ANACOM AUTORIDADE NACIONAL DE COMUNICAÇÕES

2021

SECURITY BREACHES OR LOSS OF INTEGRITY

ANNUAL REPORT

Contents

List of Charts

List of Tables

List of Figures

Executive summary

ANACOM's Security Regulation 303/2019 determines the rules to be followed by publicly available electronic communications companies when reporting security incidents with significant impact: events that make access to the electronic communications service impossible for a large number of customers simultaneously, and for a significant period of time.

In 2021, there was a significant reduction in the total number of security incidents reported to ANACOM by companies providing electronic communications networks and services: 38 security incidents, 41% less than the previous year and the lowest figure recorded since 2015.

The 1st and 2nd quarters, with 66% of incidents, were the most serious in terms of the number of reported incidents. The northern and central regions of Portugal had the most incidents in electronic communications networks and services.

Similar to recent years, 47% of the causes associated with the occurrence of security incidents in 2021 were due to failure in the supply of goods or services by third parties, that is, they resulted from events or issues outside the sector. For the entire period, from 2015 to 2021, incidents attributable to causes associated with factors external to the sector amounted to 75%.

During the year, three types of incident stood out: 20 incidents with a direct impact on customers, 9 incidents affecting the delivery of calls in the 112 service centres, and 6 incidents impacting the functioning of all networks and services offered by one company in the entire territory of an island in the Autonomous Region of the Azores or the Autonomous Region of Madeira.

Generally, most security incidents impact on more than one publicly available electronic communications service simultaneously. Fixed telephony was the most affected service, with 61% of total security incidents received; followed by mobile telephony, with 58%; and mobile Internet, with 39% of all security incidents.

In 2021, the 20 security incidents referred to above impacted around 145,000 subscribers/accesses, which is a decrease of around 92% compared to 2020.

"Accident or natural phenomenon (depression, thunderstorm)" and "maintenance or failure of hardware or software", accounting for 79% and 11% respectively, were the two causes with the highest occurrence of the mentioned 20 security incidents.

The total service downtime of the 20 security incidents in 2021 was 247 hours, 31% less than the previous year, with an average impact duration per incident of about 12 hours. This reduction follows the trend seen in the last five years and is significantly lower than the average of 51 hours recorded in 2017.

Of the 20 security incidents notified which fall within the levels, two were covered by the obligation of public disclosure by the companies MEO/ALTICE and IP TELECOM. This obligation applies whenever any security incident affects the operation of their networks and services falls into one of the four most significant severity levels.

ANACOM reported eight security incidents to the European Commission and the European Network and Information Security Agency (ENISA). European bodies are advised whenever any incident falls within the more demanding criteria for reporting at the European Union level.

There were no security incidents directly attributable to the occurrence of the pandemic in either 2020 or 2021.

1 Introduction

This report gathers, presents, and analyses the information contained in notifications of a security breach or loss of integrity with significant impact (hereinafter referred to as "security incident"). These data include *initial*, *end-of-significant impact* and *final* notifications sent to the Autoridade Nacional de Comunicações (ANACOM) in 2021 by companies offering public communications networks or publicly available electronic communications services. The constituent components and annual security reports received are also reflected, with a summary of developments since 2015.

Under the terms of Article 54-B of Law 5/2004 of 10 February 2004, in its current wording (hereinafter "Electronic Communications Law"), all companies providing public communications networks or publicly available electronic communications services (hereinafter "companies") are obliged to notify ANACOM of any security breach or loss of integrity with a significant impact on the operation of networks and services.

By decision dated 14 March 2019, ANACOM approved the Regulation on the security and integrity of ANACOM's electronic communications networks and services (hereinafter "Security Regulation 303/2019"), published on 1 April.

Nevertheless, since 2014, ANACOM has had a Notification Reporting Centre (CRN) for companies to notify security incidents. This information must be provided in real time and whenever a security breach or loss of integrity significantly affects the functioning of electronic communications networks and services. The commissioning of the CRN has enhanced the systematisation and publication of security data in the sector.

As in previous years, in 2021 ANACOM continued to submit to the European Commission and the European Network and Information Security Agency (ENISA) a summary report on communications of security breaches or losses of integrity, as well as the measures taken.[1]

The year 2021 was again an atypical and demanding year in terms of access to electronic communications because of the pandemic situation. However, the number of incidents that occurred and the average annual duration of service downtime reached the lowest values ever recorded, showing stability in terms of the security and integrity of electronic communications.

[1] In accordance with the ENISA *Technical Guideline on Incident Reporting Under The EECC, Version 2.2, March 2021,* available at https://www.enisa.europa.eu/publications/enisa-technical-guideline-on-incident-reporting-under-the-eecc

The actions implemented by the companies to improve their networks and services contributed a lot to this. Furthermore, there were no security incidents related to the pandemic, largely thanks to the companies adapting the networks to intense traffic scenarios (particularly during periods of mandatory teleworking).[2]

Section 2 analyses incidents in terms of their evolution over time, impact per root cause and impact per service. Section 3 describes the circumstances and respective impact, namely the levels and rules, format and procedures, together with the conditions, content, means, and deadlines for disclosing incidents to the public.

[2] ANACOM recently assessed the impact on the use of communications services in 2021. The respective link can be found at https://www.anacom.pt/render.jsp?contentId=1719175.

2 Security incidents in 2021

With regard to the identification of security incidents and pursuant to Article 21(1) - Circumstances of Security Regulation 303/2019, any breach of security or loss of integrity that causes a serious disturbance to the operation of networks and services, with a significant impact on the continuity of such operation, according to the circumstances and rules provided for in (2) of the same Article, must be subject to notification. This means that not all episodes of degradation or breakdown of service are reported, only those that reach certain levels and special reference cases are reported. Therefore, the situational picture that emerges with this report is necessarily an approximate and partial representation, but absolutely fundamental and current to understanding the nexus of soundness and strength of the Portuguese electronic communications system.

The main highlights and trends for the 2015-2021 period are listed next. In this section, the focus is on the number and variety of events that occurred. Thus, the course of the number of incidents is recorded, and the intra-annual pattern and causality profile are characterised, and finally the effects they had on services are noted.

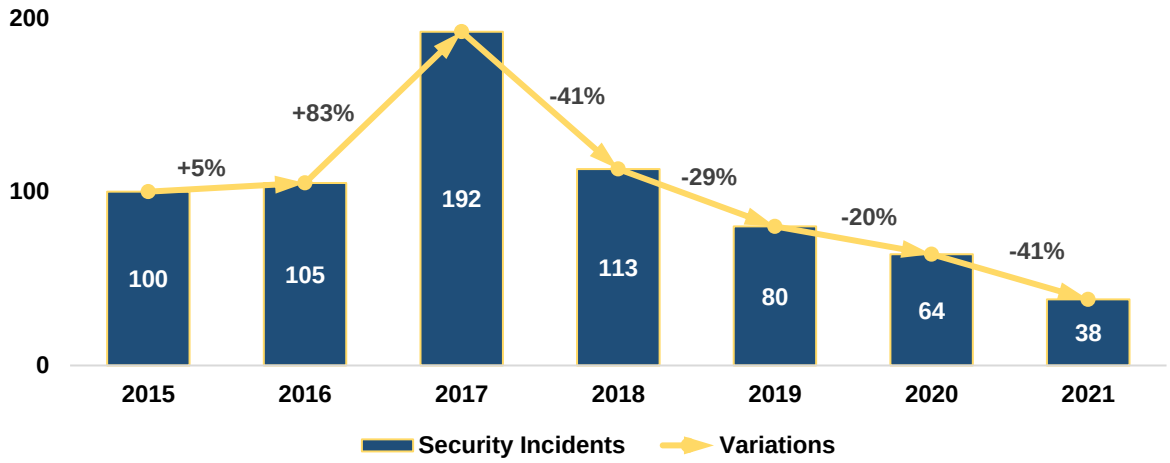
2.1 Number of security incidents notified

In 2021, the group of companies together reported an absolute total of 38 security incidents to ANACOM.

This was the lowest number of occurrences since 2015. During the 2015-2021 period, companies reported a total of 692 security incidents (annual average of 99 occurrences).

Chart 1 shows that the initial upward trend in the annual number of security incidents reported was reversed, with a peak value in 2017 (linked to the wave of serious forest fires that year) followed by a sharp drop in the following four years.

Chart 1 - Number and annual change of security incidents notified, 2015-2021.

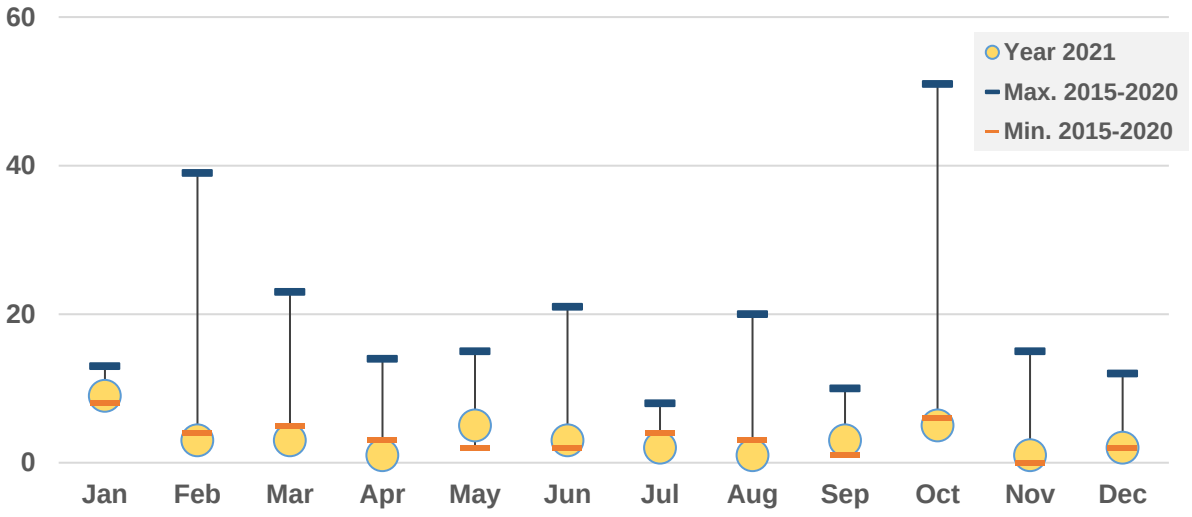


Unit: Number of security incidents

Source: ANACOM

Chart 2 shows the monthly trend of the number of incidents received during 2021 compared to the maximums and minimums obtained during the 2015-2020 period.

Chart 2 - Monthly figures for security incidents reported in 2021, compared with the period of 2015-2020.



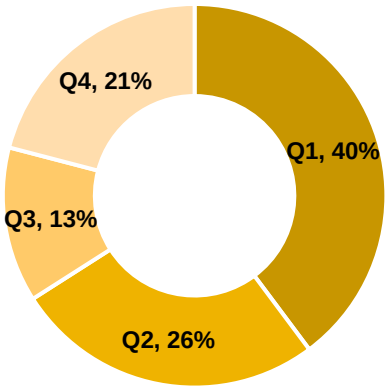
Unit: Number of security incidents

Source: ANACOM

Thus, in 2021, a maximum occurred in January, with nine incidents, with a low figure of one incident in April, July, August and November. In the last seven years the highest figures for security incidents notified occurred in 2017, with 39 in February and 51 in October.

The analysis of Chart 3 shows that in 2021, the 1st and 2nd quarters (Q1 and Q2) were the most serious in terms of the number of incidents received.

Chart 3 - Percentage of security incidents received in 2021, by quarter.



Unit: % of security incidents

Source: ANACOM

2.2 Root cause

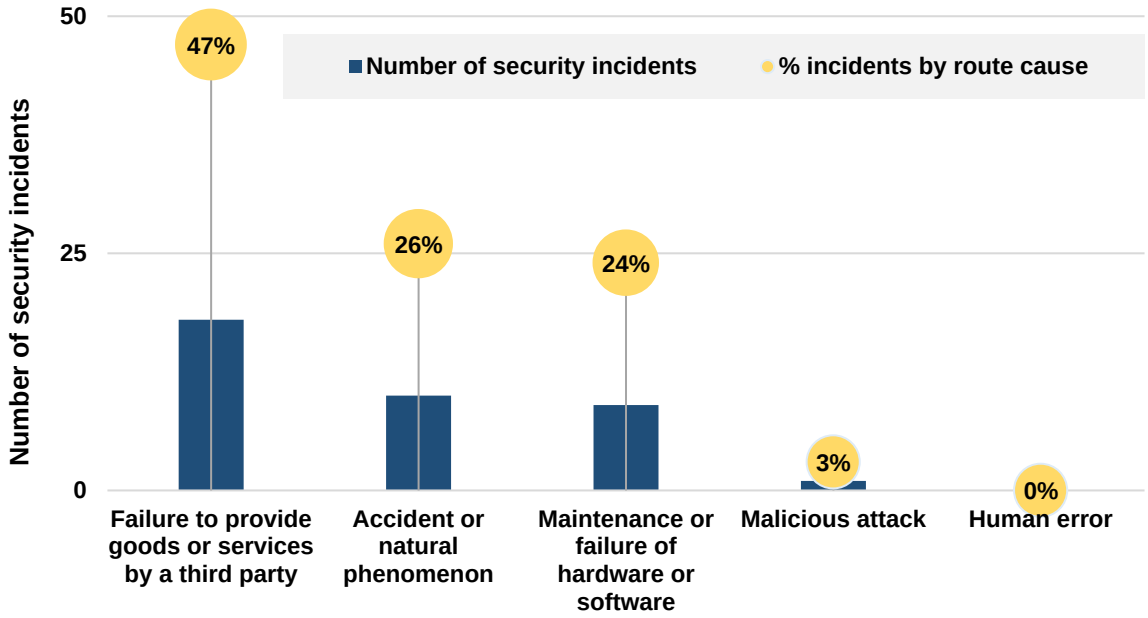
According to Article 22(11) – Format and Procedures of Security Regulation 303/2019, security incidents can have the following categories of root cause:

- **Accident or natural phenomenon** - due to severe weather conditions, earthquakes, floods, pandemics, forest fires, wildlife, etc;
- **Human error** - due to errors made by employees of the company providing the service or its suppliers during the operation of equipment or facilities, the use of tools, the execution of procedures, etc;
- **Malicious attack** - due to the deliberate act of a person or an organisation
- **Maintenance or failure of hardware or software** - due to technical system failure in the hardware and/or software components;

- **Failure to provide goods or services by a third party** - due to a breakdown in the provision of a good or service, such as power supply or leased circuits, or any other good or service supplied by a third party.

As shown in Chart 4, the failure to provide goods or services by third parties was the major root cause in 2021, generally involving the failure to supply electricity or leased lines.

Chart 4 - Security incidents received for different root cause categories, 2021.



Unit: Number of security incidents and percentage of total incidents (%)

Source: ANACOM

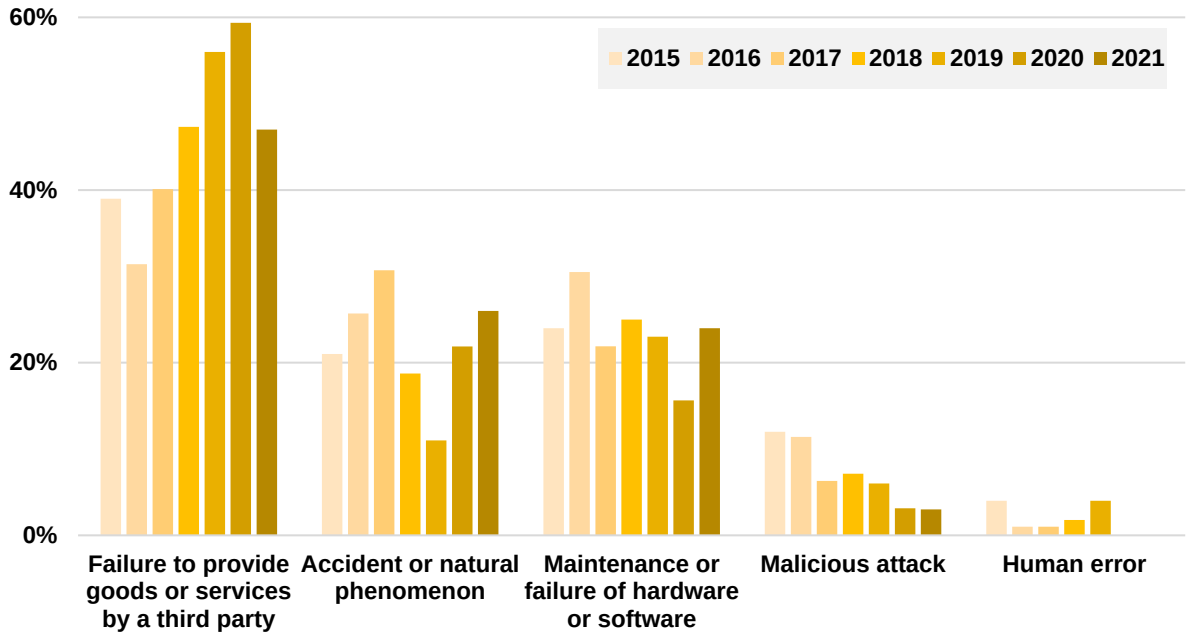
The root causes of *accidents or natural phenomena* and *maintenance or failure of hardware or software*, in second and third place respectively this year, represent half of the total number of security incidents reported, in particular due to causes associated with severe weather conditions and technical malfunctions of systems/equipment.

Chart 5 shows the change or stability in the relative importance of the various root causes. They include:

- the relative decrease in 2021 of incidents associated with *failure to provide goods or services by a third party*;

- the fluctuation, i.e., an undetermined tendency, of the reasons for an *accident or natural phenomenon*;
- the relative increase in the number of incidents originating from problems related to *maintenance or failure of hardware or software*;
- the downward trend in the number of incidents due to *malicious attacks* (the only root cause with a deliberate or intentional character) as well as the residual expression of *human error* (incidentally zero in 2021).

Chart 5 - Percentage of security incidents reported for each root cause, 2015-2021.

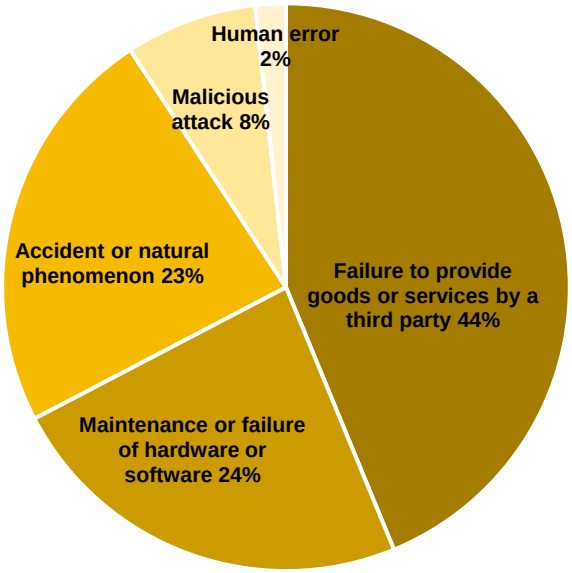


Unit: % of security incidents

Source: ANACOM

In cumulative terms, for the 692 incidents confirmed in the 2015-2021 period, the distribution of their underlying causes is shown in Chart 6, where *failure to provide goods or services by a third party* is prominent.

Chart 6 - Distribution of security incidents reported (692 in total) for each root cause, 2015-2021.

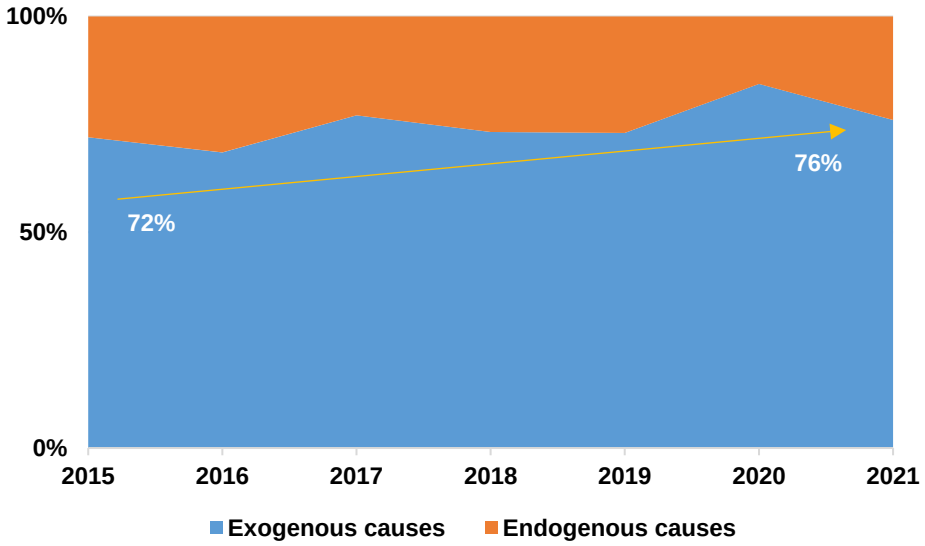


Unit: % of security incidents

Source: ANACOM

For analysis purposes, it is also possible, for the 2015 to 2021 period, to carry out a breakdown between *exogenous causes*, i.e., derived from outside the companies and the from sector as a whole (i.e.: *Failure to provide goods or services by a third party, accident or natural phenomenon, malicious attack*), and *endogenous causes,* that is, emerging from within the companies (i.e.: *maintenance or failure of hardware or software, human error*). For the whole period, the exogenous component represents 75% of the causal structure, with the endogenous component corresponding to 25%. Chart 7 reveals the annual progress of this splitting up of root causes, and a slight trend towards an increase of the exogenous component can be seen (the minimum was recorded in 2016 with 69% and the maximum in 2020 with 84%).

Chart 7 - Distribution of root causes by causes external and internal to the sector, 2015-2021.



Unit: % of security incidents

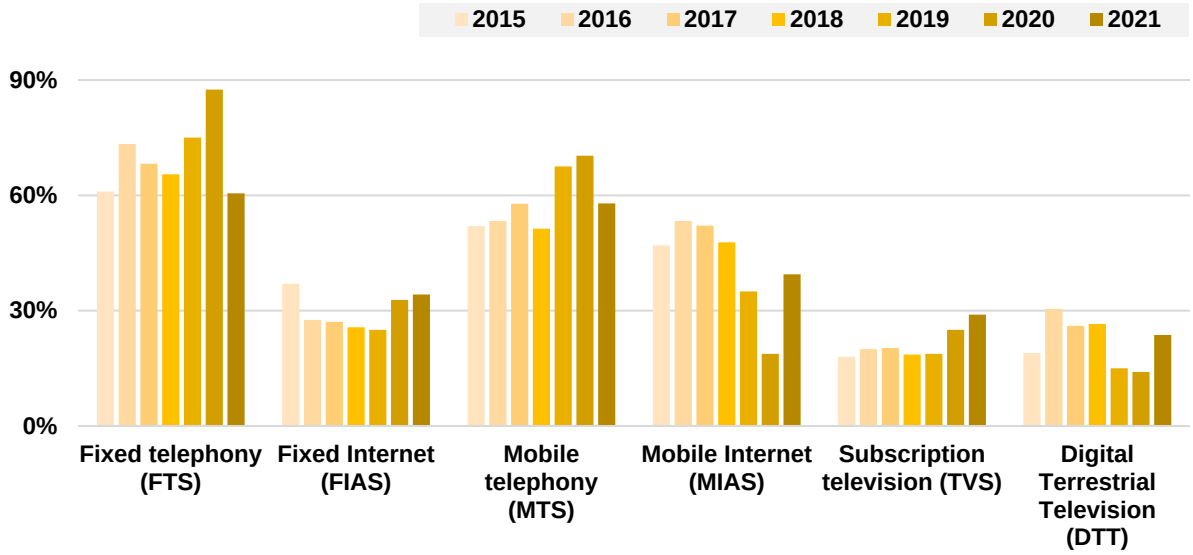
Source: ANACOM

2.3 Impact on service

Regarding the impact on electronic communications services, incidents can affect one or more services: fixed or mobile telephony (FTS and MTS), fixed or mobile Internet (FIAS and MIAS), pay television (TVS) or digital terrestrial television (DTT).

Chart 8 details the security incidents reported per service affected during the last seven years. According to the information received, fixed telephony and mobile telephony were the services most affected in this period. In particular, the fixed telephony service was the service most often affected during this period, with figures above 60% in all years. In 2021, 61% of the security incidents reported affected fixed telephony.

Chart 8 - Percentage of security incidents reported for each type of service, 2015-2021.



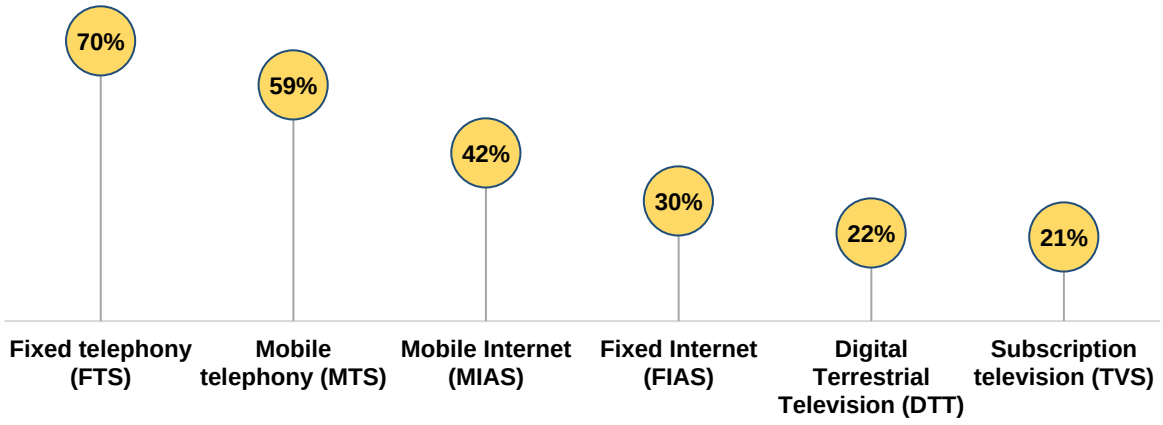
Unit: % of security incidents

Source: ANACOM

Note: Most security incidents affect more than one service (which is why the percentages in the chart add up to more than 100%).

During these seven years it was found that the three services most affected were, in descending order (Chart 9): fixed telephony (70%), mobile telephony (59%), and mobile Internet (42%).

Chart 9 - Distribution of security incidents reported for each type of service affected, 2015-2021.



Unit: % of security incidents

Source: ANACOM

3 Analysis of incidents in 2021

Those circumstances which exceeded the levels of significant impact established in Article 21 of ANACOM Security Regulation 303/2019, thus giving rise to the security incidents notified and seriously disturbing the operation of networks and services, were as follows:

a) number of subscribers/accesses affected and respective duration of significant impact, a criterion that is divided into 6 levels (**Subscribers/Accesses - Levels**);

b) direct or indirect effect on the delivery to Public Safety Answering Points (112 Service Centres) of 112 calls for a period of 15 minutes or more (**112**);

c) effect on the operation of all networks and services offered by a company in the entire territory of an island of the Autonomous Region of the Azores or the Autonomous Region of Madeira, lasting 30 minutes or more (**Islands**[3]);

d) other circumstances set out in Article 21 (**Other**):

   i. effect occurring on a date when the normal and continuous functioning of networks and services is particularly relevant (i.e., national election day - parliamentary, presidential, European or local elections);

   ii. cumulative impact of their occurrence over a four-week period.

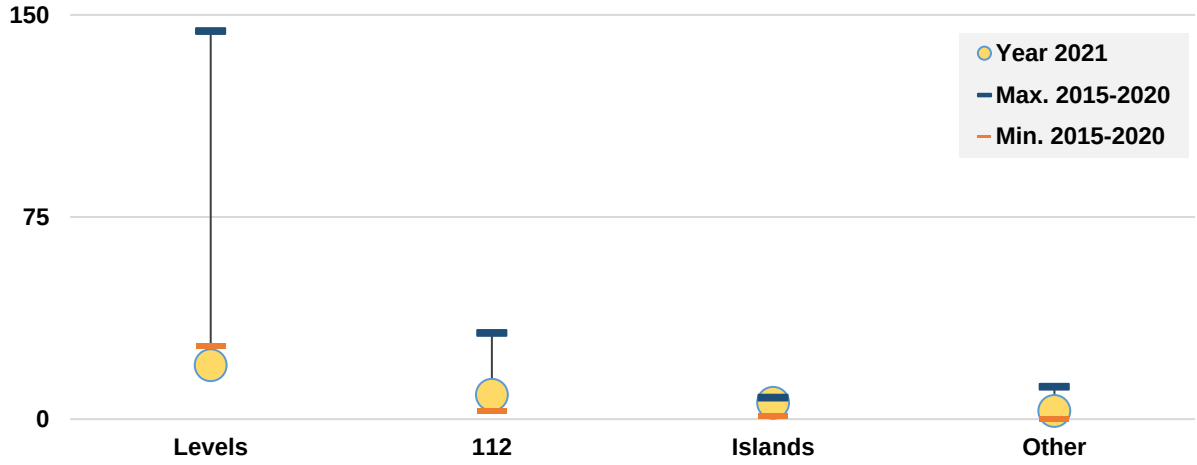
In 2021 we highlight the occurrence of security incidents with a direct impact on the services provided to customers, subparagraph (a), those related to the delivery of calls to 112 Service Centres, subparagraph (b), and incidents affecting the entire territory of one island (isolated island), subparagraph (c).

3.1 Distribution of reported incidents

Chart 10 distributes the reported incidents, comparing figures with the maximum and minimum in the period 2015-2020.

[3] The circumstance of “Islands” does not include 112 incidents, and corresponds to the classification of incidents involving the failure of all networks and services offered by a company in part of an island’s territory.

Chart 10 - Security incidents reported in 2021 per circumstance, compared to the period 2015-2020.



Unit: Number of security incidents

Source: ANACOM

Of the 38 incidents in 2021, the number of subscribers/accesses affected and respective duration of significant impact ("Levels") recorded 20 incidents, corresponding to 53%, while the circumstance relating to the impact on the delivery to the PSAPs (112 Service Centres) recorded nine incidents, or 24%.

3.2 Subscribers or accesses affected (Levels)

Table 1 shows the circumstance that combines the number of affected subscribers or accesses with the duration of the significant impact. This criterion is divided into six levels (I to VI), where level I corresponds to the highest number of affected subscribers/accesses and level VI to the lowest.

Each level is defined by a specific minimum impact duration and by an interval between the minimum and maximum number of subscribers or accesses affected.

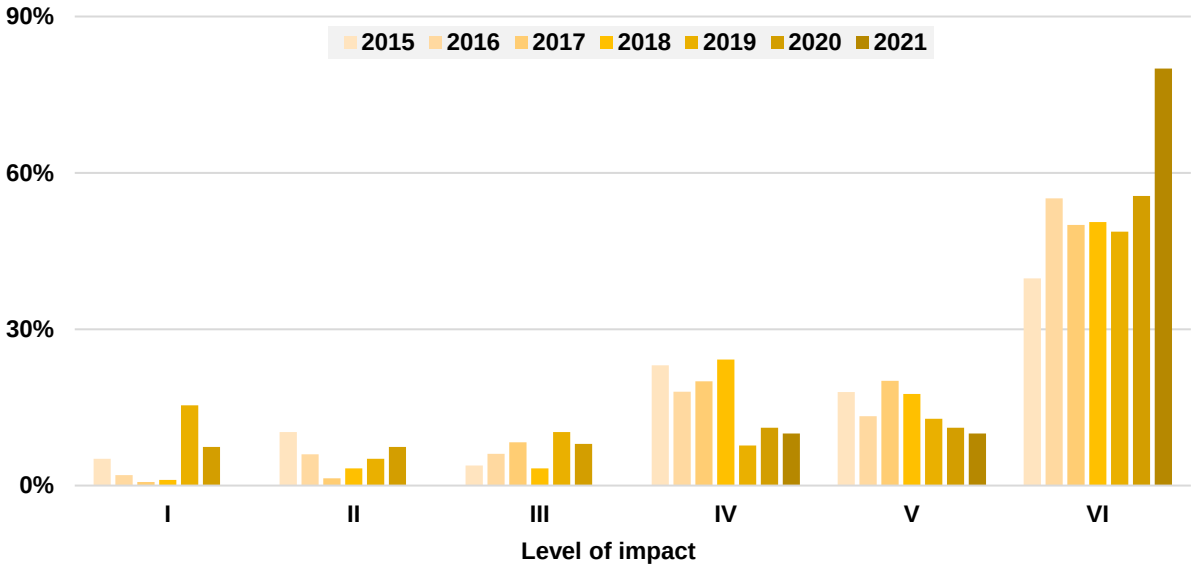
Chart 11 shows the number of security incidents reported, relative to the 2015-2021 period, distributed by each of the aforementioned levels.

Table 1 - Impact levels on subscribers/accesses.

Duration, and	Number of subscribers or accesses affected (or, pursuant to (3)(e) of this Article, geographical area affected)	Plateau
≥ 30 minutes	no. of subscribers or accesses affected ≥ 500 000 (or, in accordance with paragraph I.4(e), affected geographical area ≥ 3000 km$^{2)}$	I
≥ 1 hour	500 000 > no. of subscribers or accesses affected ≥ 100 000 (or, in accordance with paragraph I.4(e), 3000 km^2 > affected geographical area ≥ 2000 km^2)	II
≥ 2 hours	100 000 > no. of subscribers or accesses affected ≥ 30 000 (or, in accordance with paragraph I.4(e), 2000 km^2 > affected geographical area ≥ 1500 km^2)	III
≥ 4 hours	30 000 > no. of subscribers or accesses affected ≥ 10 000 (or, in accordance with paragraph I.4(e), 1500 km^2 > affected geographical area ≥ 1000 km^2)	IV
≥ 6 hours	10 000 > no. of subscribers or accesses affected ≥ 5000 (or, in accordance with paragraph I.4(e), 1000 km^2 > affected geographical area ≥ 500 km^2)	V
≥ 8 hours	5000 > no. of subscribers or accesses affected ≥ 1000 (or, in accordance with paragraph I.4(e), 500 km^2 > affected geographical area ≥ 100 km^2)	VI

Source: ANACOM, Security Regulation 303/2019

Chart 11 - Security incidents notified for each level of impact subscribers/accesses, proportion, 2015-2021



Unit: % of security incidents

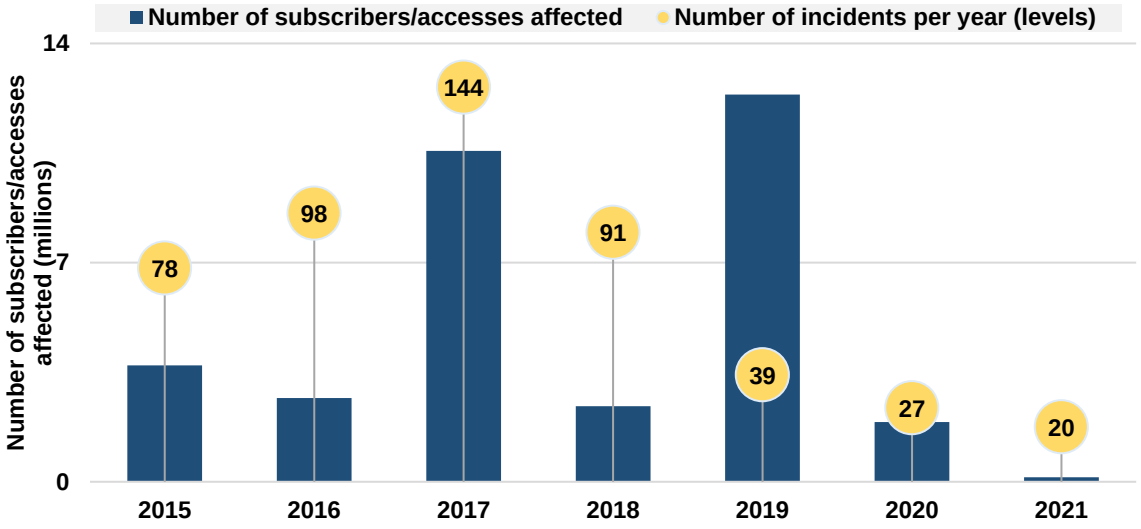
Source: ANACOM

In 2021, the level of the number of subscribers/accesses affected, corresponding to the lowest level of severity (level VI), was the most common among the security incidents reported, with 16 incidents being recorded.

Note the relative weight of the number of incidents associated with the lower levels IV, V and VI, which had an annual average of 85% in the period of 2015-2020.

Chart 12 shows the number of security incidents due to the circumstance of the number of subscribers/accesses affected and the annual value of the total number of subscribers/accesses affected in 2015-2021.

Chart 12 - Security incidents notified due to the circumstance of the number of subscribers/accesses affected



Unit: number of subscribers/accesses affected (millions) and annual number of incidents (levels)

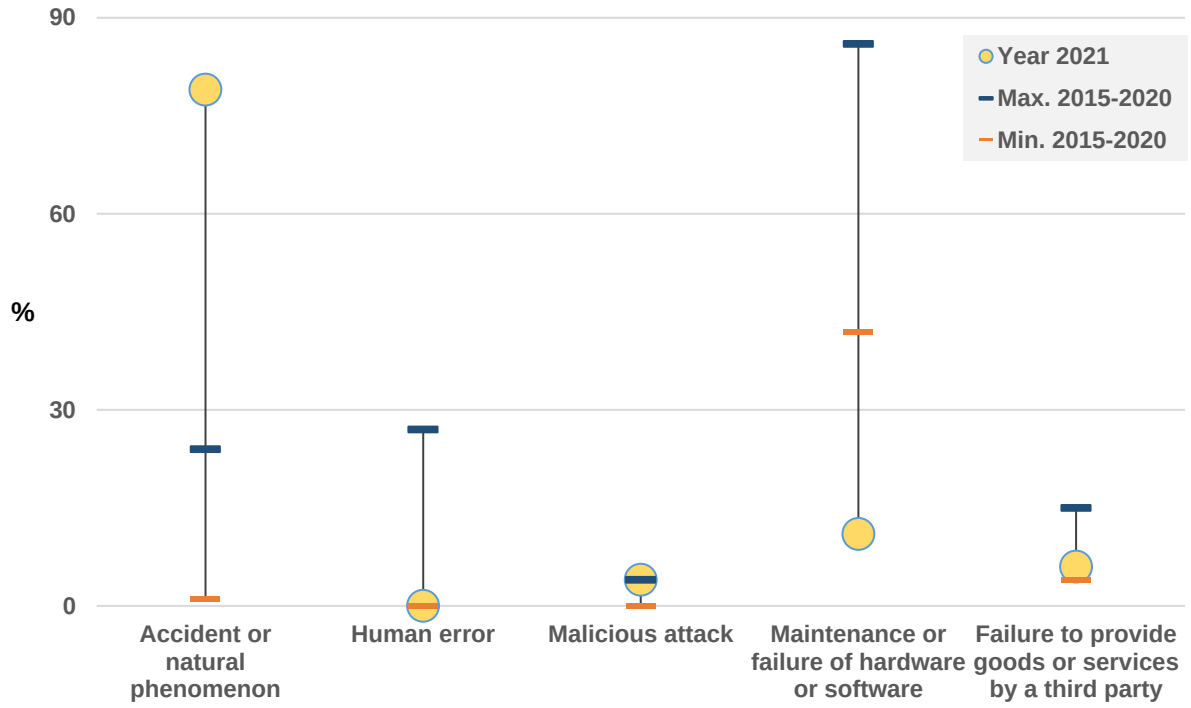
Source: ANACOM

Comparing 2021 with the previous year, the total number of security incidents due to the number of subscribers/accesses affected (levels) fell from 27 to 20 (a decrease of about 26%). Simultaneously, the total number of subscribers/accesses affected fell from about 2 million to a figure close to 145 thousand (a decrease of about 92%).

Chart 13 shows the root causes that were at the origin of the number of subscribers/accesses affected, comparing the maximum and minimum values for the 2015-2020 period. The root cause accident or natural phenomenon stands out in the chart, since it was the origin of incidents impacting 79% of the total number of subscribers/accesses affected in 2021,

corresponding to about 114 thousand, compared with about 280 thousand (15%) in 2020. There were around 16.5 thousand (11%) security incidents caused by root cause maintenance or failure of hardware or software in 2021, when in 2020 the figure was about 1.5 million (76%).

Chart 13 - Percentage of the number of subscribers/accesses affected by root cause in 2021, compared to 2015-2020.

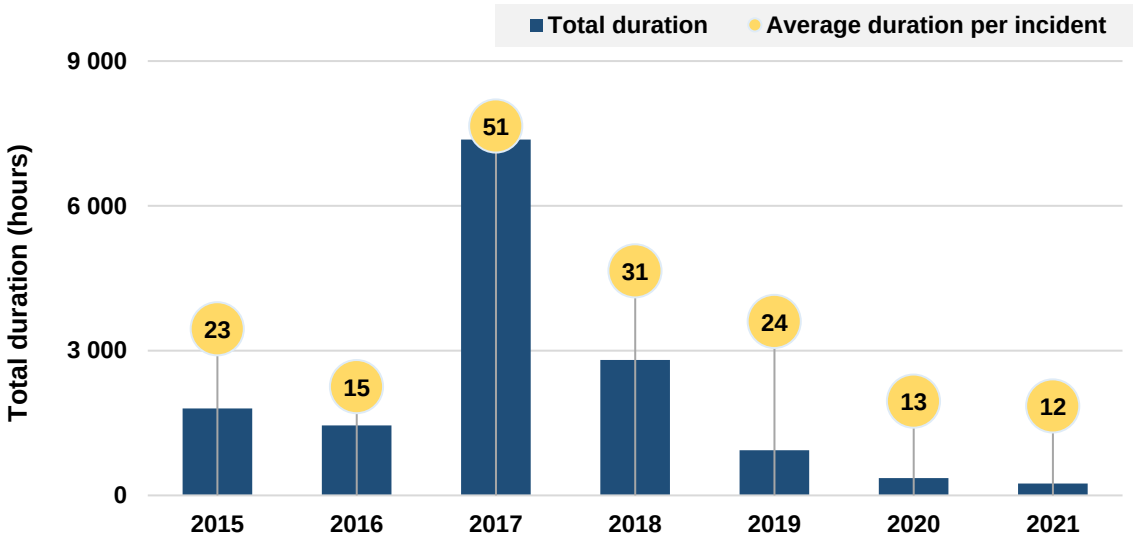


Unit: number of security incidents and number of subscribers/accesses

Source: ANACOM

In addition to the total number of subscribers/accesses affected in each year, it is also important to analyse the cumulative annual duration of the impact caused by the security incidents that occurred in that year (annual duration of impact) and the average duration of impact of the security incidents in that year (average annual duration of impact). This last value gives an approximate idea of the recovery time for security incidents. Chart 14 shows the figures for these seven years.

Chart 14 - Annual impact duration and average annual impact duration, 2015-2021.



Unit: Hours

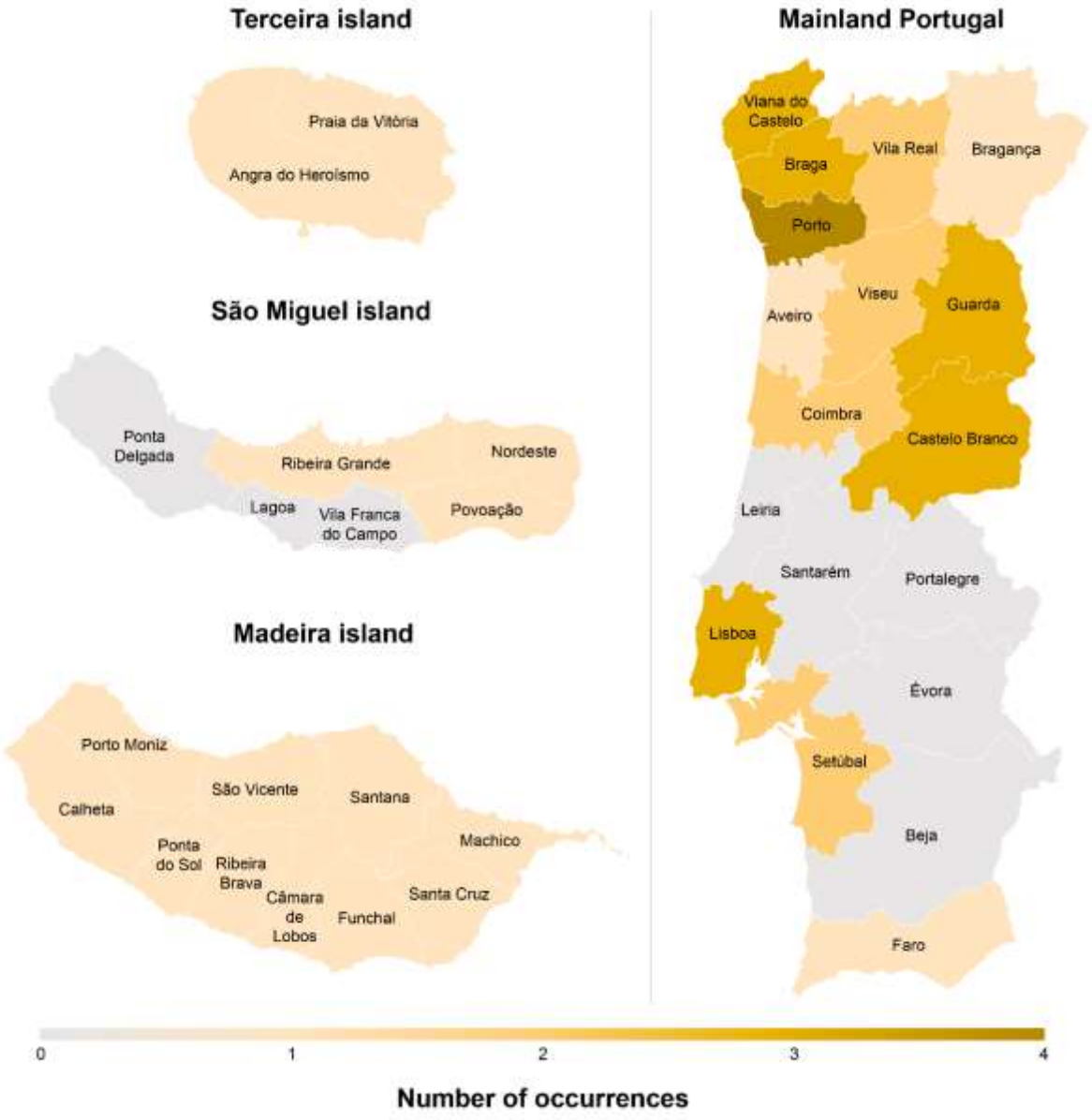
Source: ANACOM

In 2021 the total impact duration was 247 hours, while in 2020 this figure was 360 hours, which corresponded to a 31% reduction. Similarly, in 2017 and 2018 there were long-lasting security incidents resulting in the high annual impact duration recorded for those years, a situation that has no longer occurred in recent years.

With regard to the average duration of impact per incident, 2021 showed a reduction of 8% compared to 2020, from 13 to around 12 hours.

Two of the 20 security incidents had nationwide coverage, while the others had a significant impact on the networks and services in the districts of mainland Portugal and municipalities in the Autonomous Region of the Azores and the Autonomous Region of Madeira, shown in Figure 1.

Figure 1 - Identification of districts in mainland Portugal and municipalities of the Autonomous Region of the Azores and the Autonomous Region of Madeira affected by incidents with non-nationwide coverage notified in 2021.



Source: ANACOM

3.3 Calls to 112 emergency number

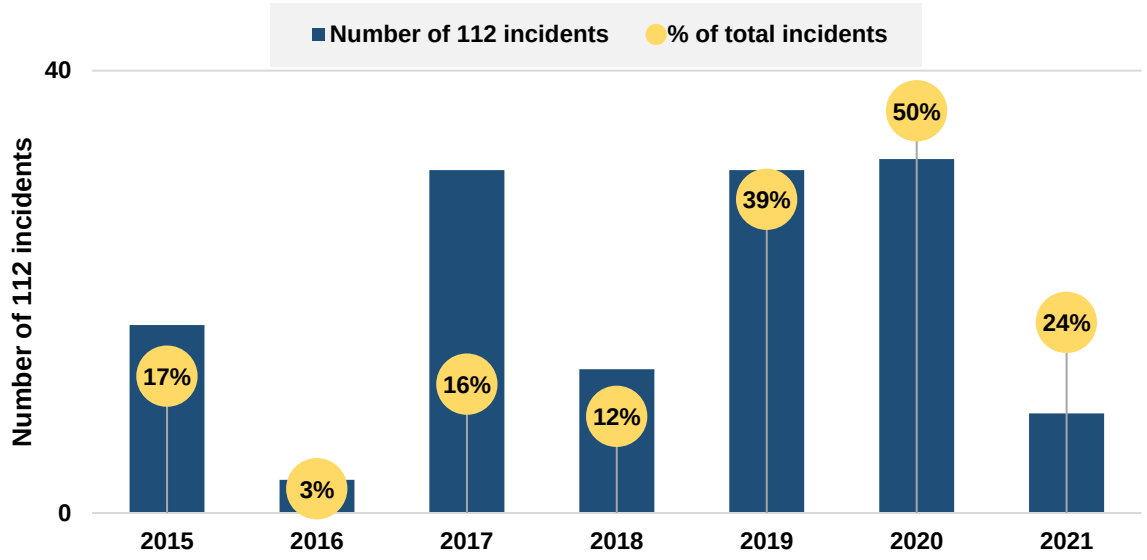
Under Article 21(2)(b) of Security Regulation 303/2019 of 1 April, companies notify ANACOM of security incidents affecting the delivery to PSAPs - Public Safety Answering Points (112 Service Centres), directly or indirectly, of calls to the European emergency number 112 for a period equal to or greater than 15 minutes.

Note that this is to distinguish access to 112 for those who have the telephone service but cannot access the PSAPs, and those who do not have the telephone service but cannot make any successful call, be it emergency 112 or otherwise.

Mobile service, however, provides for an exception to this by allowing access to 112 when the mobile service provider's network is unavailable, in which the call can be routed through the network of another mobile operator, if available, through "national roaming".

Chart 15 shows the security incidents reported in relation to the circumstance of the 112 calls and to the total.

Chart 15 - Security incidents notified relating to the 112 circumstance, 2015-2021.



Unit: number of security incidents and percentage of total incidents (%)

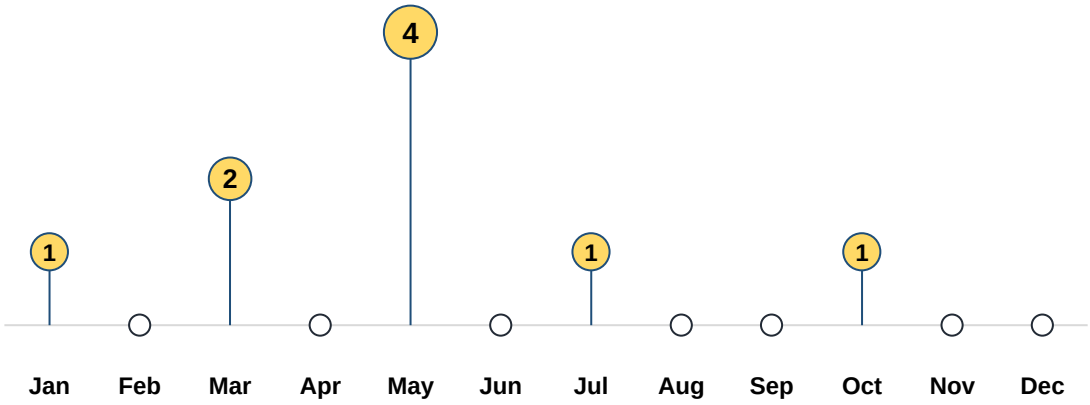
Source: ANACOM

In 2021, of the 38 security incidents reported, 9 impacted access to 112 service centres (PSAPs), i.e., on the ability of users to contact the emergency service centres affected, using the 112 emergency number.

It can be seen that the value of reported security incidents decreased from 2020 to 2021, from 32 to 9 in absolute figures, and in percentage terms, from 50% to 24%.

Chart 16 shows the monthly figures for the 9 security incidents related to 112 calls.

Chart 16 - Security incidents notified monthly relating to 112 calls, in 2021.



Unit: Number of security incidents

Source: ANACOM

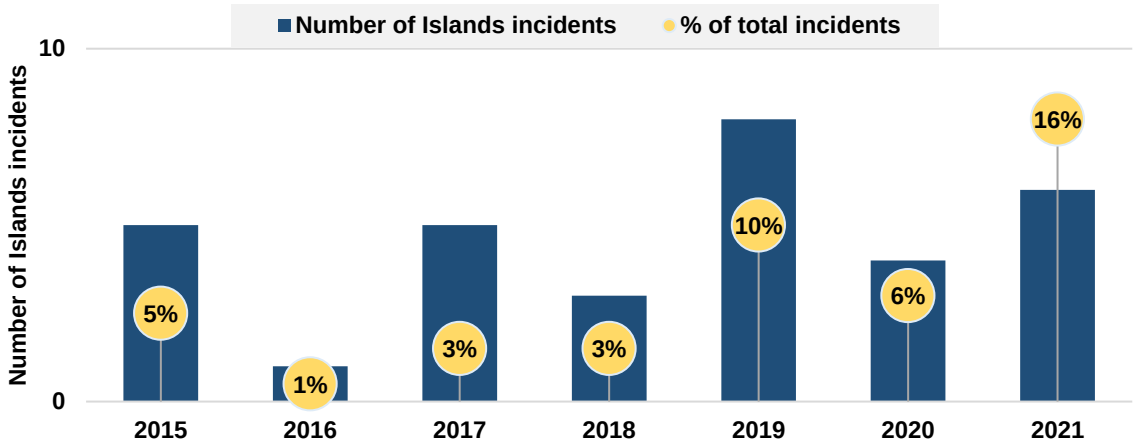
3.4 Islands ("Isolated")

Under the terms of Article 21(2)(e) of Security Regulation 303/2019 of 1 April, companies must notify ANACOM of security incidents that impact the operation of all networks and services offered by a company in the entire territory of an island in the Autonomous Region of the Azores or the Autonomous Region of Madeira, provided that it lasts 30 minutes or more, regardless of the number of subscribers or accesses affected or the geographical area affected.

An *"isolated" Island* incident means that all customers of a given operator were unable to access the electronic communications service solely within the territory of one island.

Chart 17 shows the occurrence of six special island situations, which took place in the months of January, February, August, October and December, corresponding to 16% of all incidents recorded in 2021.

Chart 17 - Security incidents notified relating to the Islands circumstance, 2015-2021.

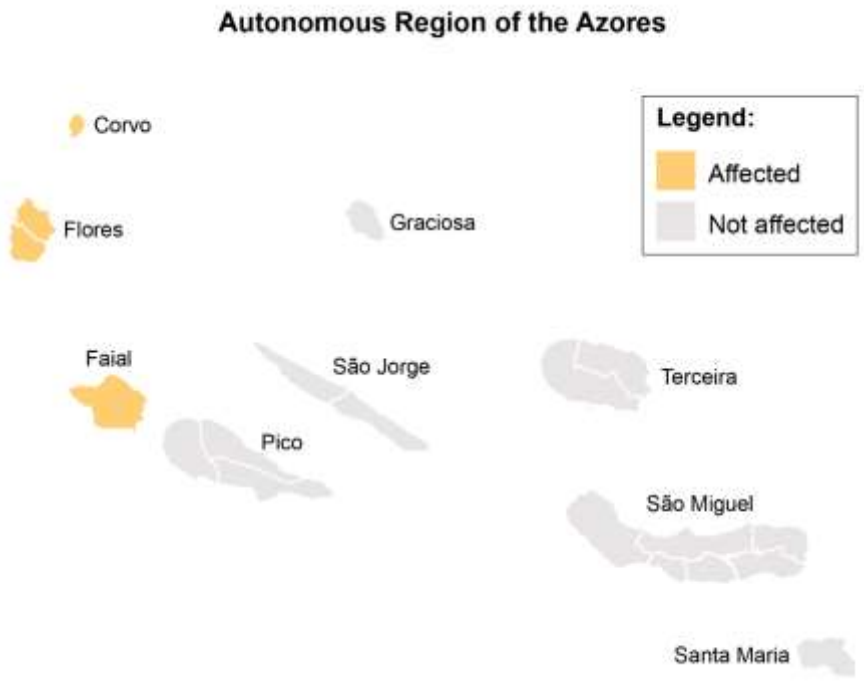


Unit: Number of security incidents and percentage of total incidents (%)

Source: ANACOM

Figure 2 identifies the islands where security incidents occurred that impacted the operation of all networks and services offered by a company in the entire territory of one island in the Autonomous Region of the Azores.

Figure 2 - "Isolated" Islands of the Autonomous Region of the Azores due to security incidents, in 2021.



Source: ANACOM

3.5 Other circumstances

In 2021, three security incidents were also recorded which are considered in the other circumstances provided for in Article 21 of Security Regulation 303/2019. These are: one security incident relating to the cumulative impact of the occurrence of a security breach or loss of integrity that recurs over a period of four weeks, and two security incidents with significant impact on a relevant date (i.e., national [presidential] election day).

Both security incidents had a root cause of *maintenance or failure of hardware or software*.

Figure 3 shows the affected districts in which the three security incidents occurred.

Figure 3 - Identification of districts in mainland Portugal by the incidents notified in 2021 relating to the other identified circumstances.

Source: ANACOM

3.6 Information to the public

ANACOM underscores the importance to the interests of citizens of information to the users of electronic communications networks and services.

Pursuant to Article 23(1) of Security Regulation 303/2019, companies must notify the public of any security incident whose impact on the functioning of its networks and services includes one of the following levels (Table 2):

Table 2 - Levels of obligation of disclosure to the public by companies.

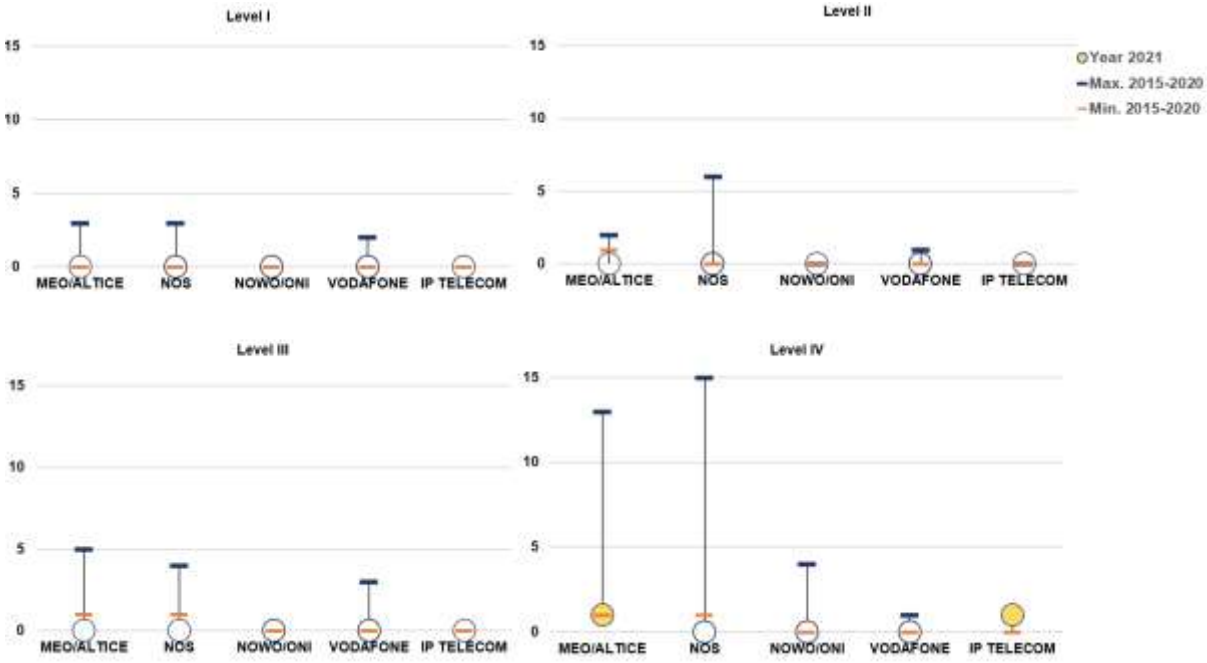
Duration, and	Number of subscribers or accesses affected (or, pursuant to paragraph 2(e) of this Article, geographical area affected)	Level
≥ 30 minutes	no. of subscribers or accesses affected ≥ 500 000 (or, in accordance with paragraph I.4(e), affected geographical area ≥3000 km^2)	**I**
≥ 1 hour	500 000 > no. of subscribers or accesses affected ≥ 100 000 (or, in accordance with paragraph I.4(e), 3000 km^2 > affected geographical area ≥ 2000 km^2)	**II**
≥ 2 hours	100 000 > no. of subscribers or accesses affected ≥ 30 000 (or, in accordance with paragraph I.4(e), 2000 km^2 > affected geographical area ≥ 1500 km^2)	**III**
≥ 4 hours	30 000 > no. of subscribers or accesses affected ≥ 10 000 (or, in accordance with paragraph I.4(e), 1500 km^2 > affected geographical area ≥ 1000 km^2)	**IV**

Source: ANACOM, Security Regulation 303/2019

Information about a particular security incident is very often of interest not only to the subscribers directly affected, but also to all other users who were prevented from communicating with them.

Of the 20 security incidents received in 2021 which fall within the levels, two were identified with the obligation to inform the public, both corresponding to level IV. A comparison of the results with the maximum and minimum of the 2015-2020 period is presented in Chart 18.

Chart 18 - Security incidents covered by the obligation of disclosure to the public by companies in 2021, compared to 2015-2020.



Unit: Security Incidents

Source: ANACOM

As provided in Article 24(1)(c) of Security Regulation 303/2019, the information must be provided as soon as possible, within a maximum period of four consecutive hours after the initial notification to ANACOM.

The means by which companies are required to provide information to the public should be, at least, on the websites used in their relationship with the users of their networks and services, through an immediately visible and identifiable hyperlink posted on the website's homepage, pursuant to (1)(b). Furthermore, this information must remain publicly available for 20 working days after the end date of the security breach or loss of integrity.

In the case of Public Safety Answering Points, no information is provided to the public from the website, since 112 Service Centres are the responsibility of the Ministry of Internal Administration (MAI).

ANACOM AUTORIDADE NACIONAL DE COMUNICAÇÕES

april
2021

Lisbon (Headquarters)
Av. José Malhoa, 12
1099 - 017 Lisbon
Portugal
Tel: (+351) 217211000
Fax: (+351) 217211001

Porto
Rua Direita do Viso, 59
4250 - 198 Porto
Portugal
Tel: (+351) 226198000

Azores
Rua dos Valados, 18 - Relva
9500 - 652 Ponta Delgada
Portugal
Tel: (+351) 296302040

Madeira
Rua Vale das Neves, 19
9060 - 325 S. Gonçalo - Funchal
Portugal
Tel: (+351) 291790200

Public attendance
800206665
info@anacom.pt

www.anacom.pt