EUROPEAN UNION AGENCY
FOR CYBERSECURITY

TELECOM SECURITY INCIDENTS 2021

Annual Report

JULY 2022

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 info@enisa.europa.eu.
For media enquiries about this paper, please email press@enisa.europa.eu.

AUTHORS

Apostolos Malatras, Georgia Bafoutsou, Edgars Taurins, 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

It should be noted that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed as a legal action of ENISA or ENISA bodies unless adopted pursuant to Regulation (EU) No 526/2013. This publication may be updated by ENISA from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

COPYRIGHT NOTICE

© European Union Agency for Cybersecurity (ENISA), 2022
Reproduction is authorised provided the source is acknowledged.

Copyright for the image on the cover: © Shutterstock
For any use or reproduction of photos or other material that are not under ENISA copyright, permission must be sought directly from the copyright holders.

Catalogue number: TP-07-22-711-EN-N
ISBN: 978-92-9204-582-1
DOI: 10.2824/528645

TABLE OF CONTENTS

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 2021*, provides anonymised and aggregated information about major telecom security incidents in 2021.

The reporting of security incidents has been part of the EU's regulatory framework for telecoms since the 2009 reform of the telecoms 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.

In 2021, 7% of the total user hours lost were due to system failures and an excessive amount was lost due to human errors (90%).

The downwards trend concerning impact on mobile telephony that commenced in 2019 continued in 2021.

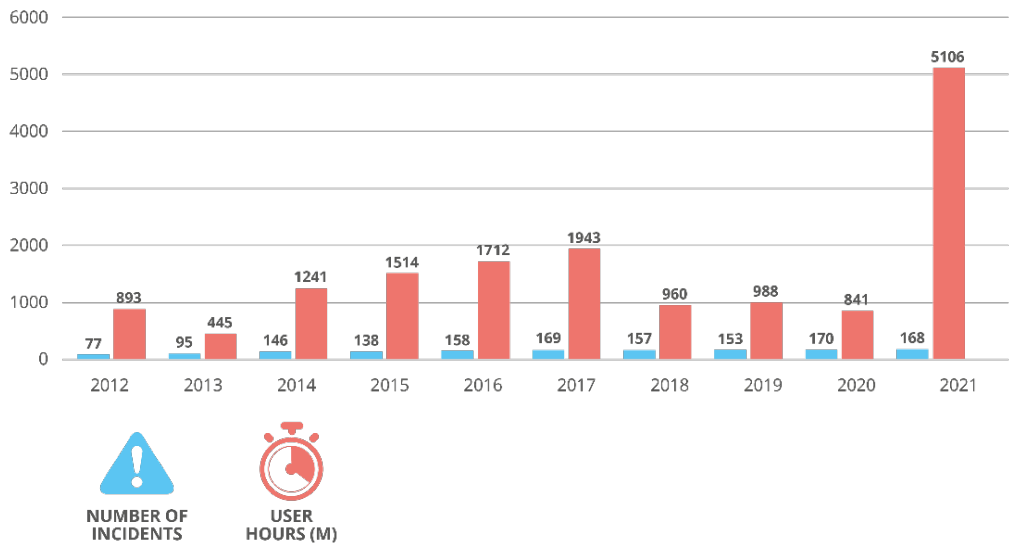
The total user hours lost in 2021 was 5,106 million user hours.

Over the course of 11 years, EU Member States reported a total of 1,431 telecom security incidents.

STATISTICS EXTRACTED FROM THE ANNUAL SUMMARY REPORTING PROCESS 2021

The 2021 annual summary contains reports of 168 incidents submitted by national authorities from 26 EU Member States (MS) and 2 EFTA countries. The total user hours lost, derived by multiplying for each incident the number of users by the number of hours, was 5,106 million user hours, a huge increase compared to 841 million user hours lost in 2020. These numbers are clearly much higher compared to those of previous years, as can be seen in the following graphic.The reason for this is the impact of a notable EU-wide incident that was reported separately by three MS. ENISA has published technical guidelines on incident reporting under the EECC[1], including on thresholds and calculating hours lost.

Figure 1: Number of incidents submitted by countries and user hours lost each year (2012-2021)



THE KEY TAKEAWAYS FROM INCIDENTS IN 2021

- **Reporting of incidents related to OTT services requires further attention.** Four per cent of reported incidents in 2021 refer to OTT communication services (4,16%). The

[1] See https://www.enisa.europa.eu/publications/enisa-technical-guideline-on-incident-reporting-under-the-eecc, March 2021

same EU-wide OTT incident was reported three times by three different MS in three different ways, so there is a need for clarity as to who reports such incidents, which authority is in charge and what information is reported. The results of incident reporting in 2021 are skewed because of the huge impact caused by this incident being reported three times.

- **For the first time, incidents concerning confidentiality and authenticity were reported.** The reporting of such incidents was a new provision of EECC and in this respect no such incidents were reported in previous years. Three relevant incidents were reported in 2021 and this number is expected to grow in coming years.

- **Malicious actions doubled in 2021.** In 2020, incidents marked as malicious actions represented 4% of the total, a number which rose to 8% in 2021. Moreover, it is interesting to highlight the significant increase in DDoS attacks compared to 2020 when only four such incidents had been reported resulting in 1 million user hours lost. By comparison, in 2021 ten DDoS related incidents were reported, leading to a loss of 55 million user hours. These results are consistent with the findings of the ENISA Threat Landscape that point to an increase in DDoS attacks and a general increase in attacks against availability of services.

- **System failures continue to dominate in terms of impact but the downward trend continues.** System failures accounted for 363 million user hours lost compared to 419 million user hours in 2020. Despite the skewed nature of the 2021 results, it is noteworthy that there was a 14% decrease in user hours lost, whereas in terms of the number of incidents in 2021 they represent 59% of the total compared to 61% in 2020. This highlights the growing maturity of electronic communication providers in handling and containing the impact of system failures.

- **Incidents caused by human errors remain at the same level as in 2020.** Around a quarter (23%) of total incidents have human errors as a root cause (a slight decrease compared to 26% in 2020), however 91% of the total user hours lost have been lost due to this kind of incident. These results however are skewed due to the OTT communication services incident reporting issues mentioned above.

- **In 2021, there was a noteworthy decrease in incidents flagged as failures by third parties.** Only 22% of incidents were reported as being related to third-party failures compared to 29% in 2020 and 32% in 2019. No third-party failures related to malicious actions were reported. Overall, the finding suggests that electronic communication providers have started introducing targeted security controls to better protect their supply chains, echoing the relevant ENISA calls for attention[2].

[2] See https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

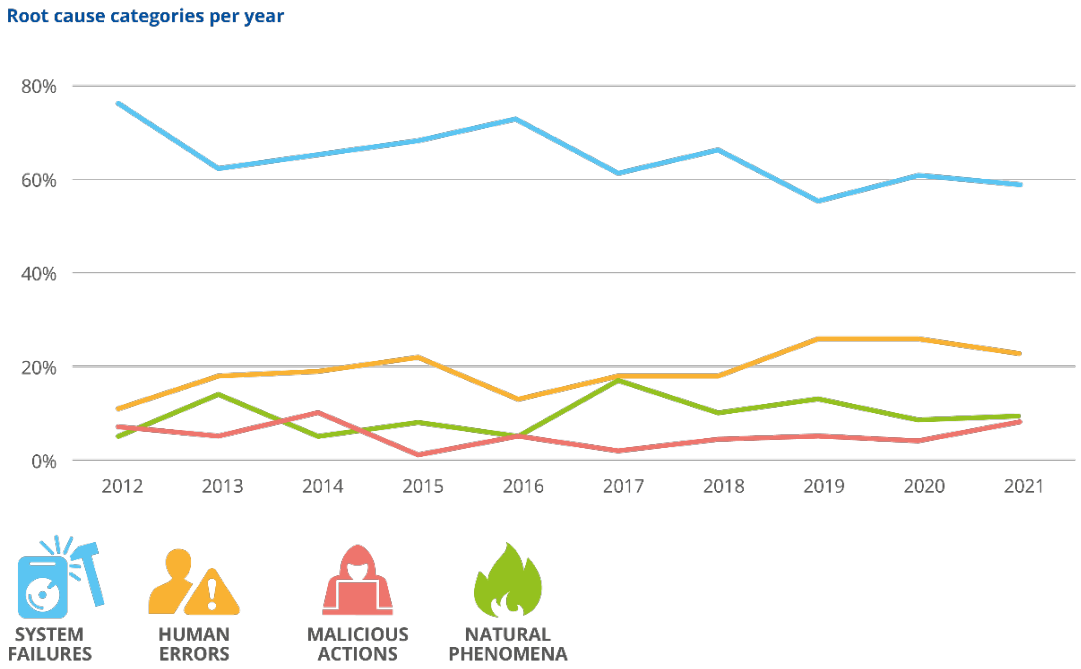
Figure 2: Share of users' hours lost for each root cause category

ENISA offers an online visual tool for analysing incidents, which can be used to generate custom graphs. See: https:/ciras.enisa.europa.eu.

MULTI-ANNUAL TRENDS OVER THE LAST DECADE

For more than 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 11 years, EU Member States reported 1,431 telecom security incidents. ENISA stores these in a tool called CIRAS (Cybersecurity Incident Reporting and Analysis System) and the statistics are accessible online.

Figure 3: Root cause categories for telecom security incidents in the EU reported over 2012-2021 period



Over the last couple of years, the following trends have been noted:

- **Number of incidents is stabilising:** the total number of incidents reported is stabilising at around 160 annually. Over the period 2014-2021, a consistent over the years number of incidents have been reported and this is stabilising at around 160 incidents per year.
- **Malicious actions continue to constitute a minority of incidents:** over the reporting period, the frequency of malicious actions was stable (accounting for approximately 5% of incidents each year, although in 2021 there was a spike at 8%). Their impact in terms of user hours was stable also.

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 addition, the arrival of the Network and Information Security (NIS) Directive 2 in 2022 is expected to be a game changer in incident reporting, since it consolidates the reporting of security breaches across a variety of legislations including but not limited to the EECC.

Moreover, 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 wiretapping or a BGP hijack, would be reportable under Article 40 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, i.e. the most significant incidents, based on a set of agreed EU-wide thresholds. This document, the *Annual Security Incidents Report 2021*, aggregates the incident reports received in 2021 and gives a single EU-wide overview of telecom security incidents in the EU.

This is the 11th year ENISA is publishing an annual incidents report for the telecom sector. ENISA started publishing these 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 reporting of incidents under Article 13a had a specific focus on security incidents with a significant impact on the functioning of each category of telecommunication services. Over the years, the regulatory authorities have agreed to focus mostly on network/service outages (type A incidents). This would exclude from the scope of these reports targeted attacks, e.g. 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 harmonised in Member States by the end of 2020, includes a broader scope on the requirements for incident reporting in Article 40. These requirements explicitly include, for example, breaches of confidentiality. 2021 is the second 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 summarised. In addition, the types of incidents that get reported are described. Some specific but anonymised examples of incidents that occurred in 2021 are also discussed. In Section 3, key facts and statistics about incidents in 2021 are provided. In Section 4, there is a closer look at faulty software changes, and in section 5 a look at multi-annual trends over the years 2012-2021.

It is important to note that the telecom security incidents that are reported to national authorities are only the major incidents, i.e. those with significant impacts. Smaller incidents, affecting small percentages of population such as SIM Swapping attacks are not 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 that may well be more frequent).

This is the 11th ENISA annual incident report for the telecom sector.

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

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

2. BACKGROUND AND POLICY CONTEXT

In this chapter the policy context is explained as well as the main features of the incident reporting process, as described in Article 13a Technical Guideline on Incident Reporting[3], which was developed in collaboration with national authorities.

2.1 POLICY CONTEXT

Security incident reporting is a hallmark of EU cybersecurity legislation and it is an important enabler for the supervision of cybersecurity and for 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. The year 2021 saw progress in the implementation of EECC by MS; however the process has not yet been completed.

Under Article 40 of the EECC the incident reporting requirements have a broader scope, including not only outages but also, for instance, breaches of confidentiality. 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[4] (such as 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 number-based interpersonal communications services and/or number independent interpersonal communications services (OTT communications services)[5].

It is, nevertheless, important to note that the main characteristic of 2020 and 2021 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. Comparing incident reporting results from 2019 and before, it is fair to conclude that the European telecommunication networks have shown robustness and resilience.

2.2 INCIDENT REPORTING FRAMEWORK

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

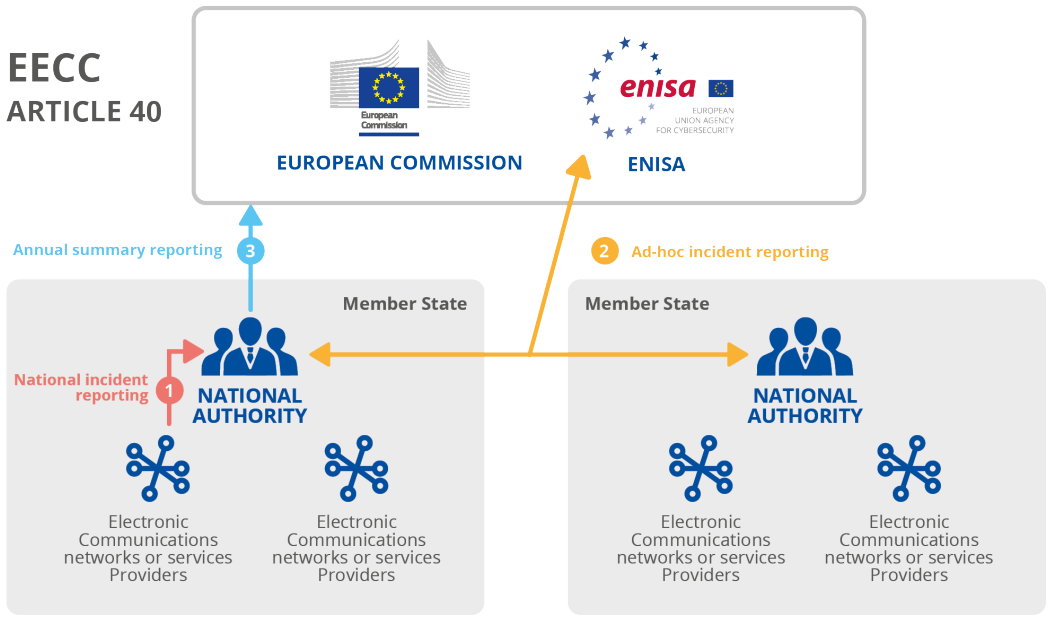
1) National incident reporting from providers to NRAs,
2) Ad-hoc incident reporting between NRAs and ENISA, and

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

3) Annual summary reporting from national authorities to the EC and ENISA.

The different types of reporting are shown in Figure 4.

Figure 4: Incident reporting under EECC article 40



Note that in this setup ENISA acts as a collection point, anonymising, 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, 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: https://ciras.enisa.europa.eu/. This tool anonymises the country or operator involved.

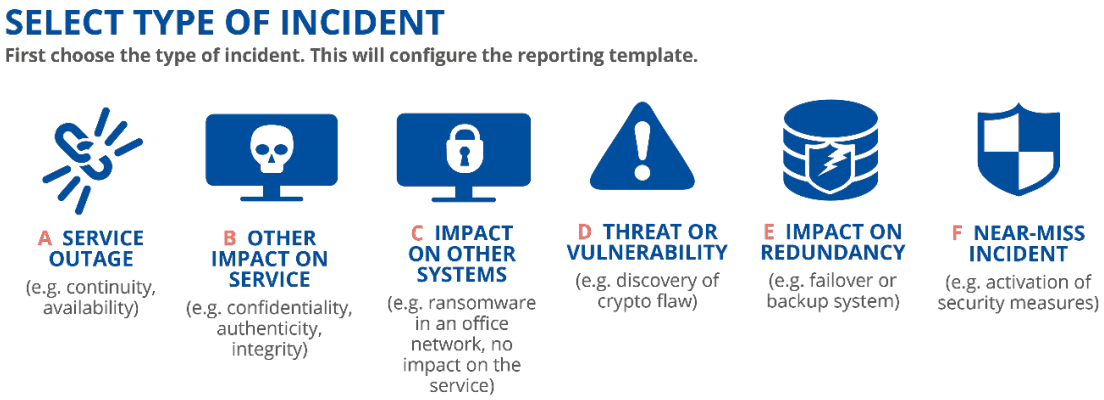
The reporting template starts with a selector for the type of incident and contains three parts:

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

CIRAS
is a free online tool where ENISA stores reported incidents and provides annual and multi-annual statistics.

The type selector distinguishes six types of cybersecurity incidents (see Figure 5). The different types are explained 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'[6]

[6] See https://www.enisa.europa.eu/publications/enisa-technical-guideline-on-incident-reporting-under-the-eecc

3. ANALYSIS OF INCIDENTS

For the year 2021, 26 EU Member States and 2 EFTA countries participated in the annual reporting process, describing 168 significant incidents (compared to 170 in 2020). In this section, the 168 reported incidents are aggregated and analysed. First, the impact on each root cause category is analysed in section 3.1. In section 3.2 the focus is 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 on each service is analysed.

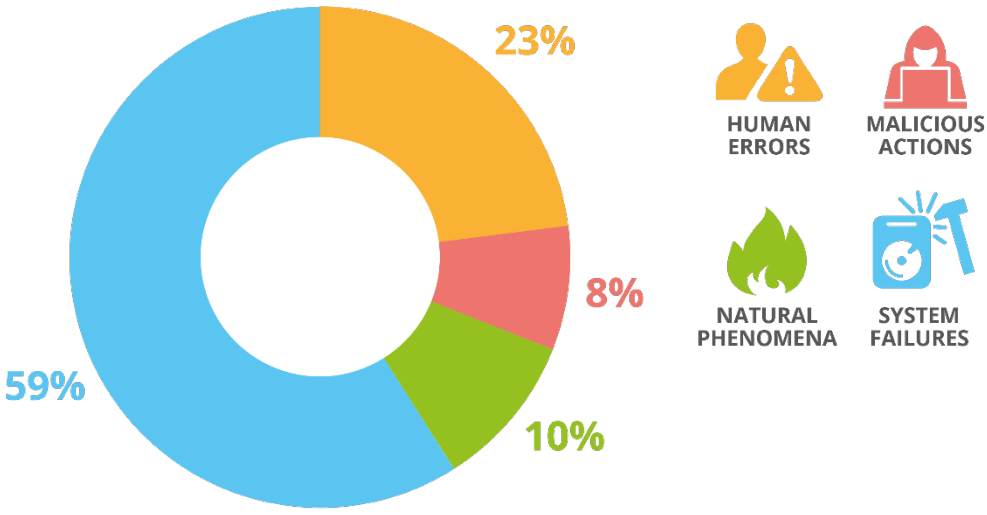
168 telecom security incidents reported in 2021 by EU Member States.

One of the highlights of incident reporting under the EECC in 2021 is the fact that for the first time three out of the 168 incidents were marked as Type B, namely as impacting confidentiality and authenticity of services. All the other incidents impacted availability and were thus marked as Type A. Incidents of the other 4 types were not reported in 2021.

3.1 CATEGORIES OF ROOT CAUSES

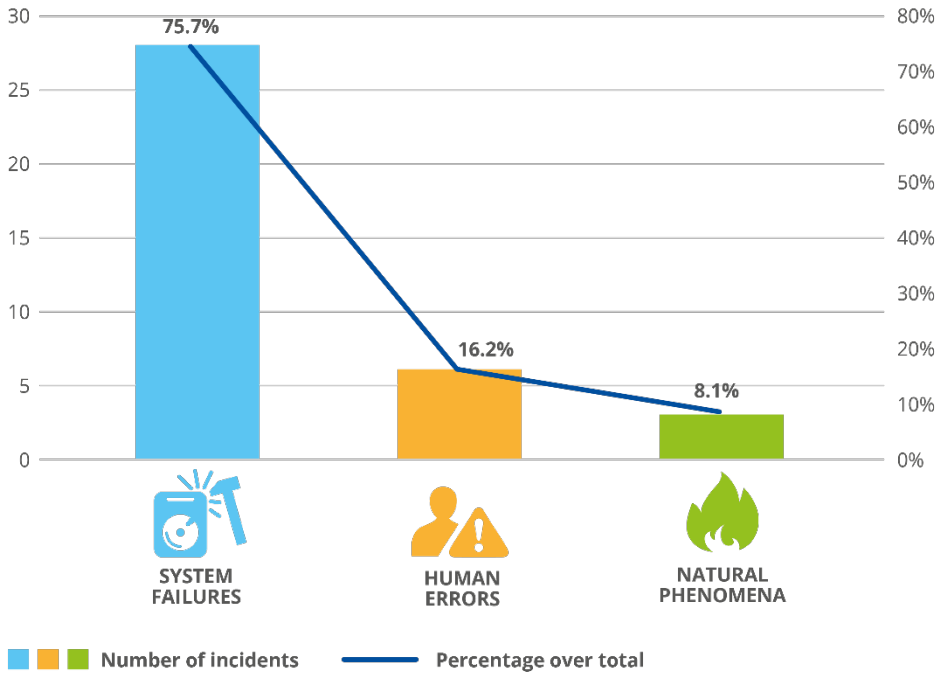
In 2021, there was a slight drop in incidents related to both system failures and human errors, the two categories which consistently rank the highest (see Figure 6). About 23% of security incidents were caused by human errors (compared to 26% in 2020) and 59% of telecom incidents were marked as system failures, a slight decrease compared to 2020 (61%). Notably, malicious actions almost doubled in the course of 2021 (8%) compared to 2020 (4%) and natural phenomena remained consistent with 2020 (10% in 2021 up slightly from 9% in 2020).

Figure 6: Root cause categories – Telecom security Incidents in 2021



In 2021, there was a noteworthy decrease in incidents that were flagged as third-party failures. Only 22% of the incidents were reported as being related to third-party failures compared to 29% in 2020 and 32% in 2019. No third-party failures related to malicious actions were reported, while the majority of them was related to system failures (see Figure 7).

Figure 7: Root cause categories – Telecom security incidents in 2021 (third-party failures)



3.2 USER HOURS LOST IN EACH CATEGORY OF ROOT CAUSES

Adding up total user hours lost for each root cause category (see Figure 8) shows that more than 90% of the total user hours lost were due to human errors (91%; 4,632 million user hours), up from 40% and 351 million user hours in 2020. This is due to the fact that a particular incident affecting an OTT (Over-The-Top) communication service provider was reported three times by three different MS and in three different ways (i.e. incident data differences) since it impacted services across the EU.

This raises the issue of cross-border and EU-wide incidents and how they should be reported under the EECC, in particular for OTT communication service providers who by nature are not generally restricted to a single MS. 4442 user hours were lost due to human errors in the case of OTT communication service providers and 7M due to system failures.

System failures accounted for 7% of the cases (363 million user hours lost) compared to 50% and 419 million lost user hours in 2020. Despite the skewed nature of the results in 2021, it is noteworthy that there was a 14% decrease in user hours lost relared to system failures, a trend observed since 2019. This highlights the growing maturity of electronic communication providers in handling and containing the impact of system failures.

Figure 8: Share of user hours lost for each root cause category

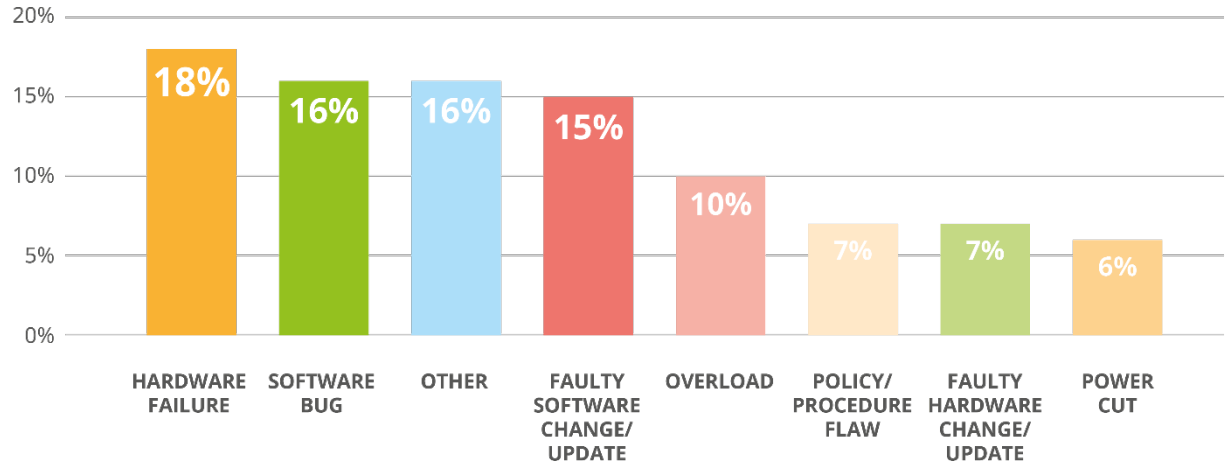
It is interesting to note the impact of incidents related to malicious actions on lost user hours. Interestingly, in 2021 lost user hours increased five times (from 13 million lost user hours in 2019 and 2020 to 70 million lost user hours in 2021). While the number of incidents doubled in 2021 compared to 2020, the significant increase in their related impact highlights the need to take further action in containing the adverse effect of such incidents.

3.3 DETAILED CAUSES AND USER HOURS LOST

Detailed causes for all incidents are tracked, in addition to root cause categories (Figure 9). An incident is often a chain of events. For instance, an incident may be triggered by a storm, which tears down power supply infrastructure, cutting cables and thus power, which in turn results in a telecom outage. In 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 for 2021 is hardware failures followed by faulty software changes/updates and software bugs. In addition, many incident reports mention policy/procedural flaws, faulty hardware changes/updates and overloads. Figure 10 shows the frequency of detailed causes across incident reports for 2021 and the corresponding lost user hours.

Figure 9: Detailed root causes – Telecom security incidents in 2021



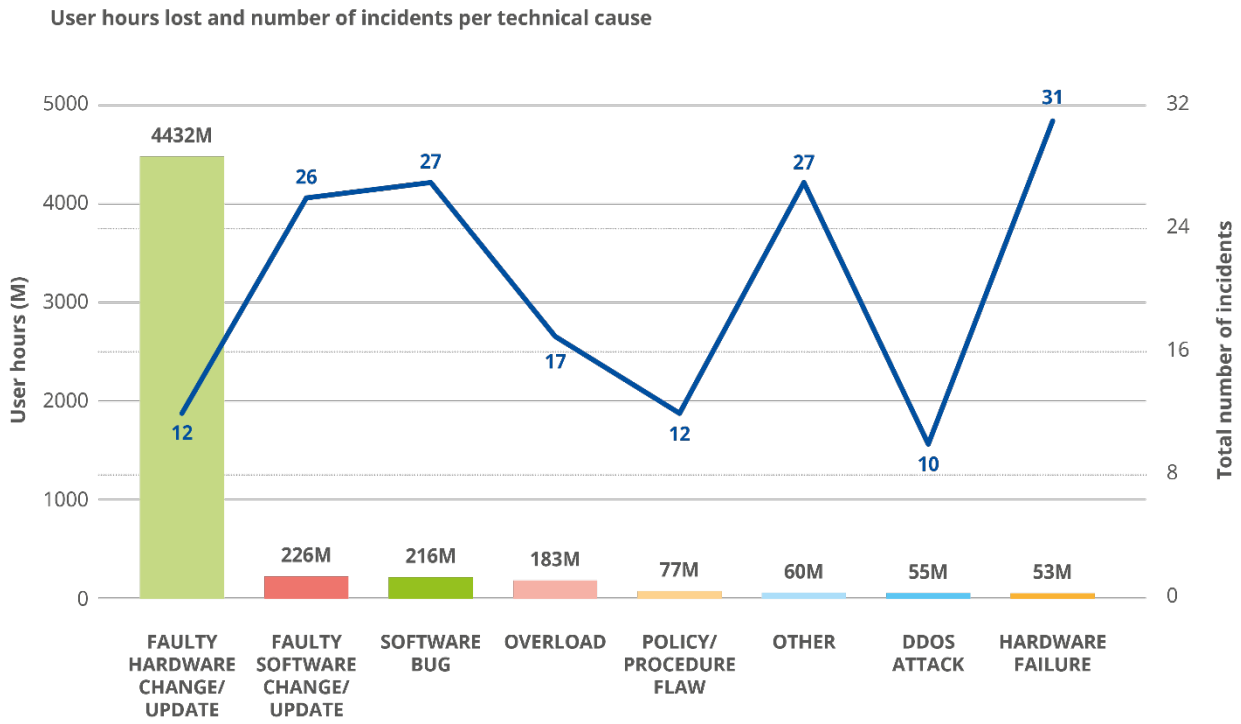
3.3.1.1 Breakdown of root causes

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

It is noteworthy to mention that the thrice reported EU-wide OTT communication services incident concerning a faulty hardware update has significantly skewed the results concerning lost user hours. This is to be expected given the EU-wide user base affected and the fact that the same incident was reported three times by three distinct MS. Accordingly, more clarification of the incident reporting process concerning OTT communication services and cross-border, EU-wide incidents is required.

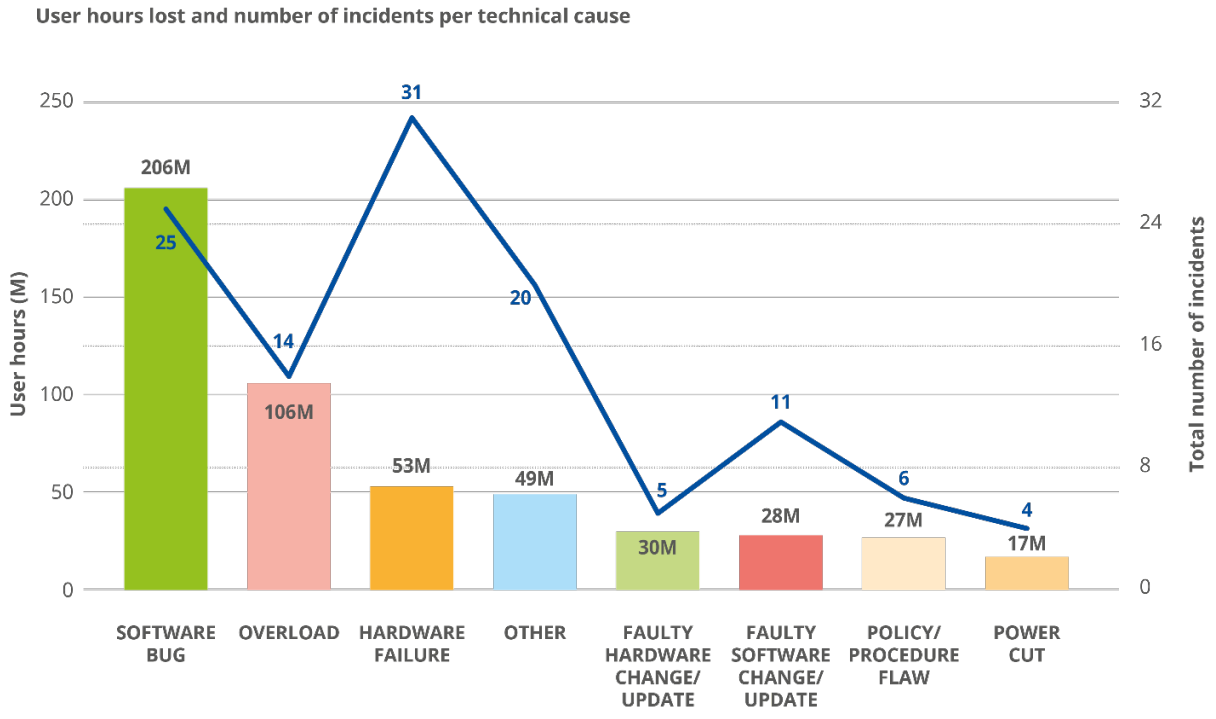
What follows is an overview of detailed causes and user hours lost for each category of incident in an effort to provide clarity and transparency for specific root causes, which differ significantly between categories of incidents.

Figure 10: Root causes of incidents vs user hours lost – Telecom security incidents in 2021



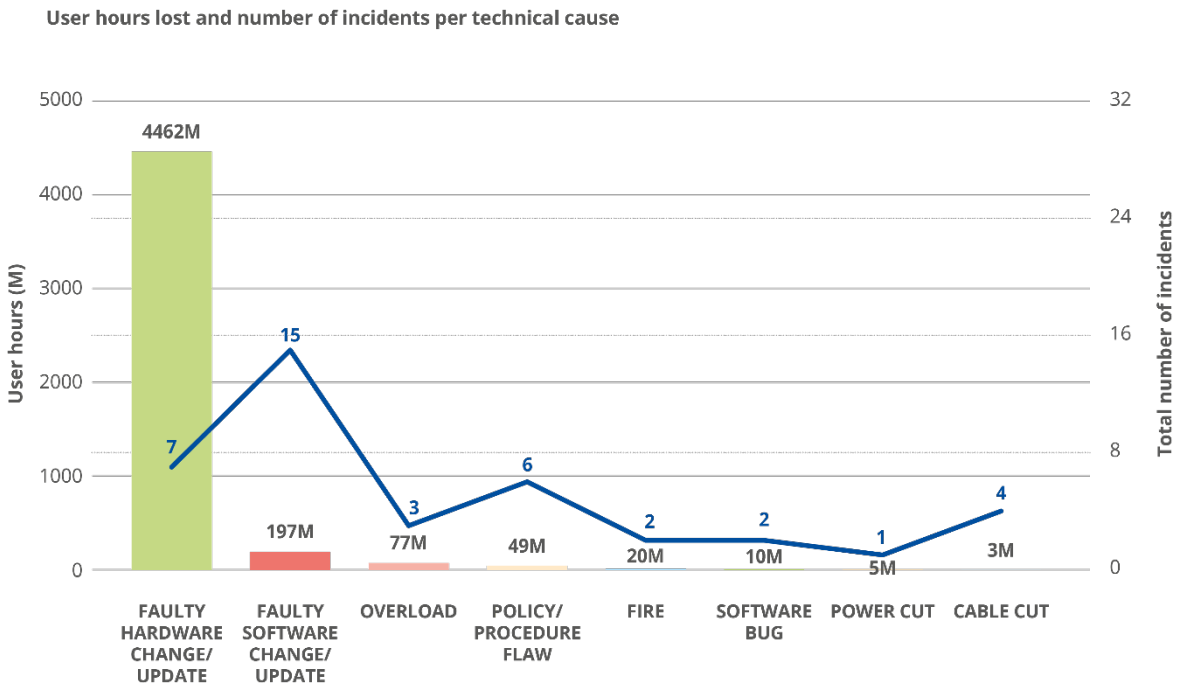
3.3.1.2 Breakdown of System failures

Figure 11: Root causes of system failure incidents vs user hours lost – Telecom security incidents in 2021 (system failures)



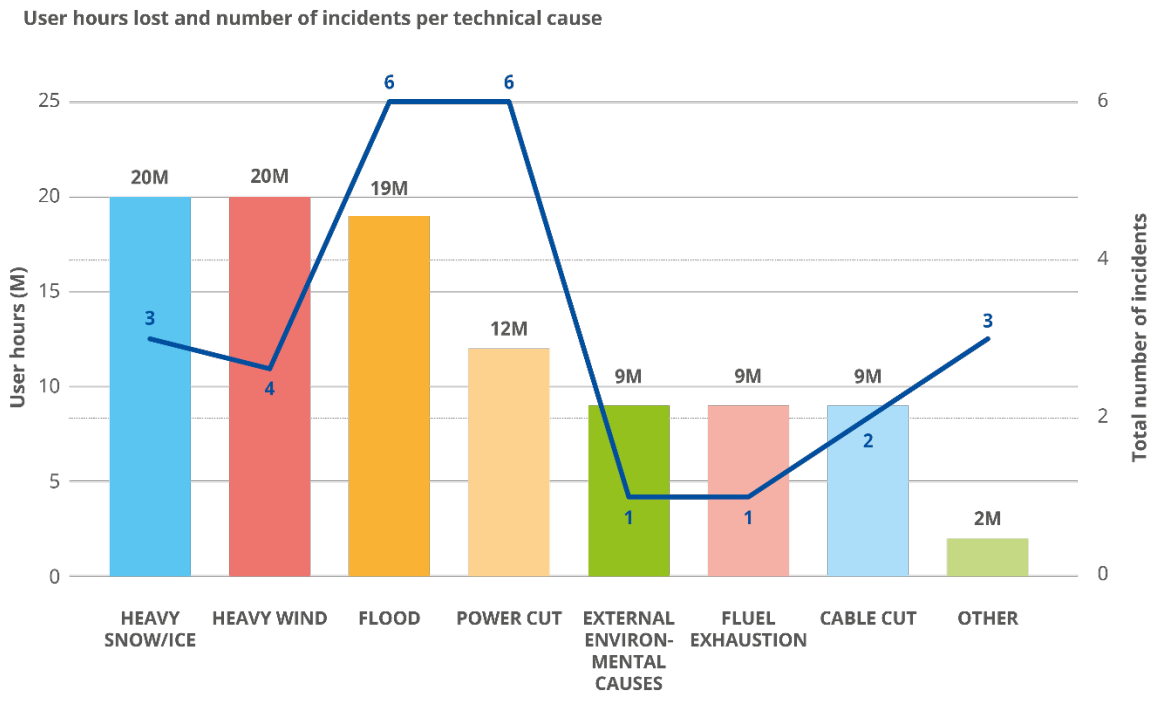
3.3.1.3 Breakdown of Human errors

Figure 12: Root causes of human error incidents vs user hours lost – Telecom security incidents in 2021 (human errors)



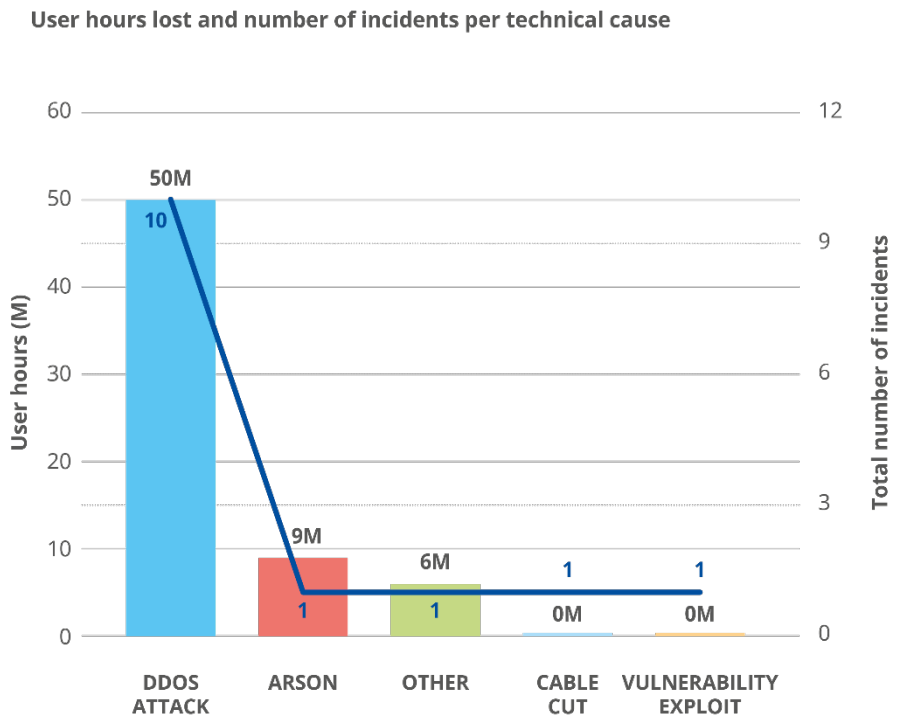
3.3.1.4 Breakdown of natural phenomena

Figure 13: Root causes of natural phenomena incidents vs user hours lost – Telecom security incidents in 2021 (natural phenomena)



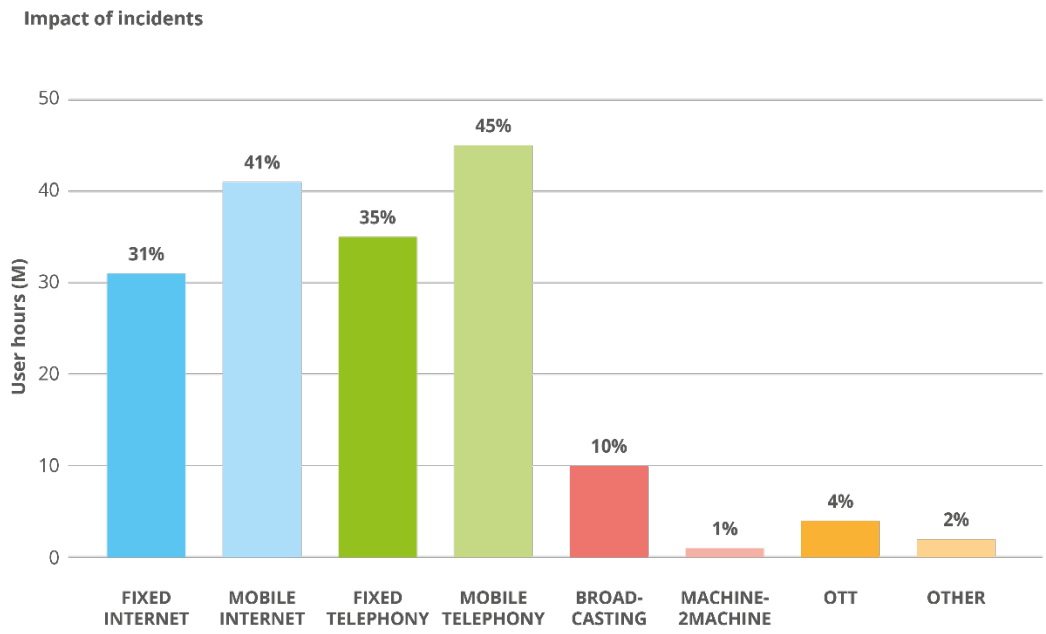
3.3.1.5 Breakdown of malicious actions

Figure 14: Root causes of malicious action incidents vs user hours lost – Telecom security incidents in 2021 (malicious actions)



When it comes to malicious actions it is interesting to highlight the significant increase in DDoS (Distributed Denial of Service) attacks compared to 2020 when only four such incidents were reported resulting in one million user hours lost. Conversely, in 2021 ten DDoS related incidents were reported, leading to a loss of 55 million user hours.

Figure 15: Services affected – Telecom security incidents in 2021



3.4 SERVICES AFFECTED

In this section the services affected by incidents are examined. For the sixth year in a row, most of the reported incidents affected mobile services. In 2021, around 45% of reported incidents 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 service only in the early years of reporting.

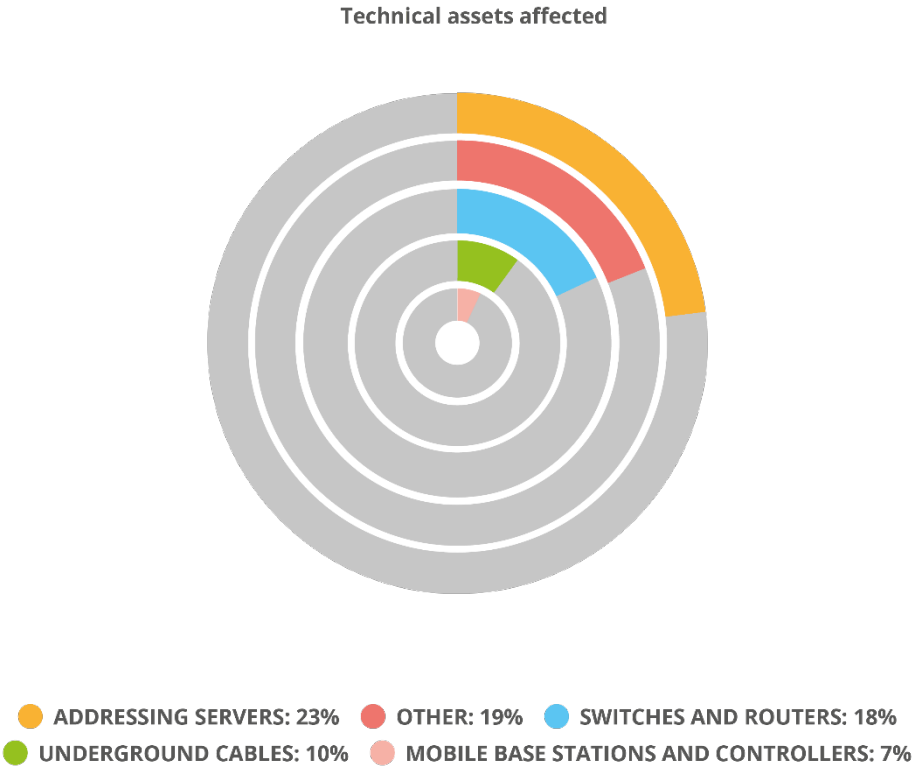
It is also important to note that in comparison to 2020 reported incidents affecting OTT services rose to 4% of all reported incidents in 2021. This highlights the growing maturity in the reporting of such incidents, albeit needing more clarifications in terms of procedures and processes given the particular thrice reported incident mentioned above.

Note that for most reported incidents there was an impact on more than one service, which explains why the percentages in Figure 15 add up to more than 100%.

3.5 TECHNICAL ASSETS AFFECTED

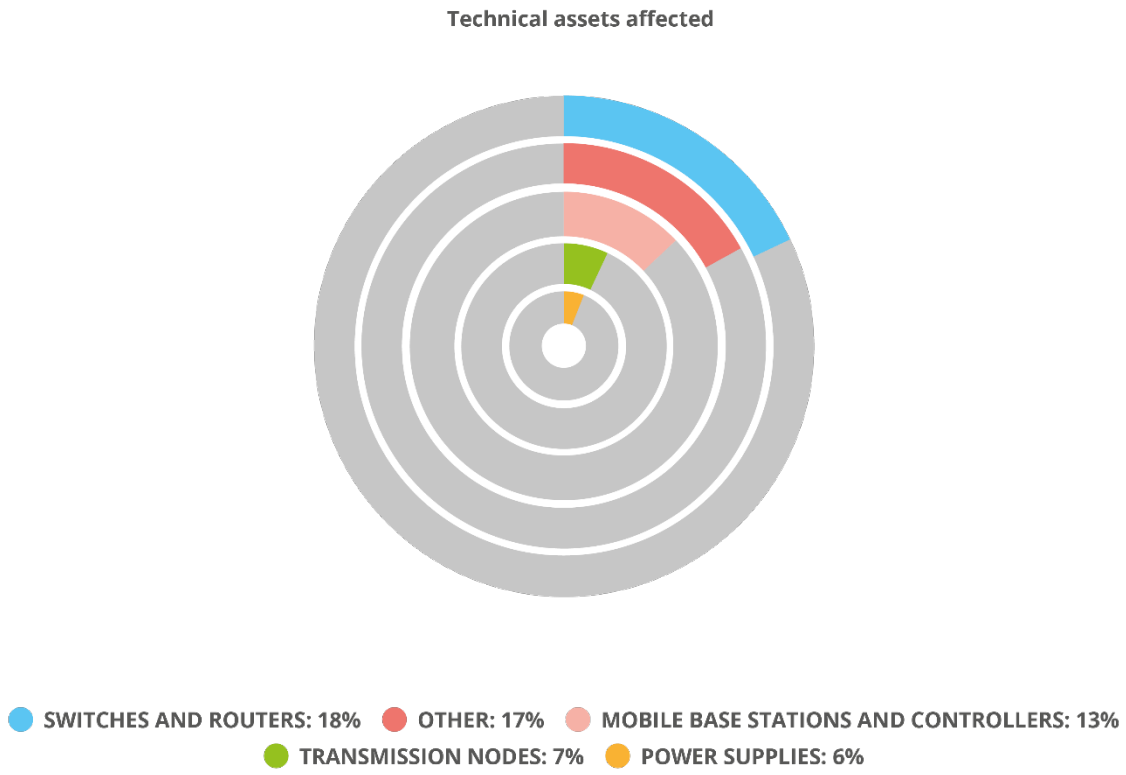
Each incident report also describes the (secondary) assets affected during the incident. Figure 16 shows the assets most affected.

Figure 16: Assets affected – Telecom security incidents 2021



It is also noticeable, taking into account incidents over the last 5 years as seen in Figure 17, that switches and routers as well as mobile base stations and controllers are the two assets that have been affected the most in recent years.

Figure 17: Assets affected – Telecom security incidents 2017-2021



4. DEEP DIVE ANALYSIS OF THE TECHNICAL CAUSES OF INCIDENTS

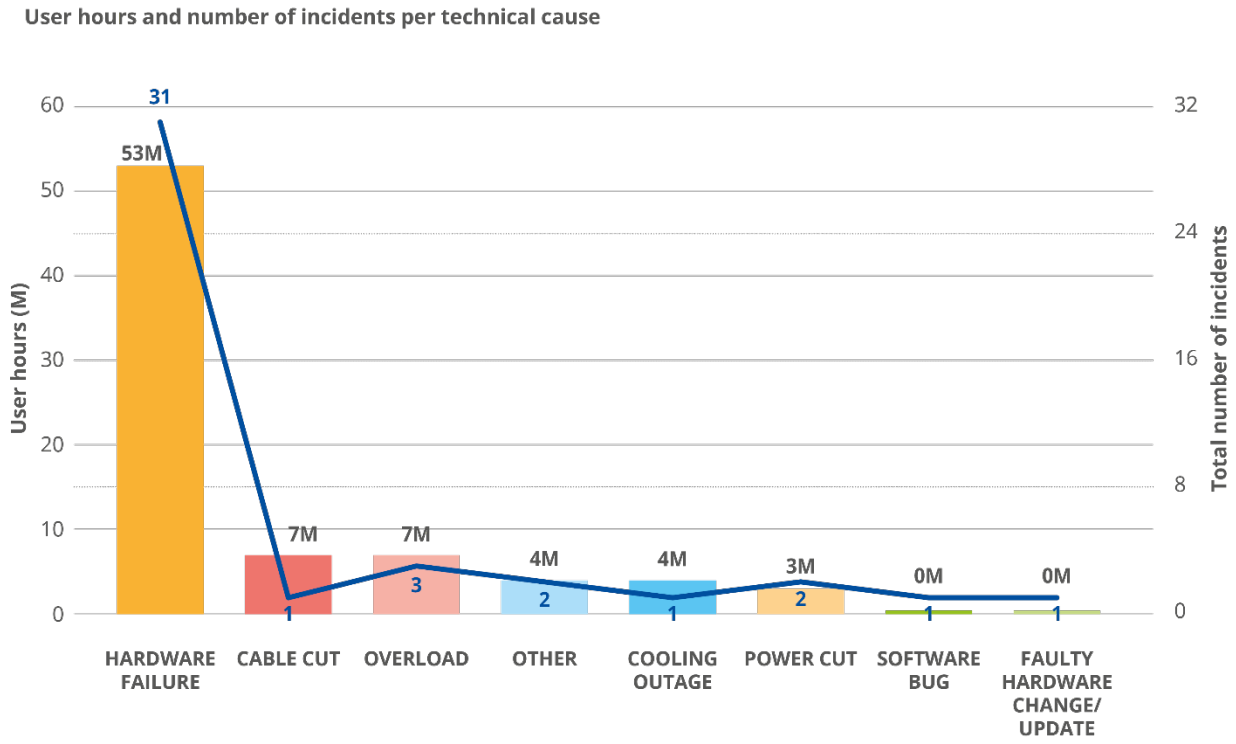
This section contains an in-depth review of the most high-profile technical causes behind reported incidents, focussing not only on 2021 but also on previous years.

53 M user hours lost due to hardware failures in 2021, 1% of the total

4.1 HARDWARE FAILURES

In 2021, 31 incidents (18% of total) were marked as hardware failures and they resulted in 53 million user hours lost (1% of the total) as seen in Figure 18. All of them were reported as system failures.

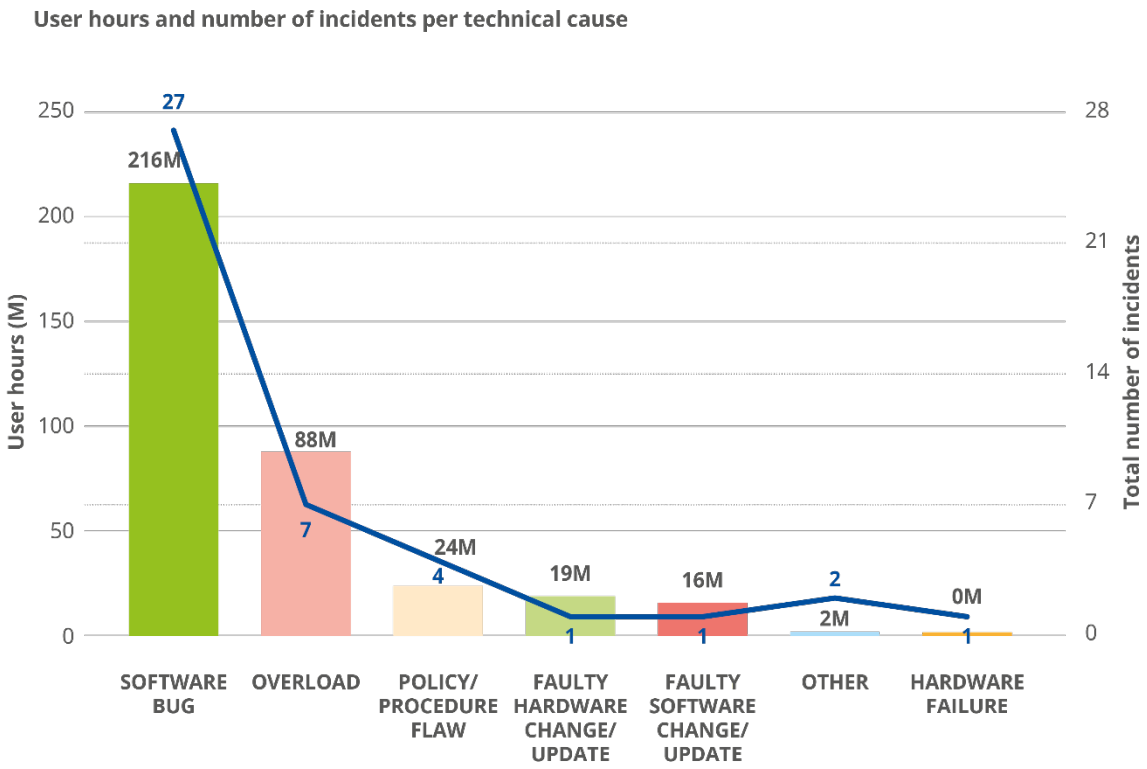
Figure 18: Incidents with hardware failures as root cause – Telecom security incidents in the EU in 2021



4.2 SOFTWARE BUGS

In 2021, 26 incidents (15% of total) were marked as being due to software bugs and they resulted in 216 million user hours lost (4% of the total) as can be seen in Figure 19. All but one of them were reported as system failures, with one incident being reported as due to human error.

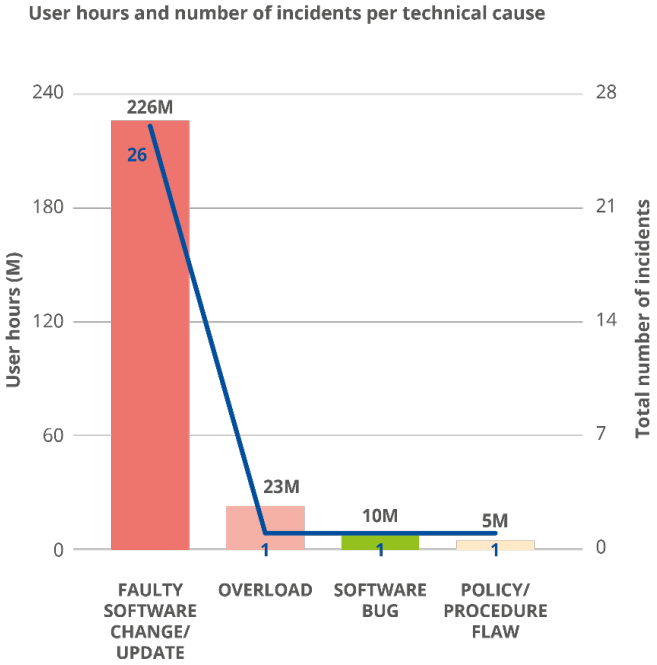
Figure 19: Incidents having software bugs as root cause – Telecom security incidents in the EU in 2021



4.3 FAULTY SOFTWARE CHANGES/UPDATES

In 2021, 15% of total incidents (26 incidents) were marked as due to faulty software changes or updates resulting in 225 million user hours lost (4% of the total) as can be seen in Figure 20.

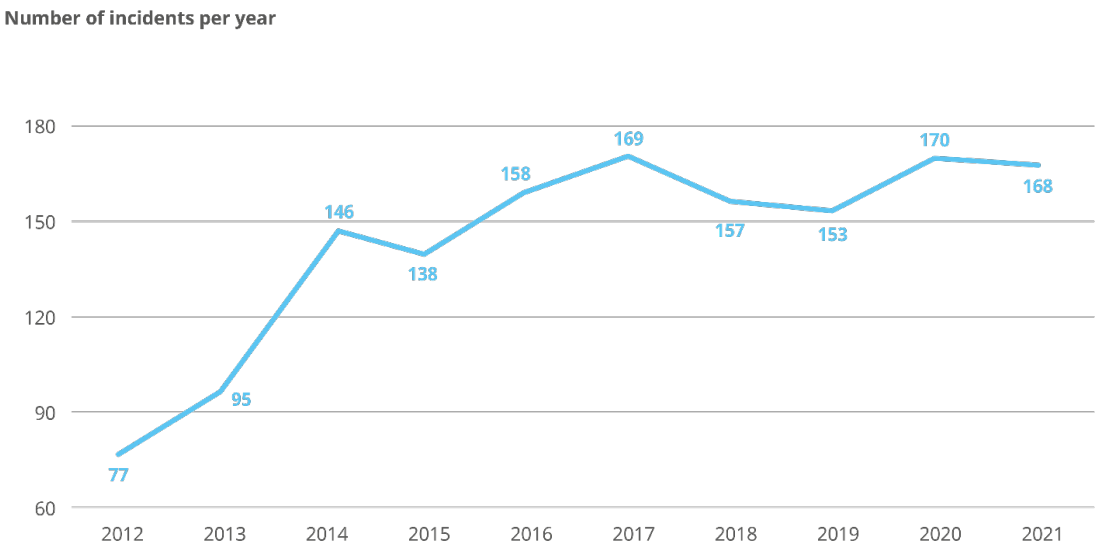
Figure 20: Incidents having faulty software changes/updates as their root cause – Telecom security incidents in the EU in 2021



5. MULTI-ANNUAL TRENDS

ENISA has been collecting and aggregating incident reports since 2012. In this section multi-annual trends over the last 11 years, from 2012 to 2021, are presented. This dataset contains 1,431 reported incidents in total (see Figure 21). Over the course of the last 5 years, the number of incidents has been stabilising at around the 160 mark per annum.

Figure 21: Number of incidents reported per year (2012-2021)



5.1 MULTI-ANNUAL TRENDS – CATEGORIES OF ROOT CAUSES

Every year from 2012 to 2021, system failures were the most common root cause. In 2021, however, system failures showed stabilisation and a slight decrease, continuing the trend first observed in 2020 as seen in Figure 22.

In total, system failures accounted for 925 incident reports (64% of the total). For this root cause category, over the last 11 years, the most common causes were hardware failures (34%) and software bugs (27%). The second most common root cause over the 11 years of reporting is human errors with nearly a fifth of total incidents (19%, 286 incidents in total). Natural phenomena come third at almost a tenth of total incidents (9%, 139 incidents in total).

Only 5% of incidents have been categorised as malicious actions (73 incidents over the course of 11 years). In the period 2012-2021 nearly two thirds of malicious actions consisted of Denial of Service attacks (64%), while the remainder were mainly comprised of lasting damage to physical infrastructure, e.g. arson, cable cuts, etc. Only 4% was attributed to malware and viruses (see Figure 23).

Interestingly, the assets affected by malicious actions differ significantly from the overall categorisation of affected assets. Addressing servers came first with 23%, followed by switches and routers at 18% (see Figure 24). Moreover, 63% referred to fixed Internet services and 41% to mobile Internet services, whereas 2% referred to OTT services.

Figure 22: Root cause categories - Telecom security incidents in the EU reported over 2012-2021

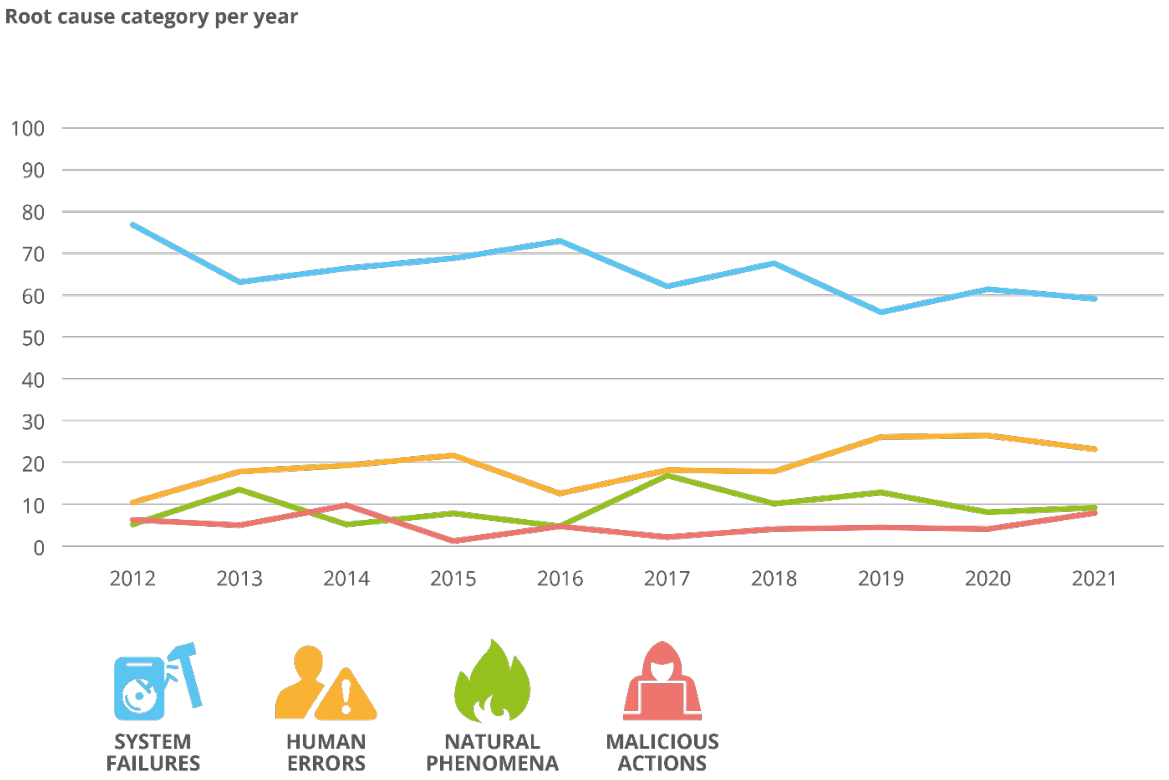


Figure 23: Technical causes for incidents due to malicious actions – Telecom security incidents in the EU reported over 2012-2021

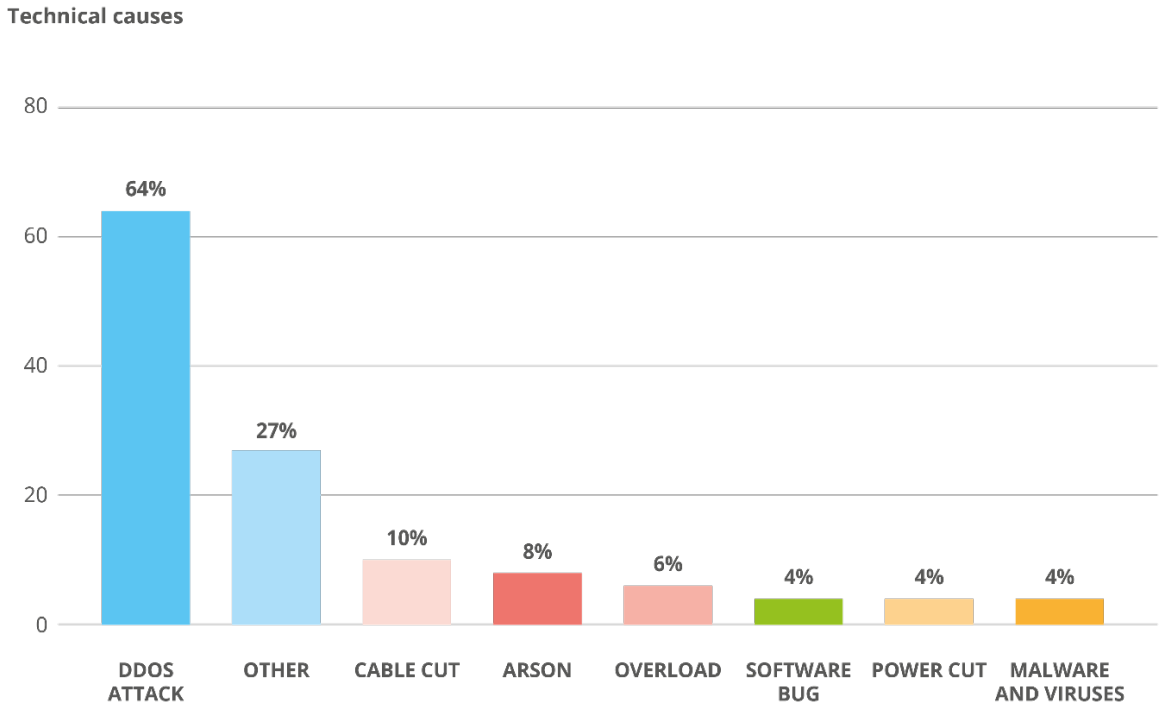
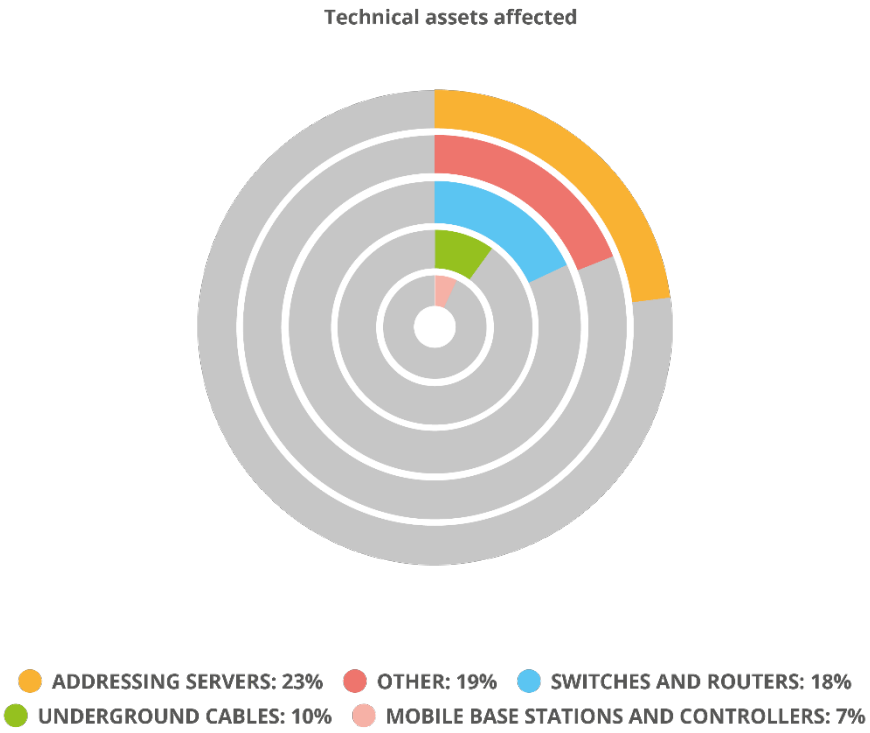


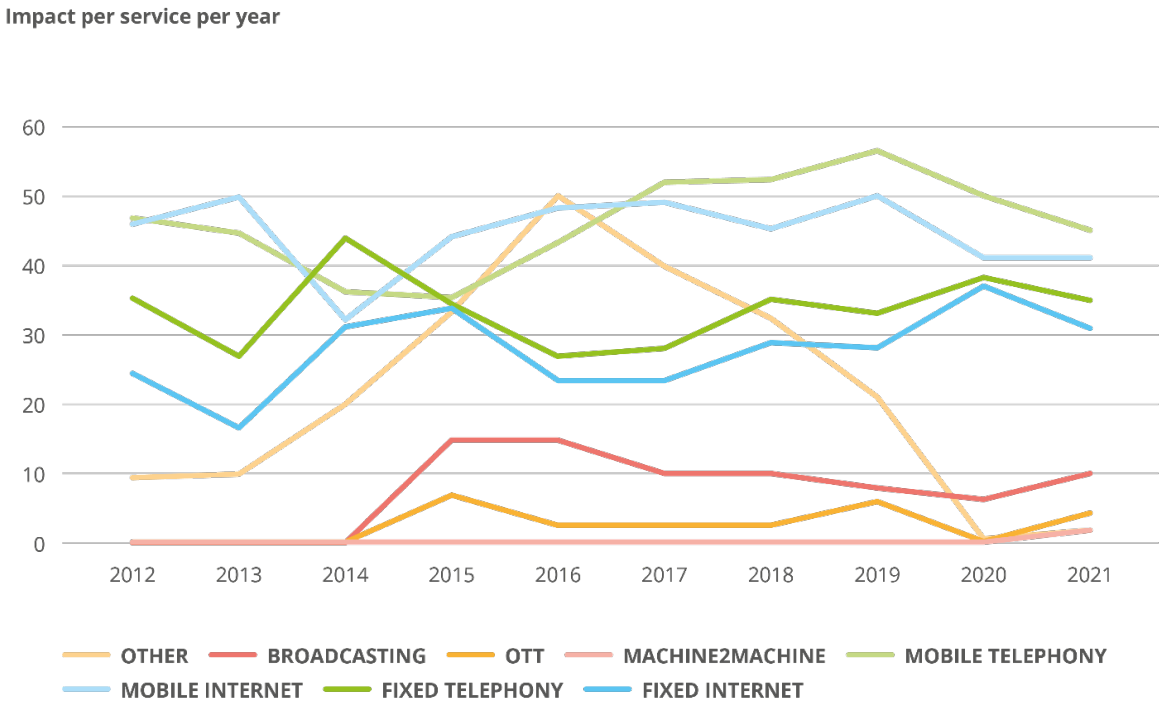
Figure 24: Assets affected by incidents due to malicious actions – Telecom security incidents in the EU reported over 2012-2021



5.2 MULTI-ANNUAL TRENDS - IMPACT FOR EACH SERVICE

In 2021, mobile networks and services were once more the most impacted by incidents. However there was a decrease compared to 2019 and 2020 and, interestingly, the statistics in terms of services affected are converging for both fixed and mobile. More importantly, in 2021 reporting of incidents related to OTT communication services took place (in contrast to 2020 where no such incidents were reported). In addition, the increase in broadcast related incidents that was observed for two years in a row (2019 and 2020) persists also in 2021.

Figure 25: Trends on impact for each service reported over 2012-2021

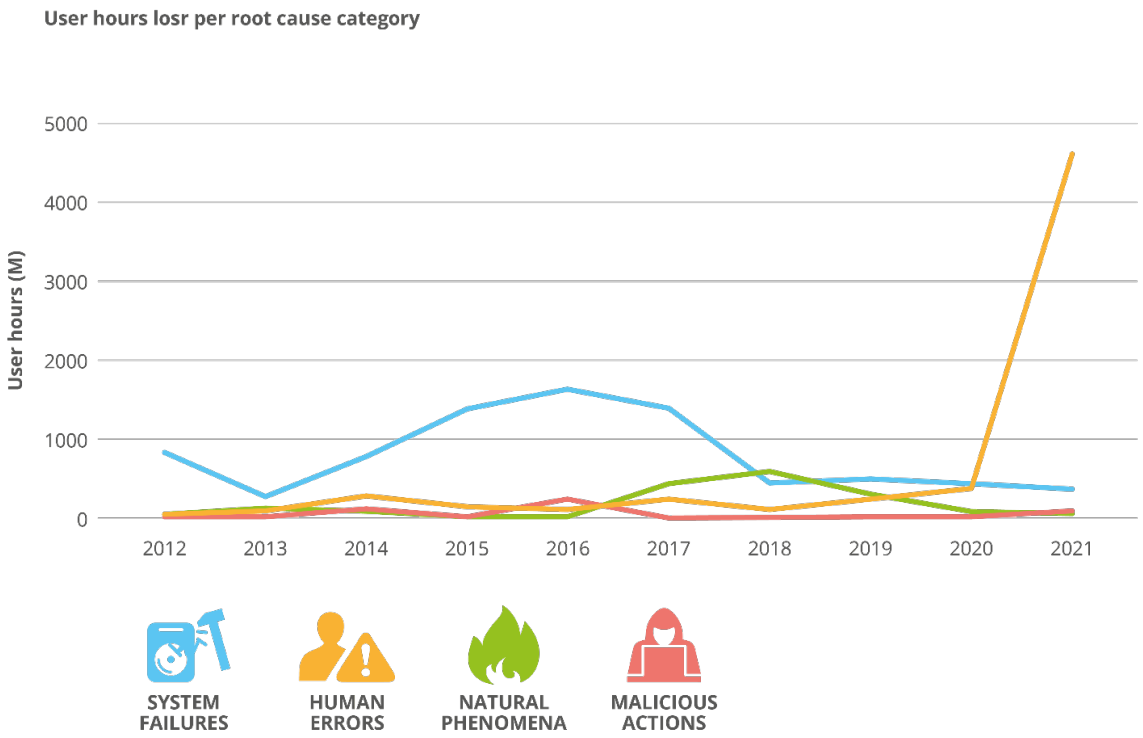


5.3 MULTI-ANNUAL TRENDS - USER HOURS FOR EACH ROOT CAUSE

In terms of overall impact, as indicated in Figure 26, human errors have been steadily increasing since 2016. In 2020, their share in terms of impact was almost the same as system failures. In 2021, given the particularities of OTT incident reporting that were previously analysed, the results are heavily skewed towards human errors.

The overall impact of natural phenomena has been trending down over the last three years after peaking in 2018 (caused by extreme weather and wildfires). Notably, the impact of malicious actions is steadily rising, reaching a 5-year high of 70 million lost user hours in 2021.

Figure 26: User hours lost for each category of root causes - multi-annual 2012-2021 (user hours lost)



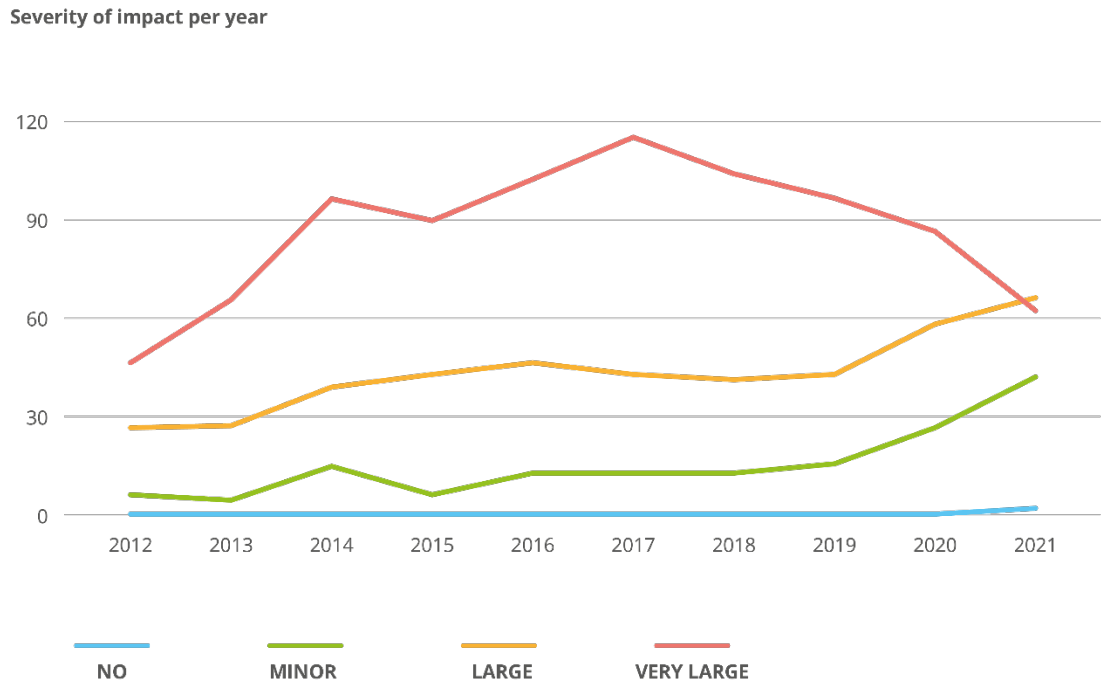
5.4 MULTI-ANNUAL TRENDS FOR THE SEVERITY OF IMPACT OF INCIDENTS

Over the last 5 years a noteworthy and constant decrease in reports of incidents with very large severity has been observed. ENISA has published technical guidelines on incident reporting under the EECC[7], including on thresholds, severity estimation and calculating hours lost. Conversely, there has been a steady increase in minor and large incidents. These findings point on one hand to the growing maturity of electronic communication providers with respect to the incident reporting process and on the other hand to the improvement of resilience and the provision of security services (including incident reporting itself) that has led to a lower number of very large severe incidents.

Relevant multi-annual trends may be found in Figure 27.

[7] See https://www.enisa.europa.eu/publications/enisa-technical-guideline-on-incident-reporting-under-the-eecc, March 2021

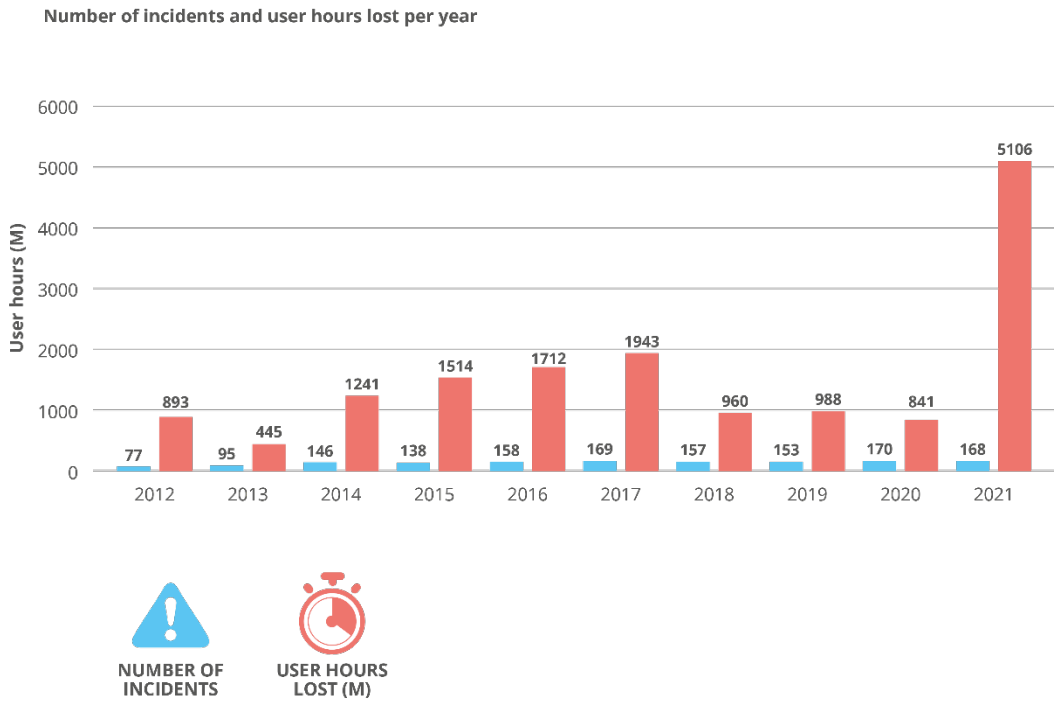
Figure 27: Severity of impact for each year - multi-annual trends 2012-2021 (number of incidents)



5.5 MULTI-ANNUAL TRENDS FOR THE NUMBER OF INCIDENTS AND USER HOURS LOST

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

Figure 28: Number of incidents and user hours lost each year



6. CONCLUSIONS

This document, the *Annual Report Telecom Security Incidents 2021*, covers the incidents reported by the authorities for the calendar year 2021 and it gives an anonymised, aggregated EU-wide overview of telecom security incidents. It marks the 11th time ENISA has published an annual report for the telecom sector. To conclude here are the main findings and some general observations about this process and the broader policy context.

MAIN FINDINGS

- **Reporting of incidents related to OTT services requires further attention.** Four per cent of reported incidents in 2021 refer to OTT services. The same EU-wide OTT incident was reported three times by three different MS in three different ways, so there is a need for clarification on who reports such incidents, which authority is in charge and what information is to be reported. The results of 2021 incident reporting are skewed because of the huge impact of this incident which was reported three times.

- **For the first time, incidents concerning confidentiality and authenticity were reported.** The reporting of such incidents was a new provision of the EECC and in this respect no such incidents were reported in the previous years. Three relevant incidents were reported in 2021 and this number is expected to grow in the coming years.

- **Malicious actions doubled in 2021.** In 2020, incidents marked as malicious actions represented 4% of the total, a number which rose to 8% in 2021. Moreover, it is interesting to highlight the significant increase in DDoS attacks compared to 2020 when only four such incidents had been reported resulting in one million user hours lost. By comparison, in 2021 ten DDoS related incidents were reported, leading to a loss of 55 million user hours. These results are consistent with the findings of the ENISA Threat Landscape that point to an increase in DDoS attacks and, in general, an increase in attacks against the availability of services.

- **System failures continued to dominate in terms of impact, but the downward trend continued.** System failures accounted for 363 million user hours lost compared to 419 million user hours lost in 2020. Despite the skewed nature of the results for 2021, it is noteworthy that there was a 14% decrease in user hours lost, whereas in terms of the number of incidents in 2021 they represent 59% of the total compared to 61% in 2020. This highlights the growing maturity of electronic communication providers in handling and containing the impact of system failures.

- **Incidents caused by human errors remained at the same level as in 2020.** Around a quarter (23%) of total incidents have human errors as a root cause (slightly decreased compared to the 26% of 2020). However 91% of the total user hours lost were due to this kind of incident. These results however are skewed due to the OTT incident reporting issues mentioned above.

- **In 2021, a noteworthy decrease in incidents that were flagged as third-party failures was observed.** Only 22% of the incidents were reported as being related to third-party failures compared to 29% in 2020 and 32% in 2019. No third-party failures related to malicious actions were reported. Overall, this finding suggests that electronic communication providers have started introducing targeted security controls to better protect their supply chains, echoing the relevant ENISA calls for attention[8].

GENERAL OBSERVATIONS

- At 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

[8] See https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

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.

- In May 2022, there was a political agreement on the Network and Information Security (NIS) Directive 2. The official text is expected in the course of 2022 with an expected transposition deadline of 21 months for MS. The NIS 2 brings significant changes to security incident reporting in the EU by consolidating all relevant streams under the NIS 2 umbrella, namely consolidating incident reporting under EECC, NIS2 and eIDAS regulations among others. ENISA will be working with national authorities and regulators in the coming years on how to implement the consolidated reporting of incidents under NIS2.
- Under Article 40 of the EECC, the incident reporting provisions have changed slightly[9]. 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, these changes were beginning to be seen in the reporting data. However, issues still persist as was evident from the EU-wide incident that was reported by three MS and was done so in three different ways. Taking into account the different reporting thresholds of Member States, there needs to be more clarity and coordination on how cross-border incidents are reported, by whom and using what thresholds. ENISA will work closely with national authorities and regulators to find an optimal way to address this issue.
- One issue that was observed in 2020 and persists in 2021 is 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, this area needs to be analysed better with the possible introduction of a summary reporting format for these smaller scale incidents. To begin with, in 2022, bulk incident reporting using machine-readable formats was introduced to CIRAS in order to facilitate reporting and alleviate the administrative burden.
- The 5G roll out will continue to require a lot of attention, both from authorities and from the providers. At ENISA, the focus is on supporting the national authorities in the ENISA ECASEC group and in the NIS Cooperation group, with technical guidance, and also by organising dedicated seminars and panels.

ENISA looks forward to continuing its 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.

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

TP-07-22-711-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: 978-92-9204-582-1
DOI: 10.2824/528645