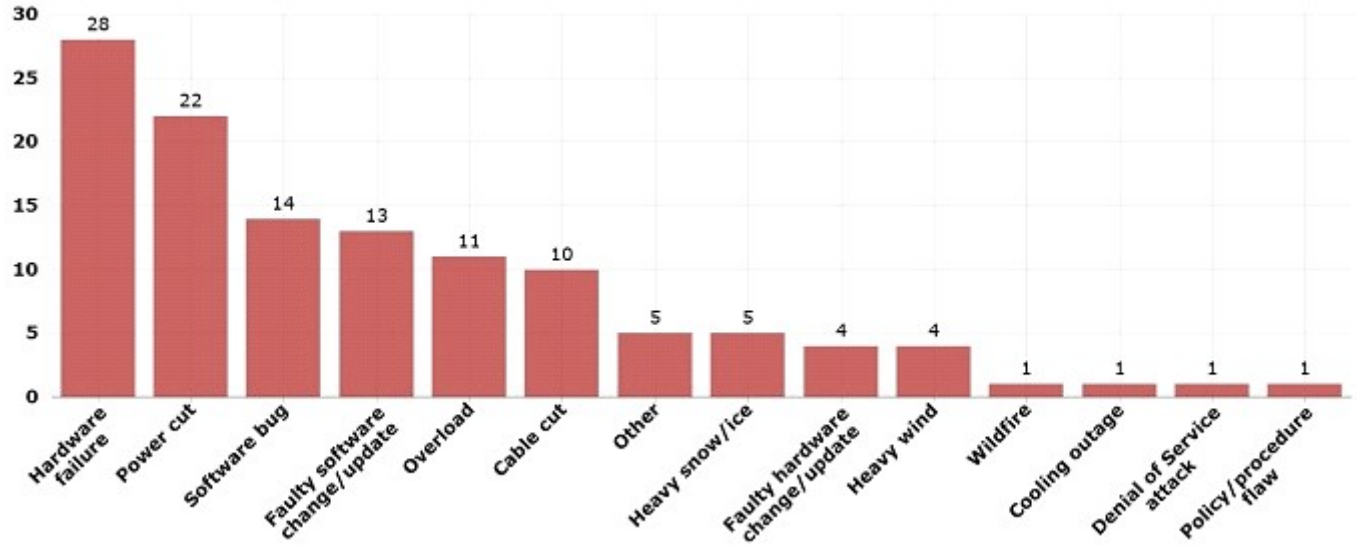


Figure 21: Detailed causes of reported incidents (percentage)

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

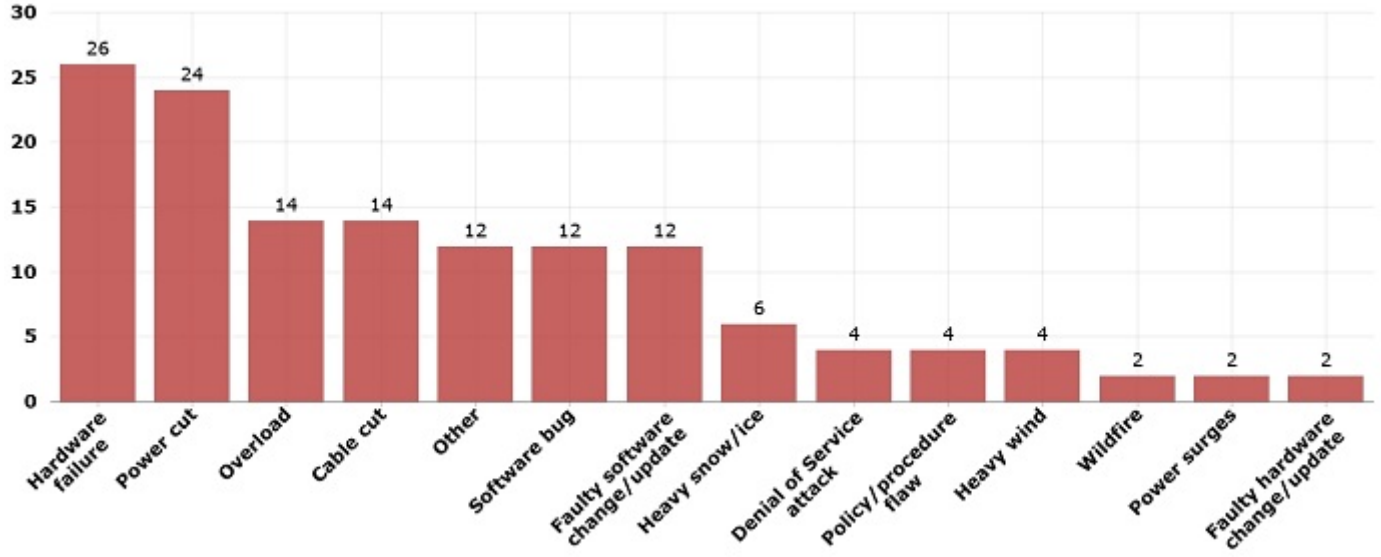


Figure 22: Detailed causes for fixed telephony (percentage).

4.3.2.2 Fixed Internet

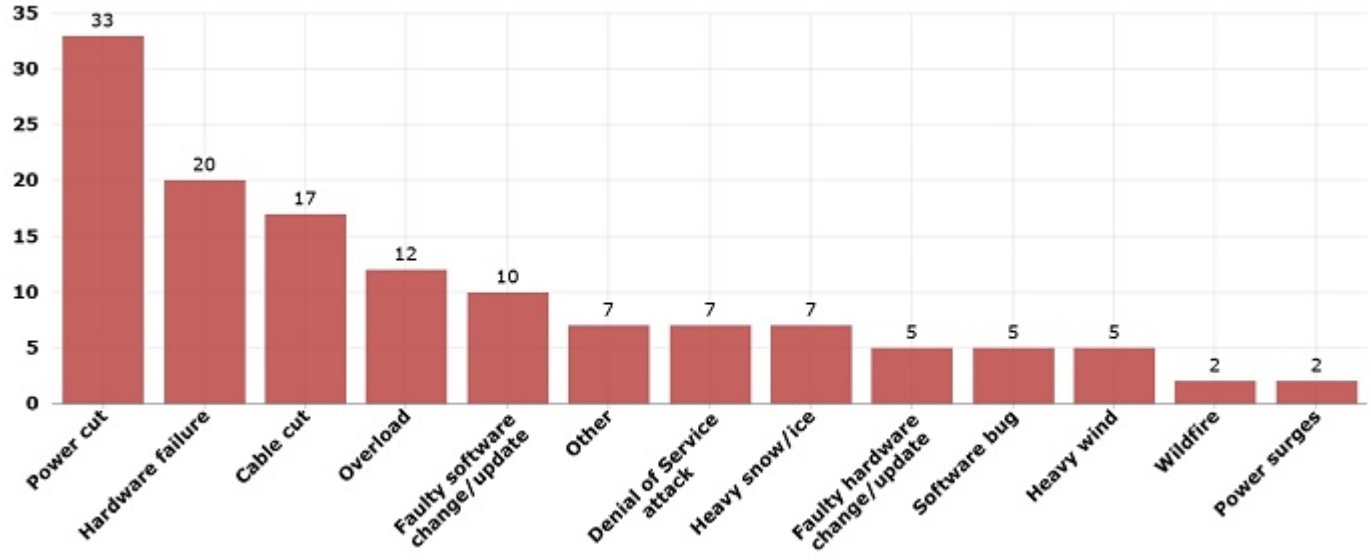


Figure 23: Detailed causes for fixed Internet (percentage).

4.3.2.3 Mobile Telephony

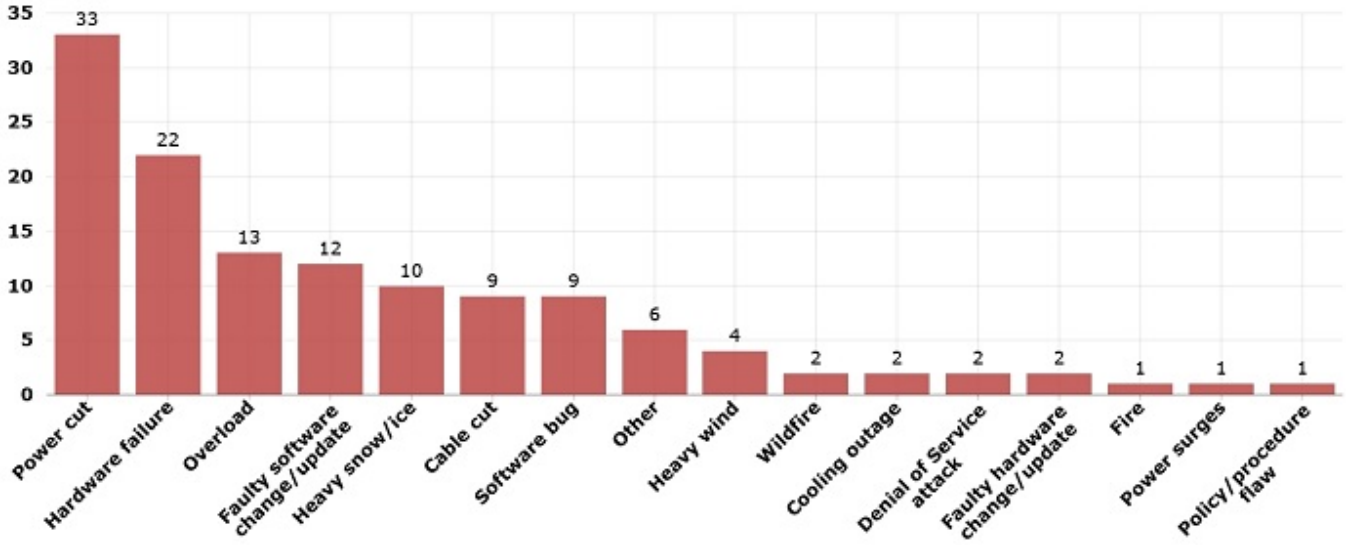


Figure 24: Detailed causes for mobile telephony (percentage).

4.3.2.4 Mobile Internet

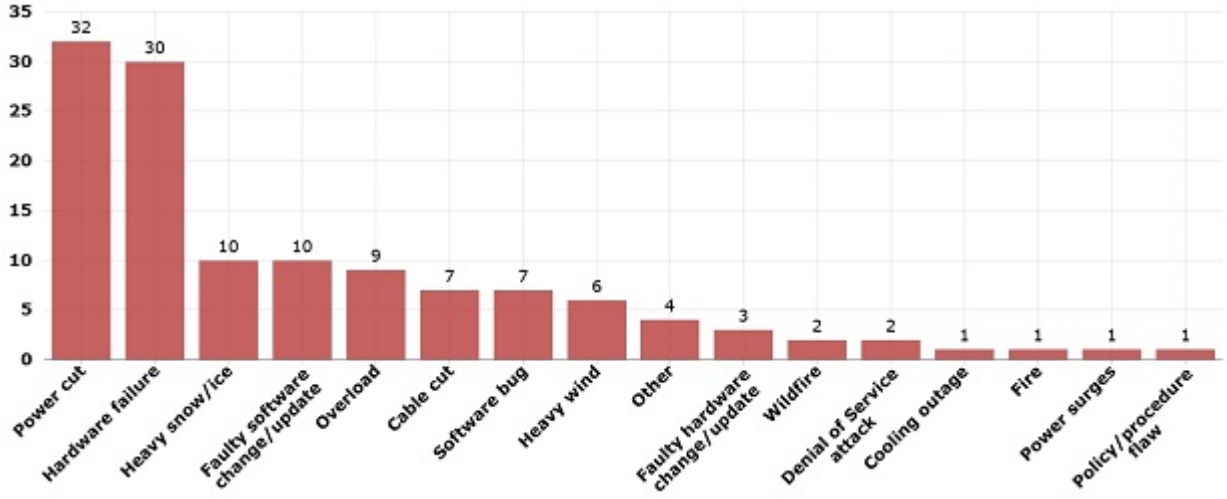


Figure 25: Detailed causes for mobile Internet (percentage).

4.3.2.5 Other services

Half of the incidents (almost 50%) with an impact on other services (other than the four main services) were caused by power cuts (33%), hardware failures (21%) and software bugs (15%), see the graph below.

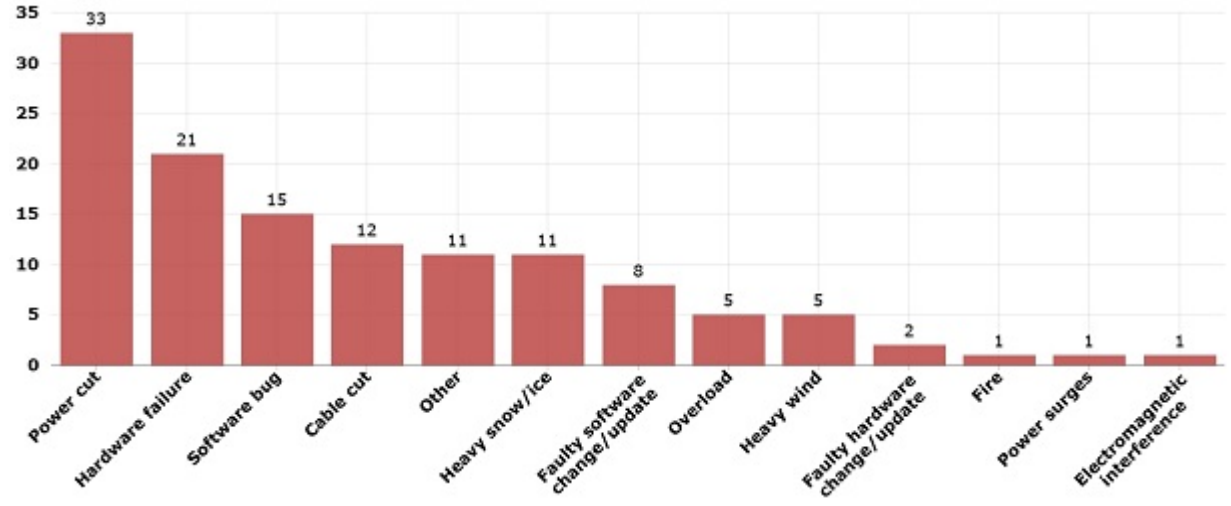


Figure 26: Detailed causes for other services (percentage).

4.3.2.6 Average number of user connections affected per detailed cause

On average software bugs cause incidents affecting most user connections.

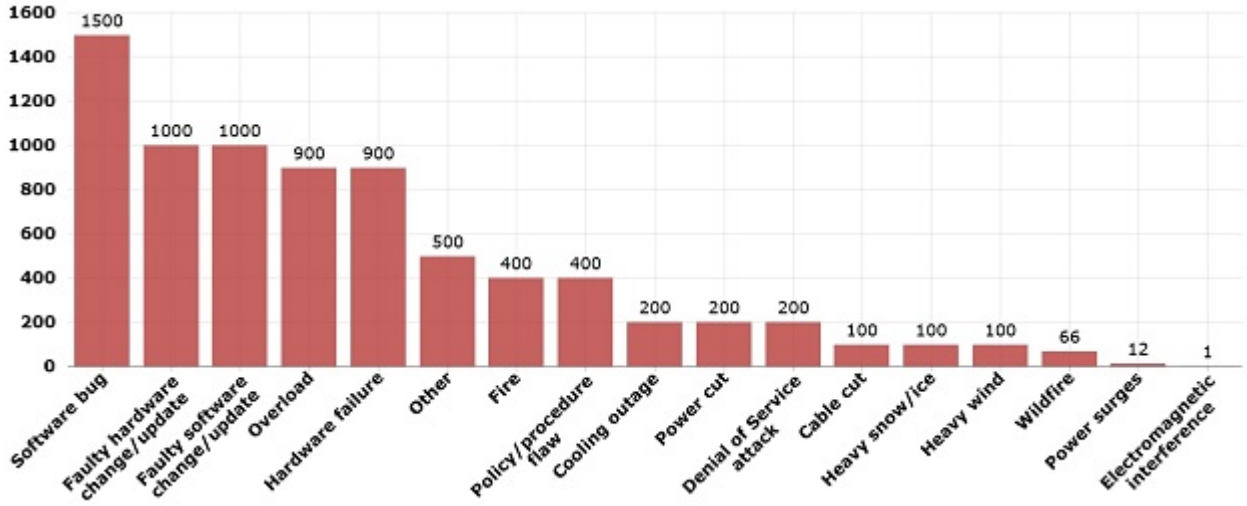


Figure 27: Average number of user connections affected per detailed cause (hours).

4.3.3 Average duration of incidents per detailed cause

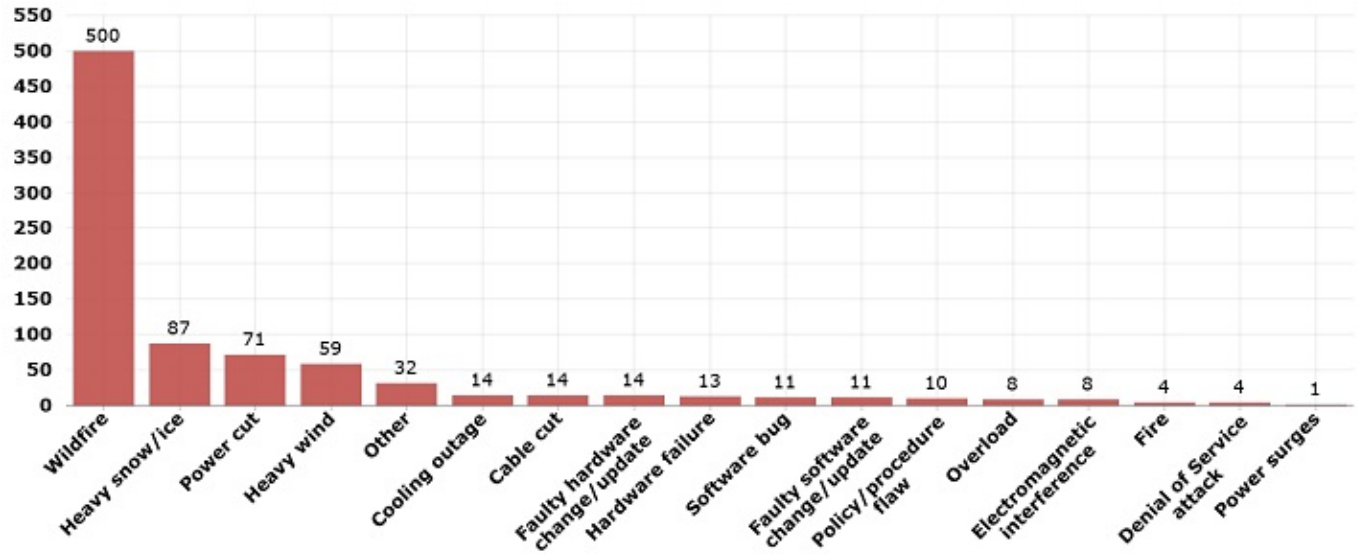


Figure 28: Average duration of incidents per detailed cause category (hours).

4.3.4 User hours lost per detailed cause

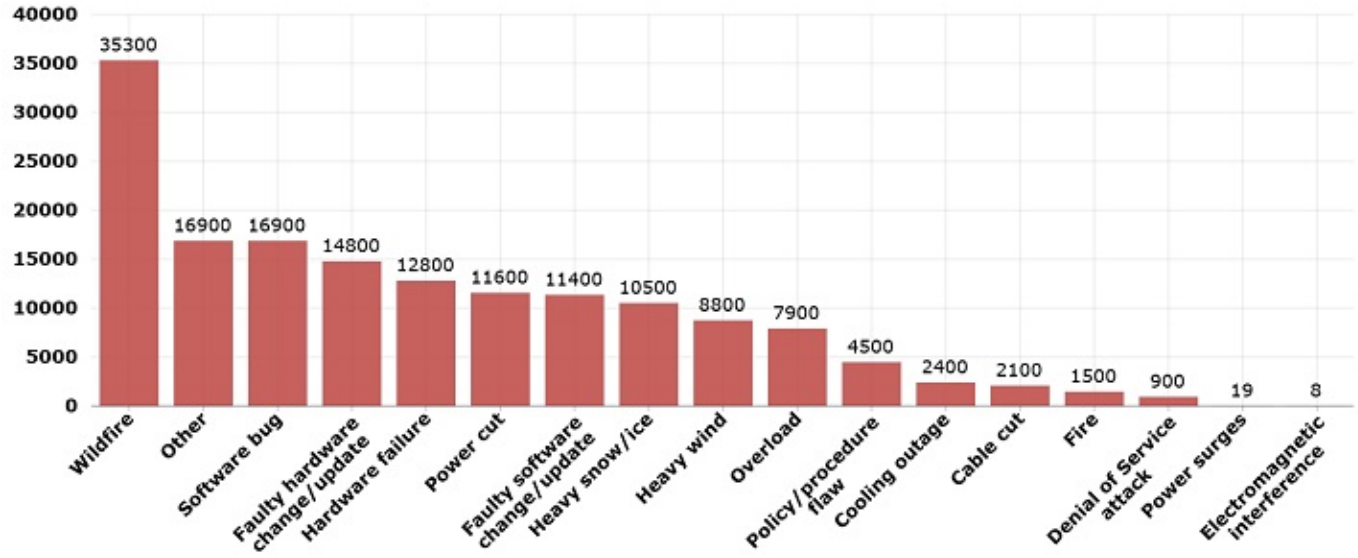


Figure 29: User hours lost per detailed cause (hours).

4.4 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.

4.4.1 Assets affected overall

In 2017, mobile base stations and controllers, and switches and routers were the assets most affected by incidents.

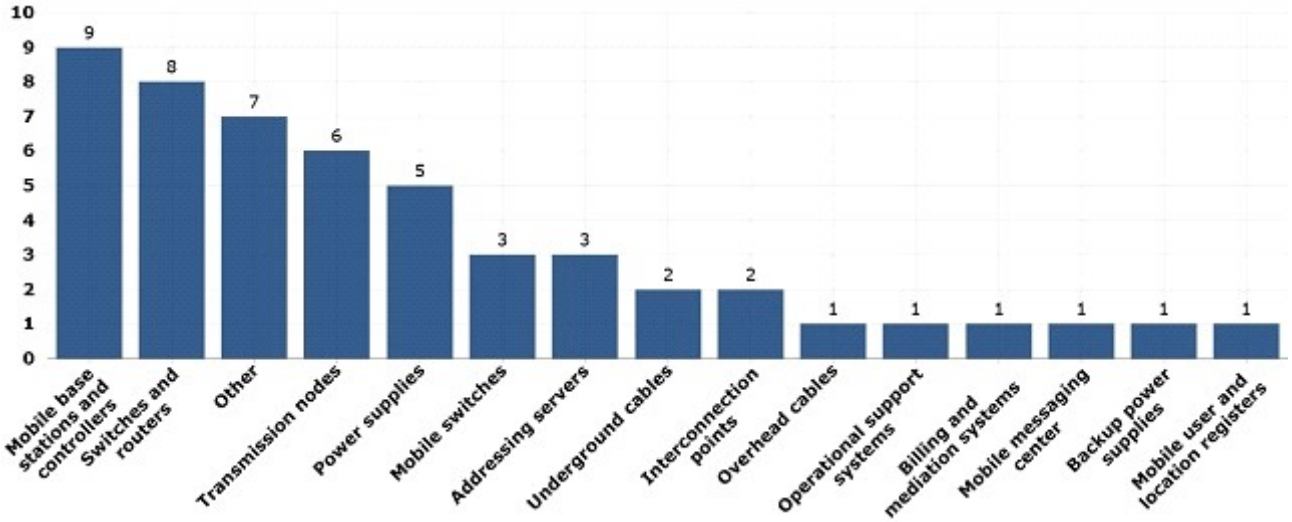


Figure 30: Assets affected by the incidents (percentage).

4.4.2 Affected assets in system failures

As for all previous reporting years, system failures (or technical failures), was the most common root cause category in 2017. In these system failures, the most common assets that failed were power supplies, switches and routers and other uncategorised assets. Also in the previous year mobile switches, and switches and routers were the most common assets to fail in this root cause category.

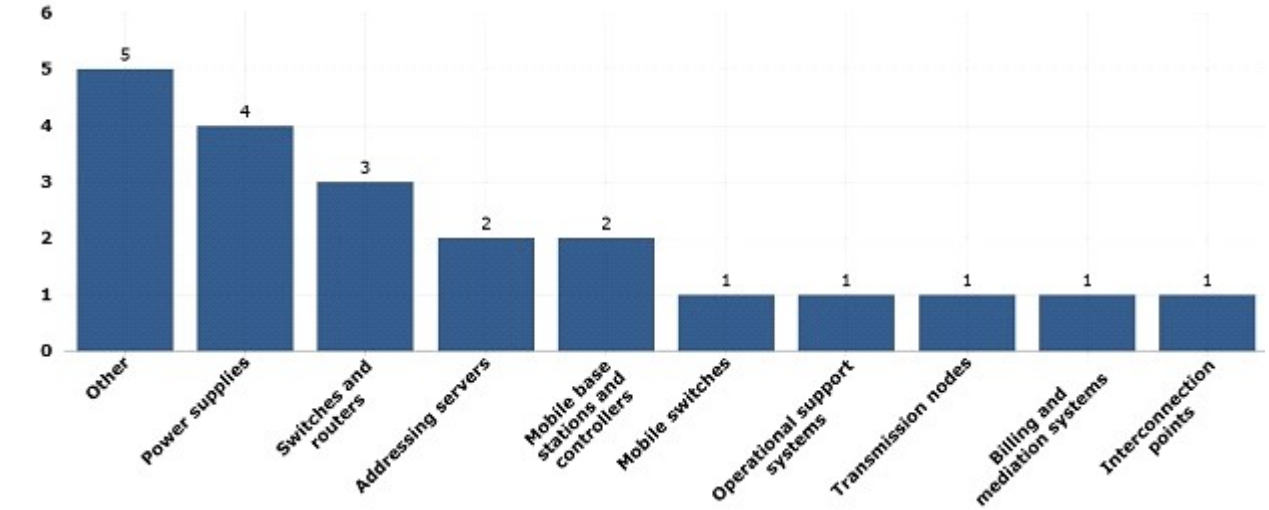


Figure 31: Assets affected by system failures (percentages).

5. Conclusions

In this report ENISA summarized and analysed the reports about 169 incidents which happened in 2017 affecting telecom networks and services in the EU. These reports were submitted by National Regulatory Authorities (NRAs) in 28 EU member states and 2 EFTA countries, as mandated by Article 13a of the Framework Directive (2009/140/EC)[Error! Bookmark not defined.].

Looking at the 2017 incidents, and looking back at the previous years of incident reporting (2012-2016), we can draw the following conclusions:

- **Mobile telephony and internet remain the most affected services:** In 2017 most incidents affected mobile telephony (51% of all reported incidents). Mobile internet and mobile telephony were the predominant affected services in the previous years also, except for 2014 when fixed telephony was the most affected.
- **Incidents with mobile telephony and mobile internet impact, on average, most users:** Incidents affecting mobile internet or mobile telephony affected most users, on average around half a million users per reported incident, around 8% of the national user base. Looking at the multiannual trend, there is a significant decrease compared to the data for 2016.
- **System failures are the dominant root cause:** In 2017 most incidents were caused by system failures, i.e. more than 62 % had system failure as a root cause. This is in line with previous years (always between 60% and 80%). In the category system failures, software bugs and hardware failures were the most common causes. The assets failing in these cases are most often switches, routers, and power supplies.
- **Natural phenomena are causing more incidents:** In 2017 a larger number of incidents (18%) were caused by natural phenomena, such as heavy snow/ice, storms and wild fires. This is significantly higher than 2016, 2015, and 2014 when natural phenomena accounted for around 5% of the incidents. Natural phenomena also cause the highest number of user hours lost, on average, per incident, with 56800 user hours. Natural phenomena will continue to be a concern for telecom providers across the EU, with extreme weather becoming more common due to climate change.
- **A fifth of the incidents are third party failures**: Almost a fifth of the incidents (18%) are third party failures. This is similar to last year (22%). Third party failure incidents are interesting for NRAs to investigate further because often third-party failures involve other sectors, and are complex and costly to tackle for providers. Most of the incidents categorized as a third party failures are also categorized as caused by natural phenomena. A common incident scenario is when a natural disaster, like a storm or wildfire, disrupts the power grid infrastructure, which then impacts the mobile network infrastructure.

ENISA will continue to work closely with the Article 13a Expert Group and the telecom sector to discuss and analyse common security incidents and good practices to mitigate them. The ongoing update of the legal framework for electronic communications (the EECC) is an important step to help the NRAs in understanding the issues facing the sector. Telecom security remains a top-priority, because, although the sector is quite mature in terms of network and information security compared to other critical sectors, it is also increasingly critical. The EU's digital economy relies on secure and resilient telecom networks and services. Improving resilience and security, while at the same time adopting new technology, phasing out the old technology, will be a key challenge in the future[17].

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

References

Related ENISA papers

- ENISA's annual reports telecom security incidents in 2011, 2012, 2013, 2014, 2015, and 2016 can be found at: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports
- ENISA commissioned in an independent impact assessment about Article 13a "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 full EU regulatory framework for electronic communications (incorporating the Framework Directive including Article 13a) right after the 2009 reform: 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 operators of essential services (OESs) 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
1 Vasilissis Sofias
Marousi 151 24, Attiki, Greece

Heraklion Office

Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Catalogue Number: TP-AD-18-001-EN-N

1 Vasilissis Sofias Str, Maroussi 151 24, Attiki,
Greece Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-257-8
DOI: 10.2824/017314