EUROPEAN UNION AGENCY
FOR CYBERSECURITY

TELECOM SECURITY INCIDENTS 2020

Annual Report

JULY 2021

ABOUT ENISA

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

CONTACT

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

AUTHORS

Vassiliki Gogou and Marnix Dekker, European Union Agency for Cybersecurity

ACKNOWLEDGEMENTS

We are grateful for the review and input received from the members of the ENISA ECASEC expert group, which comprises national telecom regulatory authorities (NRAs) from the EU and EEA, EFTA and EU candidate countries.

LEGAL NOTICE

COPYRIGHT NOTICE

Catalogue number: TP-09-21-273-EN-N
ISBN: 978-92-9204-510-4
DOI: 10.2824/774362

TABLE OF CONTENTS

1. INTRODUCTION 6

2. BACKGROUND AND POLICY CONTEXT 7

2.1 POLICY CONTEXT 7

2.2 INCIDENT REPORTING FRAMEWORK 7

2.3 INCIDENT REPORTING TOOL 8

2.4 EXAMPLES OF INCIDENTS REPORTED 10

3. ANALYSIS OF THE INCIDENTS 13

3.1 ROOT CAUSE CATEGORIES 13

3.2 USER HOURS LOST FOR EACH ROOT CAUSE CATEGORY 14

3.3 DETAILED CAUSES AND USER HOURS LOST 14

3.4 SERVICES AFFECTED 19

3.5 TECHNICAL ASSETS AFFECTED 19

4. ANALYSING INCIDENTS CAUSED BY FAULTY SOFTWARE CHANGES/UPDATES 20

4.1 FAULTY SOFTWARE CHANGES/UPDATES IN 2020 20

4.2 FAULTY SOFTWARE CHANGES/UPDATES – MULTI-ANNUAL 21

5. MULTI-ANNUAL TRENDS 22

5.1 MULTIANNUAL TRENDS - ROOT CAUSE CATEGORIES 22

5.2 MULTI-ANNUAL TRENDS - IMPACT PER SERVICE 22

5.3 MULTI-ANNUAL TRENDS - USER HOURS PER ROOT CAUSE 23

5.4 MULTI-ANNUAL TRENDS ON THE NUMBER OF INCIDENTS AND USER HOURS LOST 24

6. CONCLUSIONS 25

EXECUTIVE SUMMARY

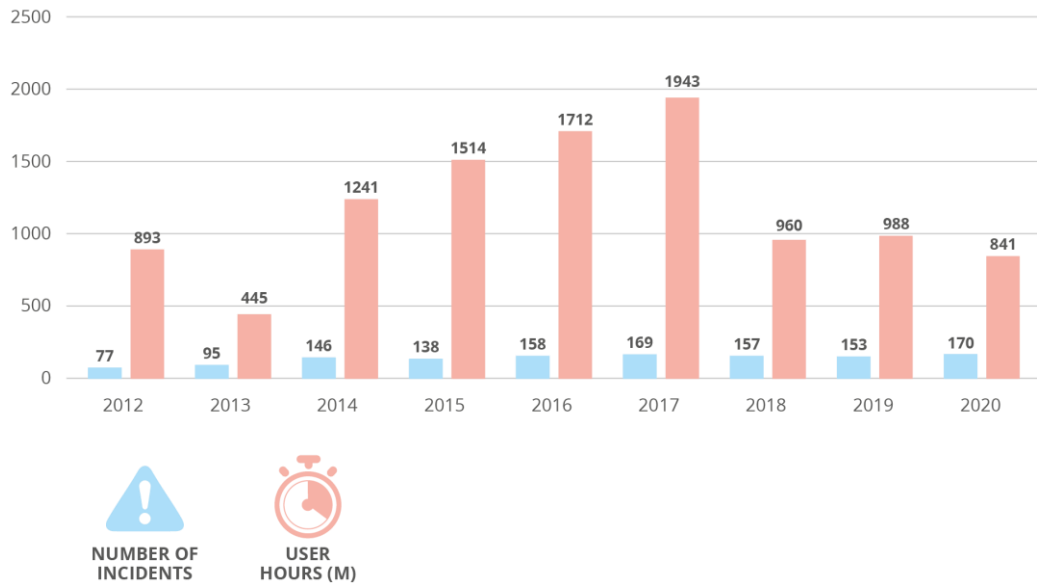
In the EU, telecom operators notify significant security incidents to their national authorities. At the start of every calendar year, the national authorities send a summary of these reports to ENISA. This report, the Annual Report Telecom Security Incidents 2020, provides anonymised and aggregated information about major telecom security incidents in 2020.

Security incident 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 European Electronic Communications Code (EECC) (2018/1972) repeals and replaces the Framework Directive. It reinforces the provisions for reporting incidents, clarifying what incidents fall within its scope and the notification criteria.

STATISTICS EXTRACTED FROM ANNUAL SUMMARY REPORTING PROCESS 2020

The 2020 annual summary reporting process contains reports of 170 incidents submitted by national authorities from 26 EU Member States and 2 EFTA countries. The total user hours lost, derived by multiplying for each incident the number of users and the number of hours, was 841 million user hours. These numbers are in line with those of previous years, as can be seen in the following graphic.

Figure 1: Number of incidents and user hours lost per year



THE KEY TAKEAWAYS FROM 2020 INCIDENTS

- **Faulty software changes/updates are a major factor in terms of impact**: In 2020, incidents related to faulty software changes/updates resulted in 346M user hours lost, which corresponds to roughly 40% of the total user hours lost. In this year's report, we dive into the numbers relating to faulty software changes (see chapter 4).
- **System failures continue to dominate in terms of impact**: System failures represent around a half of the total user hours lost (419 million user hours, 50% of

2020 HIGHLIGHTS

In 2020, half of the total user hours lost were due to system failures (50%) and almost half was lost due to human errors (41%).

All reports mention user hours lost due to high load caused by the COVID-19 pandemic.

The total user hours lost were 841 million user hours.

Over the course of 10 years, EU Member States reported a total of 1263 telecom security incidents.

total). They are also the most frequent root cause of incidents: 61% of the total reported incidents.

- **Incidents caused by human errors remain at the same level as in 2019**: More than a quarter (26%) of total incidents have human errors as a root cause and 41% of the total user hours lost were due human errors.
- **Third-party failures remain at the same level as 2019**: Almost a third of incidents were also flagged as third-party failures (29%), ie incidents that originated in a third party, say a utility company, a contractor, a supplier, etc. This number is consistent with 2019, but has tripled compared to 2018, when it was just 9%.

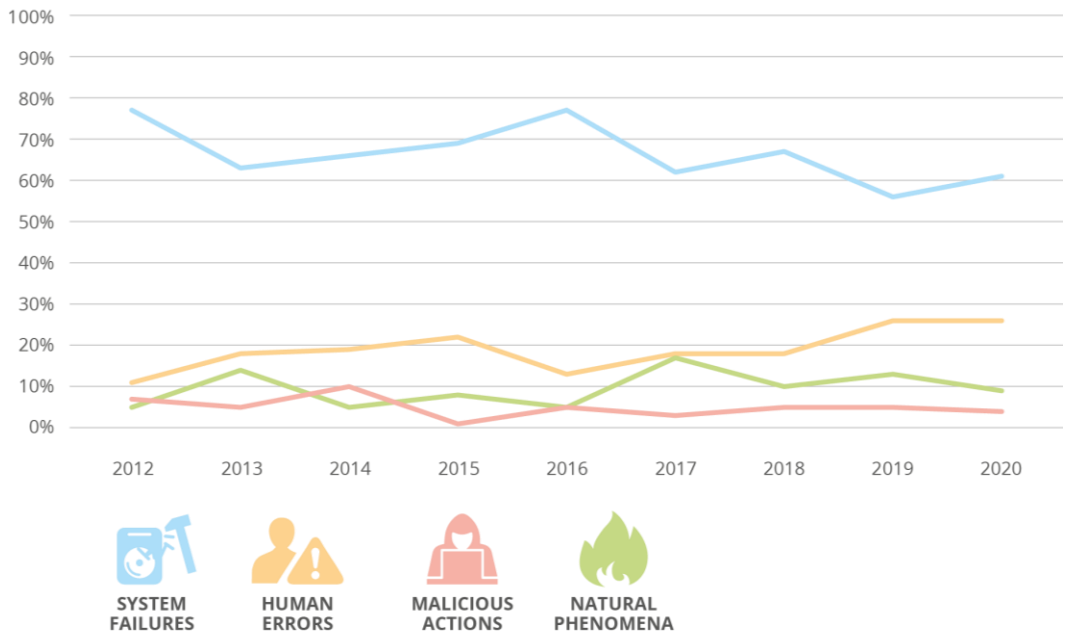
Figure 2: Share of users' hours lost per root cause category

ENISA offers an online visual tool for analysing incidents, which can be used to generate custom graphs. See: https://www.enisa.europa.eu/topics/incident-reporting/cybersecurity-incident-report-and-analysis-system-visual-analysis/visual-tool.

MULTIANNUAL TRENDS OVER THE LAST DECADE

For a decade now, ENISA and the national authorities in EU Member States have been collecting and analysing telecom security incident reports. Over the course of 10 years, EU Member States reported 1263 telecom security incidents. ENISA stores these in a tool called CIRAS and the statistics are accessible online.

Figure 3: Root cause categories Telecom security incidents in the EU reported over 2012-2020 period



Over the last couple of years, we see the following trends:

- **System failures continue to be the most frequent cause of incidents (61%), but their average size is trending downwards:** Every year system failures have been the most common category of root causes. Since 2016 the average size of these incidents has been decreasing; however, between 2019 and 2020 we observe a slight increase in user hours lost due to system failures, and a corresponding decrease in hours lost due to natural phenomena as well as due to malicious actions.
- **Number of incidents stabilizing:** The total number of incidents reported is stabilizing at around 160 annually. Over the period 2014-2020, a consistent number of incidents have been reported and this is stabilizing at around 160 incidents per year.
- **User hours lost stabilizing at a new low:** User hours lost have been stabilizing over the last three years at around 900 million a year. During these three years, stabilization in the number of user hours lost (around 900 million hours lost) was noticeable with the number of incidents approximating 160 each year.
- **Malicious actions continue to represent a minority of incidents:** Over the reporting period, the frequency of malicious actions was stable (accounting for approximately 5% of incidents per year). Their impact in terms of user hours was stable also.
- **Human errors are trending up:** The percentage of incidents caused by human errors has been trending up since 2016. In 2020 they accounted for 26% of the total number of incidents.
- **Especially in 2020 and because of the COVID-19 pandemic,** providers had to deal with major surges and shifts in usage and traffic patterns from the start of the pandemic. This gradually stabilised to what is now considered the new normal. The general take away from the pandemic is that services and networks have been resilient during the crisis, despite major changes in usage and traffic. We should not omit mentioning, however, that some countries pointed out - in the context of ENISA's relevant information-gathering exercise from the NRAs concerning the status of networks during the first months of 2020 - that there were physical attacks to base stations, masts or other telecommunication equipment, possibly related to theories that 5G can be harmful and even responsible for the COVID-19 pandemic.

Currently the focus of the national authorities for telecom security is on the transposition and implementation of the EECC, which brings several changes. The incident reporting requirements in Article 40 of the EECC have a broader scope including explicitly, for example, breaches of confidentiality. In the context of the new EECC, targeted attacks, involving for instance those using SS7 protocol vulnerabilities, SIM Swapping frauds, attacks using the Flubot malware or even more extended attacks that cause no outages, such as a wiretap on an undersea cable or a BGP hijack, would be reportable under Article 40 of the EECC.

It should be noted here also that the Commission recently made a proposal for a revised NIS Directive, the NIS2 proposal, which incorporates Article 40, and the incident reporting provisions, of the EECC.

ENISA will continue to work with national authorities as well as the NIS Cooperation group to find and exploit synergies between different pieces of EU legislation, particularly when it comes to incident reporting and cross-border supervision.

1. INTRODUCTION

Electronic communication providers in the EU have to notify security incidents that have 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, ie the most significant incidents, based on a set of agreed EU-wide thresholds. This document, the Annual Security Incidents Report 2020, aggregates the incident reports reported in 2020 and gives a single EU-wide overview of telecom security incidents in the EU.

This is the 10th year ENISA is publishing an annual incident report for the telecom sector. ENISA started publishing such annual reports in 2012. Mandatory incident 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 mandatory incident reporting under Article 13a had a specific focus on security incidents with a significant impact on the functioning of each category in telecommunication services. Over the years, the regulatory authorities have agreed to focus mostly on network/service outages (type A incidents). This would leave out of the scope of these reports targeted attacks, eg those involving the use of SS7 protocol vulnerabilities, SIM Swapping frauds, or even more extended attacks that nevertheless do not cause outages.

The relevant update of the EU telecom rules, namely the European Electronic Communications Code (EECC), that was expected to be harmonized in Member States by the end of 2020, includes a broader scope on the requirements for incident reporting in Article 40. These requirement explicitly include, for example, breaches of confidentiality. 2020 is the first time ENISA has also received three type B reports of incidents (breaches of confidentiality).

This document is structured as follows: In section 2, the policy context and background is provided. The reporting procedure is briefly summarized. In addition, the types of incidents that get reported are described. We also discuss some specific but anonymized examples of incidents that occurred in 2020. In Section 3, key facts and statistics about incidents in 2020 are provided. In Section 4, we take a closer look at faulty software changes and in section 5 we look at multi-annual trends over the years 2012-2020.

It is important to note that the telecom security incidents that are reported to national authorities are only the major incidents, those with significant impact. Smaller incidents, for example targeted DDoS attacks or SIM swapping attacks do not get reported.

Note that conclusions about trends and comparisons with previous years have to be made with a degree of caution as national reporting thresholds change over the years. Indeed reporting thresholds have been lowered in most countries in recent years and, as mentioned, reporting only covers the most significant incidents (and not smaller incidents which may well be more frequent).

10TH YEAR OF REPORTING

This is the 10th ENISA annual incident report for the telecom sector.

Mandatory incident reporting has been part of the EU's telecom regulatory framework since the 2009

2. BACKGROUND AND POLICY CONTEXT

We briefly explain the policy context and the main features of the incident reporting process, as described in Article 13a Technical Guideline on Incident Reporting[1], which was developed in collaboration with national authorities.

EECC REFORM

Reform of the telecom package: Article 13a of the Framework directive (2009/140/EC) further expanded in the European Electronic Communications Code.

2.1 POLICY CONTEXT

Security incident reporting is a hallmark of EU cybersecurity legislation and it is an important enabler for cybersecurity supervision and policymaking at national and EU level. Since 2016 security incident 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 incident 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.

By the end of 2020, the European Electronic Communications Code (EECC) came into effect across the EU, but was only implemented into national legislation in some EU countries.

Under Article 40 of the EECC the incident reporting requirements have a broader scope, including not only outages but also breaches of confidentiality, for instance. In addition, there are more services within the scope of the EECC, including not only traditional telecom operators but also, for example, over-the-top providers of communications services[2] (Messaging services like Viber and WhatsApp, etc.).

In 2020, the annual reporting guideline was updated to include new thresholds for annual summary reporting to ENISA. These combine quantitative and qualitative parameters as well as the notification of security incidents affecting not only the services of fixed and mobile internet and telephony, but also the number-based interpersonal communications services and/or number independent interpersonal communications services (OTT communications services)[3].

It is, nevertheless, important to note that the main characteristic of 2020 was the COVID-19 pandemic, which radically transformed the way people around the globe live and work, turning everything digital. As such, there was extensive supervision from the European Commission on the reporting by all Member States of incidents of network congestion.

2.2 INCIDENT REPORTING FRAMEWORK

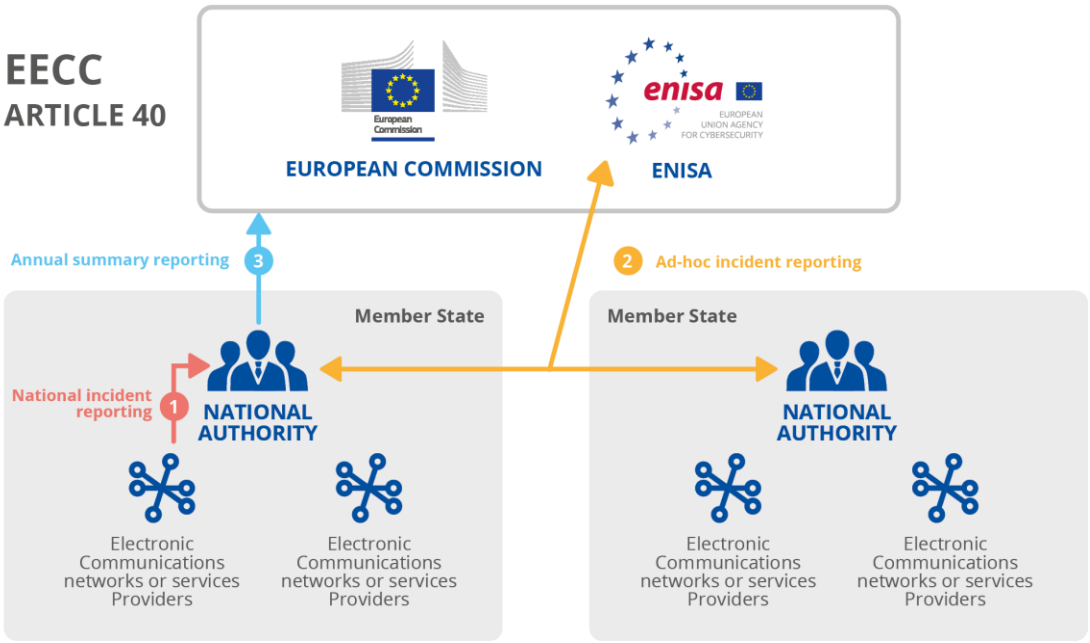
Article 13a of the Framework Directive and Article 40 of the EECC, provide for three types of incident reporting:

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

The different types of reporting are shown in the following diagram.

[1] See https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting
[2] See Security supervision changes in the new EU telecoms legislation — ENISA (europa.eu)
[3] See When & How to Report Security Incidents — ENISA (europa.eu)

Figure 4: Incident reporting under EECC article 40



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.

2.3 INCIDENT REPORTING TOOL

ENISA maintains an incident reporting tool, called CIRAS, for the authorities, where they can upload reports, and search for and study specific incidents.

For the public, ENISA also offers an online visual tool, which is publicly accessible and can be used for custom analysis of the data. This tool anonymizes the country or operator involved.

CIRAS

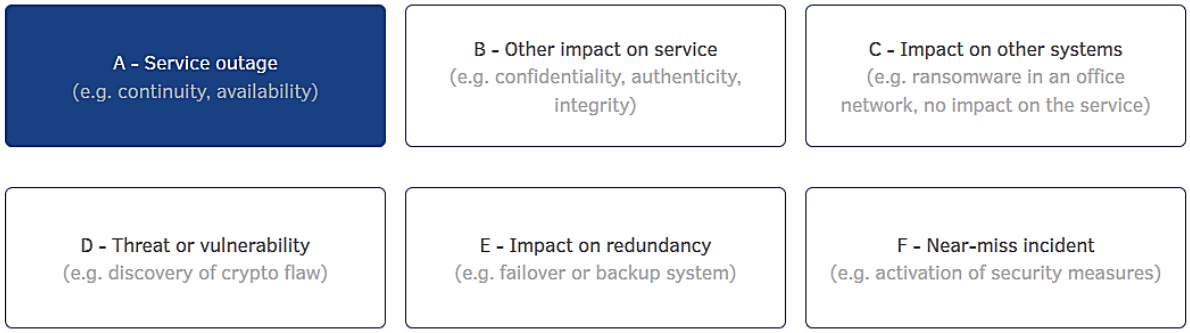
is a free online tool where ENISA stores reported incidents and provides annual and multiannual statistics: https://www.enisa.europa.eu/ciras

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

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

The type selector distinguishes six types of cybersecurity incidents. We explain the different types below.

Figure 5: Types of cybersecurity incidents



- **Type A:** Service outage (e.g. continuity, availability). For example, *an outage caused by a cable cut due to a mistake by the operator of an excavation machine used for building a new road* would be categorised as a type A incident.
- **Type B:** Other impact on service (e.g. confidentiality, authenticity, integrity). For example, *a popular collaboration tool has not encrypted the content of the media channels, which are being established when a session is started, between the endpoints participating in the shared session. This leads to the interception of the media (voice, pictures, video, files, etc.) through a man-in-the-middle attack*. This incident would be categorised as a type B incident.
- **Type C**: Impact on other systems (e.g. ransomware in an office network, no impact on the service). For example, *a malware has been detected on several workstations and servers of the office network of a telecom provider*. This incident would be categorised as a type C incident.
- **Type D:** Threat or vulnerability (e.g. discovery of crypto flaw). For instance, *the discovery of a cryptographic weakness* would be categorised as a type D incident.
- **Type E:** Impact on redundancy (e.g. failover or backup system). For example, *when one of two redundant submarine cables breaks* would be categorised as a type E incident.
- **Type F:** Near-miss incident (e.g. activation of security measures). For instance, *a malicious attempt that ends up in the honeypot network of a telecom provider* would be categorised as a type F incident.

For more information about the incident reporting process: please refer to 'Technical Guideline on Incident Reporting under the EECC'

2.4 EXAMPLES OF INCIDENTS REPORTED

Below we give some specific examples of incidents to give an idea of the types of incidents notified to NRAs by operators at a national level:

Incident example 1	
Incident type	A-Core service outage
Service affected	Emergency call routing
Root cause	System failure
Technical causes	Faulty software change/update
Assets affected	Transmission nodes, public safety answering points
Significance factors	Impact on economy and society
Comment	A failed software change for IP routing impacted the emergency call routing of 50 public safety answering points (PSAP) nationwide. The affected emergency call connections were rerouted to alternative destinations. After the server failure was resolved, the connections could be routed back to IP destinations.

Incident example 2	
Incident type	A-Core service outage
Service affected	Fixed and mobile telecommunications network
Root cause	System failure
Technical causes	Faulty software change/update
Assets affected	Switches and routers
Significance factors	Services impacted were mobile and fixed services, broadcasting services
Comment	A planned maintenance gone wrong led to the loss of all internet-based services fixed and mobile including VoLTE. The cause was a cascade of human errors. A rollback fixed the problem. The consequences were not as severe as they might have been because of the late-night maintenance window. Media coverage was huge, in large part because we had several major incidents in the space of a few weeks.

Incident example 3	
Incident type	A-Core service outage
Service affected	Mobile telecommunications network
Root cause	Malicious action
Technical causes	Arson
Assets affected	Mobile base stations and controllers
Significance factors	Number of users affected, duration of the incident, impact on economy and society
Comment	Due to an arson attack on a cell phone tower, an outage occurred on the GSM, UMTS, and LTE services.

Incident example 4	
Incident type	A-Core service outage
Service affected	Fixed Broadband Services
Root cause	System failure
Technical causes	Software bug
Assets affected	Transmission nodes
Significance factors	Services impacted were mobile and fixed services, broadcasting services
Comment	The fixed internet service (cable internet) was not available for 130 minutes. It was caused by a software error. The fault was caused by equipment operating at an international centre. The error was fixed with a software update. Due to this incident, the outage affected the whole territory of the country.

There were also some incidents reported that were related to the Covid-19 pandemic:

Incident example 5 - COVID-19 related	
Incident type	A-Core service outage
Service affected	Mobile telephony services
Root cause	System failures/third party failures
Technical causes	Overload
Assets affected	Mobile base stations and controllers
Significance factors	Medium
Comment	About 40 percent of end-users were unable to make calls to other networks (the 4G network was uninterrupted, making call apps available). About 40% of all calls in the network did not reach the recipient. The problem was caused by an unplanned load on the communication servers caused by COVID-19 quarantine. As also mentioned in the ENISA report "Telecom Security during the Pandemic"[4], in general the networks were proven adequately resilient.

Incident example 6 - COVID-19 related	
Incident type	A-Core service outage
Service affected	Fixed and mobile voice services
Root cause	System failure
Technical causes	Overload
Assets affected	Interconnection points
Significance factors	Services impacted were mobile and fixed services
Comment	Registered customer complaints that one company's users were not able to reach other networks users. Interconnect links were overloaded due to measures taken by the national government in reaction to the situation caused by the Corona virus (COVID19). Augmenting interconnection capacity and implementing gradual configuration changes eventually ameliorated the problem.

[4] See Telecom Security During a Pandemic — ENISA (europa.eu)

3. ANALYSIS OF THE INCIDENTS

For the year 2020, 26 EU Member States and 2 EFTA countries participated in the annual reporting process, describing 170 significant incidents. In this section, the 170 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 were lost in each root cause category. Detailed causes are then examined in Section 3.3, and in Section 3.4 the impact per service is analysed.

170
telecom security incidents reported in 2020 by EU Member States

3.1 ROOT CAUSE CATEGORIES

In 2020, about 26% of security incidents were caused by human errors. This is consistent with what happened in 2019 (also 26%). In addition, 61% of telecom incidents were system failures, a slight increase compared to 2019 (56%) (see figure 5).

In 2020, 29% of the incidents were also flagged as third-party failures, which is consistent with 2019 - when it was 32%. Third party failures are fairly equally represented across the four root cause categories (see figure 6).

Figure 5: Root cause categories – Telecom security Incidents in 2020

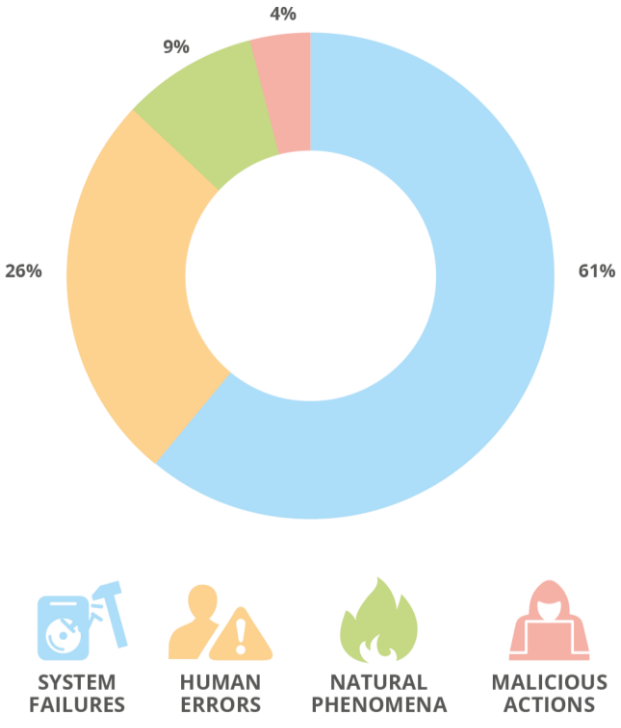
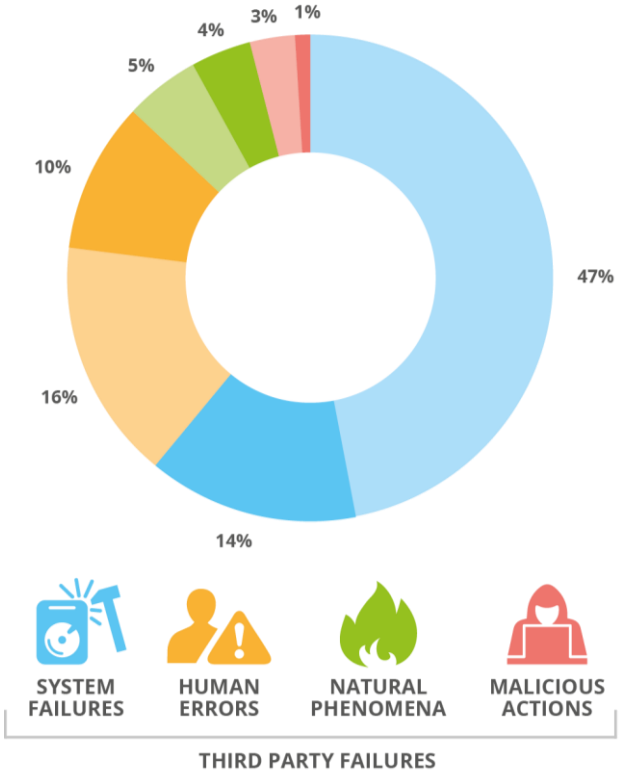


Figure 6: Root cause categories – Telecom security Incidents in 2020



3.2 USER HOURS LOST FOR EACH ROOT CAUSE CATEGORY

Adding up total user hours lost for each root cause category we find that half of the total user hours lost were due to system failures (50%, 419 million user hours). Human errors account for approximately 40% (351 million user hours).

This means that system failures are again not only the most frequent but they also cause the most impact. Human errors remain the second more common cause and this year the share of natural phenomena is smaller than in 2019, although the number of incidents caused by natural phenomena has risen.

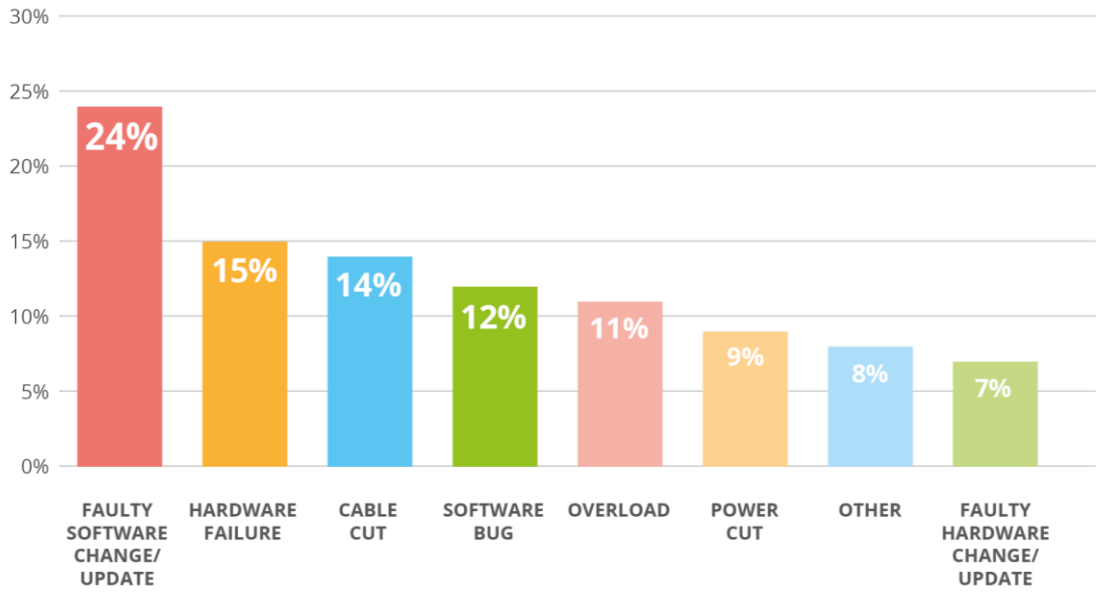
Figure 7: Share of user hours lost per root cause category

3.3 DETAILED CAUSES AND USER HOURS LOST

In all incidents we keep track of detailed causes, in addition to root cause categories. An incident is often a chain of events. For instance, an incident may be triggered by a storm, which tears down power supply infrastructure, power cuts and cable cuts, which in turn leads to a telecom outage. For this example, the root cause of the incident would be natural phenomena and the detailed causes would be: Heavy wind, Cable cut, Power cut, Battery depletion.

The most frequent detailed cause appearing in incident reports is faulty software changes/updates. Secondly, many incident reports mention hardware failures, cable cuts, software bugs and overloads. The graph below shows the frequency of detailed causes across incident reports for 2020.

Figure 8: Detailed causes – Telecom security incidents in 2020



3.3.1.1 Breakdown of System failures

The graphs below break down the main root causes of system failures, in terms of detailed causes and we show the total number of incidents and user hours lost for each detailed cause.

Figure 9: System failures – detailed causes

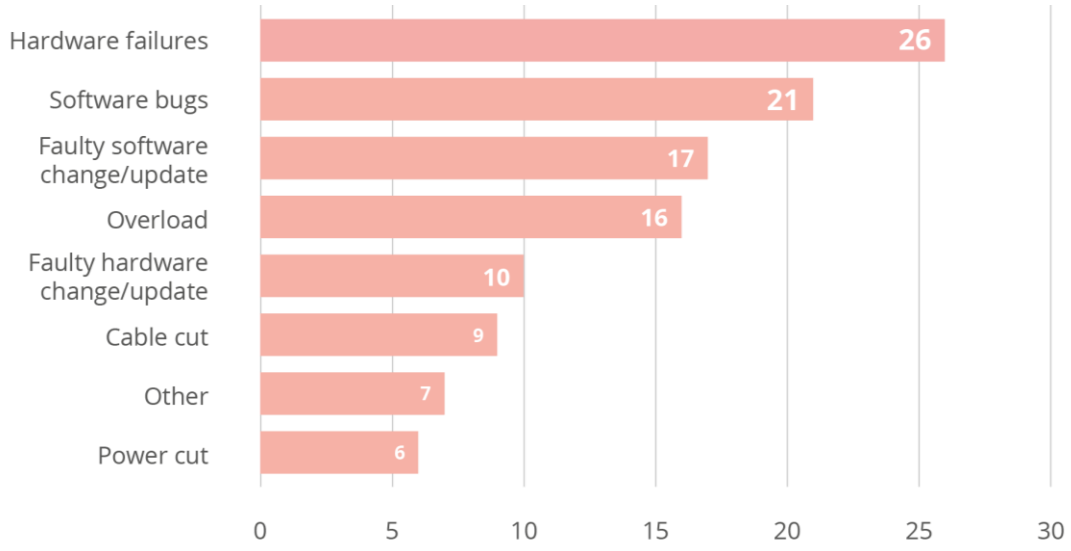
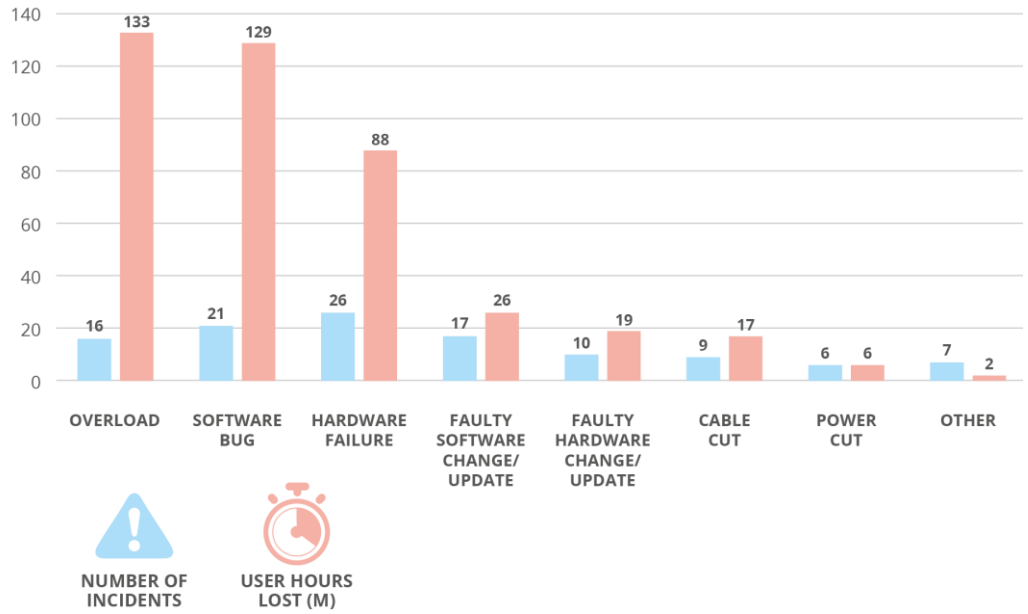


Figure 10: System failures vs detailed causes: number of incidents and user hours lost



3.3.1.2 Break down of Human errors

Figure 11: Human errors detailed causes

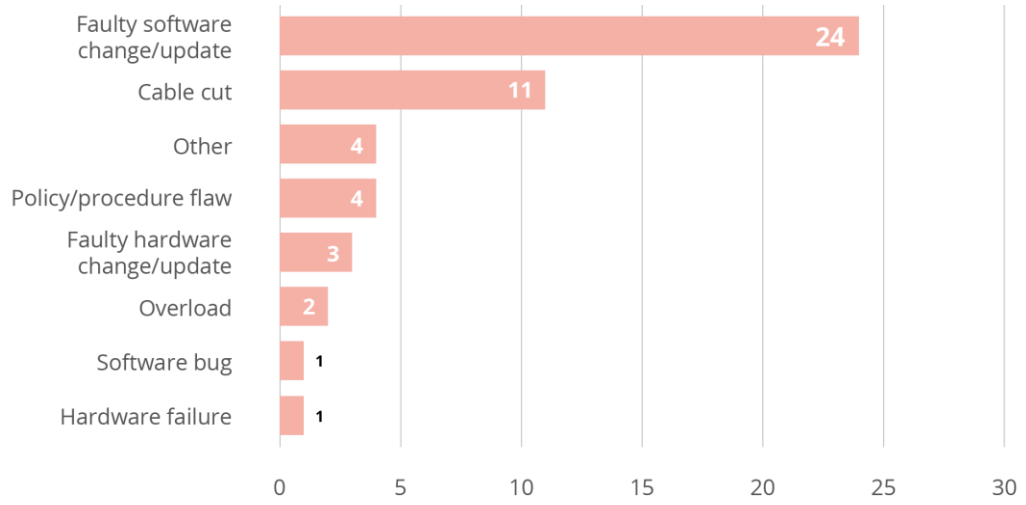
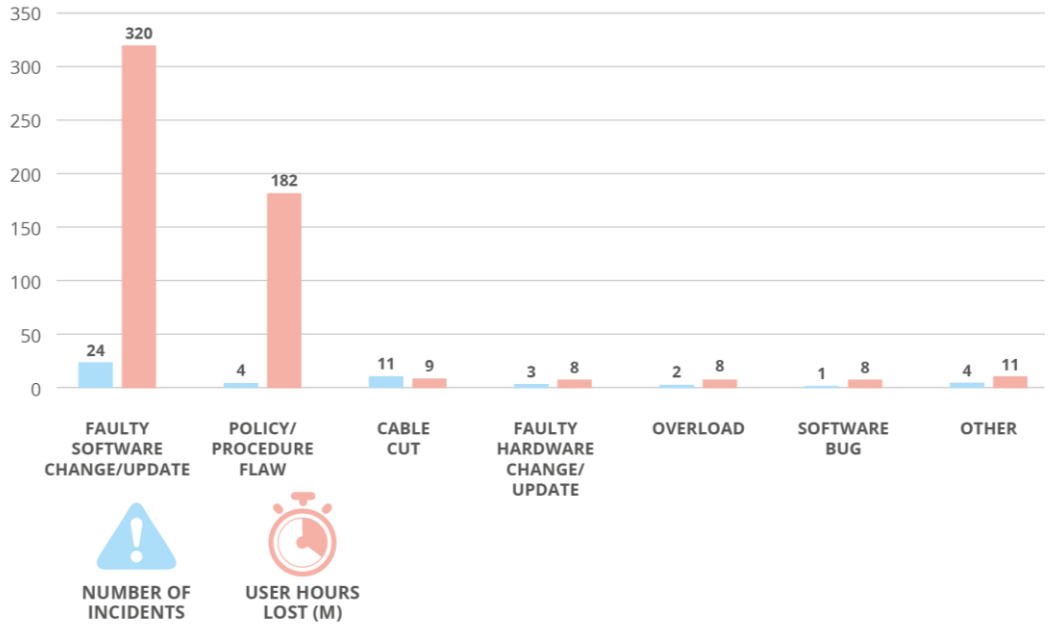


Figure 12: Human errors vs detailed causes: number of incidents and user hours lost



3.3.1.3 Break down of natural phenomena

Figure 13: Natural phenomena – detailed causes

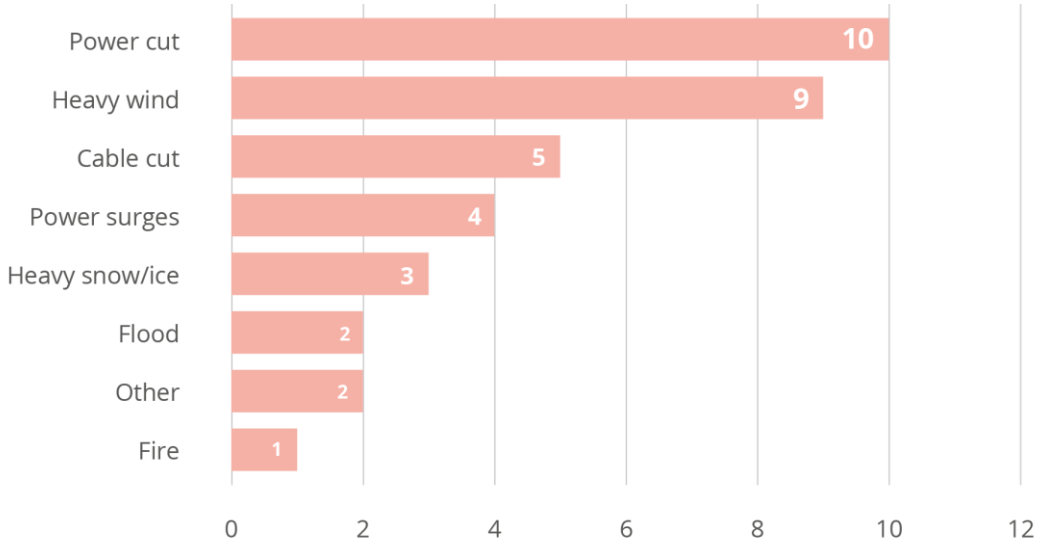
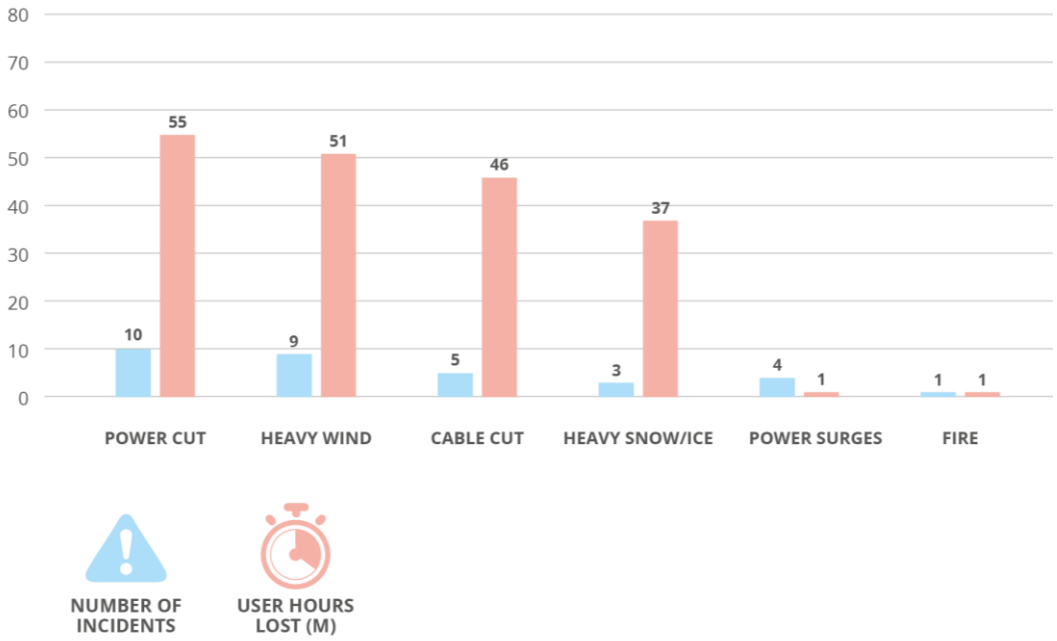


Figure 14: Natural phenomena vs detailed causes: number of incidents and user hours lost



3.3.1.5 Break down of malicious actions

Figure 15: Malicious actions – detailed causes

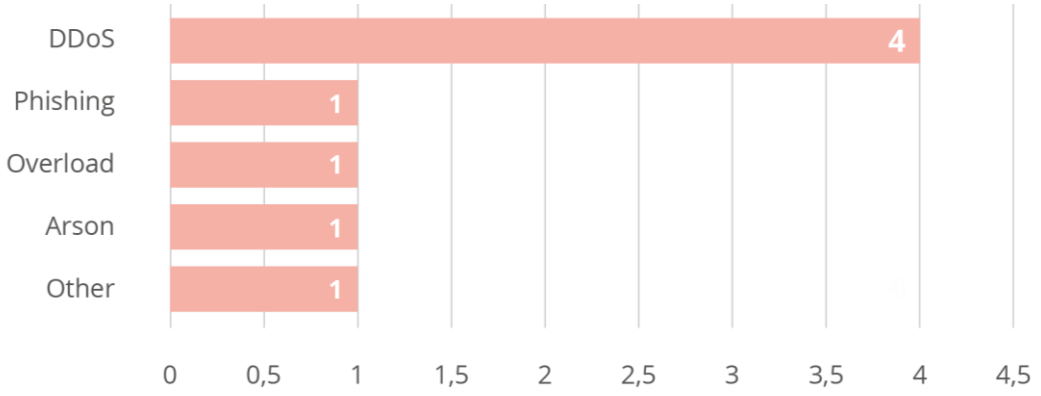
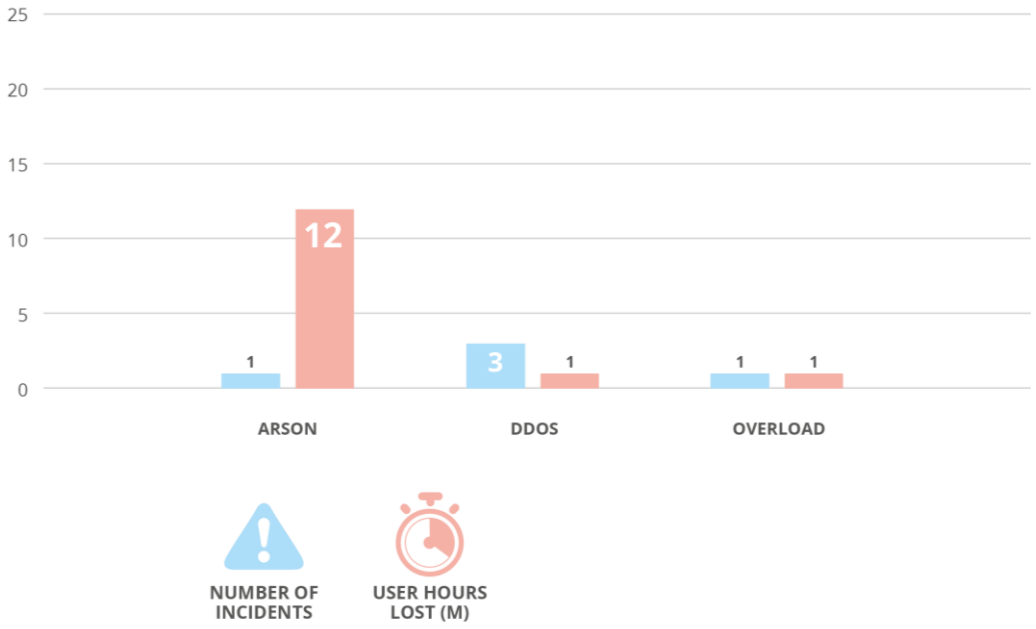


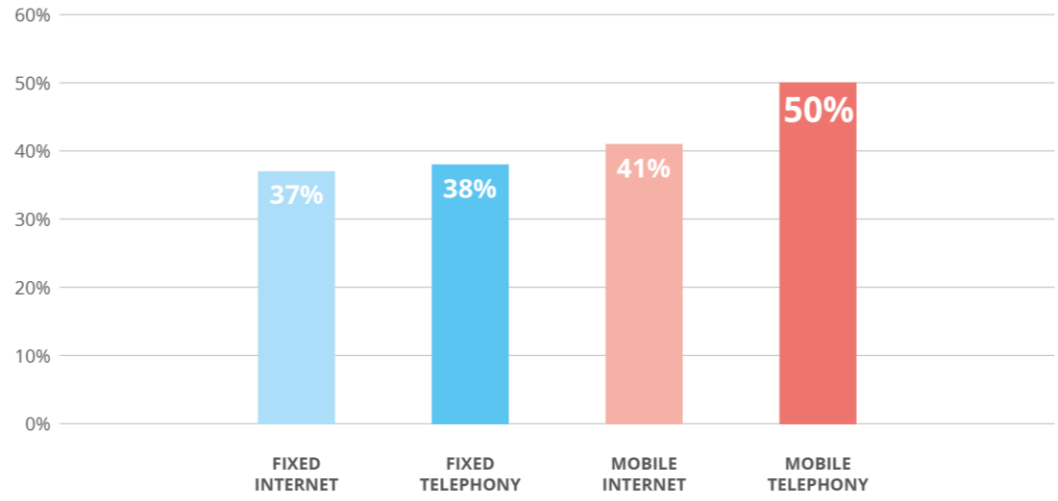
Figure 16: Malicious actions vs detailed causes: number of incidents and user hours lost



3.4 SERVICES AFFECTED

In this section we look at the services affected by the incidents. For the fifth year in a row, most of the reported incidents affected mobile services. In 2020, half of the incidents reported had an impact on mobile telephony and internet in the EU. This confirms the shift observed over the last few years from fixed telephony, which was most affected as a service only in the early years of reporting.

Figure 16: Services affected – Telecom security incidents in 2020

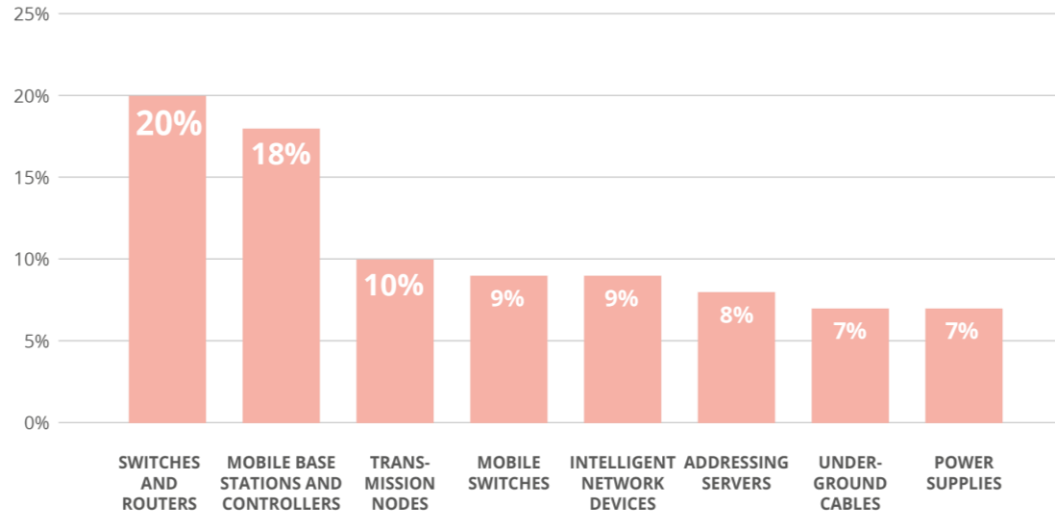


Note that for most reported incidents there was an impact on more than one service, which explains why the percentages in the chart here add up to more than 100%.

3.5 TECHNICAL ASSETS AFFECTED

Each incident report also describes the (secondary) assets affected during the incident. The graph below shows the assets most affected.

Figure 17: Assets affected – Telecom security incidents in 2020



What we noticed also, taking multinational trends into account, is that switches and routers as well as mobile base stations and controllers are the two assets affected the most over the last few years.

4. ANALYSING INCIDENTS CAUSED BY FAULTY SOFTWARE CHANGES/UPDATES

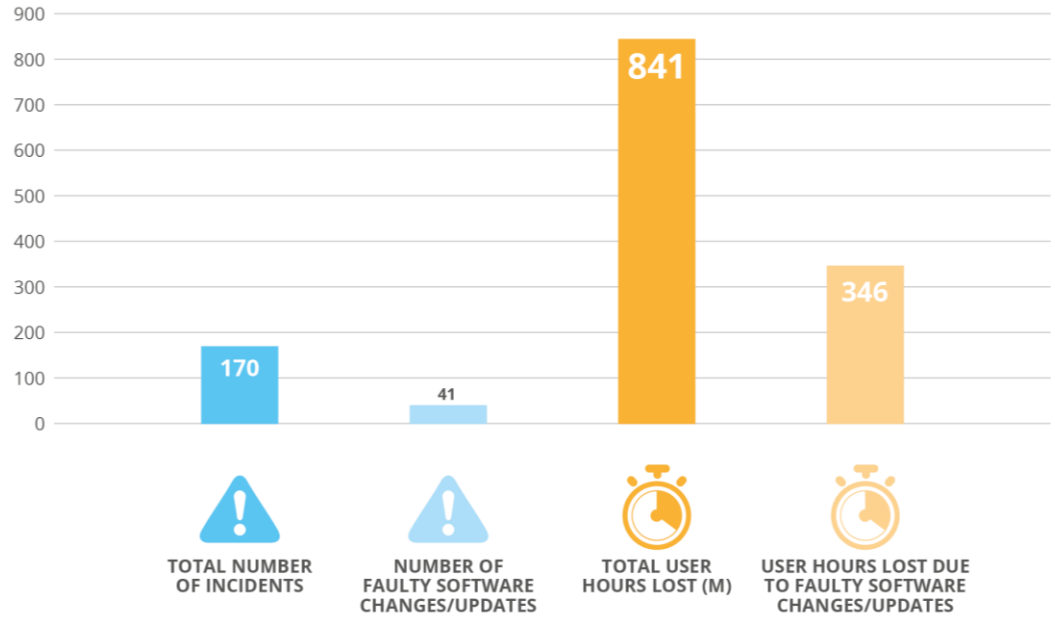
In this section we dive into faulty software changes, which have been a major cause of incidents, not only last year but also in previous years.

346 M
user hours lost due to faulty software changes/updates in 2020, 41% of the total

4.1 FAULTY SOFTWARE CHANGES/UPDATES IN 2020

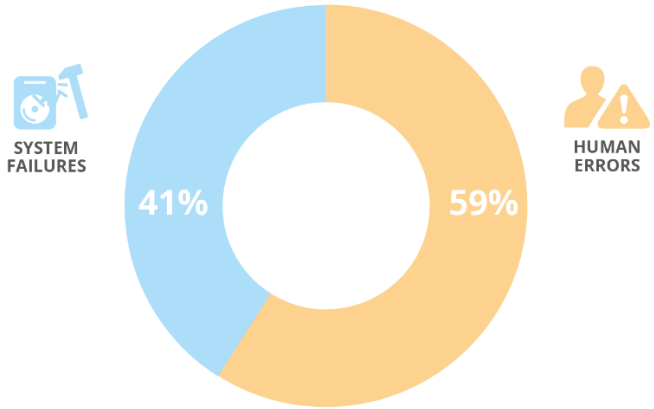
In 2020, 24% of total incidents marked as faulty software changes/updates resulted in 346 million user hours lost (41% of the total).

Figure 18: Faulty software changes/updates in 2020



In 2020, 60% of incidents having faulty software changes/updates as a cause were categorized under human errors, while the remaining 40% was classified under system failures.

Figure 19: Root cause - Faulty software changes/updates in 2020



4.2 FAULTY SOFTWARE CHANGES/UPDATES – MULTI-ANNUAL

Over the past 10 years of reporting, ENISA has collected 220 incidents where a faulty software change/update was a detailed cause. In total, these incidents caused a loss of 2,176M user hours. The majority of these incidents were categorized under either system failures or under human errors.

Figure 20: Faulty software changes/updates per year

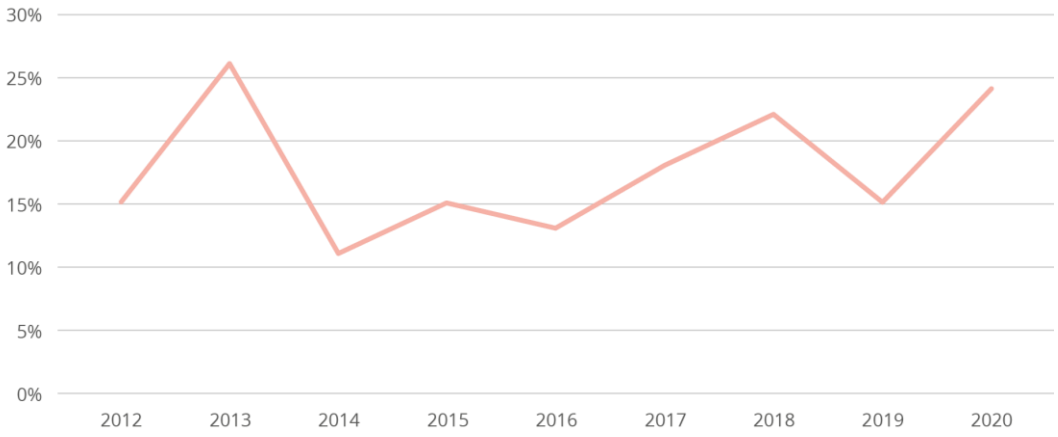
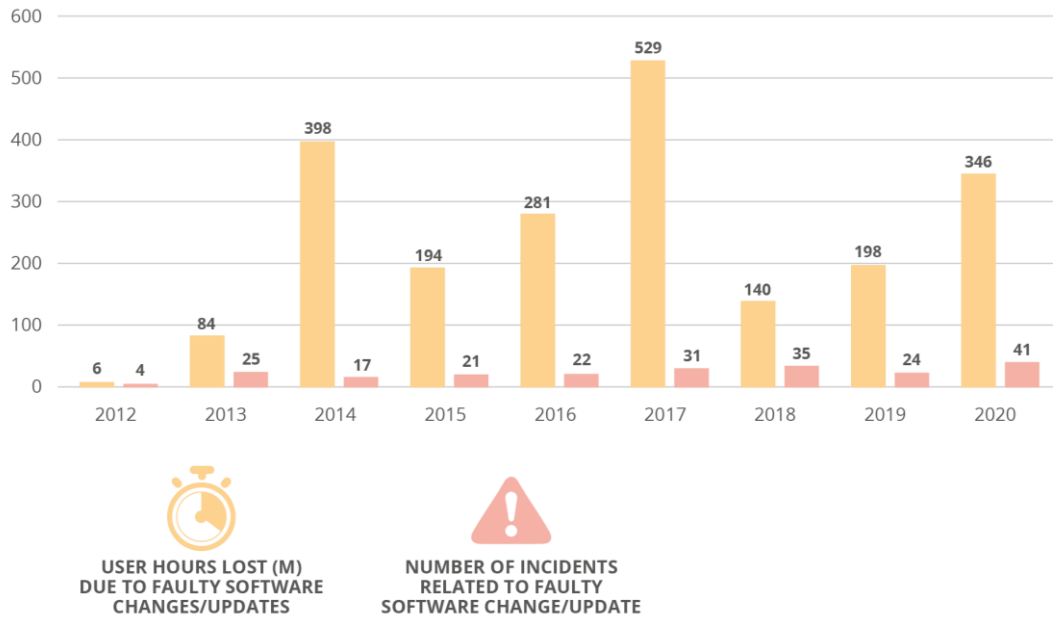


Figure 21: Frequency and impact of faulty software changes/updates per year



5. MULTI-ANNUAL TRENDS

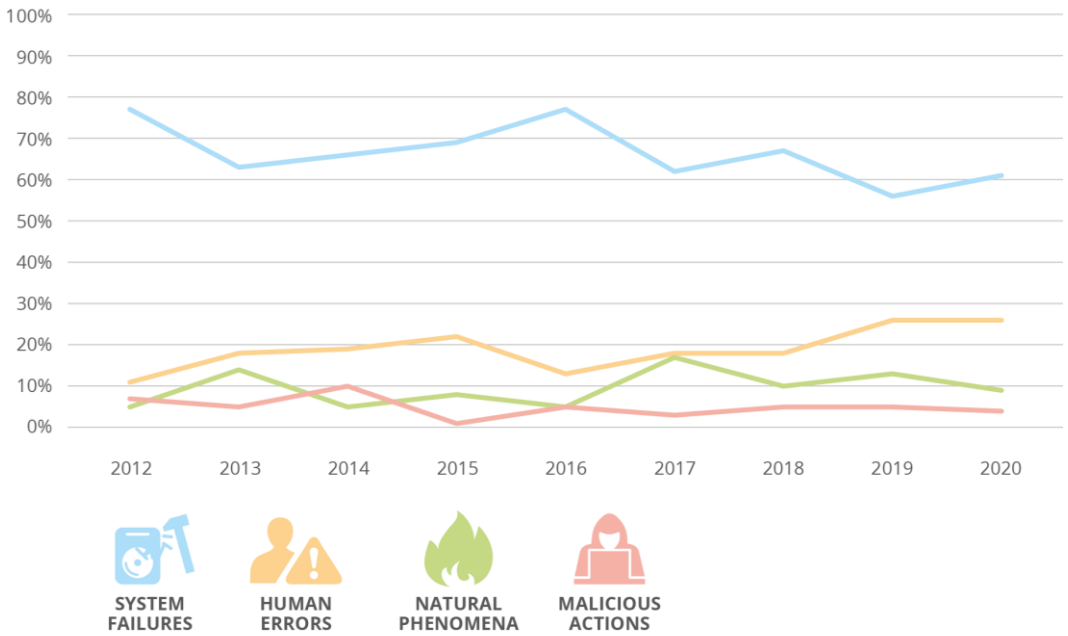
ENISA has been collecting and aggregating incident reports since 2012. In this section, we present multiannual trends over the last 10 years, from 2012 to 2020. This dataset contains 1263 reported incidents in total.

1263
telecom security incidents reported in 10 years by EU Member States.

5.1 MULTIANNUAL TRENDS – ROOT CAUSE CATEGORIES

Every year from 2012 to 2020, system failures were the most common root cause. In 2020, however, system failures show stabilization and a slight decrease. In total, system failures accounted for 826 of incident reports (65% of the total). For this root cause category, over the last 9 years, the most common causes were hardware failures (36%) and software bugs (28%). The second most common root cause over the 9 years of reporting is human errors with nearly a fifth of total incidents (19%, 202 incidents in total). Natural phenomena come third at almost a tenth of total incidents (9%, 109 incidents in total). Only 5% of the incidents are categorized as malicious actions. In the period 2012-2020 nearly two thirds of the malicious actions consist of Denial of Service attacks, and the rest resulted mainly in lasting damage to physical infrastructure.

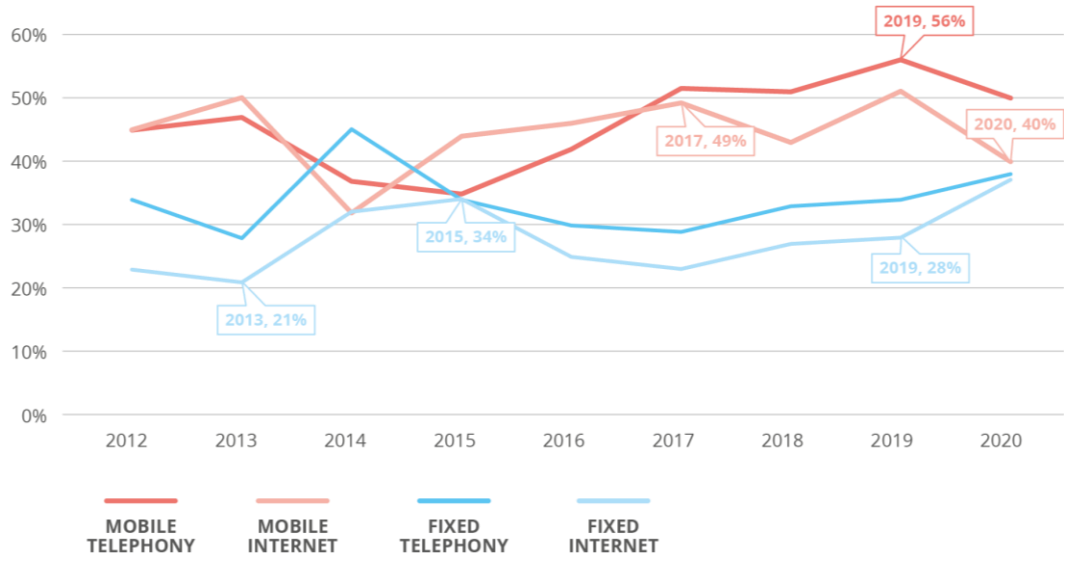
Figure 22: Root cause categories - Telecom security incidents in the EU reported over 2012-2020



5.2 MULTI-ANNUAL TRENDS - IMPACT PER SERVICE

In 2020, mobile networks and services were once more the most impacted by incidents. However there was a decrease compared to 2019 and interestingly the statistics in terms of services affected are converging for both fixed and mobile.

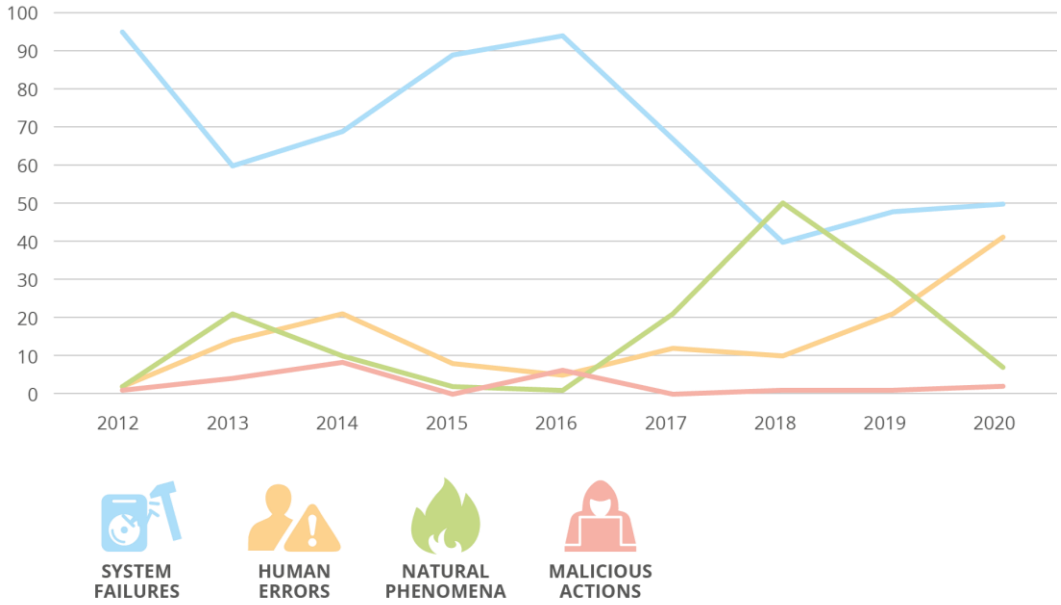
Figure 23: Trends on impact per classic services reported over 2012-2020



5.3 MULTI-ANNUAL TRENDS - USER HOURS PER ROOT CAUSE

In terms of overall impact, human errors have been steadily increasing since 2016. In 2020, their share in terms of impact was almost the same as system failures. The overall impact of natural phenomena has been trending down over the last two years after peaking in 2018 (caused by extreme weather and wildfires).

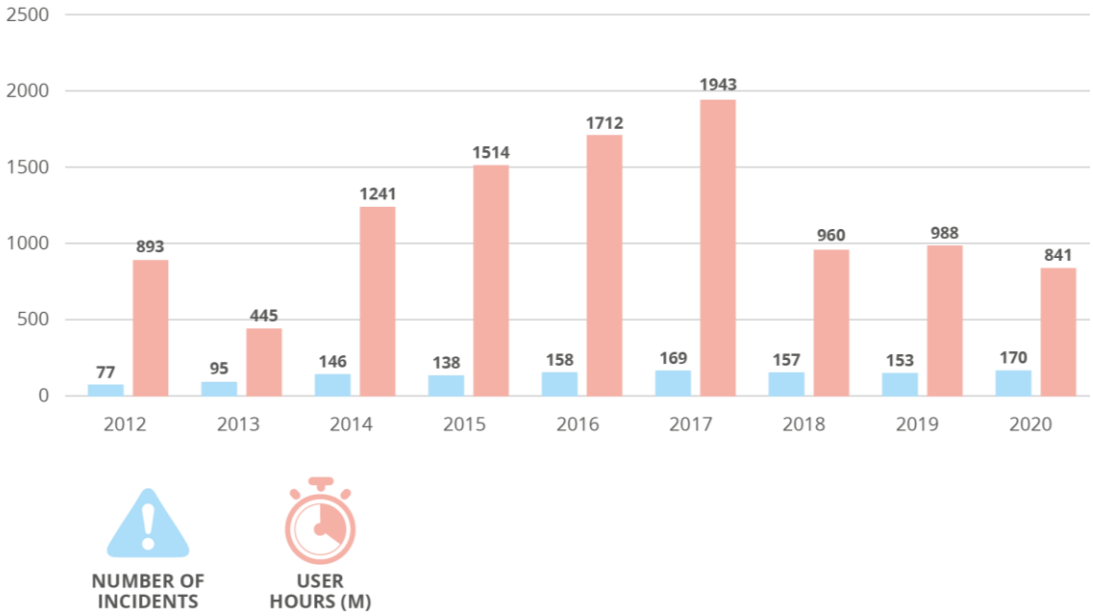
Figure 24: User hours lost per root cause category - multi-annual 2012-2020 (percentage of total user hours lost)



5.4 MULTI-ANNUAL TRENDS ON THE NUMBER OF INCIDENTS AND USER HOURS LOST

Over the years, the number of incidents has increased steadily and is now stabilizing at around 160-170 per year.

Figure 24: Number of incidents and user hours lost per year



6. CONCLUSIONS

This document, the Annual Report Telecom Security Incidents 2020, covers the incidents reported by the authorities for the calendar year 2020 and it gives an anonymised, aggregated EU-wide overview of telecom security incidents. It marks the 10th time ENISA has published an annual report for the telecom sector. We conclude with the main findings and some more general observations about this process and the broader policy context.

MAIN FINDINGS

- **Faulty software changes/updates are a major factor in terms of impact.** In 2020, incidents related to faulty software changes/updates resulted in 346M user hours lost, which corresponds to roughly 40% of the total user hours lost.
- **System failures continue to dominate in terms of impact.** System failures represent around a half of the total user hours lost (419 million user hours, 50% of total). They are also the most frequent root cause of incidents: 61% of the total reported incidents.
- **Incidents caused by human errors remain at the same level as in 2019.** More than a quarter (26%) of total incidents have human errors as a root cause and 41% of the total user hours have been lost due to this kind of incident.
- **Third-party failures remain at the same level.** Almost a third of the incidents were also flagged as third-party failures (29%), ie, incidents which originated in a third party, say a utility company, a contractor, a supplier, etc.

GENERAL OBSERVATION

- By the end of 2020, the European Electronic Communications Code (EECC) came into effect across the EU. Some countries have already implemented the EECC but many are still transposing. Transposing the EECC and implementing its provisions will be a key focus for ENISA and the national authorities this year and in the coming years.
- Under Article 40 of the EECC, the incident reporting provisions have changed slightly[5]. For instance, under the EECC, mandatory incident reporting also applies to independent interpersonal communications services (OTT communications services). To address these changes ENISA published a new incident reporting guideline at the start of 2020. From 2021, we will start to see these changes in the reporting data
- One issue already mentioned is the fact that many smaller scale incidents, however frequent, remain under the radar. Some of these incidents, such as targeted DDoS attacks, SIM swapping and SS7 attacks, can still have major impacts on individual customers. In coming years, we would like to analyse this area better and possibly introduce a summary reporting format for these smaller scale incidents.
- The 5G roll out will continue to require a lot of attention, both from authorities and from the providers. At ENISA, we are focusing on supporting the national authorities in the ENISA ECASEC group and in the NIS Cooperation group, with technical guidance, but also by organizing dedicated seminars and panels.

We look forward to continuing our close collaboration with EU Member States, the national telecom authorities and experts from the telecom sector from across Europe to implement security incident reporting efficiently and effectively.

[5] Technical Guideline on Incident Reporting under the EECC — ENISA (europa.eu)

TP-09-21-273-EN-N

ABOUT ENISA

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

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14, Chalandri 15231, Attiki, Greece

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

enisa.europa.eu

ISBN: 978-92-9204-510-4
DOI: 10.2824/774362