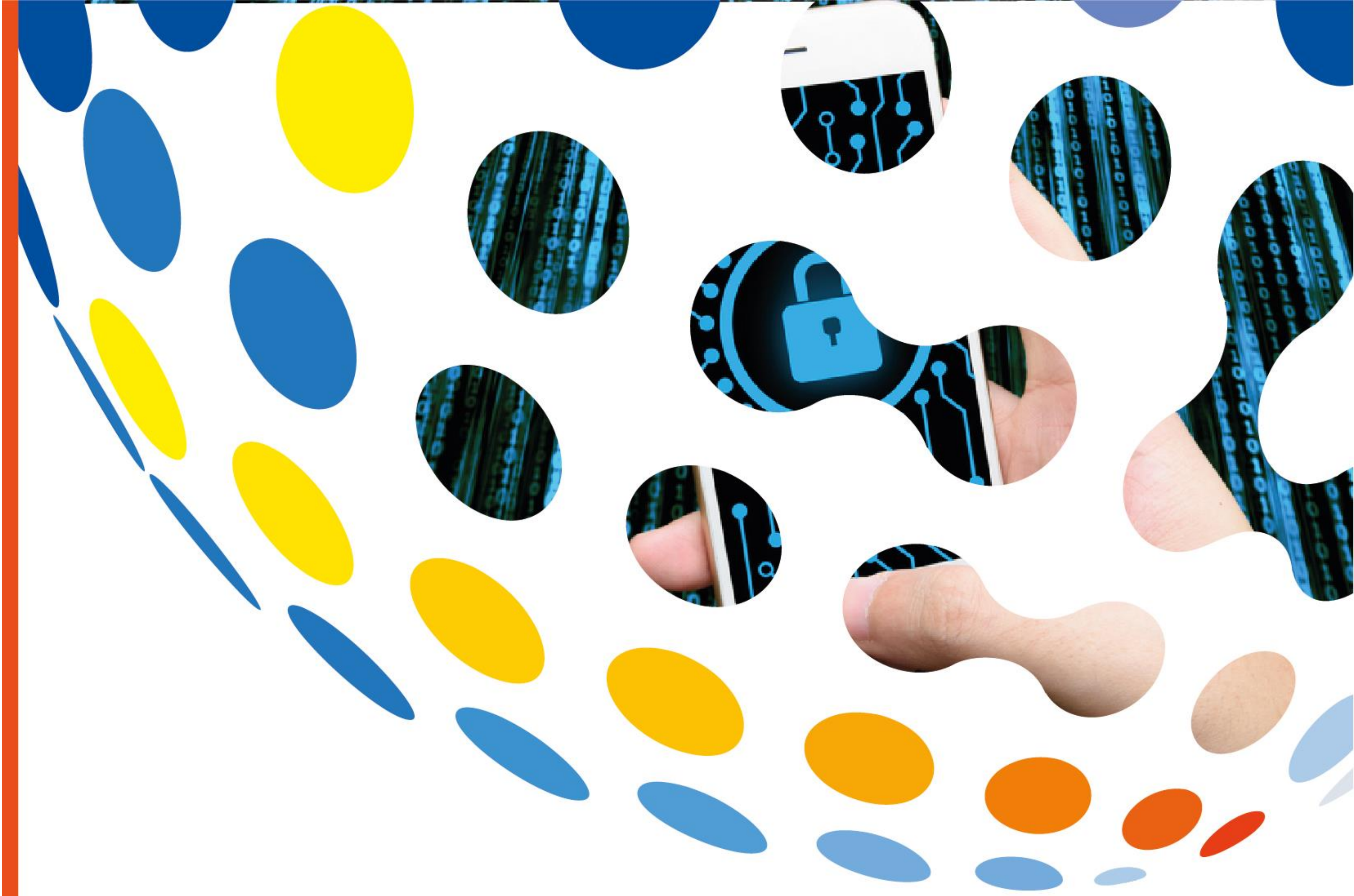


Annual report NIS Directive incidents 2024

CG Publication

August 2025

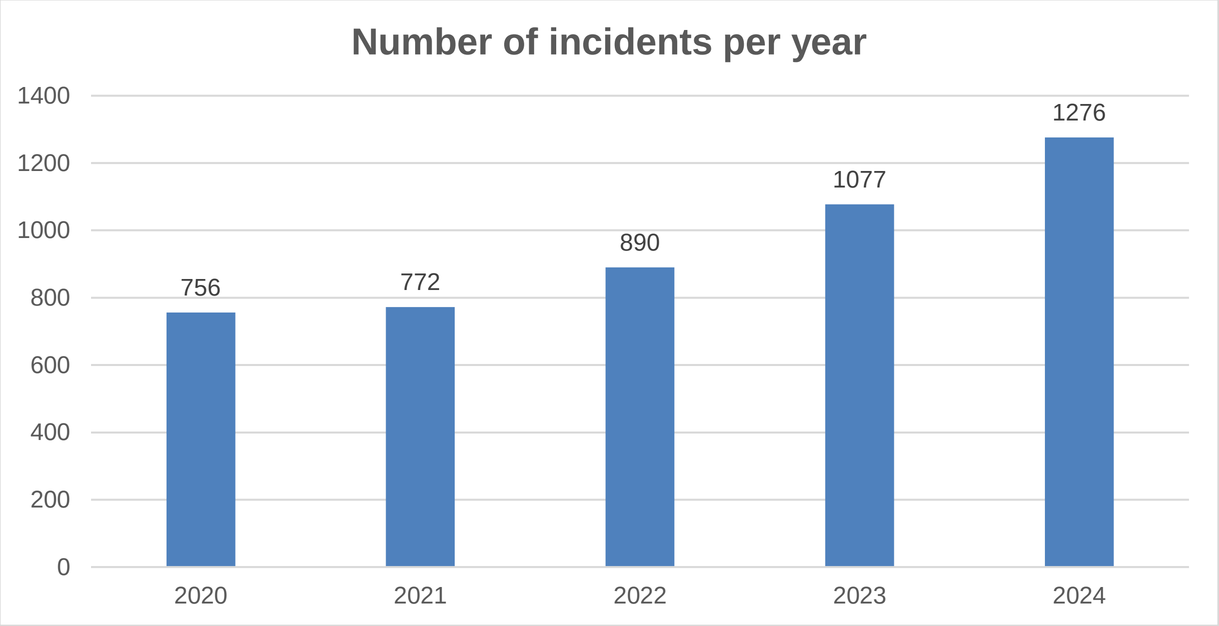
Contents

Executive summary

Under the NIS Directive (NISD)[1], operators of essential services in critical sectors (Article 14), as well as digital service providers (Article 16), have to report cybersecurity incidents to their designated national authorities. This process of mandatory cybersecurity incident reporting is an important enabler for supervision and policy-making, both at national and at EU level.

Member States send annual summaries about the national incident reporting to the NIS Cooperation Group (NIS CG). This document provides an aggregated overview of the annual summary for the incidents that were reported in 2024.

The figure below shows the incident reports submitted per sector, comparing 2021, 2022, 2023 and 2024.



Member States set the national criteria and thresholds for reporting cybersecurity incidents affecting operators of essential services. These criteria may be different for each country and often depend on the sector.

The NIS Cooperation Group's Work Stream on Incident Reporting works on the formats and procedures for this process and aggregates this information in an annual report.

The key takeaways regarding the incidents reported for the year 2024 are as follows:

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&qid=1697127825732

- **The number of reported incidents has increased by 18 % compared to previous year.** In this round, covering the year 2024, summary information about 1276[2] cybersecurity incidents was submitted, compared to 1077 for the previous year.
- **Most incident reports in 2024 regard the health, energy and transport sectors**, accounting for 50% of the total number of reports. The health sector had the most incident reports in 2020, 2021, 2022, 2023 as well.
- **System failures are the most frequent root cause (51%) of reported incidents.** The detailed causes for these incidents are most often software bugs, faulty software changes/updates and hardware failures, similar to 2020, 2021, 2022 and 2023.
- **Incidents with cross-border impact.** There were only 2 incident reports with possible cross-border impact submitted through CIRAS.
- **The detailed technical causes for a 12% of incidents were defined as 'other'**, which is the similar level as 2023.
- **Malicious actions (in particular DDoS attacks) caused the most outages and the respective lost hours.** System failures was the second cause of incidents and the respective outages and lost hours.

Some caveats which should be considered in the contextual and quantitative analysis of the reported incidents and give grounds to further improvement of the process in the future:

- **Incidents are categorised in 4 broad root cause categories** and too often the generic category “Other” is being used for reporting. Lack of information makes analysis of information and extrapolation of trends and patterns challenging and skewed.
- **Cross-border incident reporting remains challenging –** This should be further considered in the NIS CG Work Stream on incident reporting.

Cybersecurity incident reporting under the NIS Directive is finalizing with year 2024[3]. 2025 will be covered by NIS2 Directive (NIS2)[4] and incident reporting process is continuously improving and maturing. In 2025 Member States will submit summary of incidents on quarterly basis and ENISA will prepare reports to CSIRTs network and NIS CG every six months. In terms of processes, there are still more synergies to be explored with reporting in other sectors, under other pieces of legislation, such as DORA[5], the Network Code on Cybersecurity (NCCS)[6] and the CER Directive[7].

[2] The reported incidents are for 24 Member States compared to 26 for year 2023.

[3] Report indeed covers the entire calendar year 2024 (even though NIS2 Directive transposition deadline was 17 October 2024)

[4] EUR-Lex - 32022L2555 - EN - EUR-Lex (europa.eu)

[5] EUR-Lex - 52020PC0595 - EN - EUR-Lex (europa.eu)

[6] Delegated regulation - EU - 2024/1366 - EN - EUR-Lex

[7] Directive - 2022/2557 - EN - CER - EUR-Lex

1. Introduction

The NIS Directive (NISD) was adopted in 2016 and Member States transposed it into national law by 2018. As per the Directive, operators of essential services (OESs) and digital service providers (DSPs) are required to notify significant incidents to the national competent authorities (NCAs) in each Member State. Annual summary report is prepared by and submitted to the NIS Cooperation Group with ENISA supporting the process.

This document provides an overview, including trends of the NIS annual summary reports. This is the sixth and last annual report relating to incidents reported under the NIS Directive, prepared by the NIS Cooperation Group Work Stream on Incident Reporting, with ENISA's support.

The NIS2 Directive was adopted in January 2023 and its measures were required to be transposed into national law by October 17th, 2024. The increased scope and strengthened requirements of NIS2 are expected to have a significant impact on incident reporting. However, this did not affect reporting for 2024, which still follows the incident reporting process of the first NIS Directive. The new scope is therefore not analysed further in this document. Under NIS2 there will be summary reporting submitted by Member States every quarter and information will be aggregated by ENISA in reports to NIS CG and CSIRTs network every six months.

1.1. Methodology

This report was drafted based on the below methodology:

- This report includes only aggregated and anonymised information about incidents.
- This report uses the EU Cybersecurity incident taxonomy[8] developed by the NIS CG to categorize incidents. This taxonomy includes all the sectors listed in the NISD Annex II and includes several other critical sectors.

1.2. Structure of this document

This document is structured as follows:

- Section 2: Examples of reported incidents;
- Section 3: Overview of main statistics;
- Section 4: Sectorial information
- Section 5: Detailed statistics of all incidents reported through CIRAS system;
- Section 6: Information on all NIS sectors.

[8] CG Publication 04/2018 - Cybersecurity incident taxonomy.

2. Examples of reported incidents with very large impact

In order to provide insights into the kind of incidents that were included in the annual summary reporting in 2024, this chapter includes some of the anonymised incidents reported with very large impact. There was a total of 15 incidents with very large impact in 2024 (compared to 10 in 2023), for which the root causes related to malicious actions, system failures and human error. It has to be noted that impact not always is not indicated in the summary report

2.1. Root cause: malicious actions

- **Cable cut:** The reported incident of cut submarine cables.
- **Data leak:** Pharmaceutical wholesaler and retailer company suffered a data leak.
- **DDoS:** campaign spanning over a month using advanced techniques towards a bank service and its authentication.
- **DDoS:** attack against online channels caused intermittent issues. Mitigation measures were implemented followed by enhanced service monitoring.
- **Ransomware:** Malware in the software update in the infrastructure of the provider of the cybersecurity service which offered security services for hospitals.
- **Breach of personal data:** State entity informed of a security breach of personal data in the platform of the personnel selection process contracted to the company. Unauthorized exfiltration of documentation.

2.2. Root cause: system failures

- **Connectivity:** Due to a misconfiguration, there was a connectivity issue of some services.
- **Availability:** System failure resulted in loss of access to a National clinical diagnostic system.
- **Availability:** False positive and subsequent quarantine action by malware agent resulted in loss of National access to a clinical diagnostic system.
- **Software update failure:** Cloud services failure resulted in disruption of hospital administration systems.
- **Hardware failure:** Cooling failure in data centre impacted multiple hosted services.
- **Availability:** Patient record system unavailable to clinical staff due to a hardware disk failure. Hospital deployed a full range of mitigation measures across its clinical and administrative departments in an effort to ensure business continuity.
- **Connectivity:** Issue with network switches impacted clinical administration systems.
- **Availability:** System failure impacted on availability of patient management system

2.3. Root cause: Human error

Availability: State entity reported availability failure due to a software update.

3. Overview of reported incidents

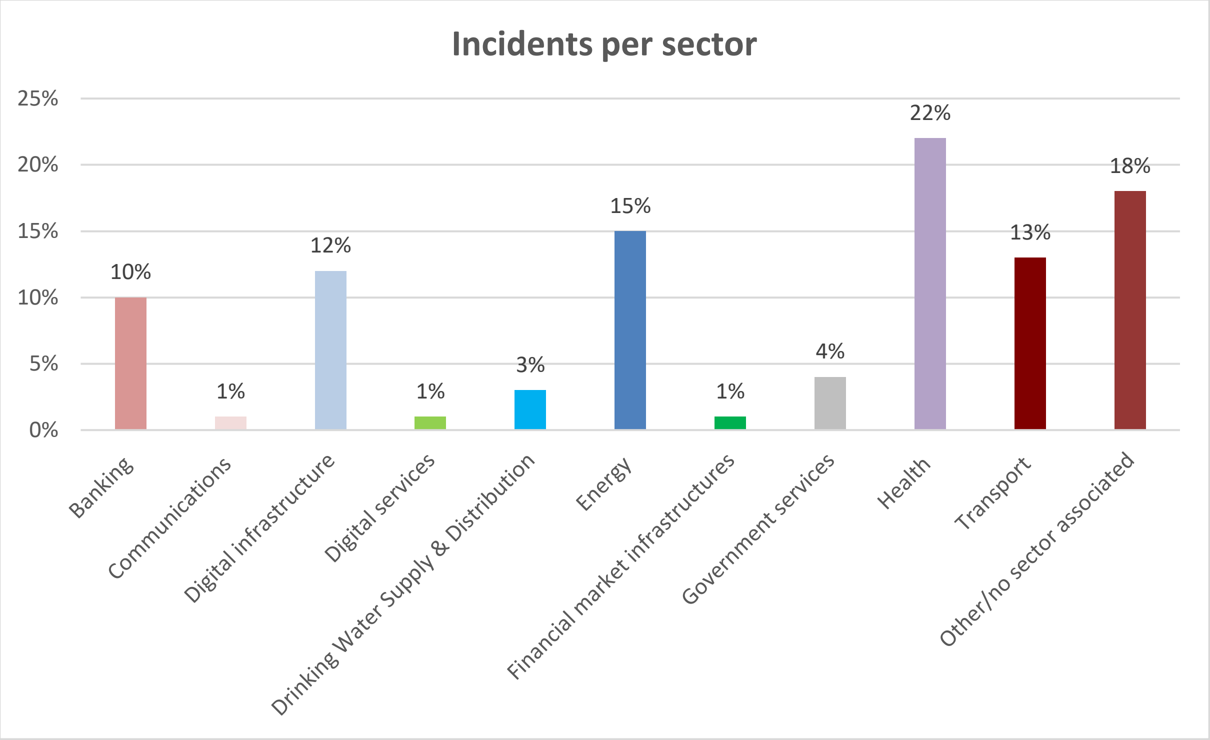
3.1. General overview

A total of 23 Member States participated in the annual summary reporting process through CIRAS. One Member State submitted a consolidated report through other means and information was extracted and was uploaded to CIRAS by ENISA and 3 Member States did not submit a report.

For 2024, a total of 1276 incident reports were included in the annual summary reporting.

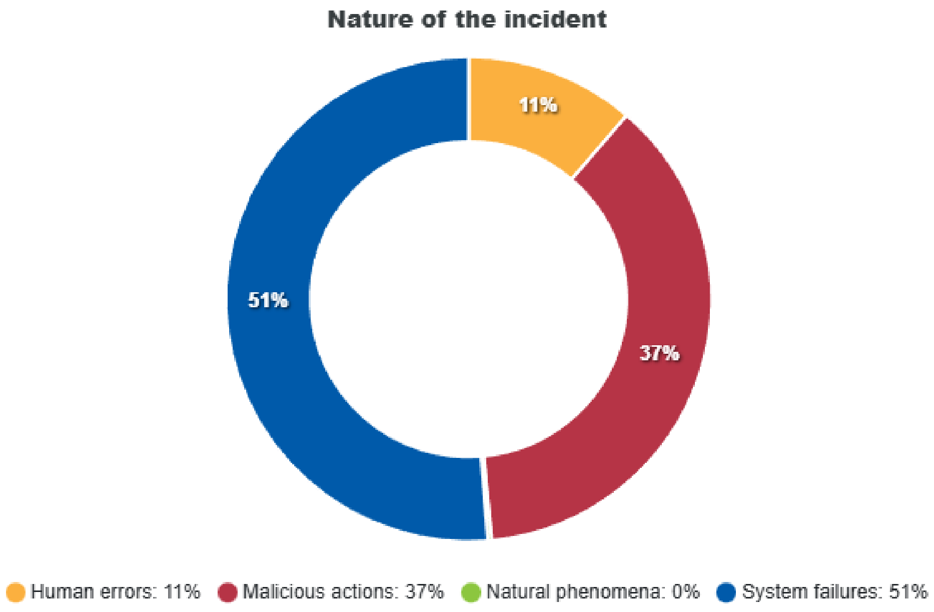
3.2. Incidents per sector

In 2024, most incident reports related to the health (22%), energy (15%), transport (13%), digital infrastructure (12%) and banking (10%) sectors, 18% of reported incidents did not have sector associated with them.



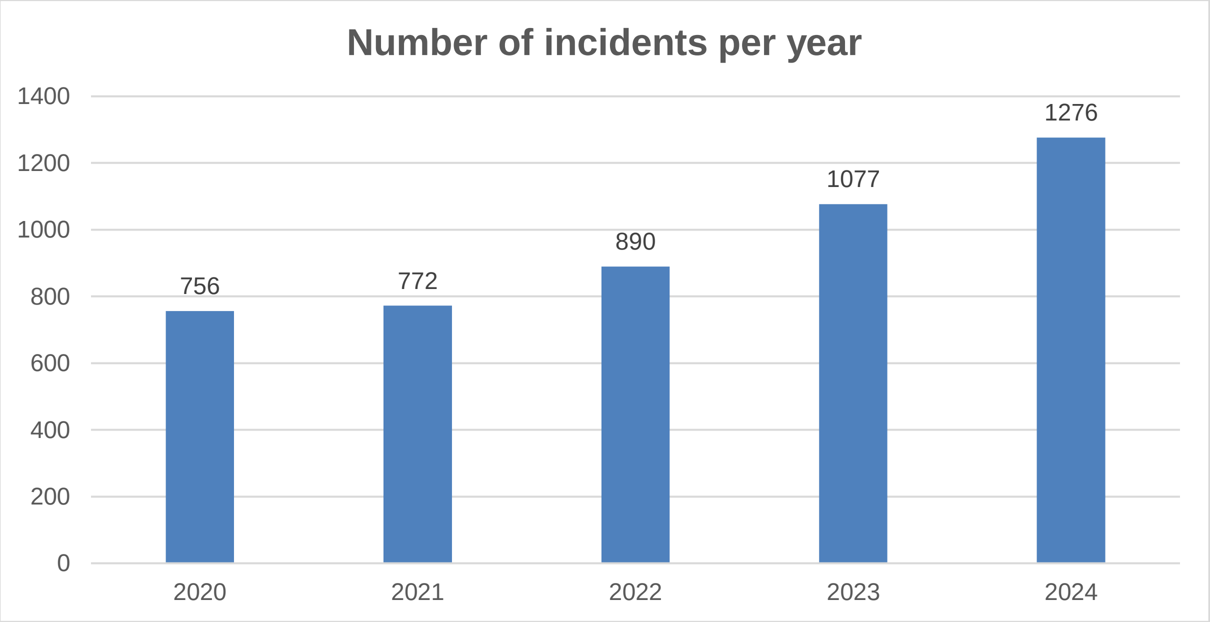
3.3. Root cause categories

Incidents are categorised in 4 broad root cause categories. In 2024 51% of the NISD incidents were system failures and 37% of the incidents were categorised as malicious actions. Human errors accounted for 11% of the incidents. Compared to 2023 there is a slight increase in system failures and decrease of malicious actions.

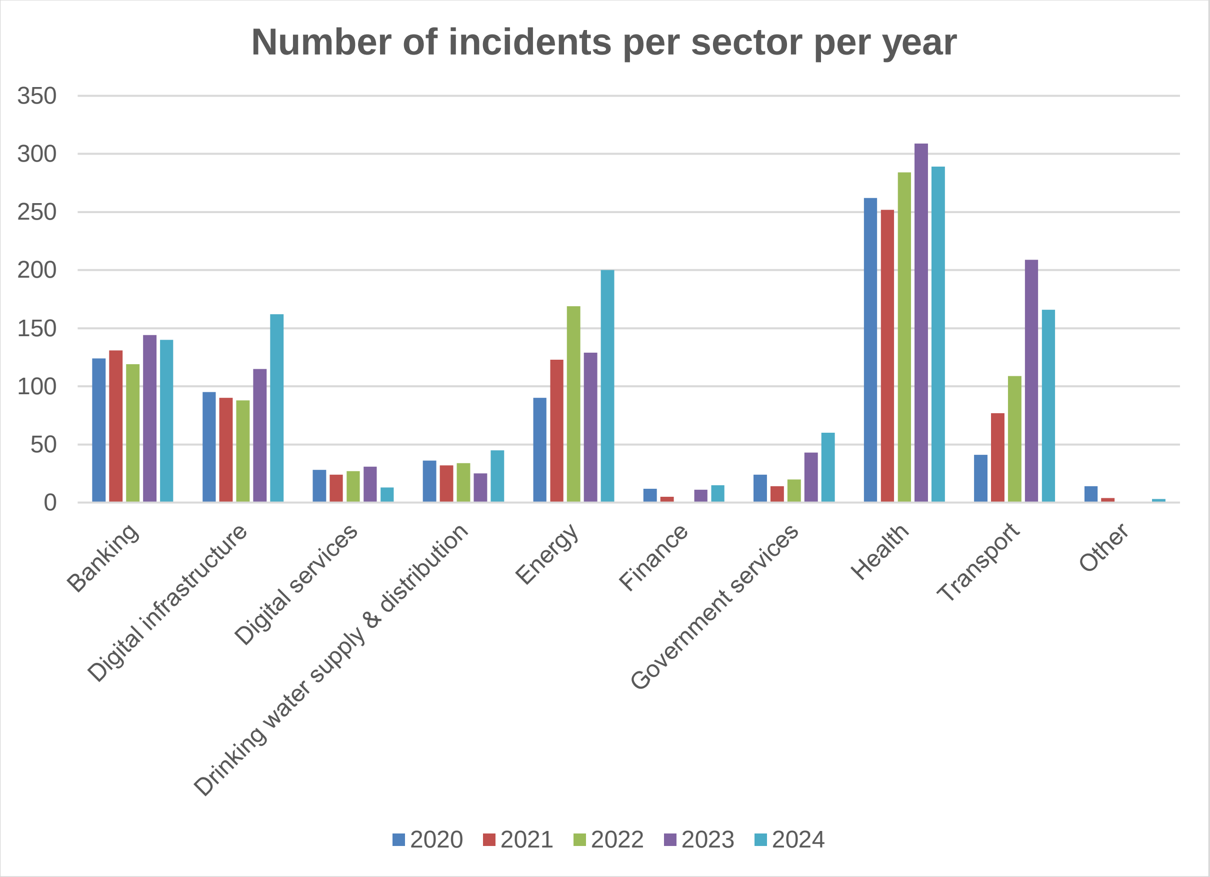


3.4. Comparison of 2024 with 2023, 2022 and 2021

While the numbers of reported incidents in 2020 and 2021 were similar, the number of reported incidents continue to increase from 2020. In 2024 increase similar to previous period is observed.

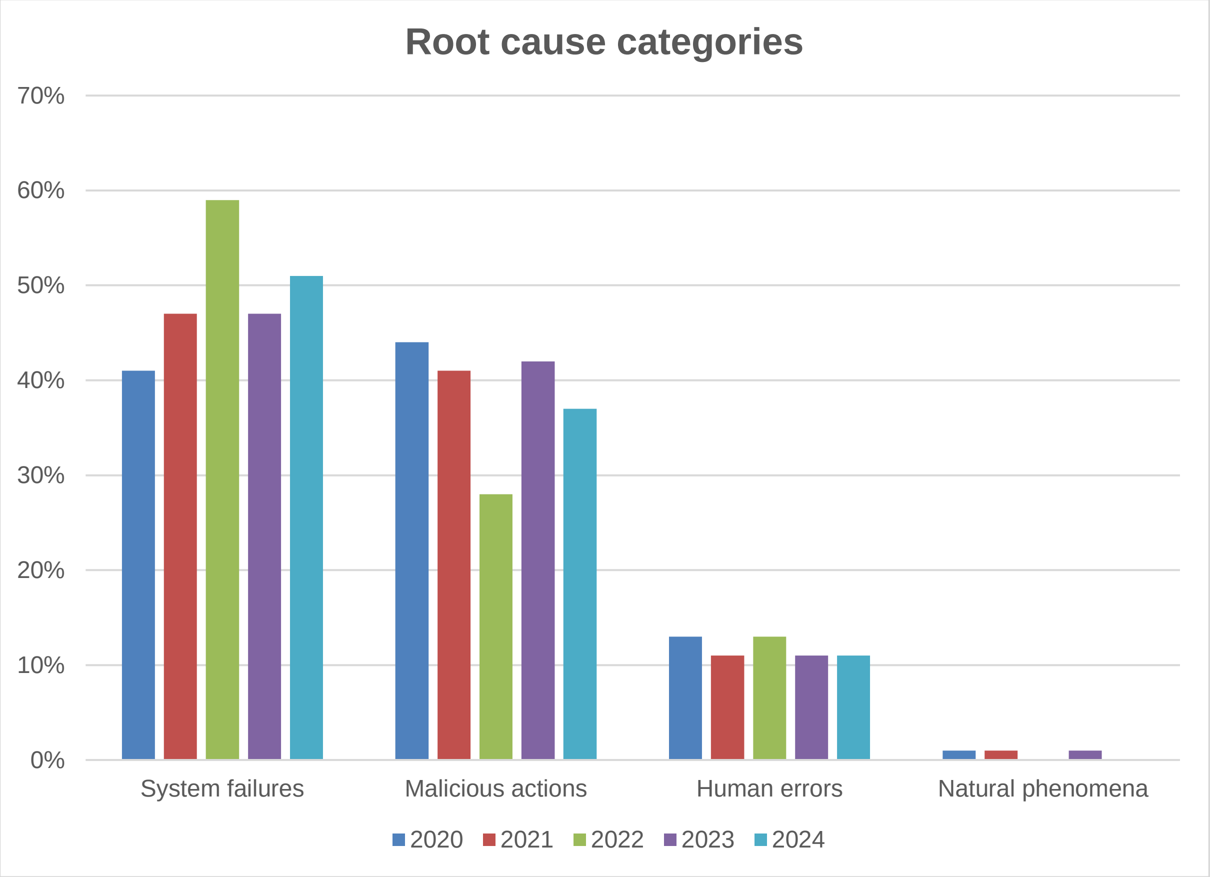


A detailed breakdown for incidents per sector is presented in the figure below, for years 2021, 2022, 2023 and 2024. An increased number of incidents is observed in Energy, Digital infrastructure, Drinking water and Finance sectors. The number of incidents reported in Health, Transport and Banking sectors has slightly decreased.



When comparing the incidents' root causes over the years, an increase of system failures is observed although these decreased in 2023. Malicious actions were decreasing during 2020-2022[9] and there was an increase in 2023 and decrease in 2024. It is noted that root causes relating to human errors and natural phenomena remain more or less at the same levels.

[9] It is noted that graph of the number of incidents per year includes all incidents reported by the Member States for 2020 and 2021, while the summary incident reports in CIRAS do not include all incidents reported for 2020 and 2021.

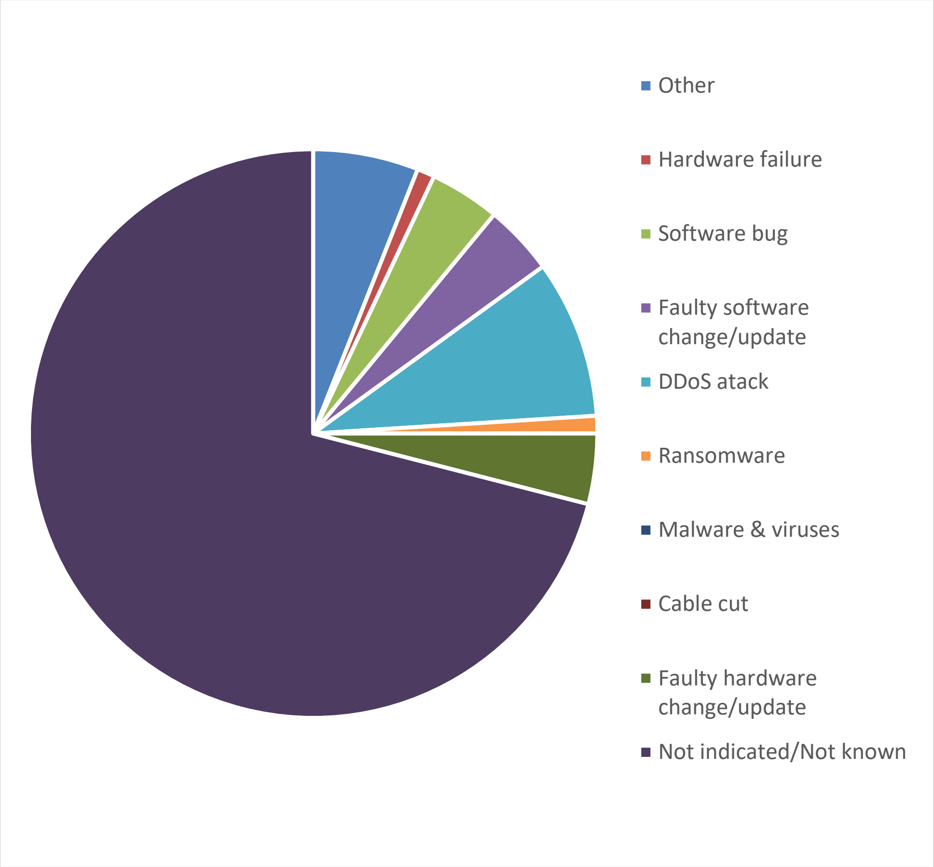

Root cause categories
70%
60%
50%
40%
30%
20%
10%
0%
System failures
Malicious actions
Human errors
Natural phenomena
2020
2021
2022
2023
2024

4. Sectorial information

In this section, the incidents across all sectors of NIS directive are presented in detail.

4.1. Detailed technical causes

The underlying technical causes leading to the reported incidents are shown in the figure below. It is noted that for 71 % underlying technical cause is either not indicated or not known.



The most common causes are:

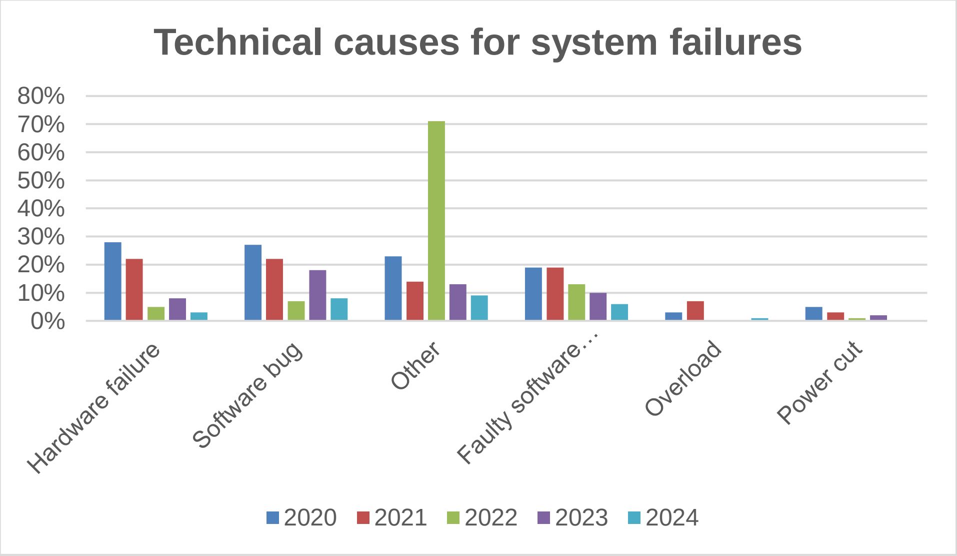
- DDoS attacks (9%);
- software bug (4%);
- faulty software change/update (4%)
- ransomware (1%)
- hardware failure (1%)

DDoS and Ransomware are among also among eight prime threat types analysed in ENISA Threat Landscape 2024.[10] It is noted though that the technical cause for a number of incidents was defined as 'other' -6%.

When going into detail for each of the 4 root cause categories (see the figures below), it is noted that for 2024:

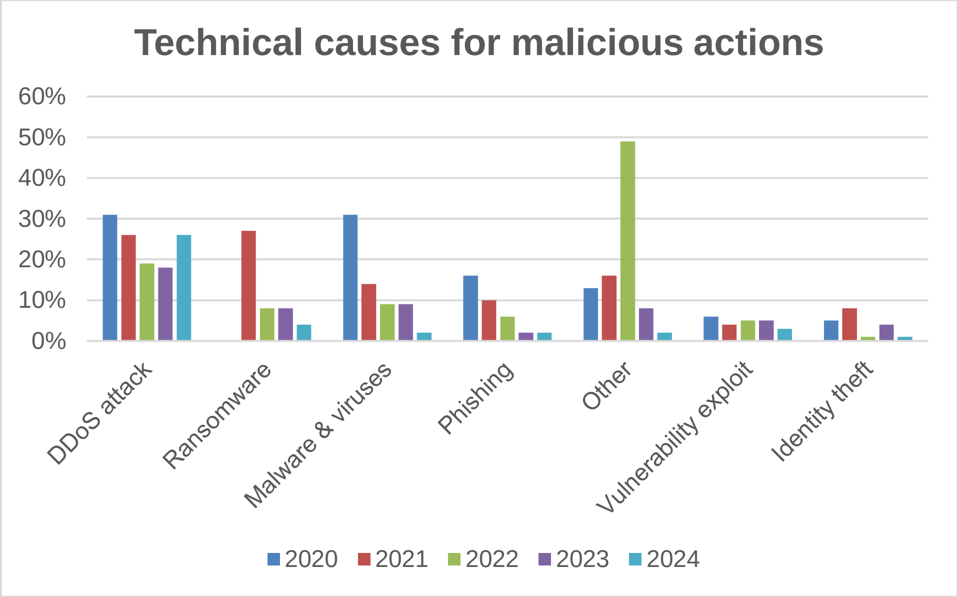
- the technical causes underlying system failures mainly relate to software bugs and faulty software changes/updates;
- the technical causes underlying malicious actions mainly relate to DDoS attacks;
- the technical causes underlying human errors mainly relate to faulty software changes/updates;

4.1.1. System failures

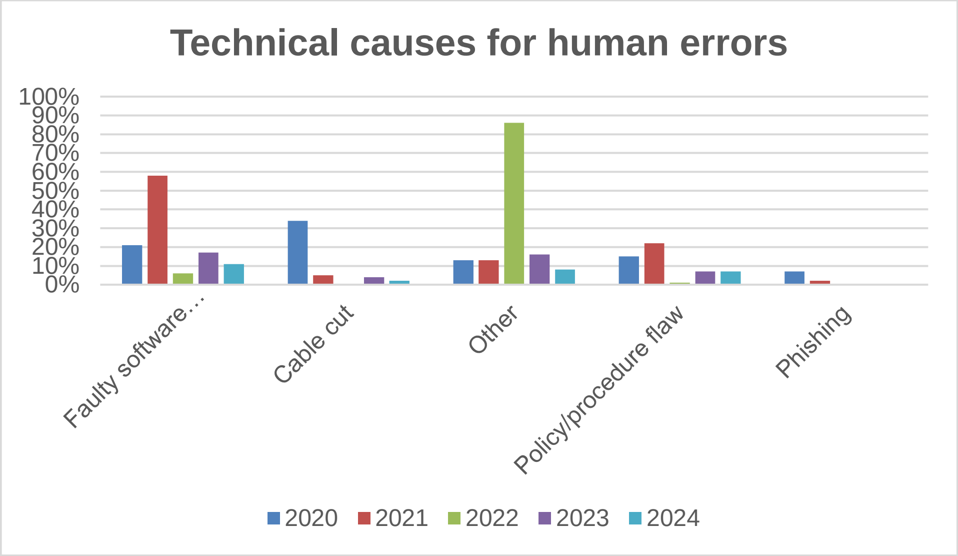


[10] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

4.1.2. Malicious actions

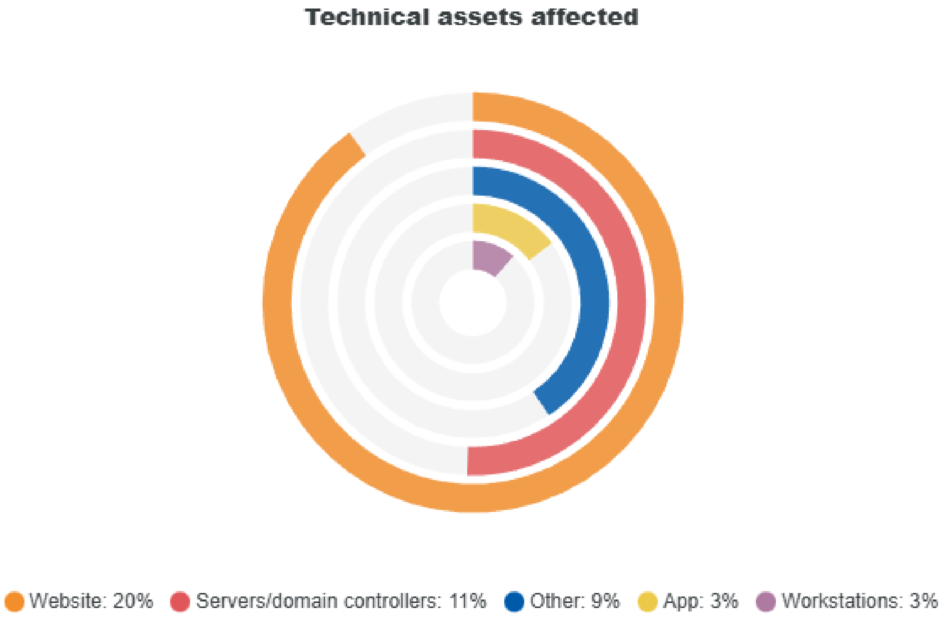


4.1.3. Human errors



4.2. Technical assets affected

When it comes to assets affected, it is observed that 20% of the incidents affected websites and 11% of the reported incidents affected servers/domain controllers while for 9% of the incidents, ‘other’ technical assets were affected.in 54% of incidents there is no information about technical assets affected.

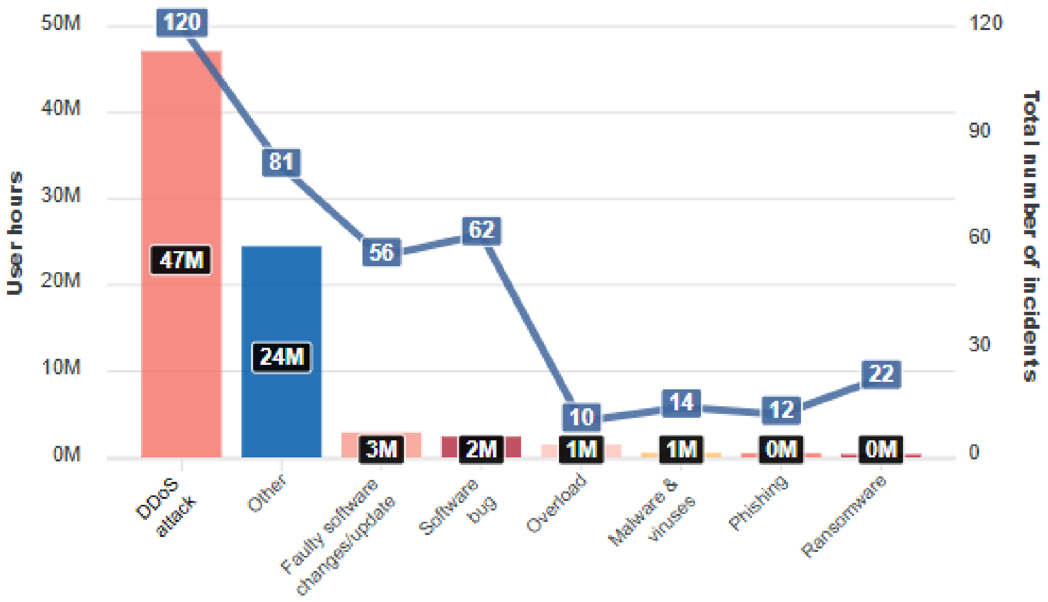


4.3. Detailed overview of incidents with outages caused

CIRAS also captures data on incidents with outages caused if this information is included in the reported incidents.

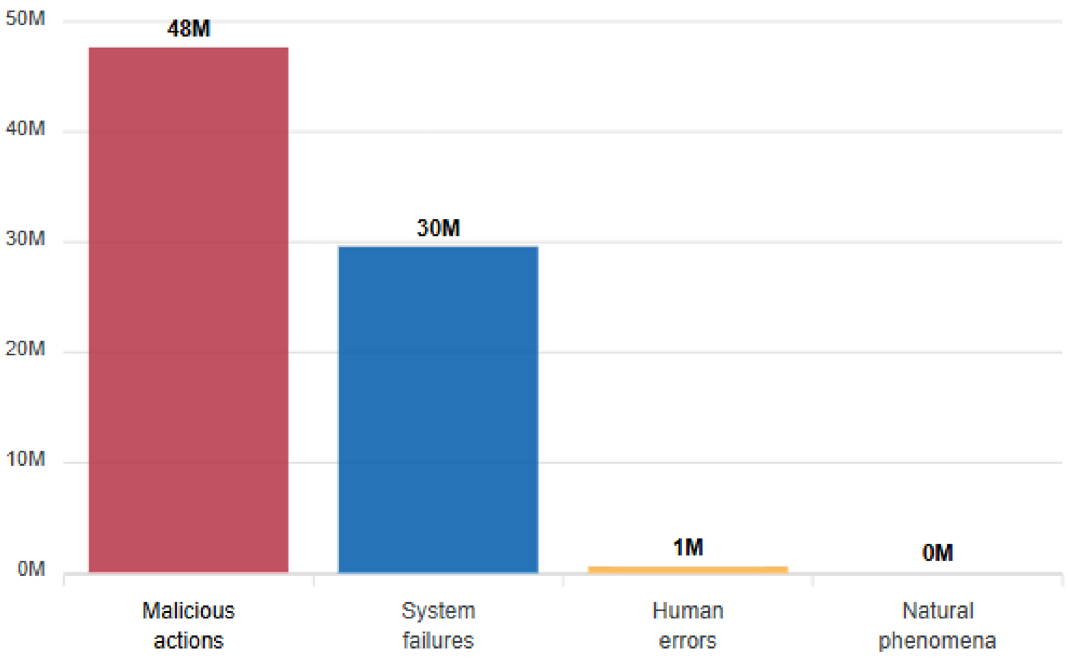
The figure below shows the user hours lost and the number of outages per technical cause. It is evident that in 2024, the leading cause for outages was DDoS attack which corresponds also with ENISA Threat landscape 2024 observation based on open source information.

User hours lost & number of incidents per technical cause



When going into detail, it is identified that malicious actions and system failures were the leading causes of user hours lost.

User hours lost per nature of incident

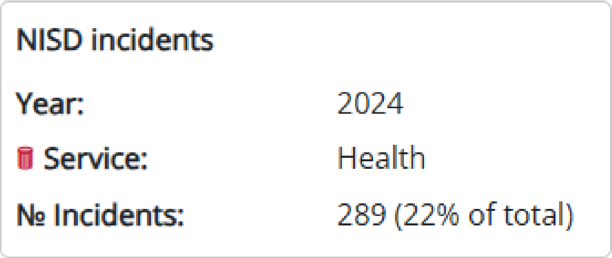


5. Detailed overview of the sectorial data

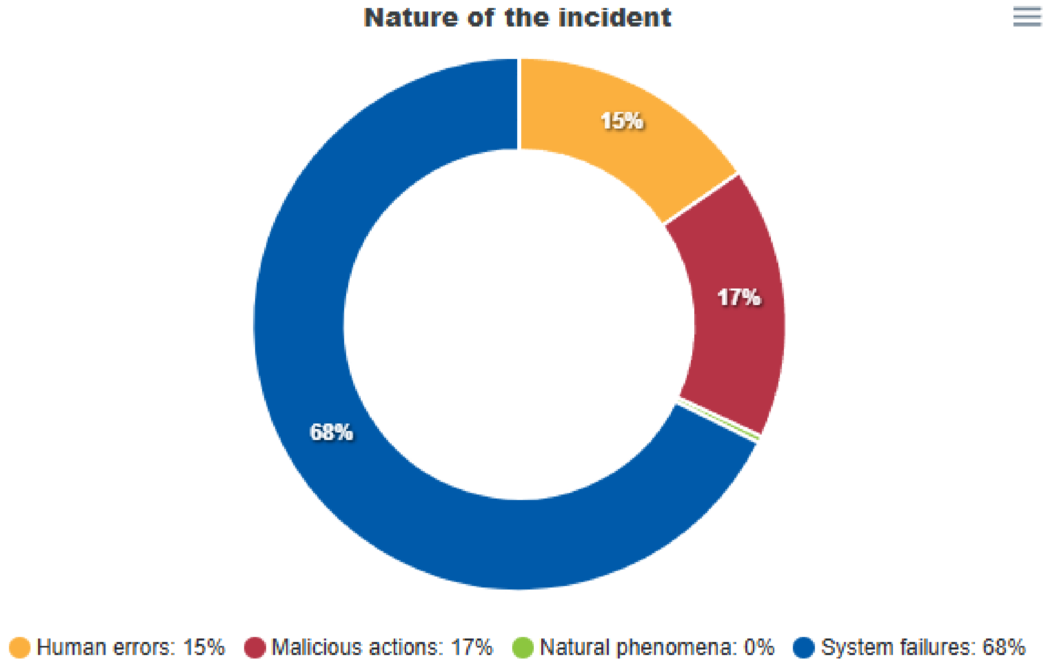
This section provides detailed information on all NIS sectors.

5.1. Health sector

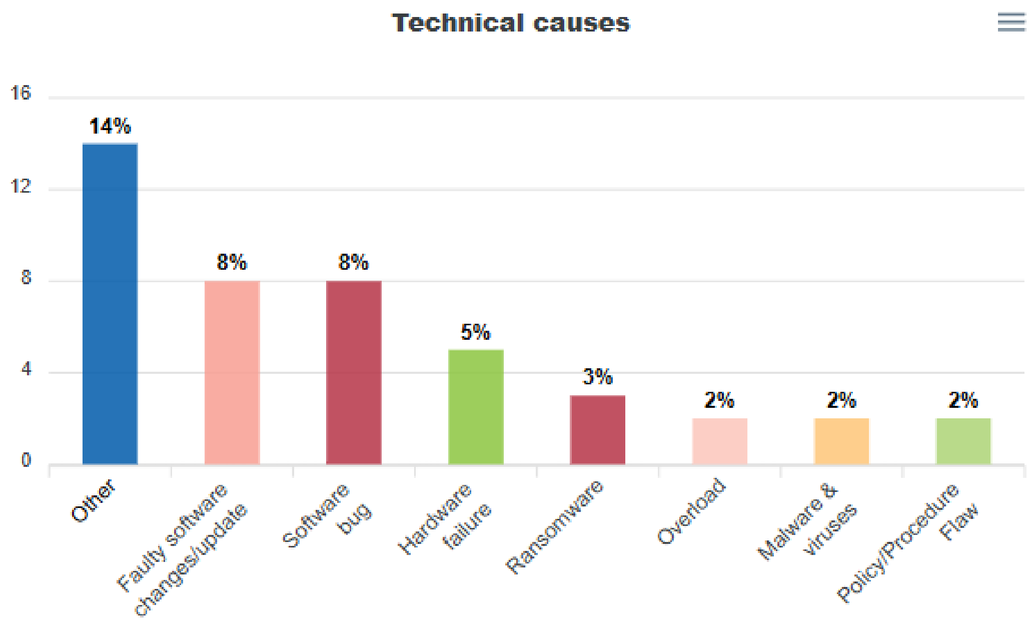
The most impacted sector for the fifth year in a row was health. A total of 289 incidents were reported for the sector, for which the nature mainly related to system failures and malicious actions.



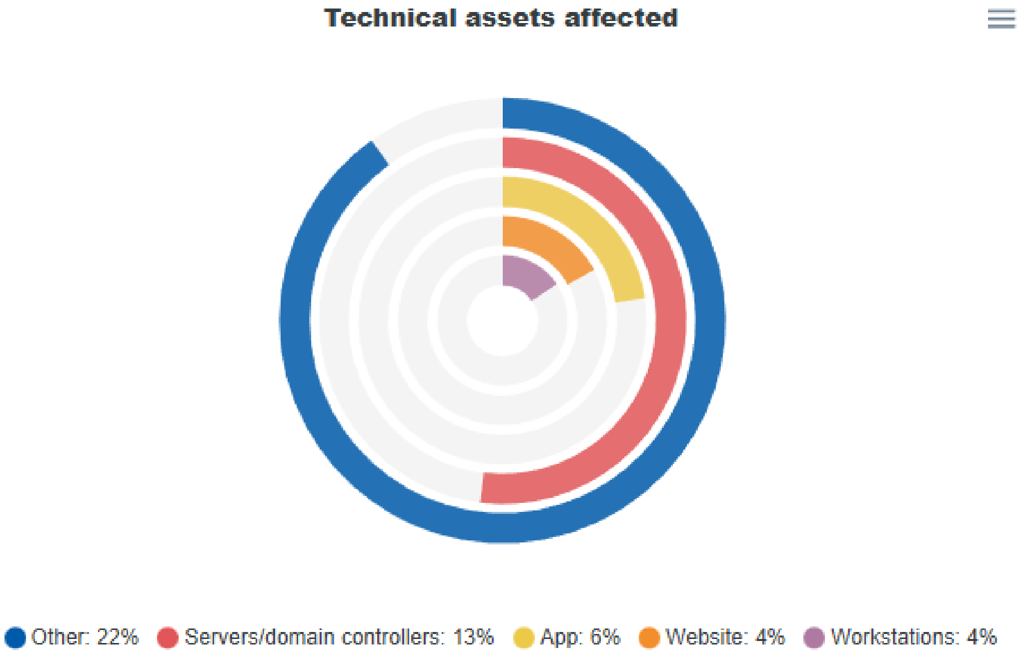
NISD incidents	
Year:	2024
Service:	Health
№ Incidents:	289 (22% of total)



In 56 % of cases technical cause is not known or not reported and in 14% of cases cause was reported as Other.

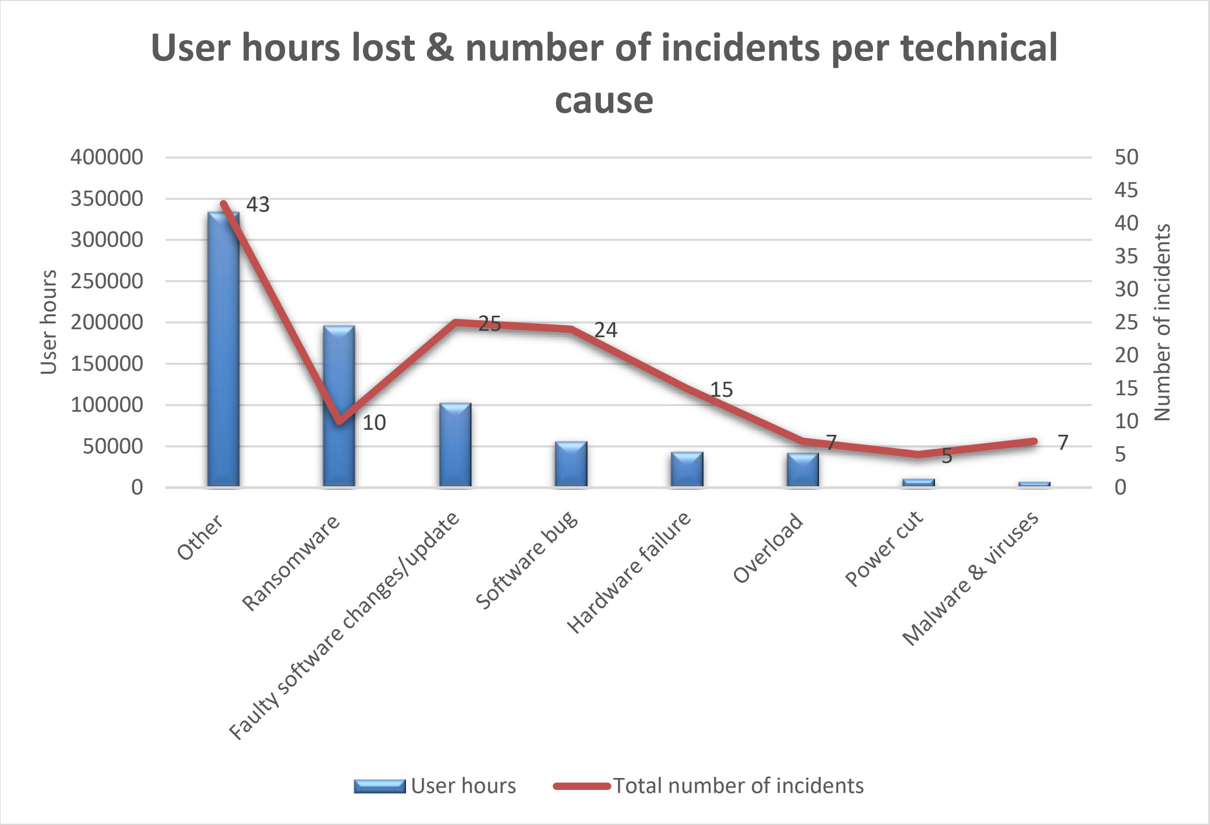


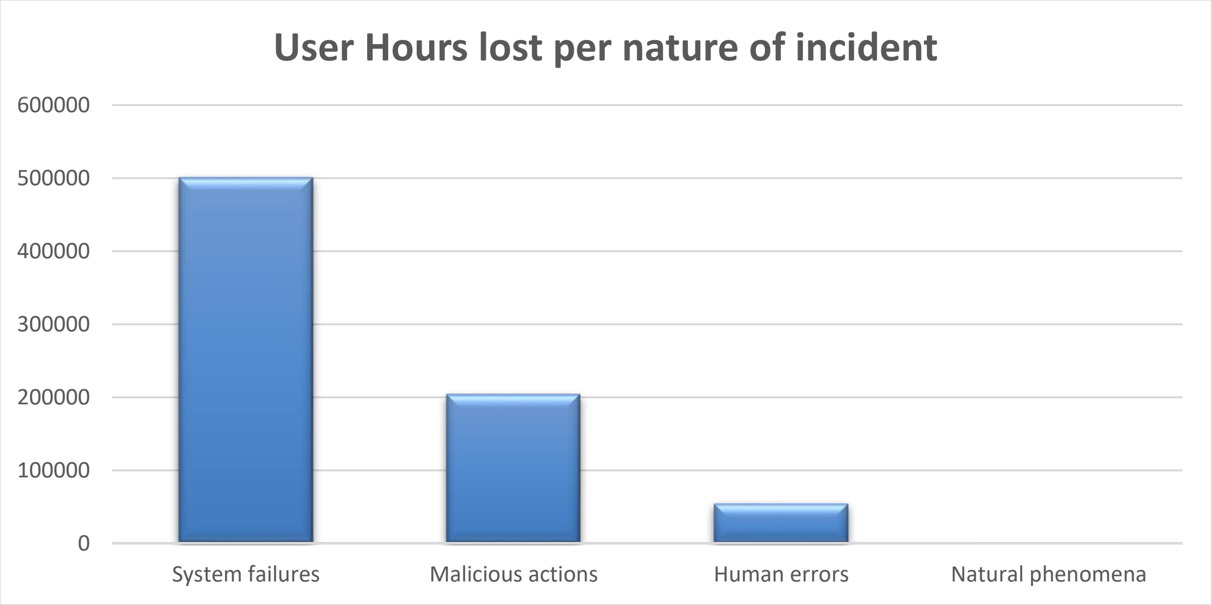
Most affected technical assets were servers/domain controllers and applications. The asset affected for 22% health related incidents was defined as ‘other’. In 56 % of cases technical cause is not known or not reported.



For incidents that are outages lost user hours and causes are considered below.

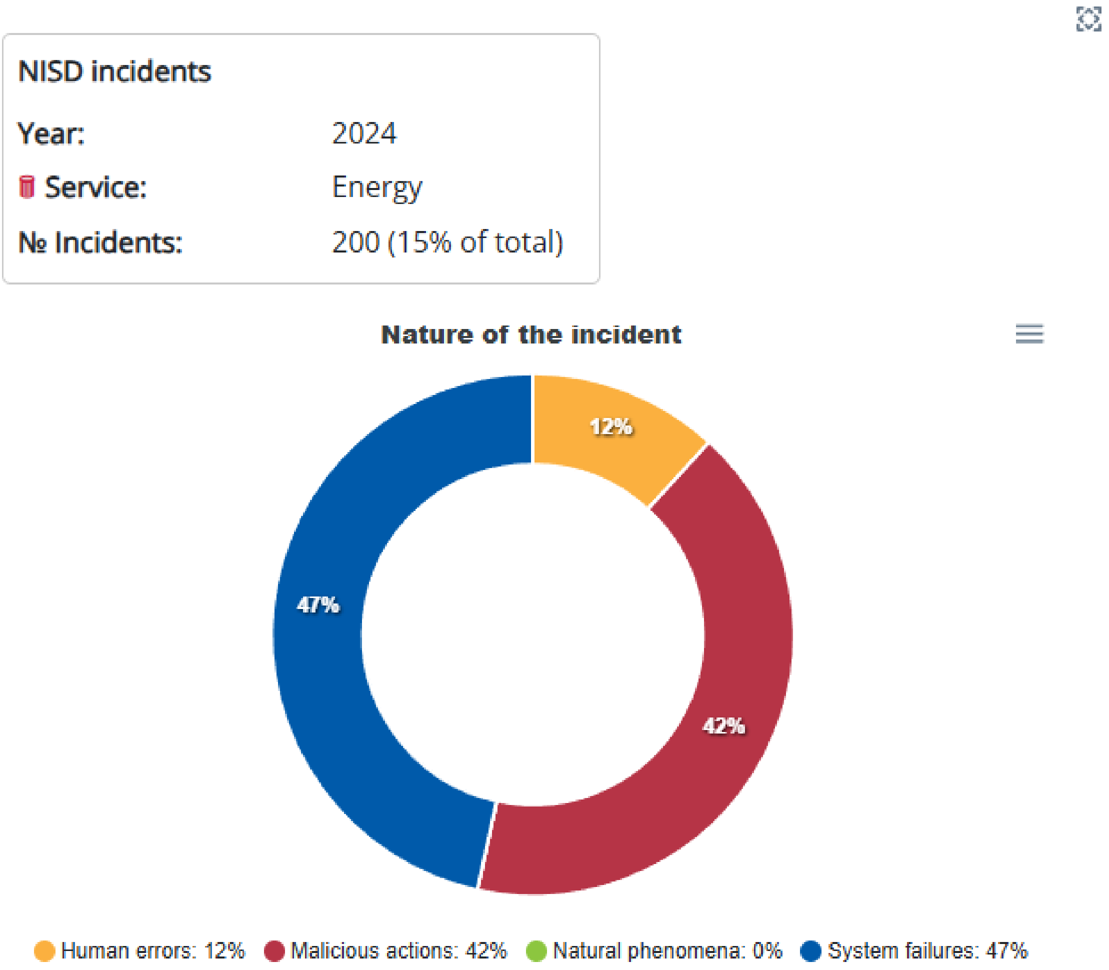
It is identified that ransomware was the main cause for user hours lost in health sector and that the leading nature for the reported incidents was system failures.





5.2. Energy sector

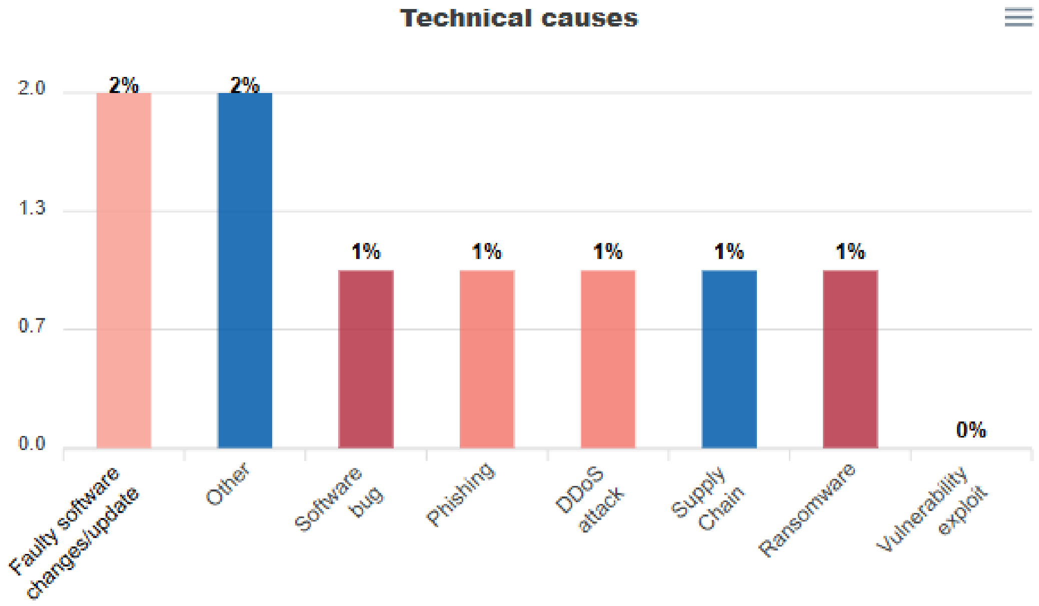
Energy was the second most impacted sector for 2024. A total of 200 incidents were reported for the sector, for which the nature mainly related to system failures and malicious actions.



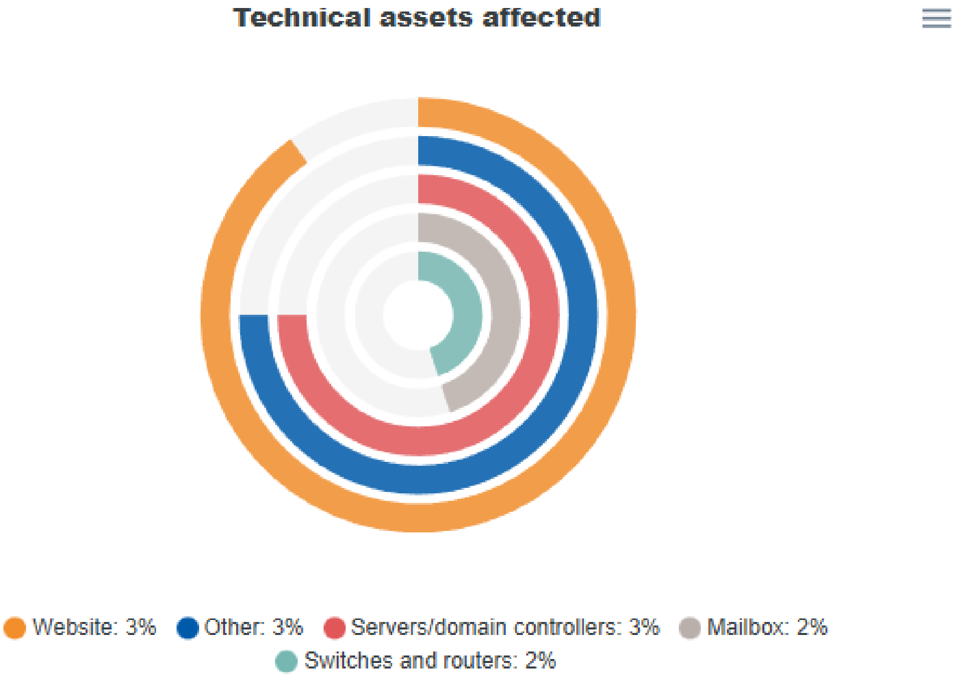
NISD incidents

Year:	2024
Service:	Energy
№ Incidents:	200 (15% of total)

The underlying technical causes for these incidents mainly related to faulty software update. However, in 91 % of cases technical cause is not known or not reported and in 2% of cases cause was reported as Other.

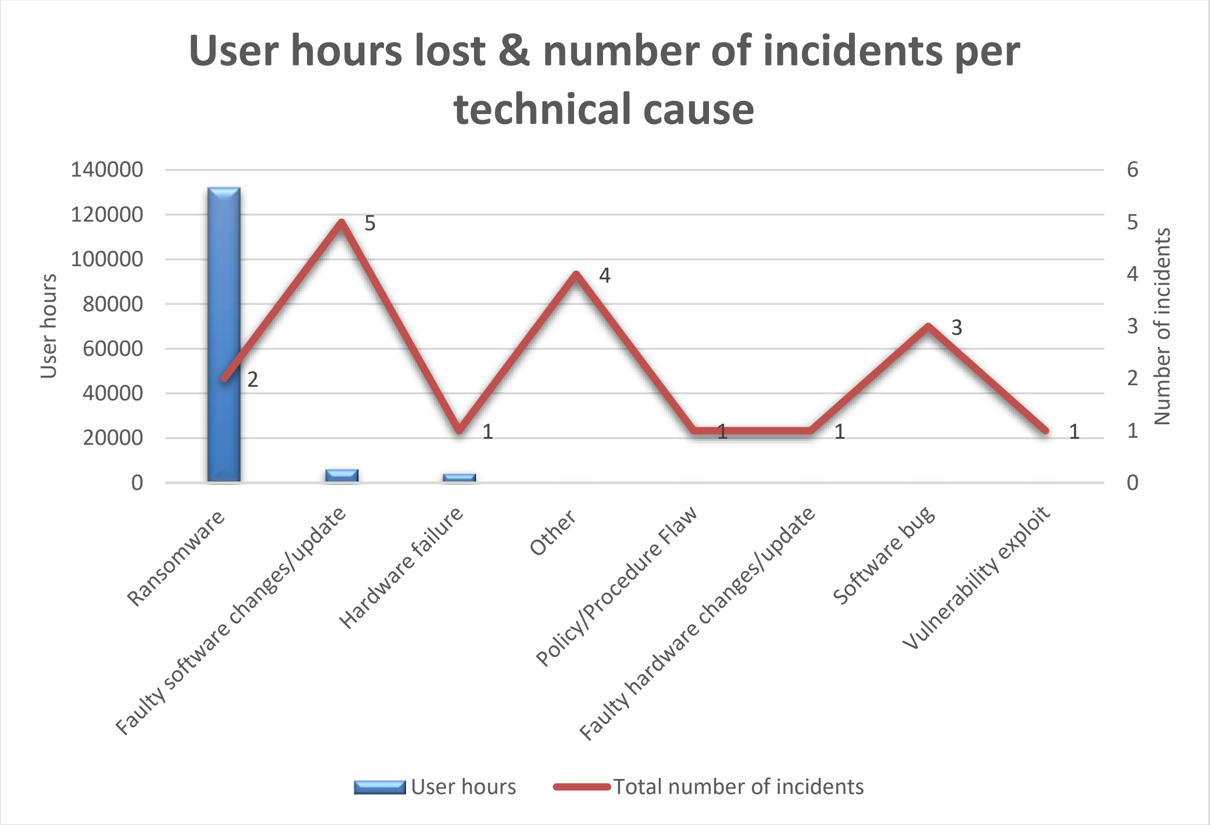


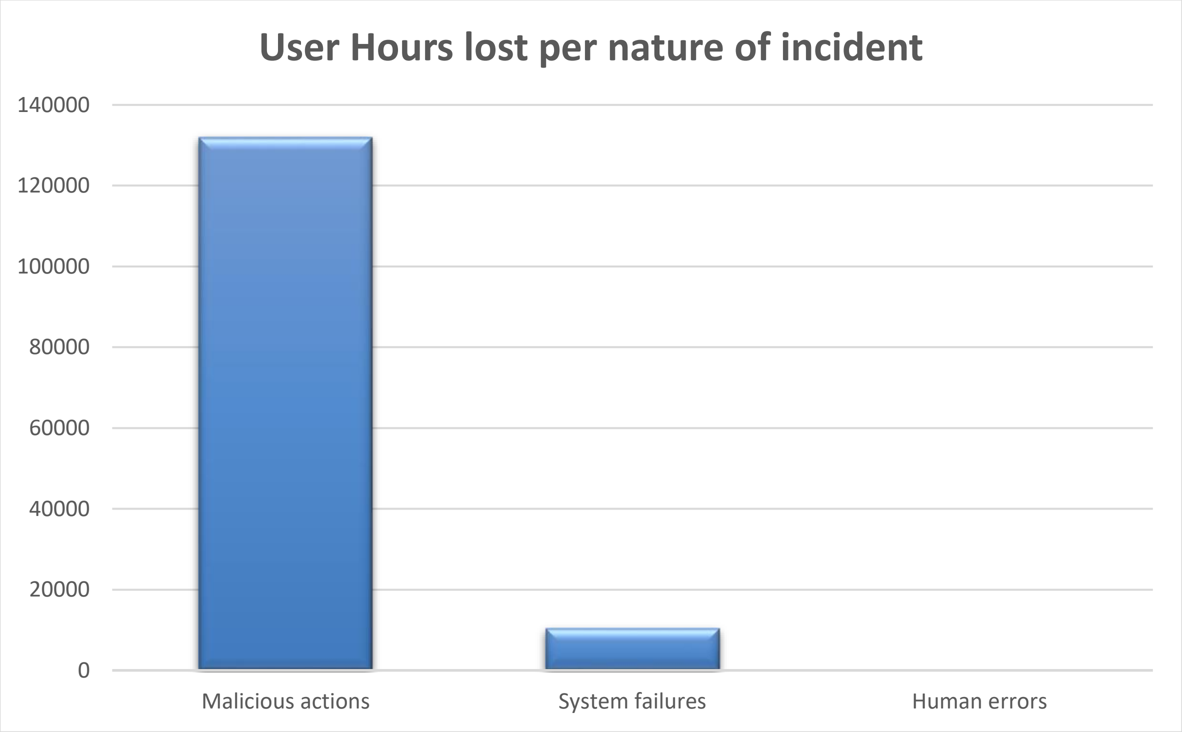
As per the incident reports for energy, the most affected technical assets were websites and servers/domain controllers. The asset affected for 23% of the energy related incidents was defined as 'other'.



For incidents that are outages lost user hours and causes are described below.

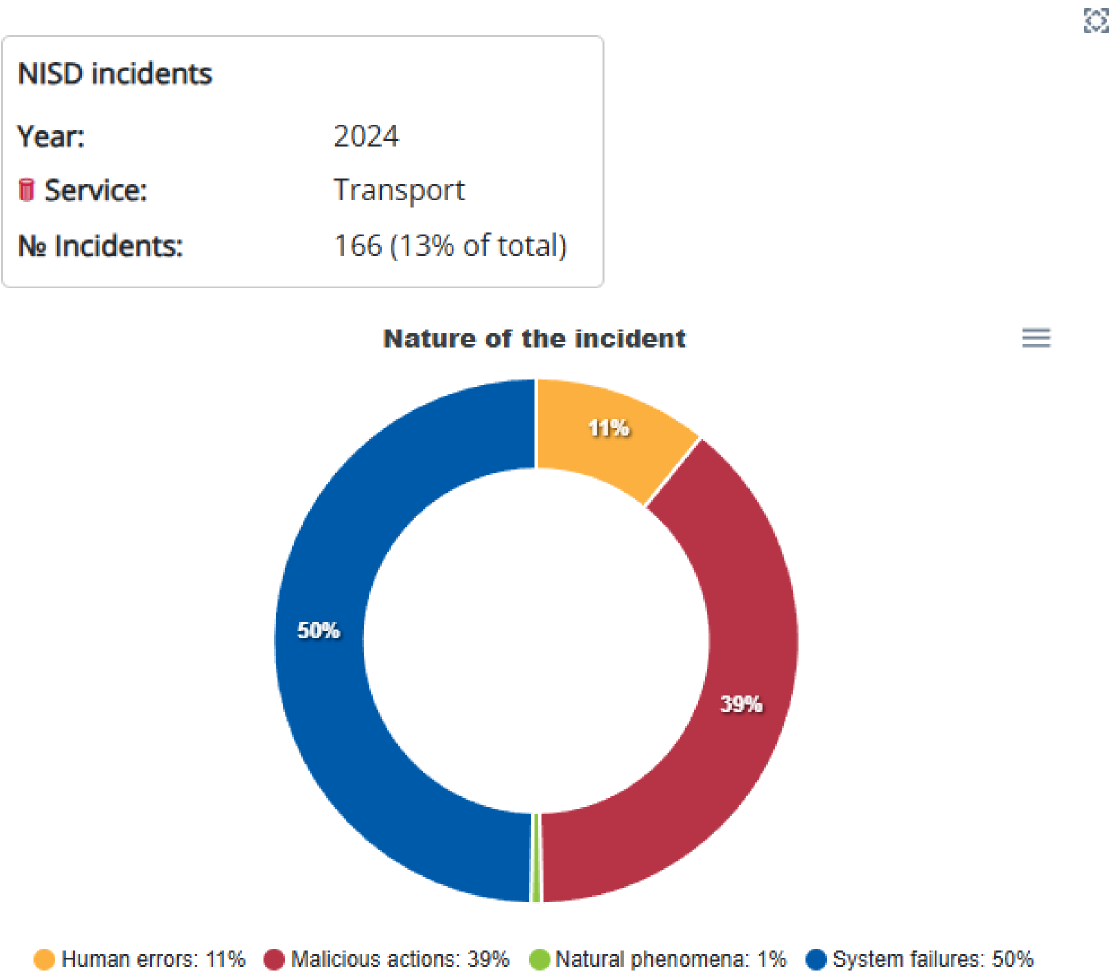
It is identified that ransomware was the main cause for user hours lost in energy and that the leading nature for the reported incidents was malicious actions.





5.3. Transport sector

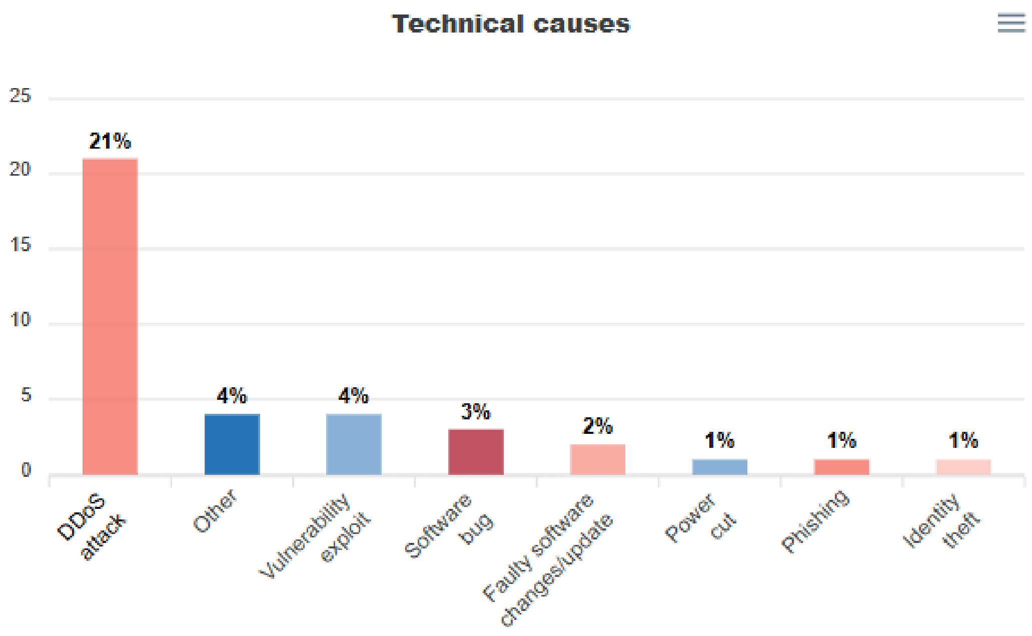
The third most affected sector in this round of reporting was the transport sector. There was a total of 166 incidents reported, for which the nature mainly related to system failures and malicious actions.



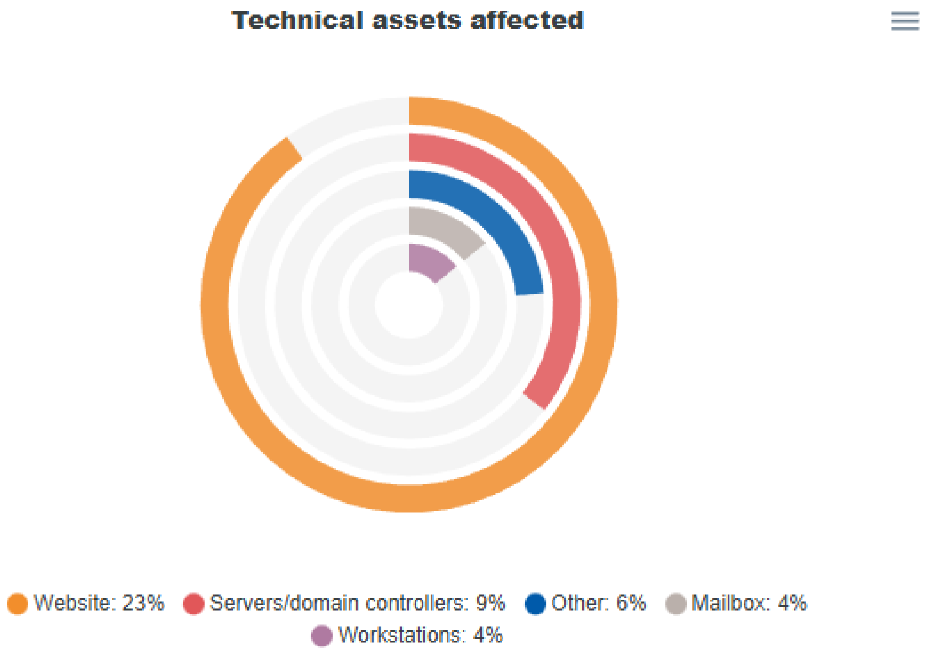
NISD incidents

Year:	2024
Service:	Transport
№ Incidents:	166 (13% of total)

The underlying technical causes for these incidents mainly related to DDoS attacks and vulnerability exploits. However, in 63 % of cases technical cause is not known or not reported and in 4% of cases cause was reported as Other.

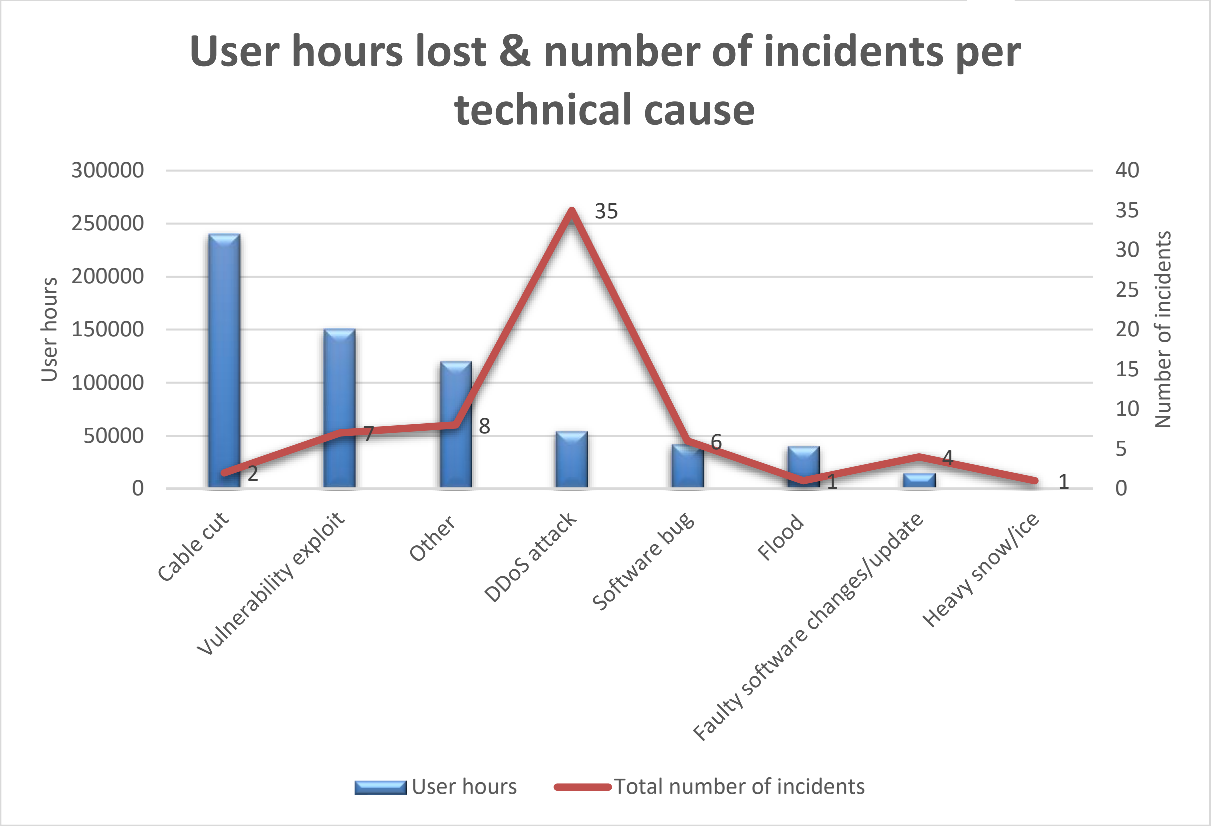


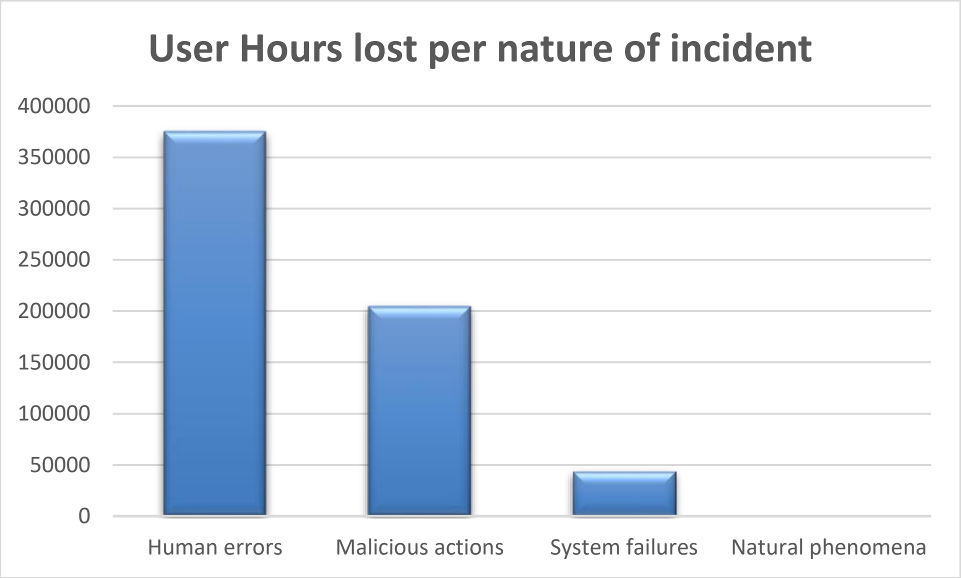
As per the incident reports for transport, the most affected technical assets were websites and servers/domain controllers.



For incidents that are outages, the lost user hours and causes are described below.

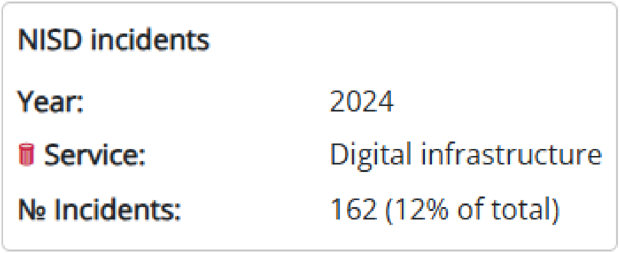
It is identified that the main cause for user hours lost in transport was DDoS attack and that the leading nature for the reported incidents was Human error.





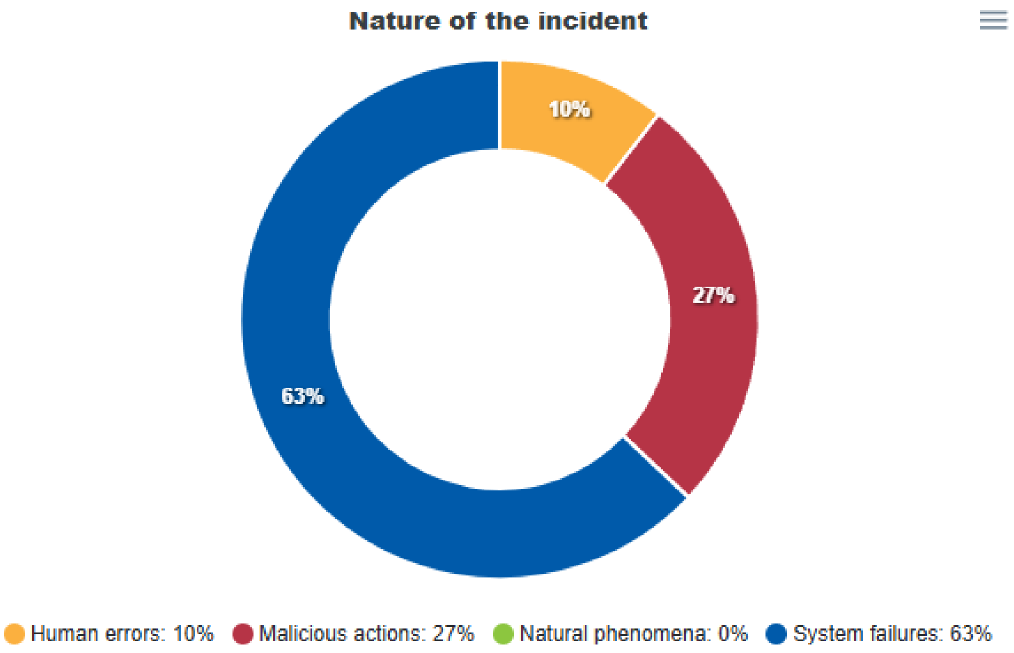
5.4. Digital infrastructure sector

The fourth sector most impacted by incidents in 2024 was the digital infrastructure sector. There was a total of 162 incidents reported, for which the nature mainly related to system failures and malicious actions.

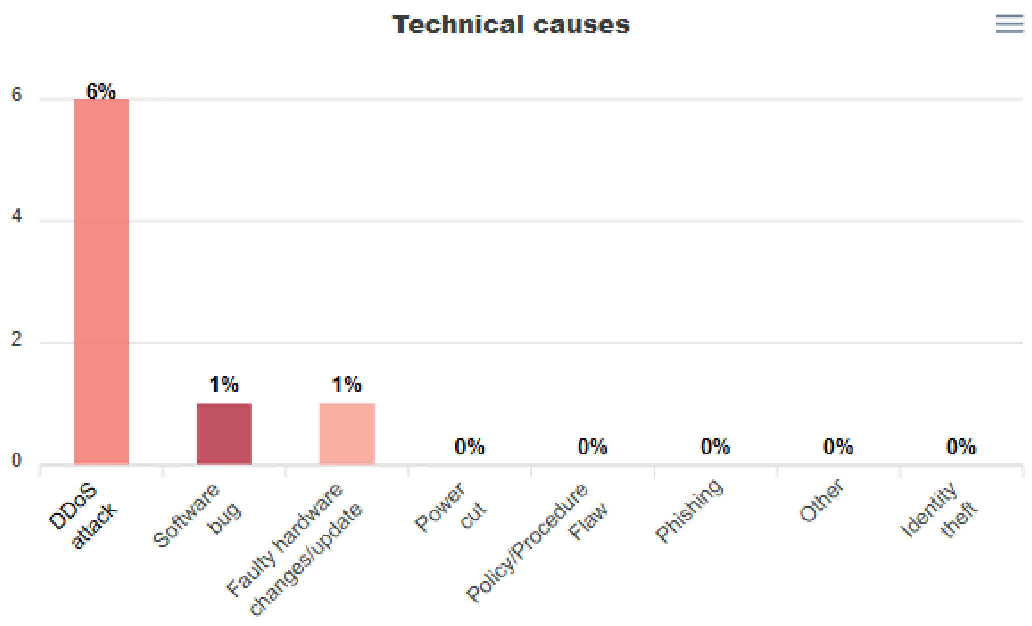


NISD incidents

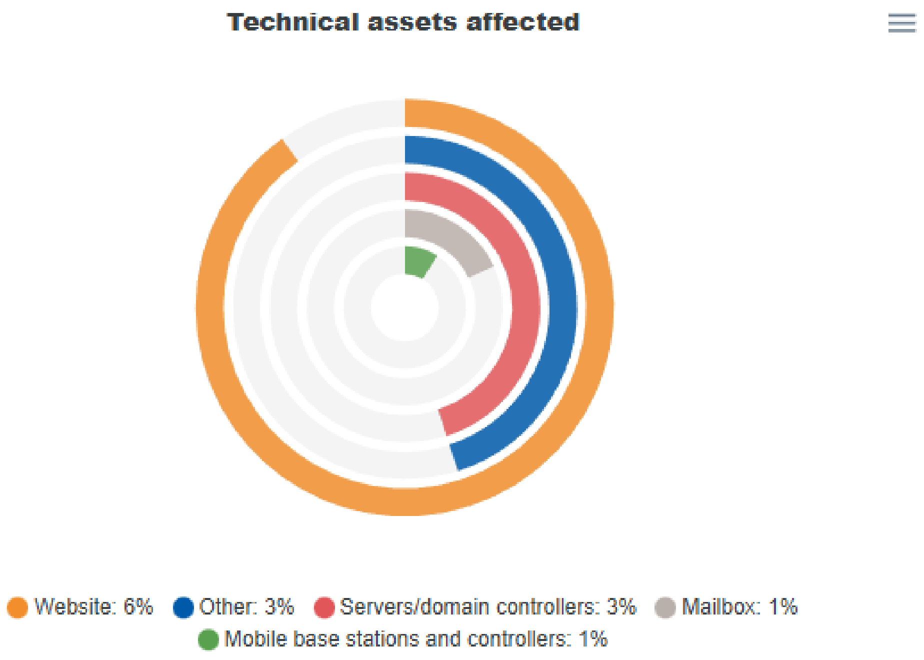
Year:	2024
Service:	Digital infrastructure
№ Incidents:	162 (12% of total)



The underlying technical causes for these incidents mainly related to DDoS attacks and software bugs. However, in 92 % of cases technical cause is not known or not reported.

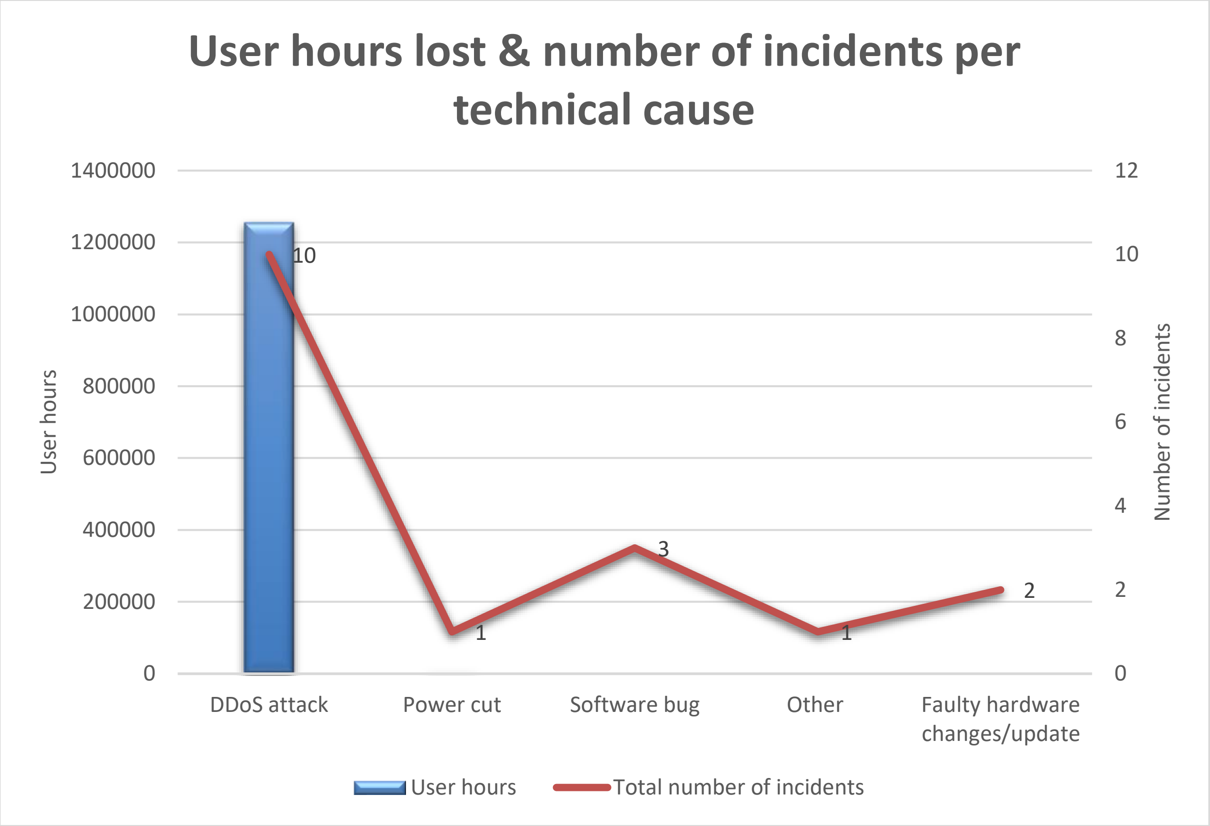


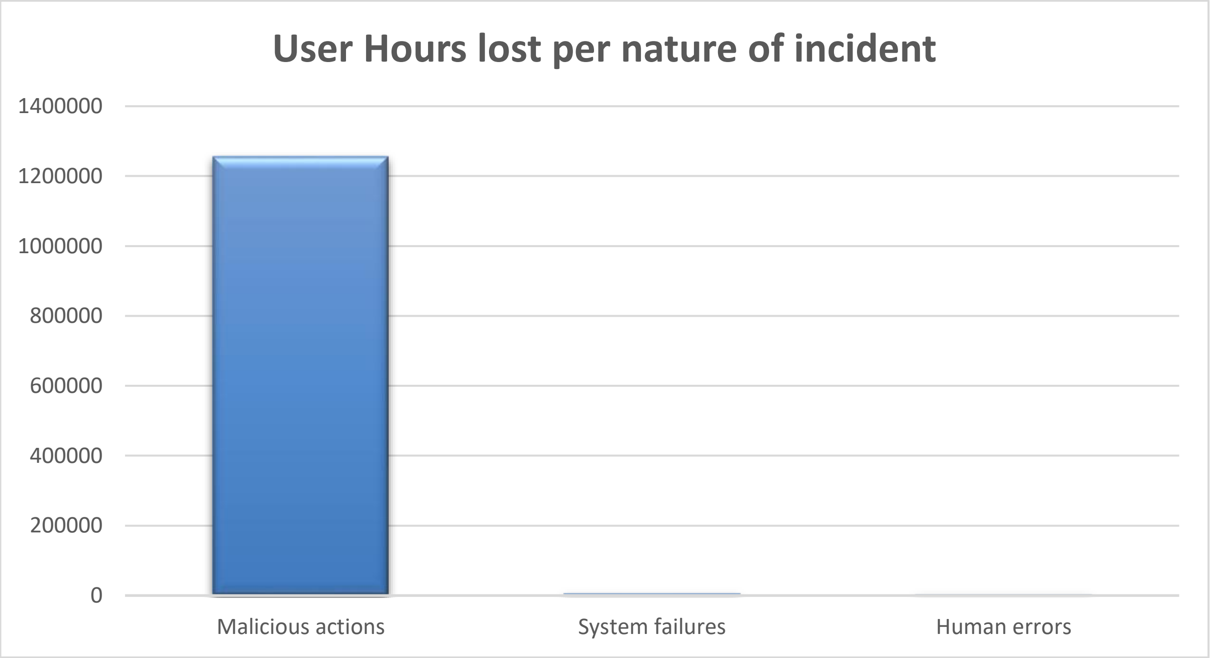
As per the incident reports for digital infrastructure, the most affected technical assets were websites and servers/domain controllers.



For incidents that are outages lost user hours and causes are described below.

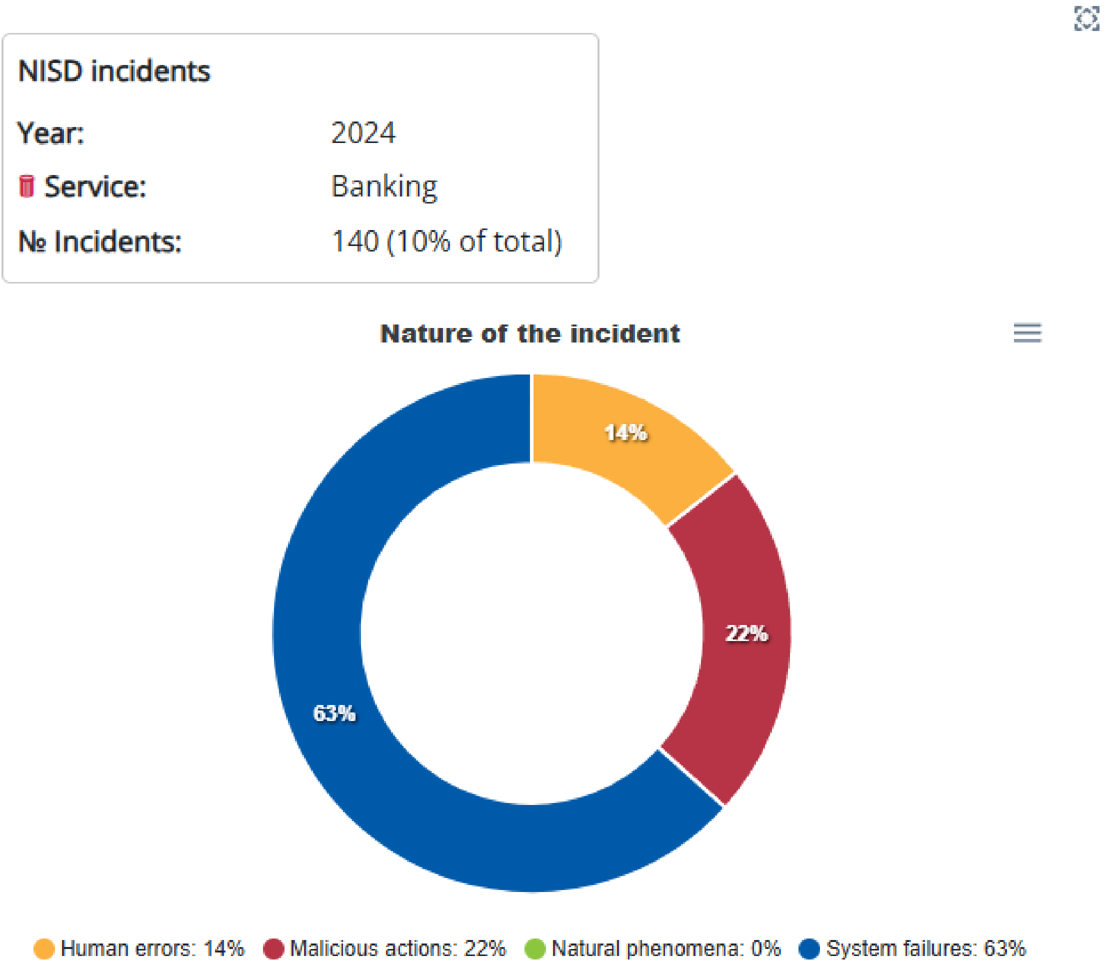
It is identified that DDoS attacks were the main cause for user hours lost in the sector and that the leading nature for the reported incidents was malicious actions.


User hours lost & number of incidents per technical cause
User hours
1400000
1200000
1000000
800000
600000
400000
200000
0
12
10
8
6
4
2
0
Number of incidents
10
1
3
1
2
DDoS attack
Power cut
Software bug
Other
Faulty hardware changes/update
User hours
Total number of incidents


User Hours lost per nature of incident
1400000
1200000
1000000
800000
600000
400000
200000
0
Malicious actions
System failures
Human errors

5.5. Banking sector

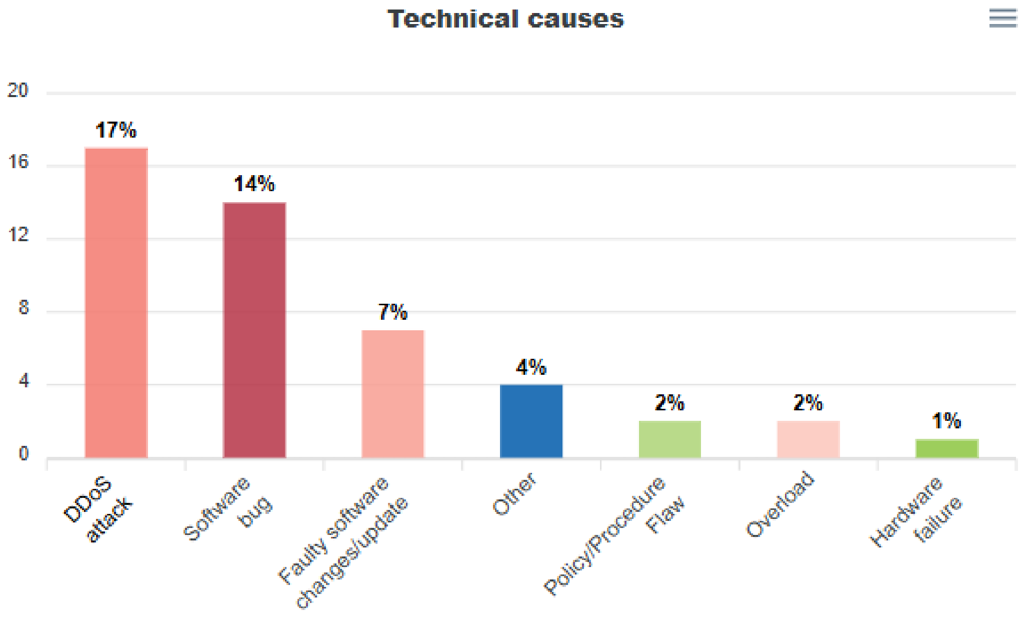
The fifth most affected sector in this round of reporting was the banking sector. There were a total of 140 incidents reported, for which the nature mainly related to system failures and malicious actions.



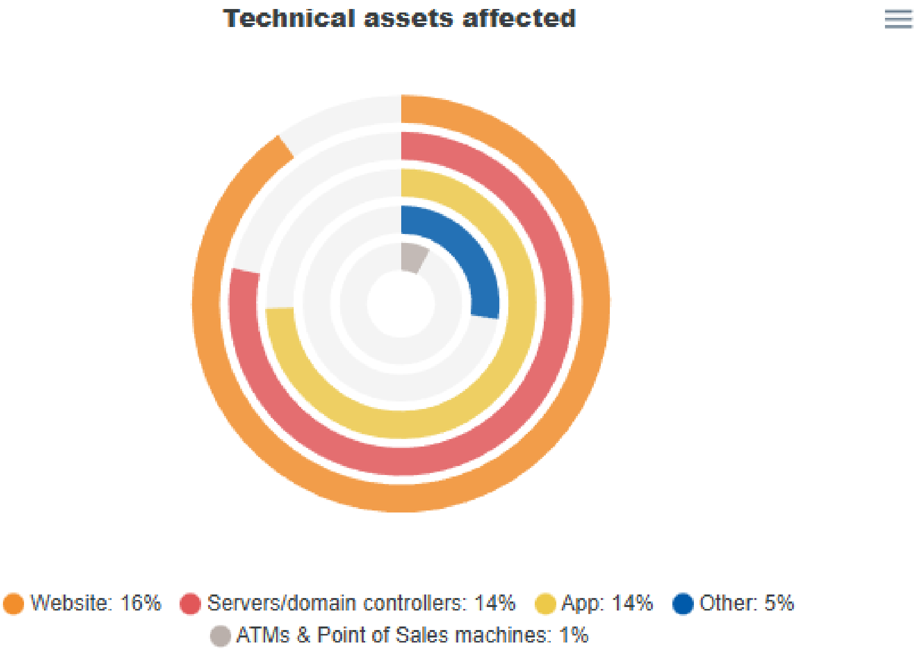
NISD incidents

Year:	2024
Service:	Banking
№ Incidents:	140 (10% of total)

The underlying technical causes for these incidents mainly related to DDoS attacks. However, in 53 % of cases technical cause is not known or not reported and in 4% of cases cause was reported as Other.

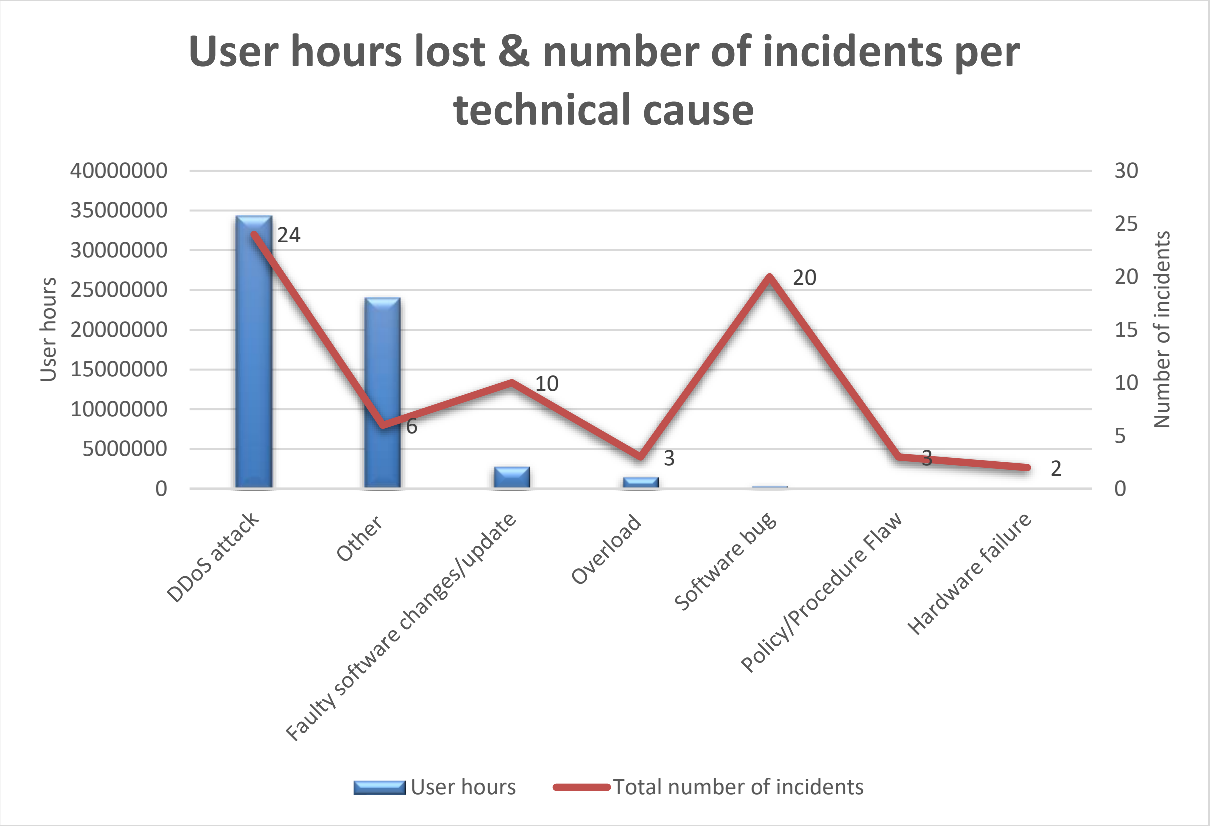


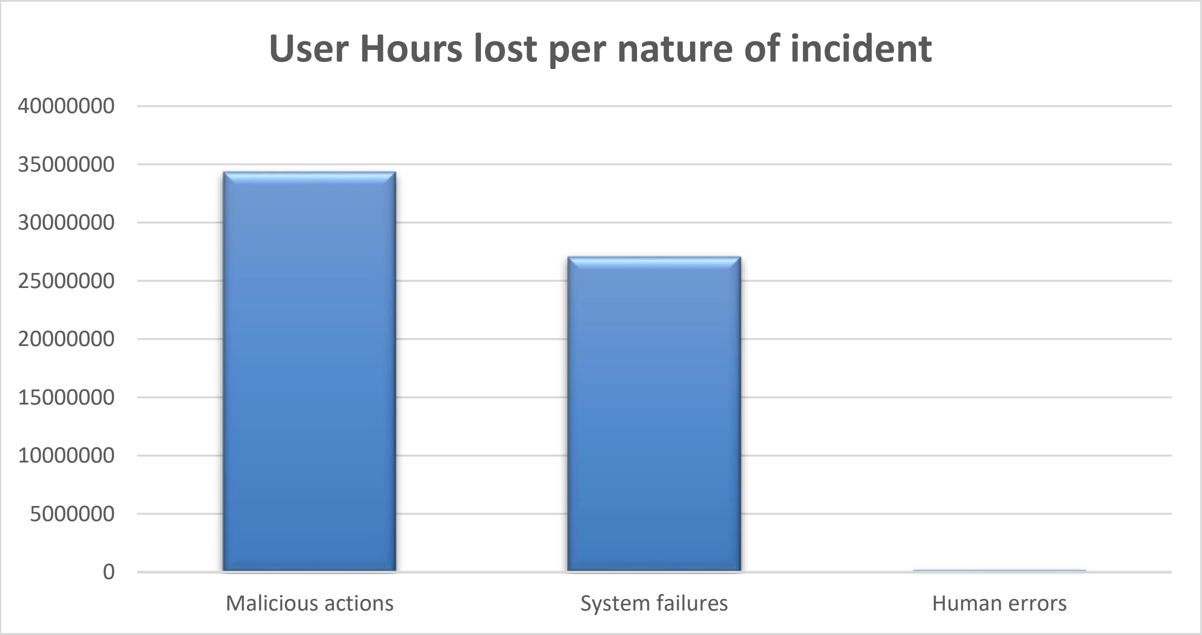
Most affected technical assets were websites and applications.



For incidents that are outages lost user hours and causes are described below.

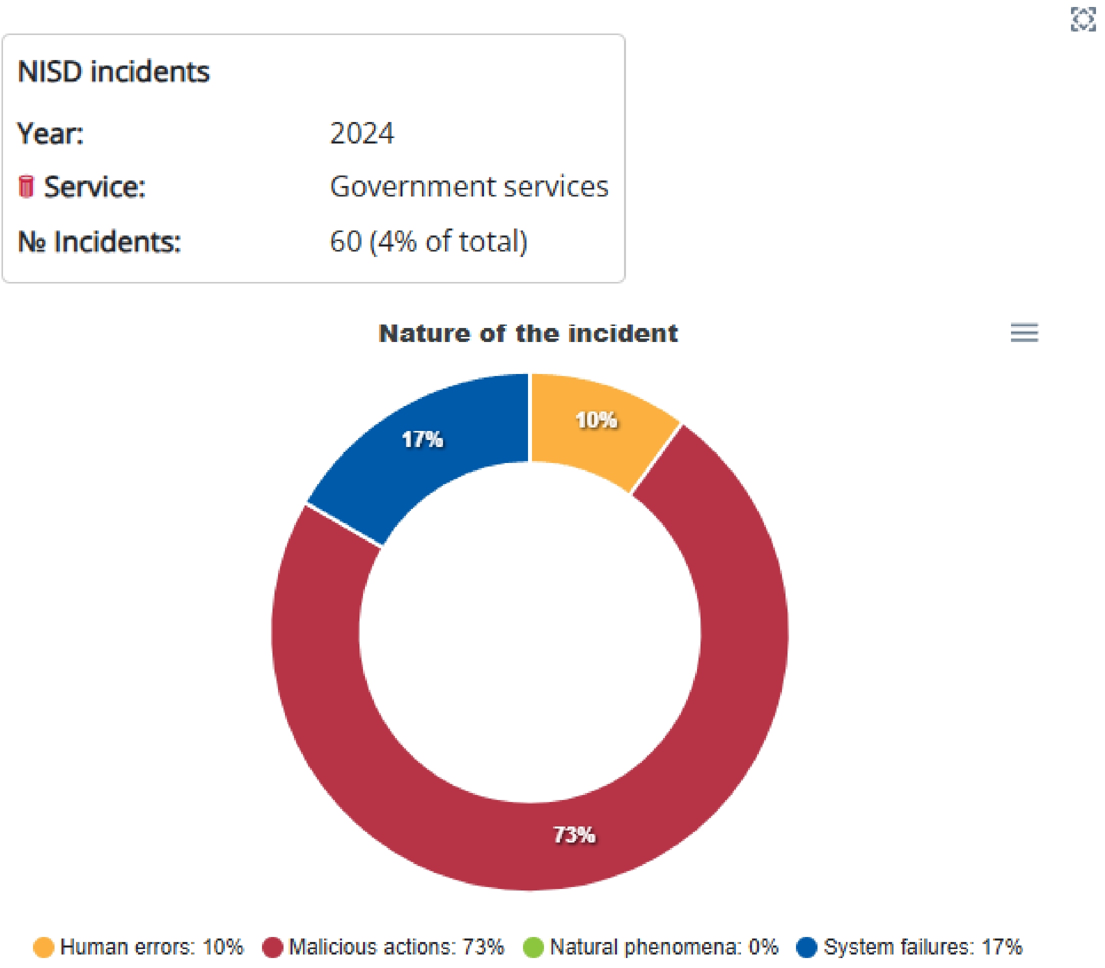
It is identified that DDoS attacks were the leading causes for user hours lost in banking.


User hours lost & number of incidents per technical cause
User hours
Number of incidents
40000000
35000000
30000000
25000000
20000000
15000000
10000000
5000000
0
30
25
20
15
10
5
0
24
6
10
3
20
3
2
DDoS attack
Other
Faulty software changes/update
Overload
Software bug
Policy/Procedure Flaw
Hardware failure
User hours
Total number of incidents


User Hours lost per nature of incident
40000000
35000000
30000000
25000000
20000000
15000000
10000000
5000000
0
Malicious actions
System failures
Human errors

5.6. Government services sector

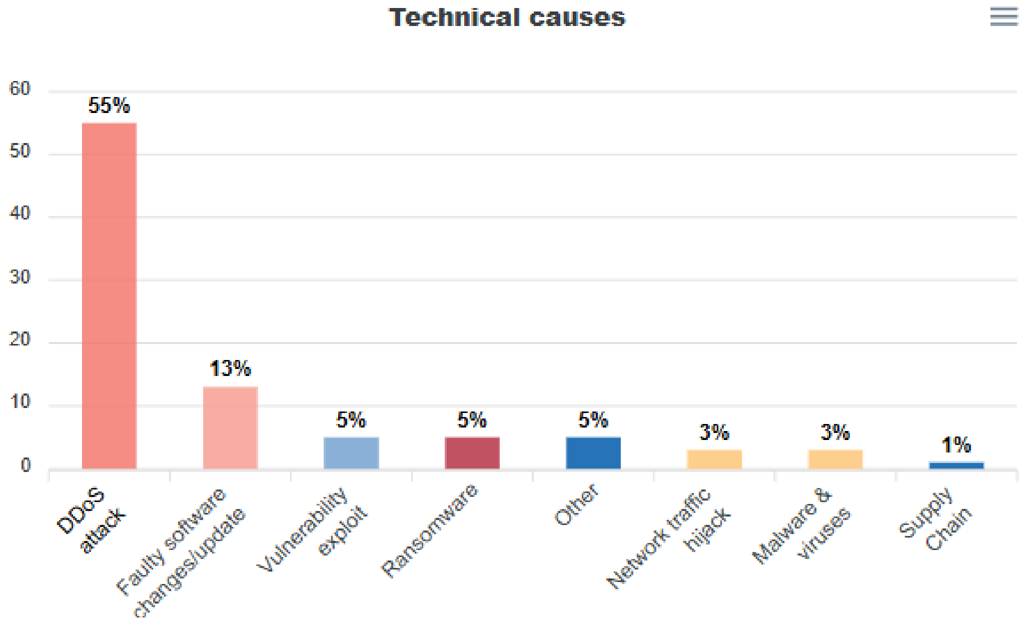
The sixth sector most impacted by incidents in 2024 was the government services sector. There was a total of 60 incident reports, for which the nature mainly related to malicious actions.



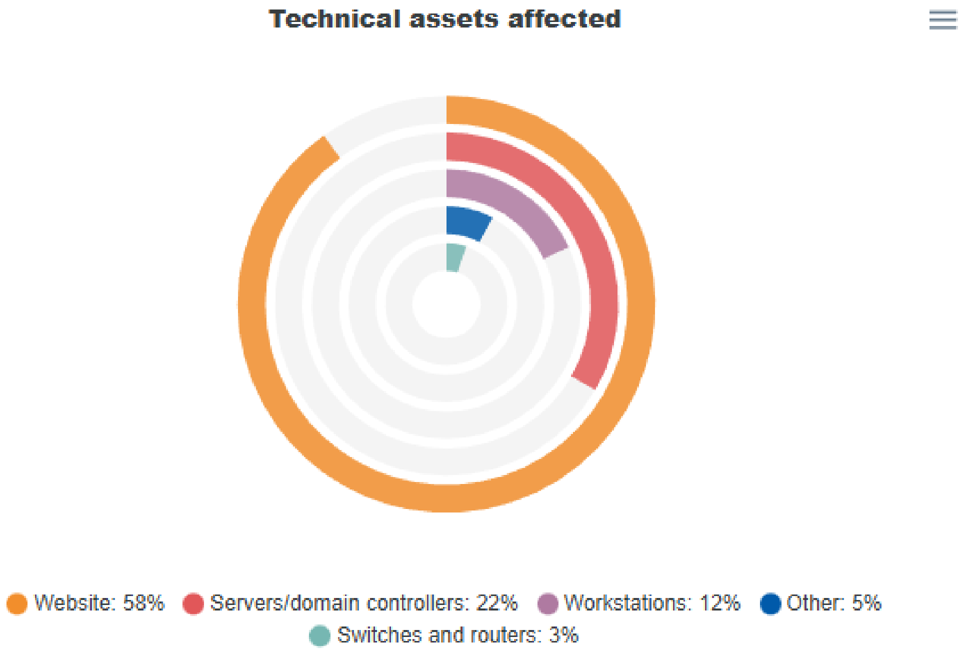
NISD incidents

Year:	2024
Service:	Government services
№ Incidents:	60 (4% of total)

The underlying technical causes for these incidents mainly related to DDoS attacks. However, in 10 % of cases technical cause is not known or not reported and in 5% of cases cause was reported as Other.

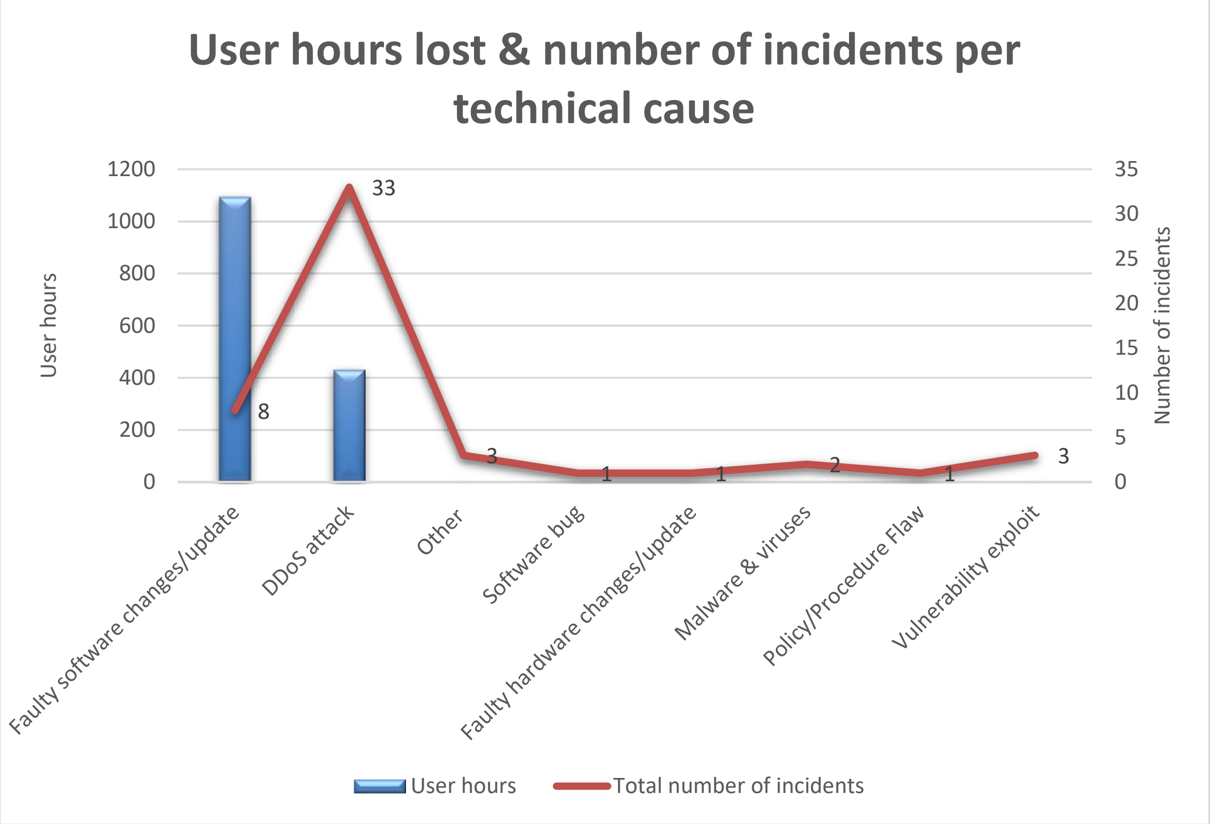


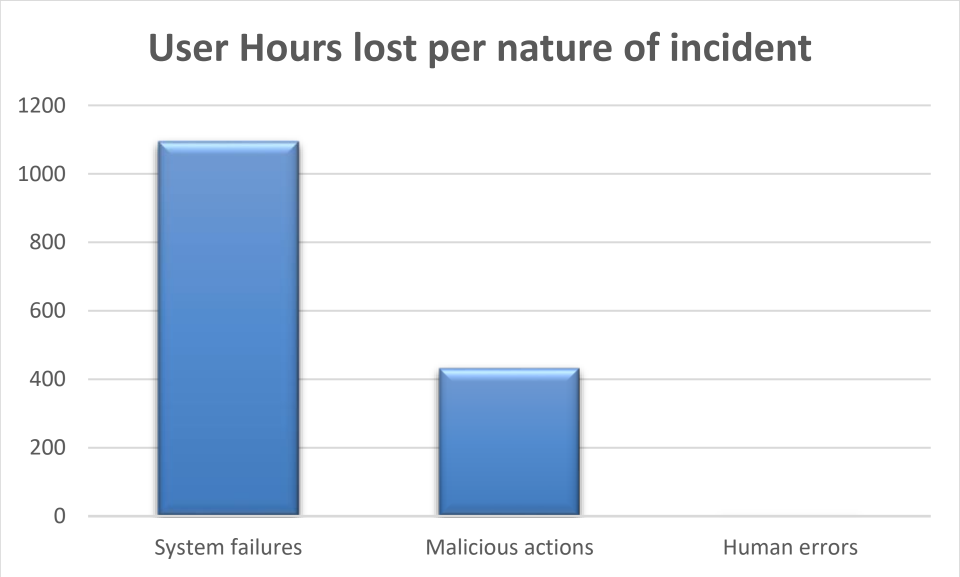
As per the incident reports for government services, the most affected technical assets were websites and servers/domain controllers.



For incidents that are outages lost user hours and causes are described below.

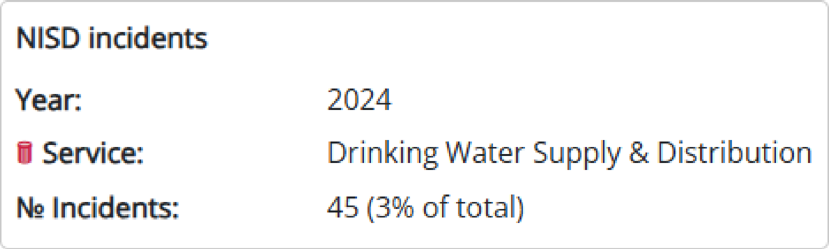
It is identified that faulty software update were the main cause for user hours lost in government services and that the leading nature for the reported incidents was system failures.





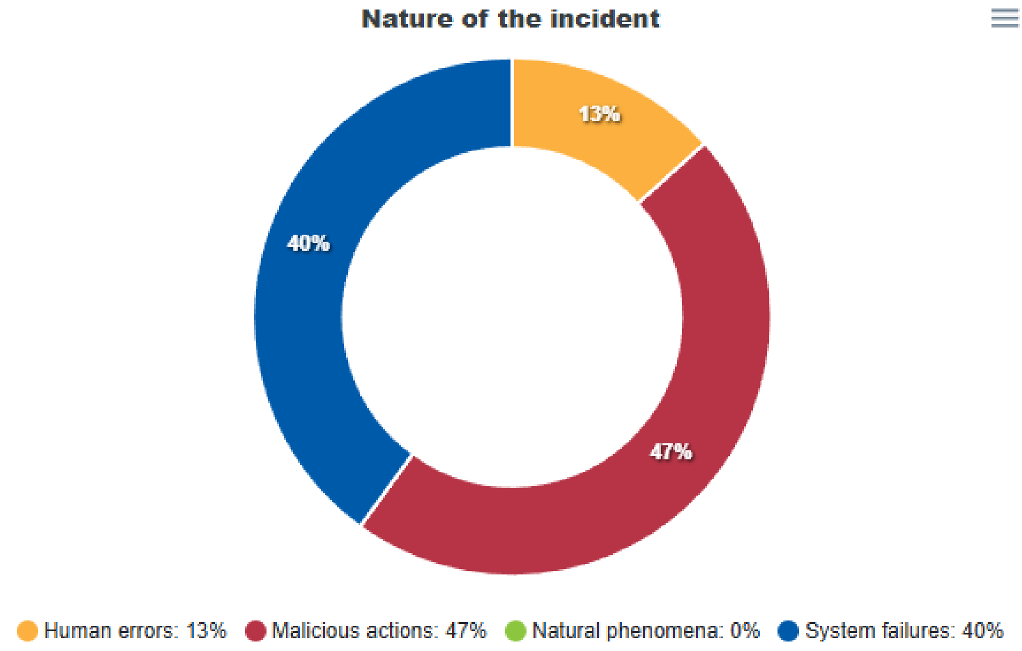
5.7. Drinking water supply and distribution sector

The seventh sector most impacted by incidents in 2024 was the drinking water supply and distribution sector. There was a total of 45 incident reports, for which the nature mainly related to malicious actions and system failures.

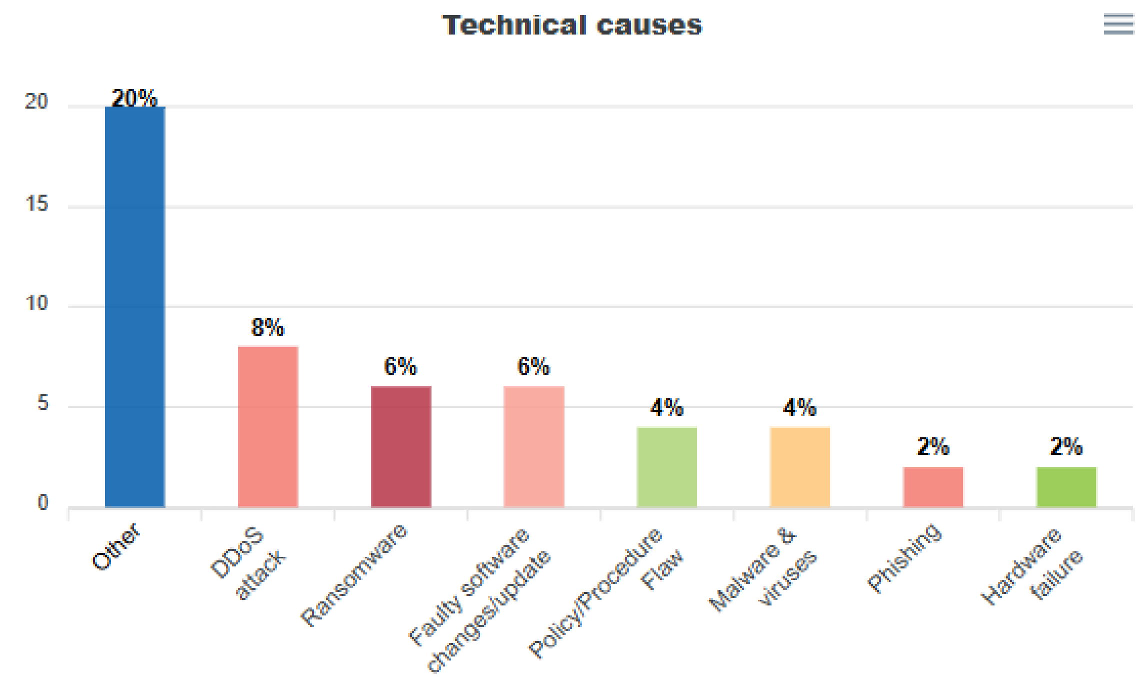


NISD incidents

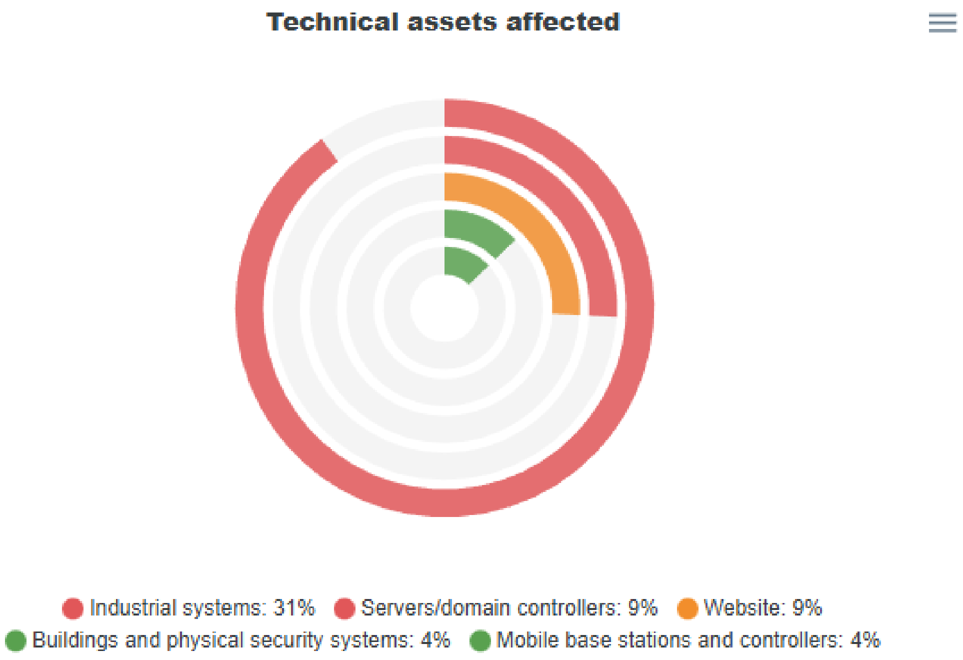
Year:	2024
Service:	Drinking Water Supply & Distribution
№ Incidents:	45 (3% of total)



The underlying technical causes for these incidents mainly related to system failures and malicious actions. In 48% of cases technical cause is not known or not reported and in 37% of cases it was defined as ‘other’.

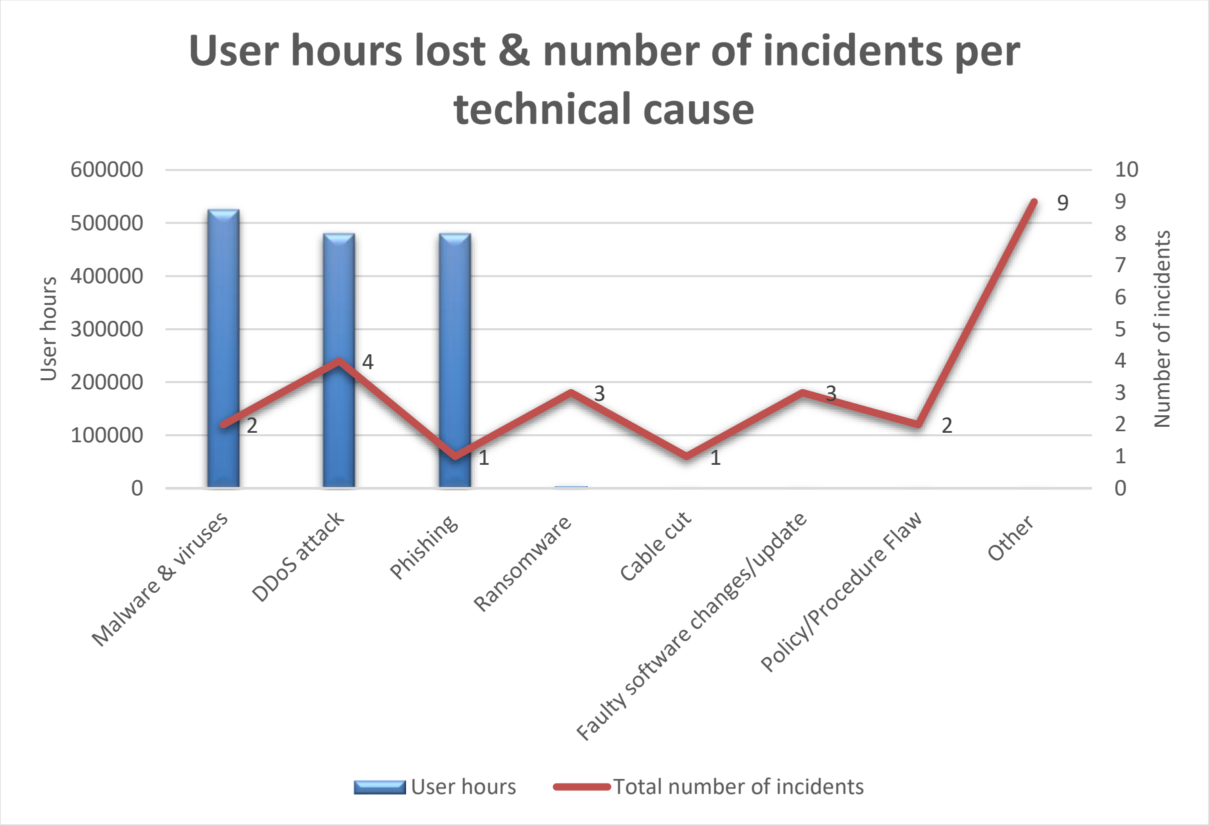


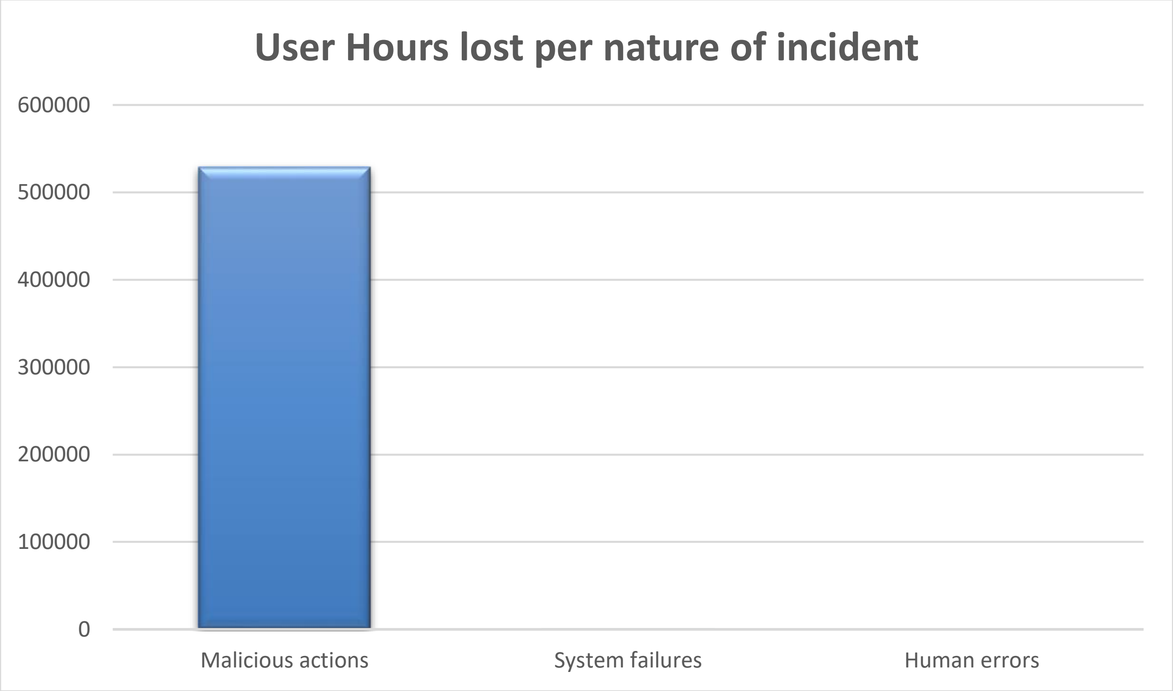
As per the incident reports for drinking water supply and distribution, the most affected technical assets were industrial systems and servers/domain controllers.



For incidents that are outages lost user hours and causes are described below.

It is identified that malware and DDoS attacks were the main causes for user hours lost in the sector and that the leading nature for the reported incidents was malicious actions.

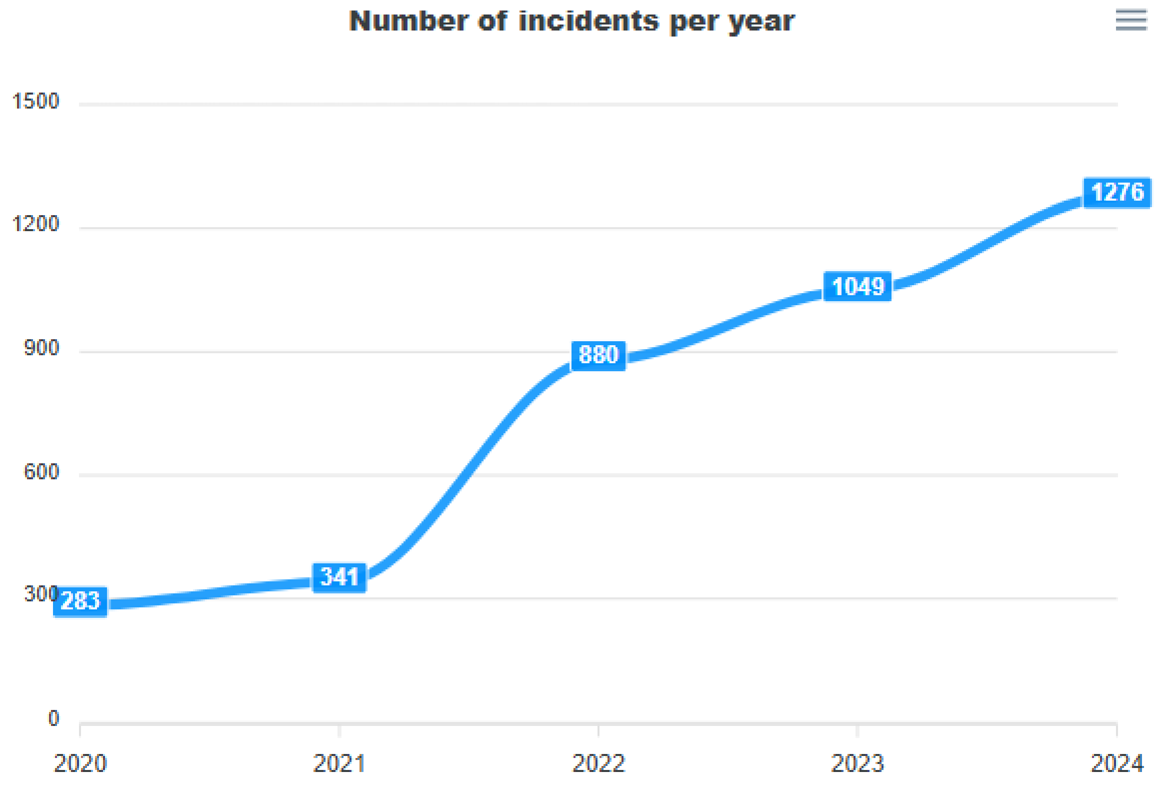




6. Multiannual trends

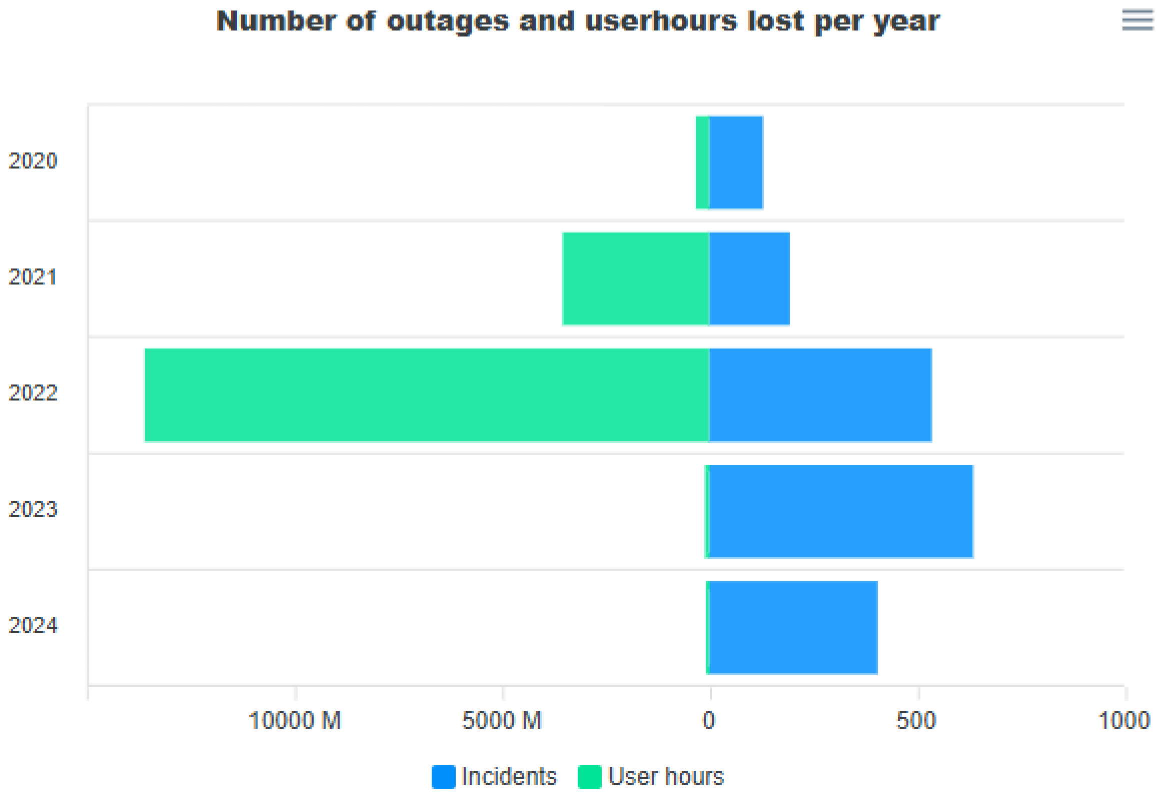
6.1. Summary

ENISA has been collecting and aggregating incident reports since 2020. In this section, multiannual trends from 2020 to 2024 are presented. This dataset contains **3829** reported incidents in total, see in figure below



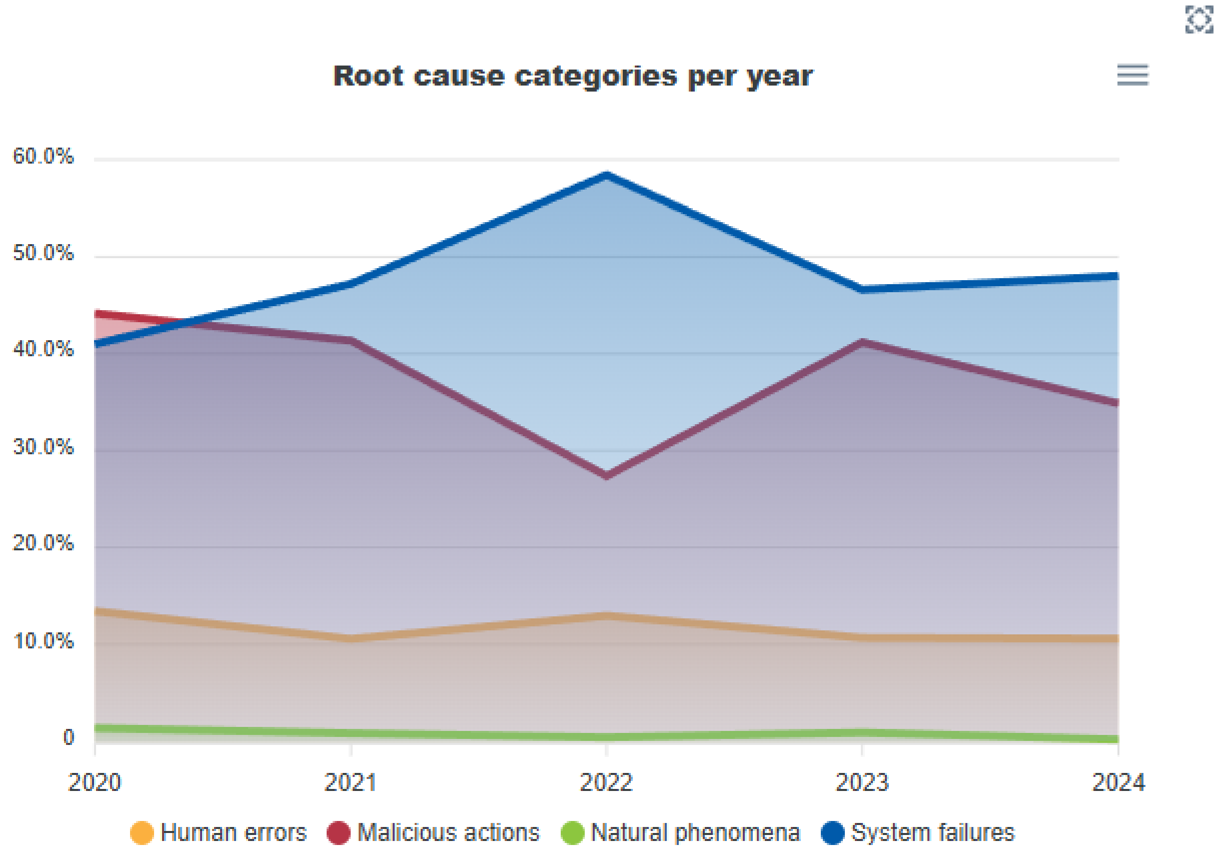
Over the course of the previous 5 years, the number of reported incidents with outages has been steadily increasing with drop in 2024. The numbers of user hours lost has decreased.

The peak of incidents in 2021 and 2022 are due to the new type of area covered in incident reporting.



6.2. Root cause multiannual trends

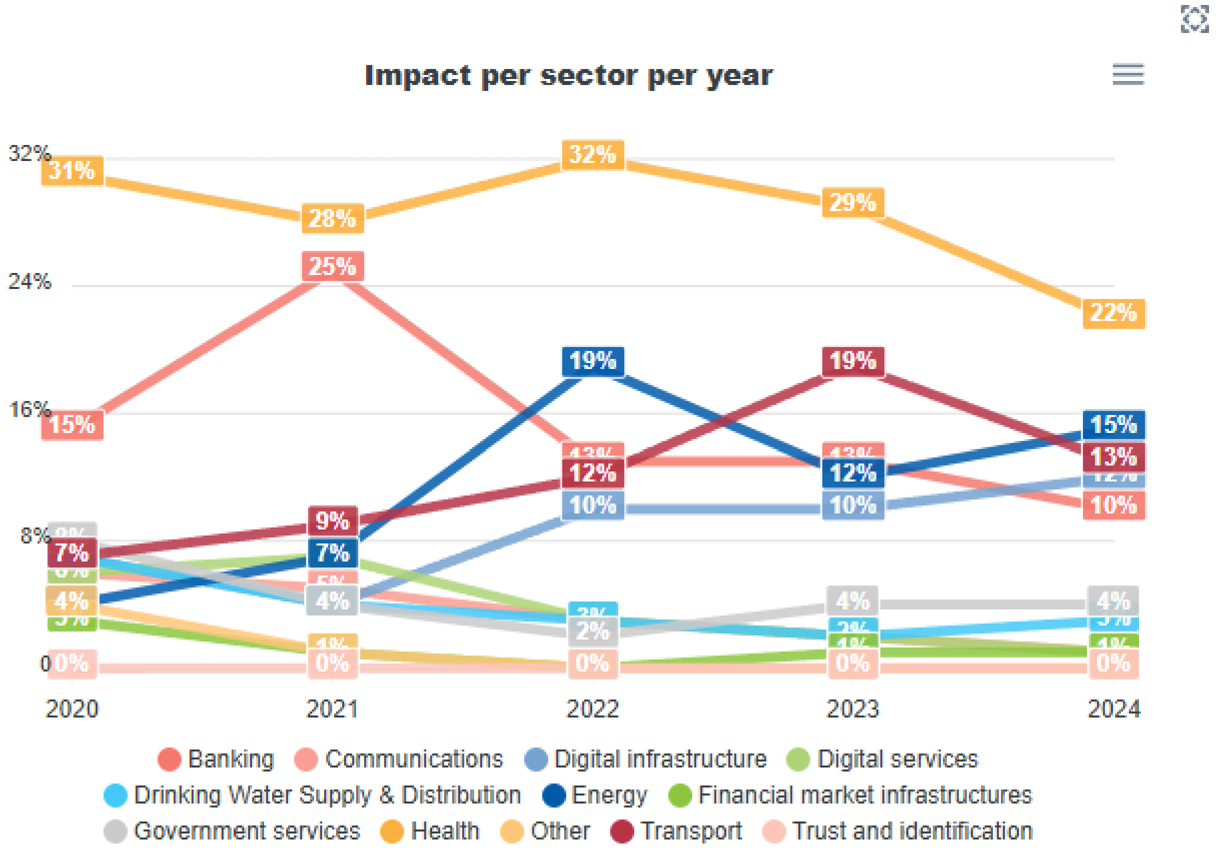
Human errors remain at the 10% mark, while malicious actions mark a small decrease over the previous one year and system failures have a small rise compared to 2023.



Overall system failures and malicious actions still remain most common root causes from 2020 to 2024, with human errors coming third.

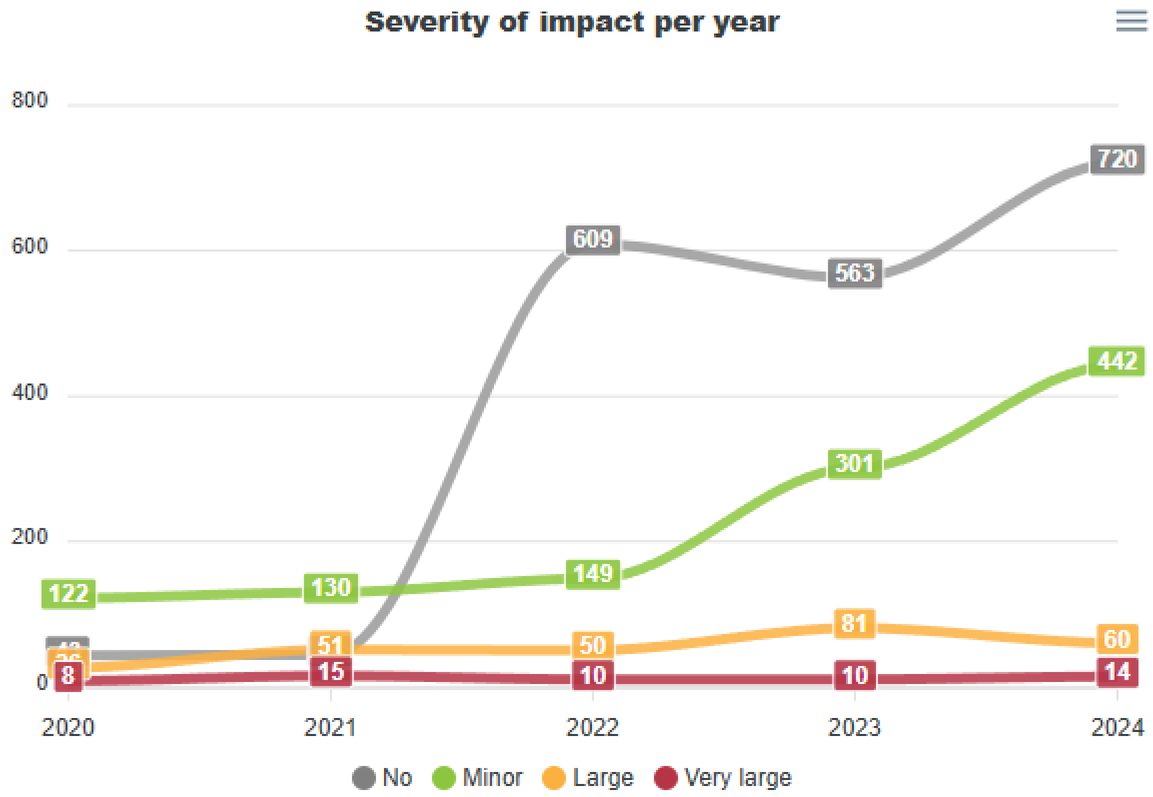
6.3. Service impact multiannual trends

Over the period, Health Transport, Banking and Government services were the most impacted by incidents.


Impact per sector per year
32%
24%
16%
8%
0
2020
2021
2022
2023
2024
31%
28%
32%
29%
22%
25%
15%
19%
19%
15%
13%
12%
12%
10%
10%
10%
9%
7%
7%
4%
4%
2%
4%
4%
0%
0%
0%
0%
0%
Banking
Communications
Digital infrastructure
Digital services
Drinking Water Supply & Distribution
Energy
Financial market infrastructures
Government services
Health
Other
Transport
Trust and identification

6.4. Severity of impact of incidents - multiannual trends

Since 2020, an **increase** in reports of **large impact incidents** is observed with exceptional raise in 2023. **Very large impact incidents** had stayed for the same level through the years. **Minor incidents** show an increase for last 3 years.



7. Key takeaways

The key takeaways regarding the incidents reported for the year 2024 are as follows:

- **The number of reported incidents has increased in total.** In this round, covering the year 2024, Member States submitted 1276 cybersecurity incident reports, compared to 1077 for the previous year.
- **Number of Member States reporting incidents has decreased** most likely due to shorter timeline and preparations for NIS2 in 2024 reports from 3 Member States are missing compared to 1 missing in 2023.
- **Most incident reports regard the health, transport and energy sectors** – by comparison ENISA Threat landscape of 2024 shows among most targeted public administration, transport and finance sectors.
- **System failures are the still most frequent root cause of reported incidents.** The root cause for the majority of the incidents (51%) is defined as system failure.
- **Incidents with cross-border impact.** There were 2 incident reports with possible cross-border impact. Due to the limited information reported through CIRAS for the incidents with potential cross-border impact, it is not possible to do any relevant assessments.
- **The health sector is the most affected for the fifth year in a row (2020-2024).**
- **The detailed technical causes for a 12% of incidents were defined as 'other'**, which could be attributed to limitations of the current taxonomy and definitions. The majority of the incidents with 'other' impact are in the health, drinking water supply and distribution, and energy sectors.
- **Similarly, more detailed information about technical causes is not reported or not know for more than 2 thirds of the incidents.**
- **DDoS attacks were the leading cause for incidents which is consistent with observations of ENISA Threat Landscape 2024**, **and caused the most outages and the respective lost hours**.