enisa

THE EU CYBERSECURITY AGENCY

ANNUAL REPORT TELECOM SECURITY INCIDENTS 2018

MAY 2019

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 technical queries about this paper, please email resilience@enisa.europa.eu
For media enquires about this paper, please email press@enisa.europa.eu

AUTHORS

Aggelos Koukounas, Eleni Vytogianni, Marnix Dekker

ACKNOWLEDGEMENTS

We are grateful for the review and input received from the experts in the ENISA Article 13a Expert Group which comprises national telecom regulatory authorities (NRAs) from all EU and EFTA countries.

LEGAL NOTICE

COPYRIGHT NOTICE

Catalogue number: TP-AD-19-001-EN-N
ISBN: 978-92-9204-296-7
DOI: 10.2824/350004

TABLE OF CONTENTS

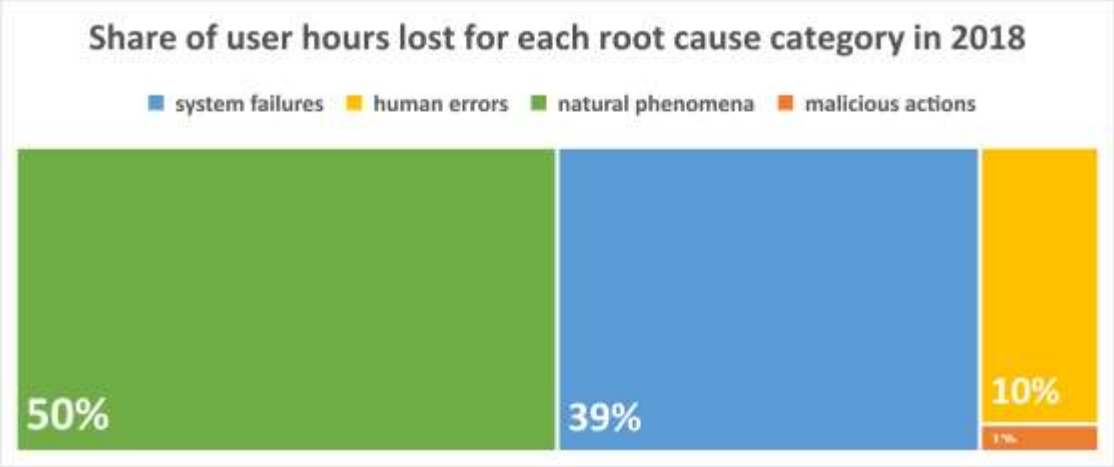
EXECUTIVE SUMMARY

In the EU, electronic communication providers notify significant security incidents to the National Regulatory authority (NRA) in their country. At the start of every calendar year the NRAs send a summary about these incidents to ENISA. This document, the Annual Report Telecom Security Incidents 2018, covers the incidents reported by NRAs for 2018 and gives an anonymised, aggregated EU-wide overview of telecom security incidents.

Security 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 with significant impact on the operation of services, i.e. outages of the electronic communication networks and/or services.

Statistics annual summary reporting 2008

The 2018 annual summary reporting contains reports about 157 incidents submitted by NRAs from the 28 EU Member States and 2 EFTA countries. The total user hours lost, multiplying for each incident the number of users and the number of hours, was 969 Million User Hours, i.e. roughly 0,02% of the total user hours in a year[1].



In 2018, half of the total user hours lost (482 million user hours) were due to natural phenomena. It is the first year that natural phenomena are the main root cause category in this respect, accounting for more user hours lost than the category of system failures.

Here are the key takeaways from about the 2018 incidents:

- **Natural phenomena dominate in terms of impact**: In 2018, half of the total user hours lost (482 million user hours) were due to natural phenomena. It is the first year that natural phenomena are the main root cause category in this respect, accounting for more user hours lost than the category of system failures.
- **System failures are the most frequent root cause of incidents**: Most incidents (67%) are caused by system failures, a percentage which is consistent with previous years. Often these system failures are hardware failures and software bugs.

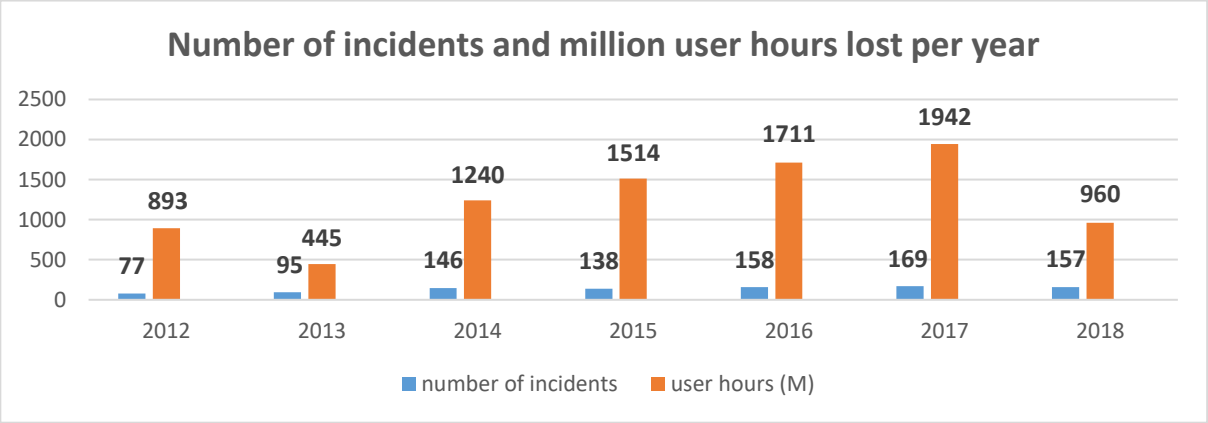
[1] Using a basis of 500M (EU citizens) times 365 (days) times 24 (hours). User hours is a metric we use throughout this report to quantify the impact of an incident, multiplying the number of subscribers/connections affected, with the duration in hours. For example 1M User Hours means 1M users were affected for one hour, or 2M users for half an hour, etc.

- **Power cuts are a major factor**: Although only a small number of incidents was caused by power cuts (15%) they had a huge impact in terms of user hours with 50% of the total, i.e. 496 million user hours lost.
- **Faulty software changes/updates are the second most common cause:** In 2018 faulty software changes/updates were the second most common cause of incident, accounting for a fifth of the incidents.

ENISA offers an online visual tool for analysing the incidents. It can be used to dive into other aspects and detailed causes. See: https://www.enisa.europa.eu/topics/incident-reporting/for-telcos/visual-tool For example, by selecting (top left) years 2018, 2017, 2016, then natural phenomena (top left), then mobile telephony and internet (top right), the charts at the bottom show detailed causes, assets affected.

Multiannual trends over 7 years of reporting

Looking back at the last 7 years of annual incident reporting we can observe a number of multi-annual trends.



- **Total number of incidents reported is stabilizing at around 160**: Over the period 2014-2018, there is a consistent number of incidents reported which is stabilizing at around 160 incidents per year.
- **Sharp drop of the average impact of incidents**: Until 2017 there was a gradual increase of total user hours lost per year. But in 2018 we see a sharp drop in the total user hours lost compared to previous years, to just 960 Million user hours. It remains to be seen if this is part of a larger trend or if this year was an exception.
- **Impact of natural phenomena trending up**: Natural phenomena have been trending up rapidly since 2016, and now account for more than half of the user hours lost. For the first time, this year natural phenomena account for more user hours lost than system failures, which used to be the leading root cause in this specific field.
- **System failures continue to be the most frequent but their average size is trending down**: Every year system failures have been the most common root cause category between 60% and 80% of the total number of incidents. Since 2016 the average size of these incidents is decreasing.
- **Frequency and impact of human errors and malicious actions stable**: Over the reporting period the frequency of human errors and malicious actions is stable (approximately accounting for 17% and 5% of incidents per year). Their impact in terms of user hours is stable also.

We refer the reader to the body of this paper for more charts and more details.

Outlook

Security breach reporting has now become a hallmark of EU cybersecurity legislation and this process is an important enabler for cybersecurity supervision and policy making, at national level as well as at EU level. Since 2016 security breach reporting is also mandatory for trust service providers in the EU, under Article 19 of the EIDAS regulation. In 2018, under the NIS Directive (NISD), security breach reporting became mandatory for Operators of Essential Services in the EU and for Digital Service Providers, under Article 14 and Article 16 of the NIS directive.

Soon, by the end of 2020, the European Electronic Communications Code (EECC) will come into effect across the EU. Under Article 40 of the EECC the breach reporting requirements have a broader scope, including not only outages, but also breaches of confidentiality, for instance. Also there are more services in scope of the EECC, including not only traditional telecom operators, but also for example over-the-top providers of communications services.

ENISA is now working with NRAs and experts from the private sector to prepare the ground for these changes and at the same time trying to find and exploit synergies between the different pieces of EU legislation, particularly when it comes to breach reporting and cross-border supervision.

We look forward to continuing our close collaboration with the EU member states, the national telecom authorities and experts from the telecom sector from across Europe.

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 2018, aggregates the incident reports reported in 2018 and gives a single EU-wide overview of telecom security incidents in the EU.

This is the 8th 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.

Note that although Article 13a itself is fairly broad, the mandatory breach reporting in Article 13a has specific focus on security incidents with a significant impact on the functioning of the service. There is some divergence and discussion about what is in scope here, but generally speaking, in most countries, this was understood to mean that there has to be a service outage. Now consider for example an attack in which attackers wiretap major undersea cables; if the attack causes no outages, then the incident does not fall under the breach reporting requirements of Article 13a. Recently the Council and Parliament agreed with an update of the EU telecom rules called the European Electronic Communications Code (EECC). The breach reporting requirements in (Article 40 of) the EECC have a broader scope, including not only incidents causing outages, but also, for example, breaches of confidentiality. An incident like the one just mentioned would be reportable under (Article 40 of) the EECC.

This document is structured as follows: In section 2 we briefly summarize the reporting procedure and to give an idea about the kind of incidents that are reported we give some specific but anonymized examples of incidents that occurred in 2018. In Section 3 we provide some key facts and statistics about the 2018 incidents. In Section 4 we take a closer look at power cuts. In section 5 we look at multiannual trends over the years 2012-2018. Conclusions about trends and comparisons with previous years have to be made with care, because national reporting has improved over the years, reporting thresholds have been lowered in most countries, etc.

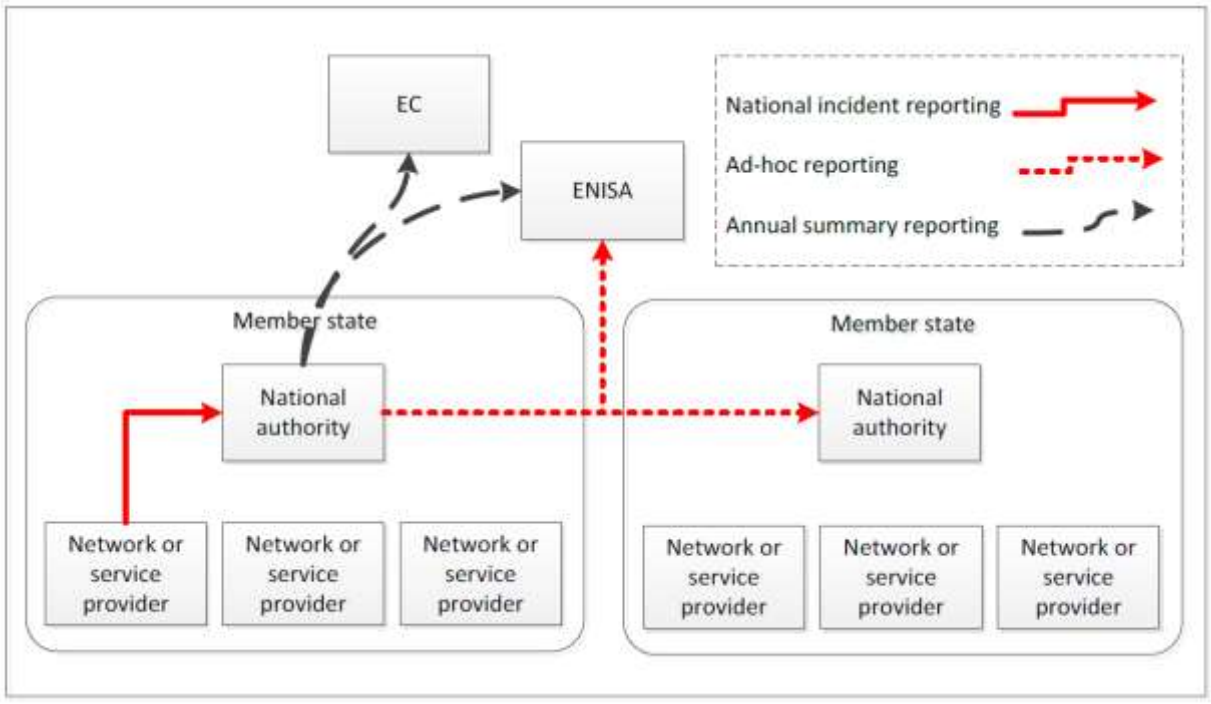
This is the 8th time ENISA publishes an annual incident report for the telecom sector. ENISA started publishing such annual reports in 2012. Mandatory breach reporting has been part of the EU's telecom regulatory framework since the 2009 reform of the telecom package: Article 13a of the Framework directive (2009/140/EC) came into force in 2011.

2. INCIDENT REPORTING FRAMEWORK AND EXAMPLES OF INCIDENTS

We briefly explain the main features of the incident reporting procedure, as described in the Article 13a Technical Guideline on Incident Reporting[2], which was developed in collaboration with the NRAs.

2.1 INCIDENT REPORTING FRAMEWORK

Article 13a introduces three types of incident reporting: 1) National incident reporting from providers to NRAs, 2) Ad-hoc incident reporting between NRAs and ENISA, and 3) Annual summary reporting from NRAs to the EC and ENISA. The different types of reporting are shown in the diagram below.



Note that in this setup ENISA acts as a collection point, anonymizing aggregating and analysing the incident reports. In the current setup NRAs can search incidents in the reporting tool (CIRAS) but the incident reports themselves do not refer to countries or providers, making the overall summary reporting process less sensitive.

2.2 EXAMPLES OF INCIDENTS REPORTED

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, telephony and SMS outage for thousands of users (duration: hours, connections: thousands, cause: software bug)**: A software bug occurred in the SPR (Subscriber Profile Repository) server. Following the repeated instability of the equipment, the signalling traffic increased and

[2] https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting

the STP (Signalling Transfer Point) platforms became overloaded. As a result, end users had difficulties to access mobile internet services as well as voice and SMS services. The vendor responded by fully restoring the functionality of the SPR equipment. In order to stop the avalanche of signalling messages, the 3G and 4G networks were partially shut off and all subscribers were located on the 2G network.

- **A power cut caused by a heavy storm affected mobile, fixed services and Cable TV for hundreds of users (duration: hours, connections: thousands, cause: heavy wind/storm)**: A heavy storm combining with heavy winds strongly affected assets in a defined area causing outages to mobile and fixed services. The operator emergency team was activated. A number of emergency generators was used and a number of VSAT antennas was installed on affected sites.
- **A malicious action caused a mobile internet outage for a million of users (duration: hours, connections: a million, cause: Denial of Service attack)**: The network was subject to a cyber-attack (Denial of Service attack) which caused congestion and degraded service. Mobile switches and routers were affected by this attack. The network had self-recovered after the attack had ceased.
- **A human error caused a mobile internet outage for millions of users (duration: hours, connections: millions, cause: faulty software change/update)**: Due to a human error (wrong software configuration) during the migration of the packet gateway, clients of one operator were not able to use mobile data. Mobile switches were affected by this incident. A rollback was successfully executed to resolve the issue.
- **Fixed telephony, broadband internet, cable TV service lost due to cable cuts (duration: hours - days, connections: thousands, cause: human errors):** *A number of network outages were suffered due to cable cuts during construction and road excavation work. Networks were restored following manual repair intervention on damaged cables.*

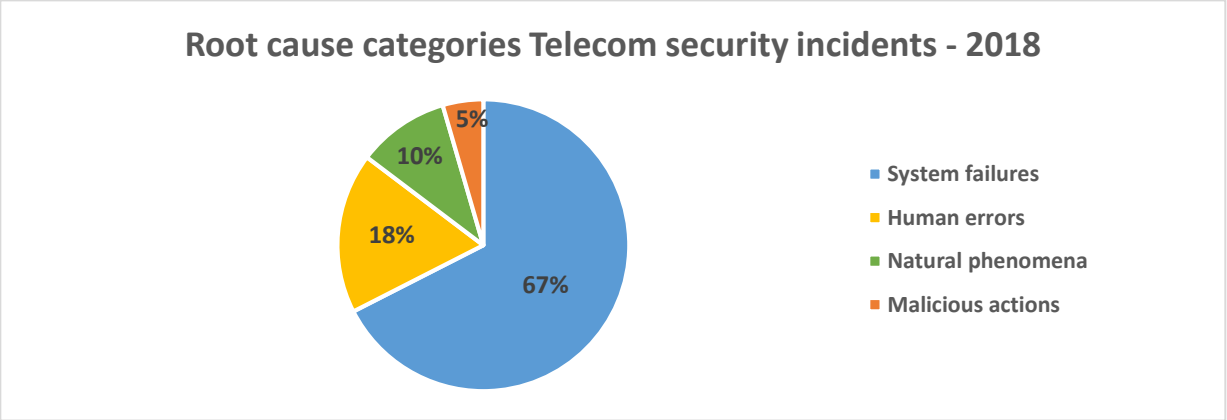
Note that the experts from NRAs have access to the CIRAS incident reporting tool where they can search for and study specific incidents. This tool anonymizes which country was involved. For externals ENISA runs an online visual tool which can be used for custom analysis of the data: https://www.enisa.europa.eu/topics/incident-reporting/for-telcos/visual-tool

3. ANALYSIS OF THE INCIDENTS

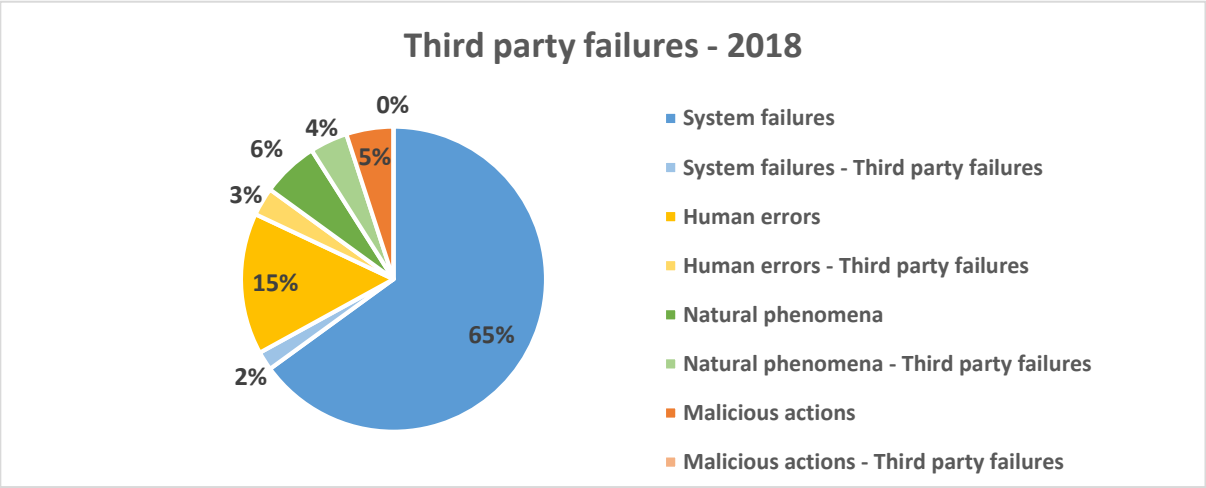
In total, all 28 EU Member States and 2 EFTA countries participated in this process. Of these, 19 Member States and 2 EFTA countries reported in total 157 significant incidents and 5 countries reported there were no significant incidents. In this section, the 157 reported incidents are aggregated and analysed. First, the impact per root cause category is analysed (in section 3.1), in section 3.2 we focus on the user hours that have been lost per root cause category, then detailed causes are examined (Section 3.3), and in Section 3.4 the impact per service is analysed.

3.1 ROOT CAUSE CATEGORIES

In 2018 roughly two thirds of the telecom security incidents were system failures. This is consistent with previous years. Often they are hardware failures and software bugs. Also human errors are stable at around 18%. Most often these are accidental cable cuts and faulty software changes/updates. 10% of the incidents are caused by natural phenomena, two times less than the previous year. Only 5% of incidents were due to malicious actions. Typically these cases are denial of service attacks and cable theft.

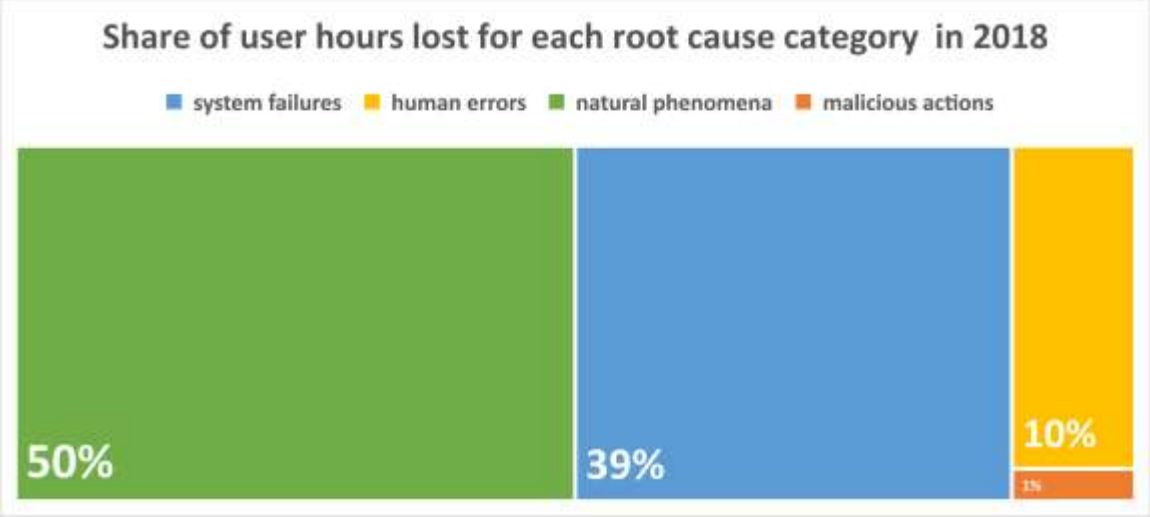


There is a fifth category called Third-party failures, which can be selected (only) in conjunction with another root cause category. Typically third party failures are incidents which happen at a utility company or supplier and then affect the telecom providers, for example a power cut. In total over 2018, 9% of incidents were flagged as third-party failures. The division is shown in the chart below.



3.2 USER HOURS LOST FOR EACH ROOT CAUSE CATEGORY

Adding up the total user hours lost for each root cause category we find that than half of the total user hours lost were due to natural phenomena (50%, 482 million user hours). All system failures combined account for two fifths of user hours lost (39%, 380 million user hours).



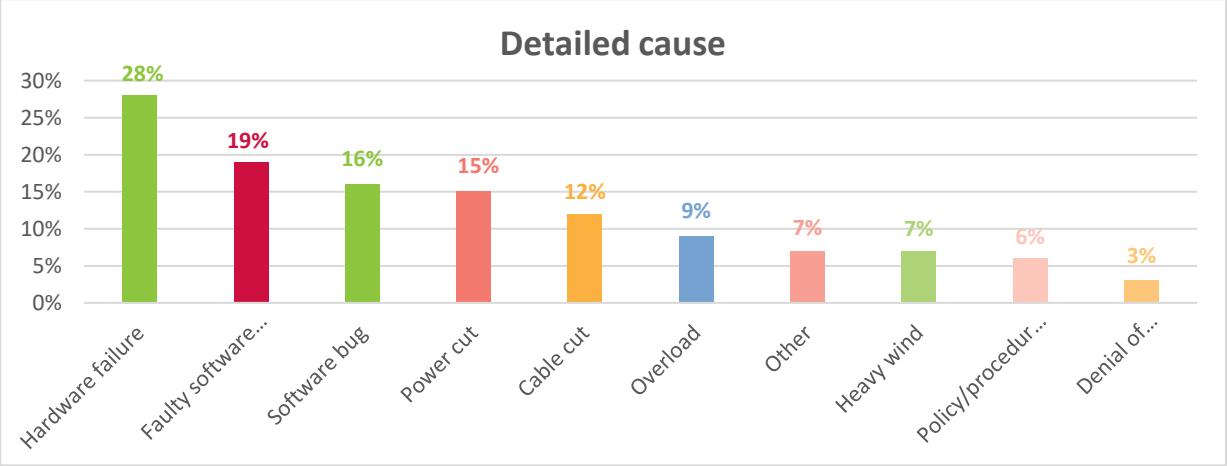
So although system failures are the most common (see section 3.1), they are having less impact than natural phenomena. In 2018 the natural phenomena are the dominant root cause category in terms of user hours lost. The multi annual trends graph for user hours lost per root cause category (see section 5.3) shows this is the first year that natural phenomena account for more user hours lost than system failures.

3.3 DETAILED CAUSES

An incident is often not only triggered by one cause but often by multiple causes and a chain of causes. For instance, detailed causes could be:

1. **Heavy snow**
2. **Power cut**

In this case, the root cause of the incident could be natural phenomena, and the description of a possible event could be as follows: an incident may initially be triggered by heavy snow, which tears down power supply infrastructure causing a power cut, which in turn leads to a telecom outage. For this example, both heavy snow 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.

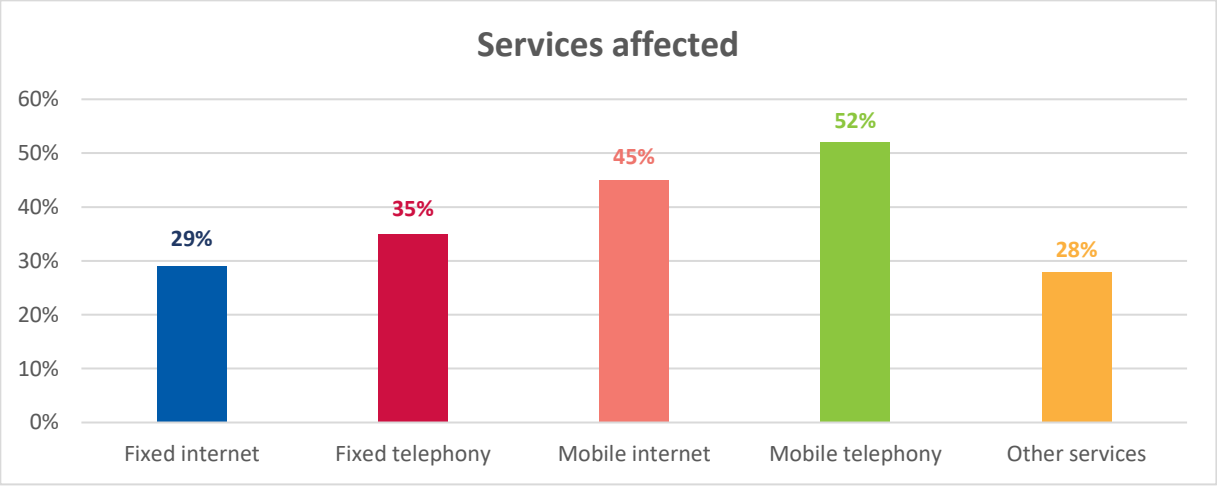


In 2018, the most common cause of incidents was hardware failures, which confirms the multi-annual trend in which hardware failure is always either the first or the second most common cause. Also, faulty software changes/updates became the second most common "detailed cause" as just under a fifth of the incidents reported were caused by them. Both with software bugs and power cuts remained at the top four causes of the last three years. Many detailed causes of incidents reports do not fall under a specific category and form the category of "Other" which has a minor position in this year's overall chart.

ENISA runs an online visual tool which can be used by externals to do custom analysis over the full dataset. See: https://www.enisa.europa.eu/topics/incident-reporting/for-telcos/visual-tool For example, by selecting system failures (top left), then fixed internet and telephony (top right), the charts at the bottom show the detailed causes for this subset.

3.4 SERVICES AFFECTED

For fourth year in a row, most of the reported incidents affected mobile services. This year, almost the half of the incidents reported had an impact on mobile telephony and internet in the EU. This confirms the shift of the last years. Fixed telephony was the most affected service only in the early years of reporting.

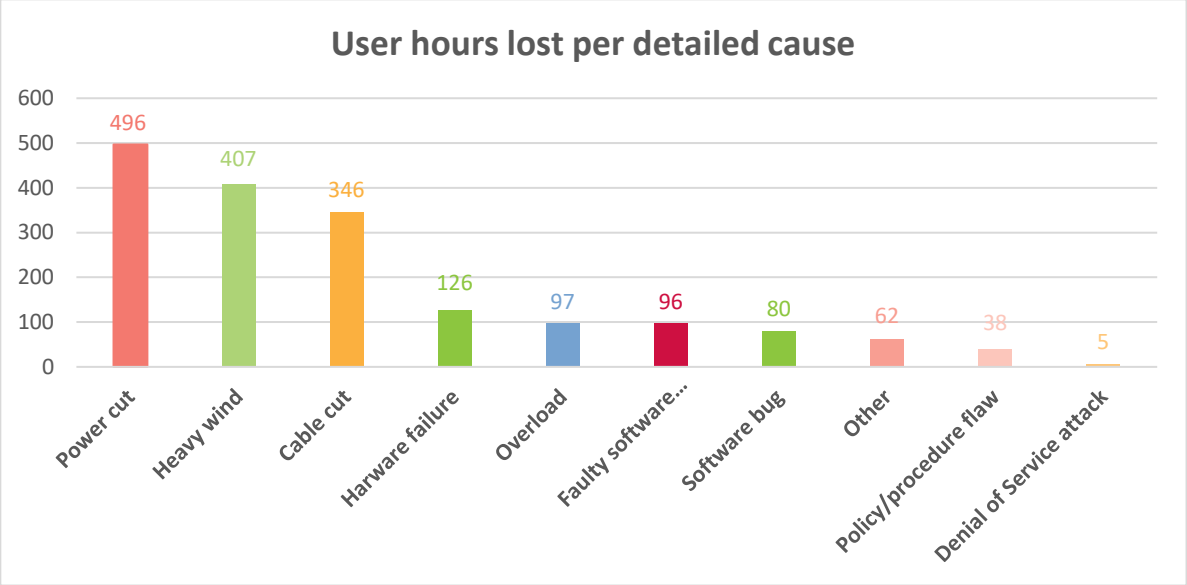


Note that for most reported incidents there is impact on more than one service, which explains why the percentages in the chart here add up to more than 100%.

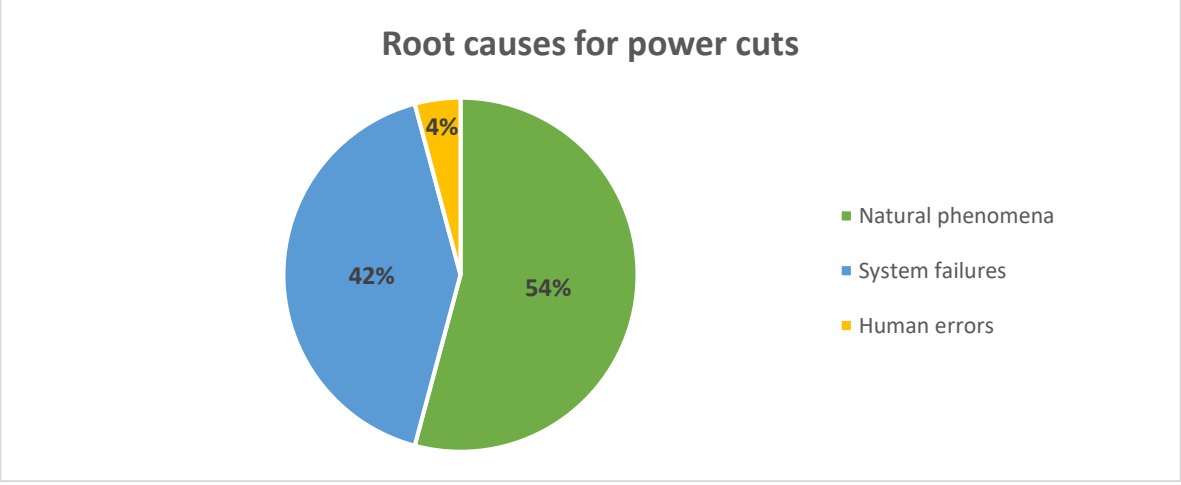
4. DETAILED ANALYSIS: POWER CUTS

In 2018 15% of the incidents involved a power cut, as a detailed cause, but these incidents accounted for half of the total user hours lost (50%, 496 million user hours). In this section, we take a closer look at the power cuts. In many countries NRAs are currently analysing and mitigating the dependencies of the telecom sector on the electricity subsector. In some countries NRAs have issued specific rules on battery-life of base stations for example. In other countries the NRA is taking stock of possible contingency measures in case of long lasting outages, such as increasing the output power of large sites.

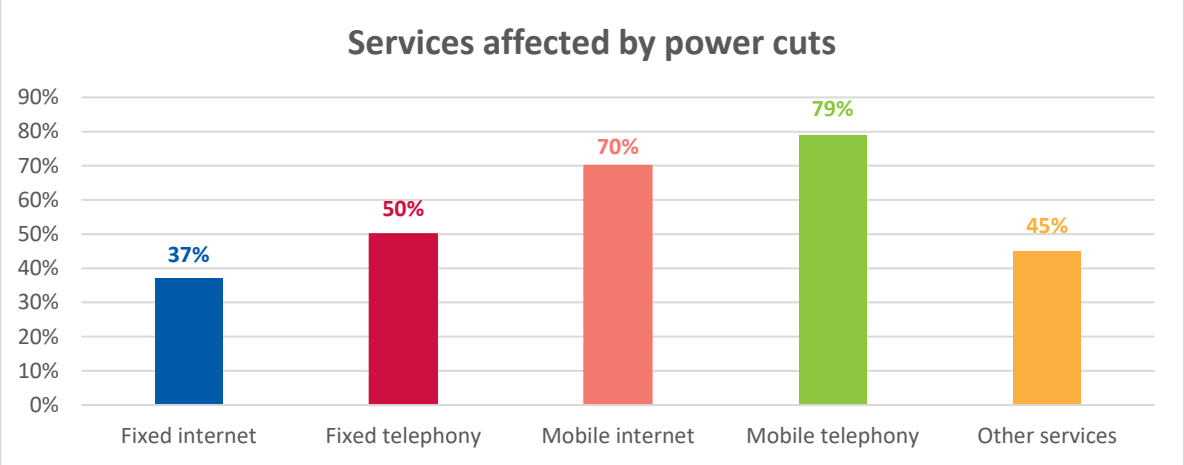
We look at the user hours lost for the main detailed causes. The graph below shows millions of user hours lost for each detailed cause. Clearly power cuts have a major impact.



For all incidents involving power cuts we show the root cause categories of these incidents in the graph below. Most incidents involving a power cut were categorized as either natural phenomena (52%) or system failures (42%).



Power cuts had a large impact on mobile services as 79% of the reported incidents affected mobile telephony while 70% of them had an impact on mobile internet. This is not surprising because the mobile network infrastructure, the mobile base stations, relies on power and it is not easy to mitigate power cuts: Batteries last only a short time, and they are vulnerable to theft.



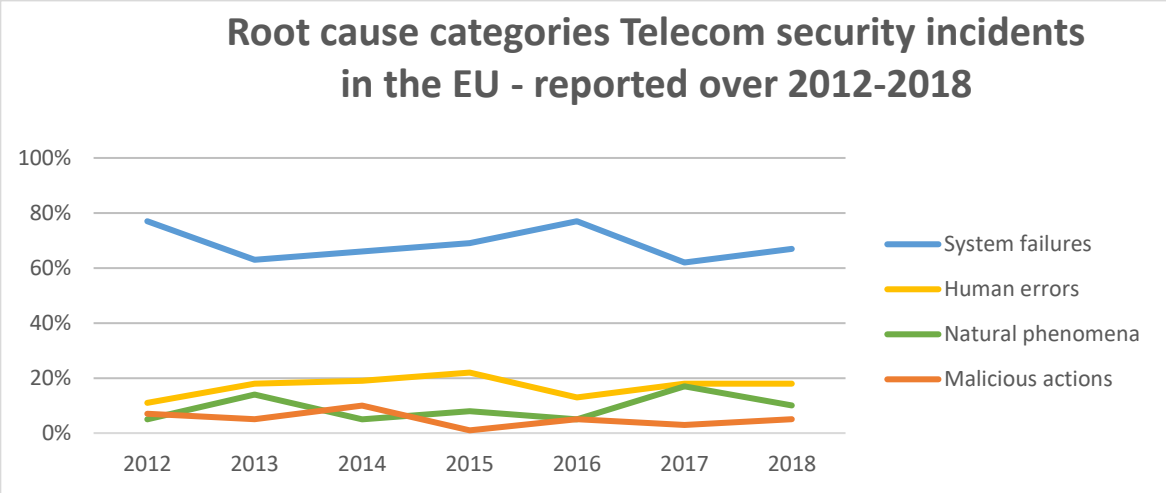
Note that by using the ENISA visual tool at https://www.enisa.europa.eu/topics/incident-reporting/for-telcos/visual-tool one can study also other detailed causes. For example by selecting all years (top) and denial of service attacks (bottom right) we see that over the years denial of service affect mostly addressing servers.

5. MULTI-ANNUAL TRENDS ON PERIOD 2012-2018

ENISA has been collecting and aggregating incident reports since 2012. In this section we look at the multiannual trends over the last 7 years, covering from 2012 to 2018. This dataset contains 940 reported incidents in total.

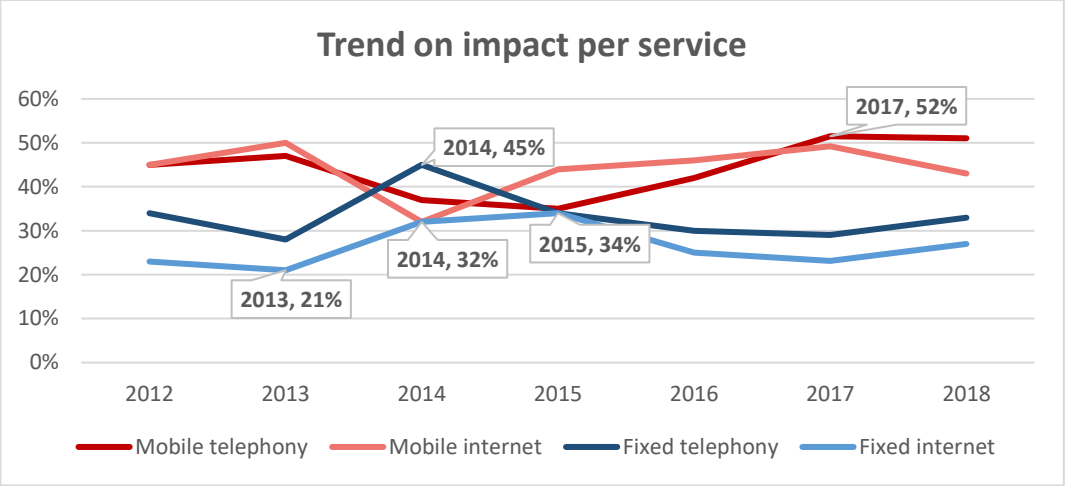
5.1 MULTIANNUAL TREND ROOT CAUSE CATEGORIES

Every year from 2012 to 2018, system failures are the most common root cause, roughly two thirds every year. In total system failures account for 636 of incident reports (68% of the total). For this root cause category, over the last 7 years, the most common causes were hardware failures (36%) and software bugs (29%). The second most common root cause over the 7 years of reporting is human errors with nearly a fifth of total incidents (17%, 162 incidents in total). Natural phenomena come third at just under a tenth of total incidents (9%, 89 incidents in total). Only 4% of the incidents are categorized as malicious actions. In the period 2012-2018 two thirds of the malicious actions consist of Denial of Service attacks, and the rest are mainly damage to physical infrastructure.



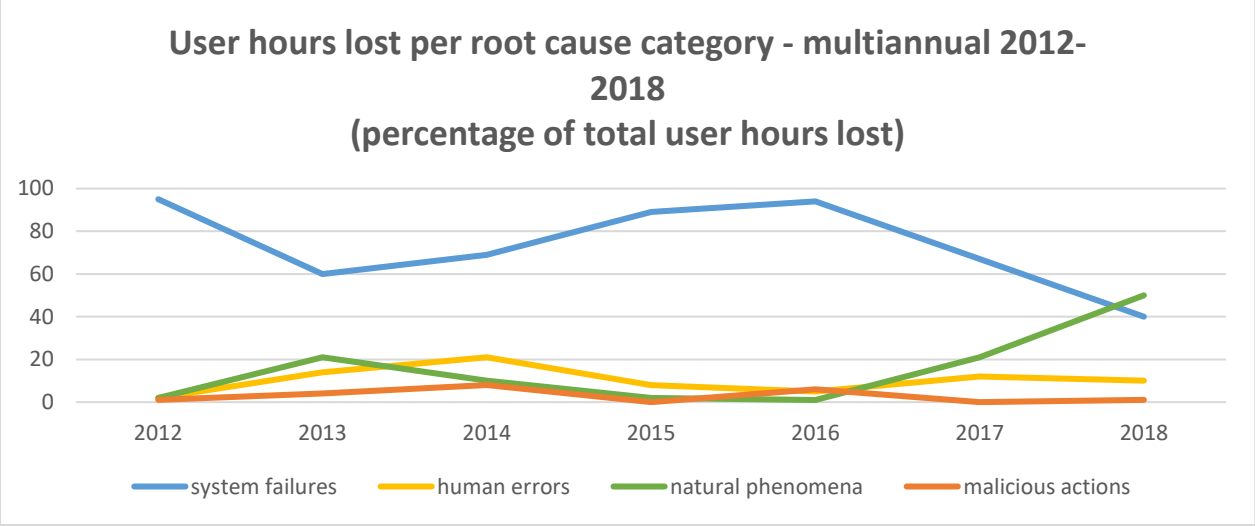
5.2 MULTIANNUAL TREND IMPACT PER SERVICE

In 2018 mobile networks and services were the most impacted by incidents. This is part of a multiannual trend. Only in 2014 the fixed networks and services was where the most affected. Looking back at the 7 years of annual incident reporting, a total of 940 incidents, almost half had an impact on mobile internet or mobile telephony. The chart below shows the multiannual trends over the 2012-2018 period.



5.3 MULTIANNUAL TREND USER HOURS PER ROOT CAUSE CATEGORY

Adding up the total user hours lost per root cause category, we observe that natural phenomena have been increasing since 2016. In 2018, for the first time, natural phenomena are the dominant root cause category. Last year natural phenomena accounted for more than half of the total user hours lost. We observe a downward trend in the user hours lost due to system failures which started in 2016. The other root cause categories are relatively stable over the years.

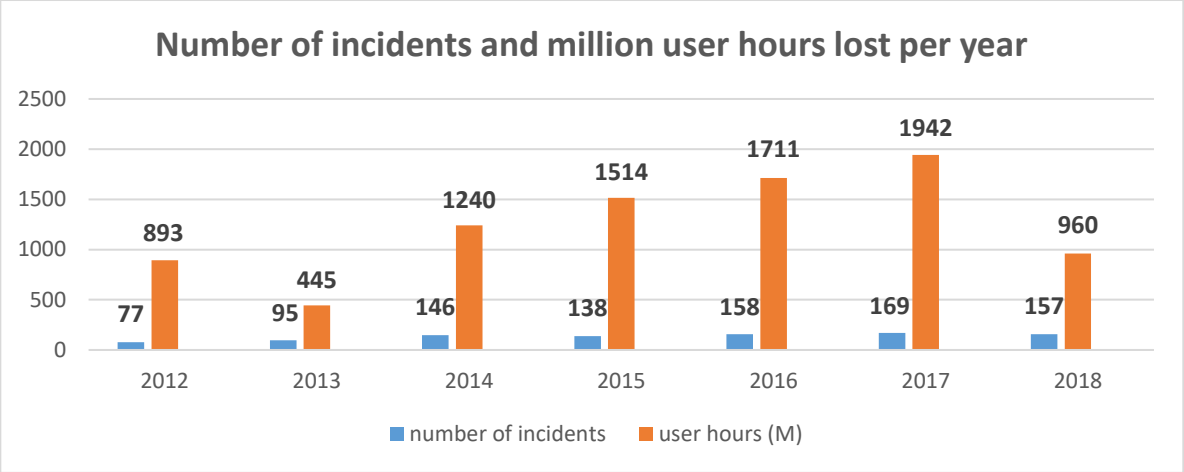


5.4 MULTI-YEAR TREND NUMBER OF INCIDENTS AND USER HOURS

In the chart below we show the total number of incidents reported over the year. Over the years, the number of incidents included in annual summary reporting to ENISA has increased slowly and it seems to stabilize at around 160 per year. This is probably due to more reporting by providers, better awareness about the reporting obligations, and partly due to lower national thresholds for annual summary reporting.

In the chart below we also show total numbers of incidents reported and total user hours lost per year over the period 2014-2018. There was an upward trend in user hours lost reaching a peak in 2017 with 1942 million user hours lost. Interestingly there was a sharp drop in the average user hours lost per incident reported over 2018. It remains to be seen if this decrease

is structural and sustained in the future, i.e. whether 2018 is the exception or the start of a longer trend. Several NRAs have remarked that overall incident size seems to be smaller, possibly due to improvements on the operator side, i.e. changed network topology, better architecture, better core components, etc.



6. CONCLUSIONS

This annual report telecom security incidents 2018 marks the 8th time ENISA publishes an annual report for the telecom sector. ENISA started publishing annual reports about telecom security incidents 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.

We refer to the executive summary for some of the key findings and statistics facts about the incidents that occurred in 2018 and the multiannual trends over 2012-2018. We would like to conclude with some more general observations about this process and the broader policy context.

- Security breach reporting under Article 13a has been implemented pragmatically and efficiently by the NRAs. Although the incidents in scope of this reporting are only a very small part of the cybersecurity universe, as near misses, risks, threats, etc. are for example not included, NRAs have said that this cross-EU process was extremely helpful[3]. The process of mandatory notification by operators yielded interesting data and facts for policy makers both at EU and national level, for NRAs, and other competent authorities.
- Security breach reporting has become a hallmark of EU cybersecurity legislation and the security breach reporting under Article 13a was the basis for the breach reporting requirements in eIDAS (Article 19) and the NIS Directive (Article 14, Article 16). All three laws take an all-hazard approach to cybersecurity incidents and they have comparable notification thresholds. This means that competent authorities can build on each other's experience when implementing such legislation.
- With the adoption of the European Electronic Communications Code (EECC), due to be transposed in national law by the Member States by the end of 2020, the telecom security breach reporting will be further aligned with the breach reporting under the NIS Directive. In particular, the definition of what is a security incident and the definition of notification thresholds are now fully aligned. This means there is a clear opportunity to synergize and harmonize taxonomy, processes and tools. ENISA is supporting the process of finding and exploiting these synergies for example by using the same taxonomy of root causes.
- Two years ago the NIS Directive (NISD) established a cooperation group (the NIS Cooperation group, or NIS CG) for strategic collaboration between EU Member States on cybersecurity issues. Specific sectoral work is now happening in subgroups, for example there is a NIS CG work stream for the Energy sector (very important for the telecom sector, see Section 4), there is a working group for NISD Competent authorities who supervise the Digital Service providers and recently a work stream on 5G security issues was started.. This means there is a clear benefit for the NRAs in the Article 13a expert group to have a good liaison with the NIS Cooperation group and we look forward to exchanging experience and doing joint work.
- When the EECC comes into effect by the end of 2020, the telecom regulators will be dealing with a new type of provider, the so-called over-the-top communication services

With the adoption of the European Electronic Communications Code (EECC), due to be transposed in national law by the Member States by the end of 2020, the telecom security breach reporting will be further aligned with the breach reporting under the NIS Directive.

[3] In 2015 ENISA commissioned an independent evaluation[3] of Article 13a and found that incident reporting has greatly supported policy making and supervision in the EU Member States. See: https://www.enisa.europa.eu/publications/impact-evaluation-article13a

like Whatsapp. This means coordination and collaboration between NRAs across the EU will become even more important.

We look forward to continue our close collaboration with the telecom regulators in the future and we look forward to develop a new reporting process for breach reporting and security supervision under the EECC, building on our joint experience and lessons learned with Article 13a.

TP-AD-19-001-EN-N

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.

ENISA
European Union Agency for Network and Information Security
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

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

enisa.europa.eu

ISBN 978-92-9204-296-7
doi: 10.2824/350004