ANACOM AUTORIDADE NACIONAL DE COMUNICAÇÕES

ANNUAL REPORT

SECURITY BREACHES OR LOSS OF INTEGRITY

2020

ANACOM AUTORIDADE NACIONAL DE COMUNICAÇÕES

Security Breaches or Loss of Integrity

2020

Annual Report

Contents

List of Graphs

List of Tables

List of Figures

Executive summary

Due to the SARS-CoV-2 pandemic, the year 2020 saw a significant reduction to the total number of security incidents notified to ANACOM by electronic communications network and service companies: 64 security incidents, 20% below the previous year and the lowest number since 2015.

ANACOM Security Regulation no. 303/2019 lays out the rules to be followed by publicly accessible electronic communications companies in reporting security incidents of major impact: events that cause an electronic communications service to be inaccessible simultaneously to a high number of customers for a significant period of time.

The first and third quarters, with 77% of the incidents, were the most burdensome with regard to the number of incidents received. Northern and central Portugal had the most incidents in electronic communications networks and services.

Similar to recent years, 59% of the causes associated with security incidents in 2020 were due to the failure to supply good or services by external entity, i.e. resulting from events or developments outside of the sector. There were two types of occurrences during the year: 32 incidents affecting 112 Service Centre call delivery, of which only 3 were received via South Operational Centre (COSUL) intervention on 26 May after ANACOM intervention with MAI and MEO, and 27 incidents directly impacting customers.

In general, most security incidents impact more than one publicly accessible electronic communications service. Fixed telephony was the most affected service, with 88% of all security incidents received; this was followed by mobile telephony, at 70%; and mobile Internet, with 33% of all security incidents.

In 2020, the 27 security incidents referred to above impacted approximately 2 million subscribers/accesses, down around 85% year-over-year (around 12.4 million in 2019). Only two incidents impacted a half million or more subscribers/accesses.

“Hardware/software failure and maintenance” and “accident/natural disaster (storms, fires)” were, at 76% and 15%, the two most commonly mentioned causes in the 27 security incidents, respectively.

The total annual service downtime was down more than 60%: 360 hours (compared to 937 hours in 2019). The average service downtime for the 27 security incidents in 2020 was 13 hours, 46% lower compared to 2019 (24 hours).

Nine of the 27 security incidents notified were covered by the obligation of disclosure to the public by the companies MEO, NOS and NOWO/ONI.

ANACOM reported three security incidents (compared to eight in 2019) to the European Commission and the European Network and Information Security Agency (ENISA), which exceeded the European Union-wide reporting threshold, based on incident duration and relative number of subscribers/accesses affected.

1 Introduction

This report presents and analyses information from notifications of security breaches or losses of integrity with a significant impact (hereinafter called “security incidents”). This data includes initial, end-of-significant impact and final notifications sent by companies that offer public communications networks or publicly accessible electronic communications services to the Autoridade Nacional de Comunicações (ANACOM) in 2020. The constituent components and annual security reports received are also accounted for, with a summary of developments since 2015.

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

By decision of 14 March 2019, ANACOM approved regulations on the security and integrity of ANACOM’s electronic communications networks and services (hereinafter “Security Regulation no. 303/2019”), published on 1 April.

Nonetheless, since 2014, ANACOM has had a Notification Reporting Centre (CRN) for companies to notify security incidents. This information must be given in real time, and whenever security breaches or losses of integrity significantly affect 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 2020, ANACOM continued to submit to the European Commission and to the European Network and Information Security Agency (ENISA) a brief report about the communications involving security breaches or losses of integrity, as well as the measures taken.[1].

Due to the pandemic, 2020 was decidedly unusual and demanding regarding access to electronic communications. However, the number of incidents occurred and

[1] In line with the ENISA *Technical Guideline on Incident Reporting, Technical guidance on the incident reporting in Article 13a Version 2.1, October 2014,* available at https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting

the average annual duration of service downtime fell to the lowest levels on record, demonstrating stability as regards the security and integrity of electronic communications.

Section 2 analyses the incidents with regard to their evolution over time, impact per root cause and impact per service. Section 3 describes the circumstances and respective impact on levels and rules, format and procedures, together with the conditions, content, means and timelines for the incidents' public disclosure.

2 Security incidents in 2020

As regards the identification of security incidents, and pursuant to Article 21 (1) – Circumstances of Security Regulation no. 303/2019, all breaches of security or loss of integrity that cause 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 the rules of (2) of this same article, should be subject to notification.

Next, we cite the main trends over the 2015-2020 period, as regards the characterisation of the causes of the incidents and the services that were affected, as well as the criteria that were most frequently applied in determining significant impact.

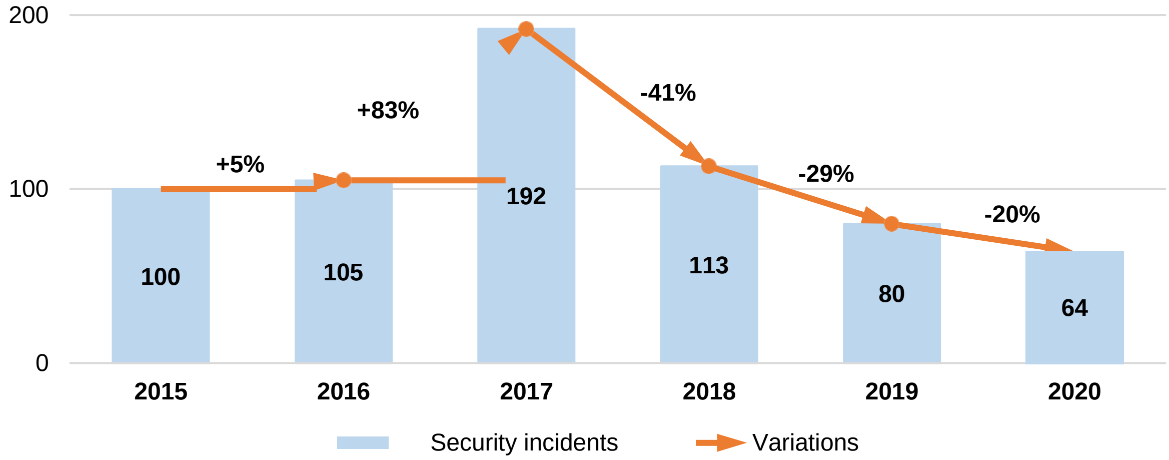
2.1 Number of security incidents notified

In 2020, the combined companies notified 64 security incidents to ANACOM.

This was the lowest figure recorded since 2015. During the 2015-2020 period, the companies notified a total of 654 security incidents (annual average of 109 occurrences).

Graph 1 shows that the initial upward trend in the annual quantity of security incidents notified was reversed, peaking in 2017 (due to the outbreak of forest fires this year) followed by a sharp decline over the past three years.

Graph 1 – Number of security incidents notified, 2015-2020.

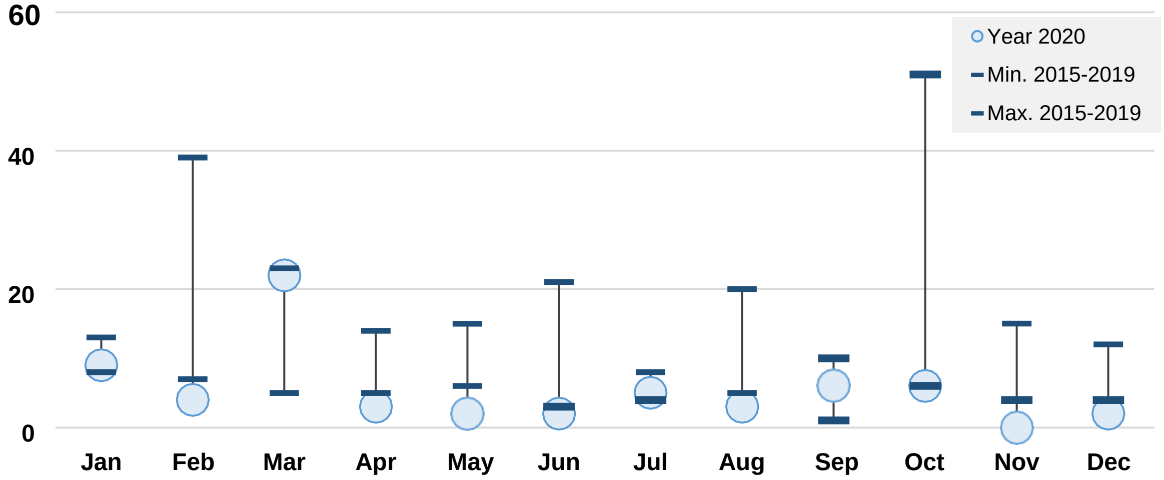


Unit: Number of security incidents

Source: ANACOM

Graph 2 shows the evolution over time of the number of monthly incidents received during 2020 compared to the maximums and minimums from 2015-2019.

Graph 2 – Monthly figures for security incidents notified in 2020, compared to the period of 2015-2019.



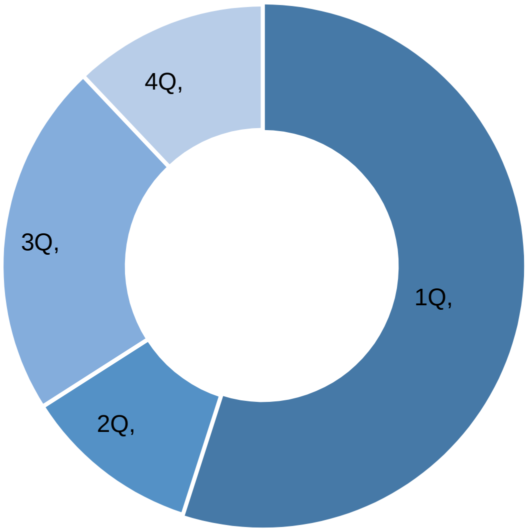
Unit: Number of security incidents

Source: ANACOM

As such, in 2020 – and having nothing to do with being the first month of the pandemic – a maximum occurred in March (largely due to the South Operational Centre [COSUL] access problem, explained below), with 22 incidents, with the minimum occurring in November, with no incidents. In the past six years, the highest figures for security incidents notified occurred in 2017, with 39 in February and 51 in October.

An analysis of Graph 3 shows that, in 2020, the first and third quarters (1Q and 3Q, respectively) were the most burdensome with regard to the number of incidents received.

Graph 3 – Percentage of security incidents received in 2020, by quarter.



Unit: % of security incidents

Source: ANACOM

2.2 Root cause

According to Article 22 (11) – Formats and Procedures of Security Regulation no. 303/2019, security incidents can have the following categories of root cause:

- *Accident/natural disaster – 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 a deliberate act of a person or an organisation;*

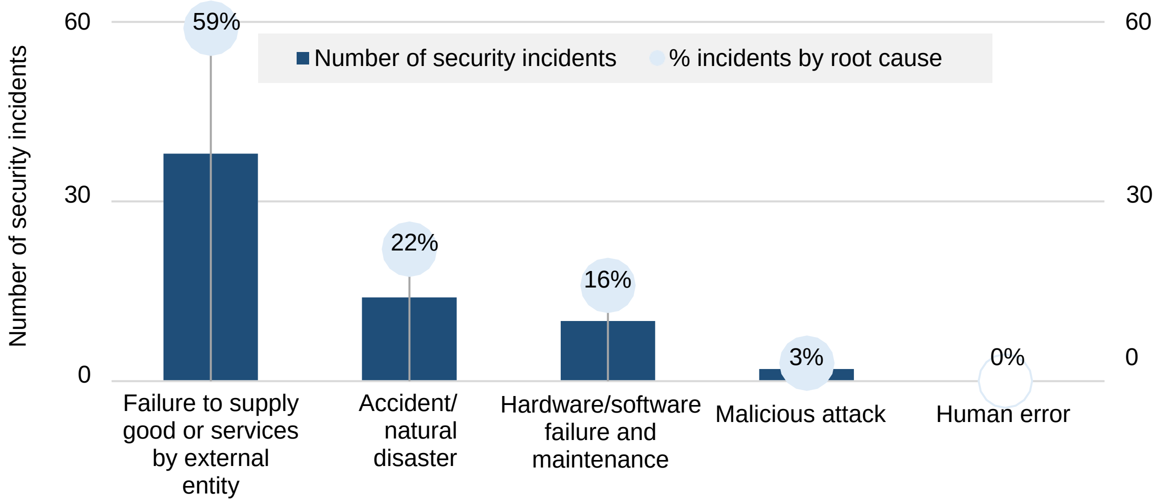
- *Hardware/software failure or maintenance – due to technical system failure, in its physical (hardware) and/or logical (software) components;*

- *Failure to supply good or services by external entity – due to a break in the supply of goods or services, such as the supply of electricity or leased lines, or any other good or service provided by third parties.*

As shown above in Graph 3, the increase occurring in 1Q was due to the failure to supply good or services by external entity. In 3Q, the root cause was essentially divided between "accident/natural disaster" and "failure to supply good or services by external entity". Virtually the same number of incidents as all of those received in 2Q and 4Q, accounting for 22% of incidents recorded over the year, occurred during this quarter.

In the period in question, as shown in Graph 4, the failure to supply good or services by external entity was the predominant root cause, primarily involving the failure to supply electricity or leased lines.

Graph 4 – Security incidents received for different categories of root cause, 2020.

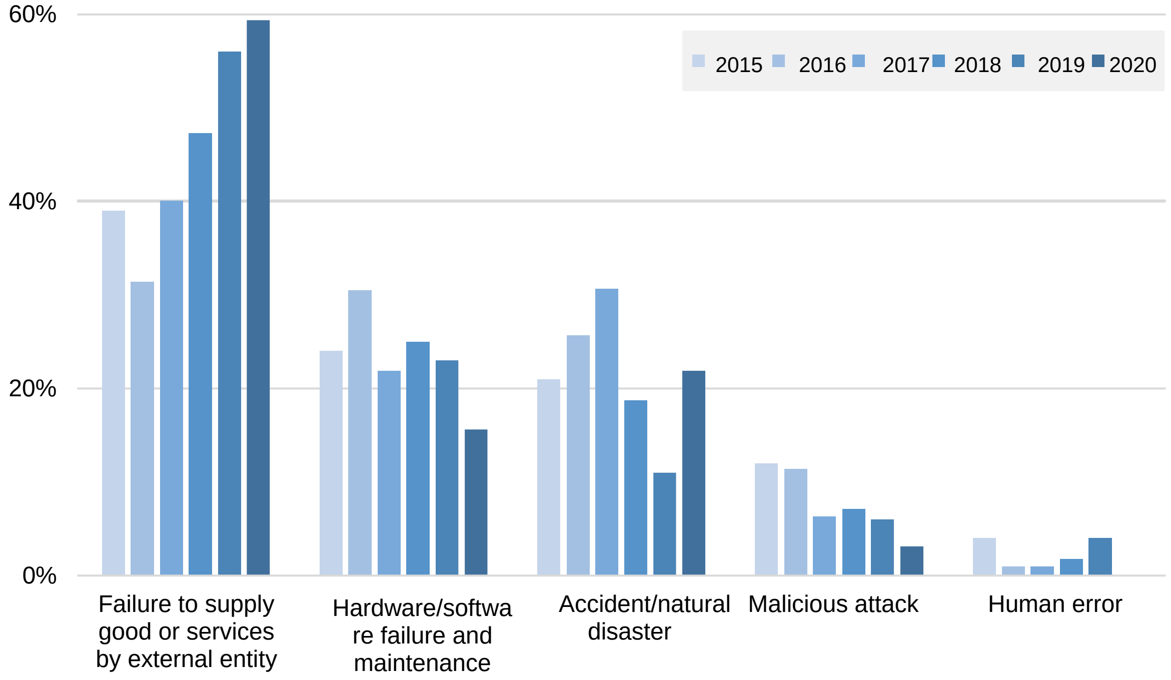


Unit: Number of security incidents and percentage of total incidents (%)

Source: ANACOM

The root cause of “accident/natural disaster”, the second most frequent this year, accounts for nearly one fourth of all security incidents notified, namely for reasons involving severe weather conditions and other natural phenomena.

Graph 5 – Percentage of security incidents notified for each root cause, 2015-2020.



Unit: % of security incidents

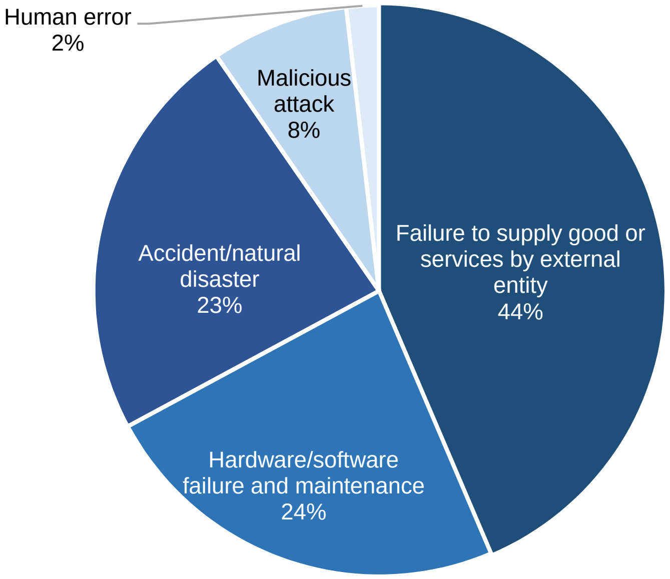
Source: ANACOM

The following are noteworthy in Graph 5:

- the relative increase in incidents associated with the failure to supply good or services by external entity;
- the downward trend in the number of incidents caused by problems involving hardware/software failure and maintenance and malicious attacks;
- the fluctuation (i.e., ambiguous trend) in reasons involving accident/natural disaster.

In cumulative terms, for the 654 incidents occurring in the period of 2015-2020, the distribution of their underlying causes is shown in Graph 6, with "failure to supply good or services by external entity" being noteworthy.

Graph 6 – Distribution of security incidents notified (654 in total) for each root cause, 2015-2020.



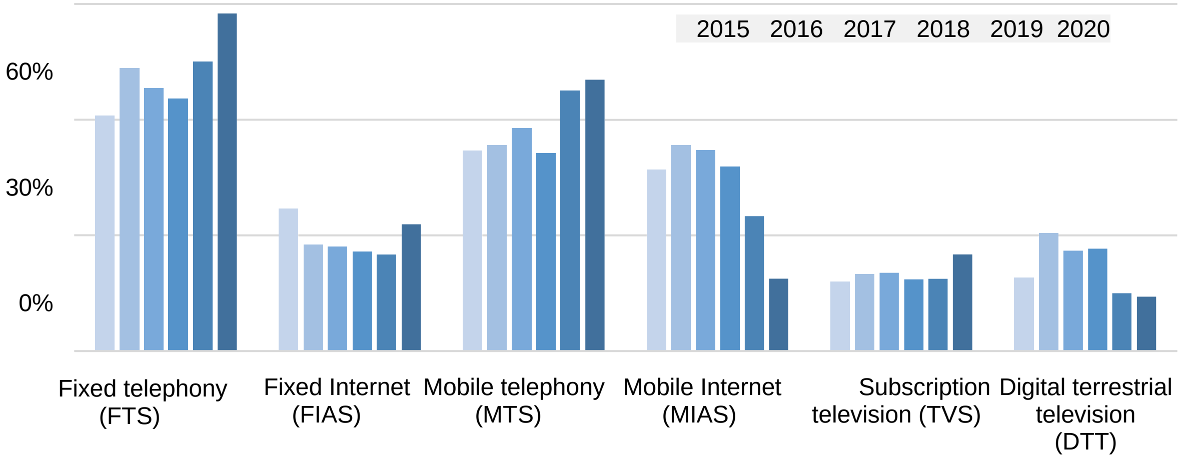
Unit: % of security incidents

Source: ANACOM

2.3 Impact on service

As regards the impact on electronic communications services, incidents can affect one or more services: fixed and mobile telephony, fixed and mobile Internet, subscription television and digital terrestrial television. Graph 7 details the security incidents notified by service affected over the past six years.

Graph 7 – Percentage of security incidents notified for each type of service, 2015-2020. 90%



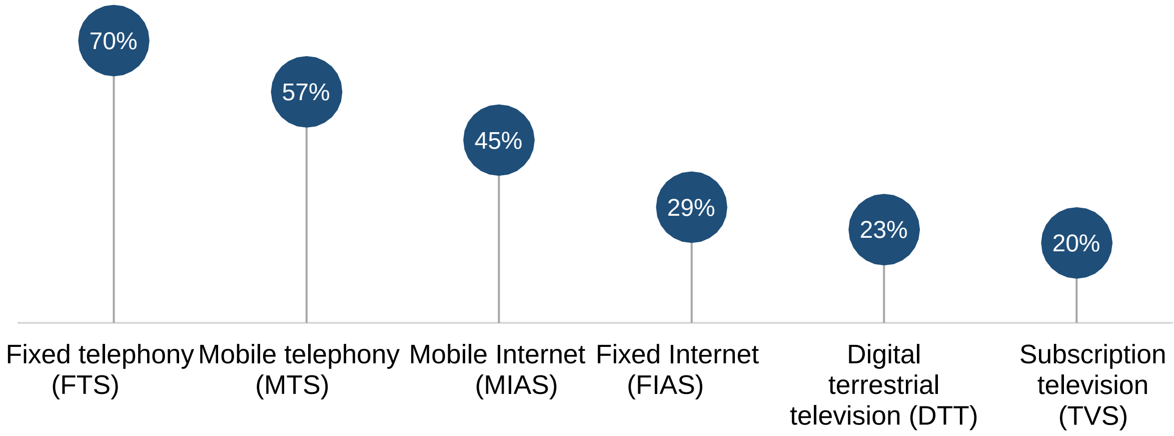
Unit: % of security incidents

Source: ANACOM

Note: The majority of security incidents notified impact more than one service (which is why the graph's percentages total more than 100%).

According to the security incidents received, fixed and mobile telephony were the services most affected during the period. In particular, the fixed telephony service was the most affected service during this period, with figures above 60% every year. In 2020, 88% of the security incidents notified impacted fixed telephony.

Graph 8 – Distribution of security incidents notified for each type of service affected, 2015-2020.



Unit: % of security incidents

Source: ANACOM

Note: Given that most security incidents had an impact on more than one service, the percentages in the graph exceeded 100% in each year.

In these six years, the three services most affected were, in descending order (Graph 8): fixed telephony (70%), mobile telephony (57%) and mobile Internet (45%).

3 Analysis of incidents, 2020

Those circumstances which, surpassing the thresholds of significant impact established in Article 21 of ANACOM Security Regulation no. 303/2019, gave rise to the security incidents notified, causing a serious disturbance to 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 subdivided into 6 levels **(Subscribers/Accesses - Levels)**;

b) Direct or indirect effect on the delivery to Public Security Service Posts (112 Service Centres) of calls to 112 for a period of 15 minutes or more **(112).**

c) Effect on the supply from 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, with a duration of 30 minutes or more **(Islands[2])**.

d) All other circumstances referred to in Article 21 **(Other)**.

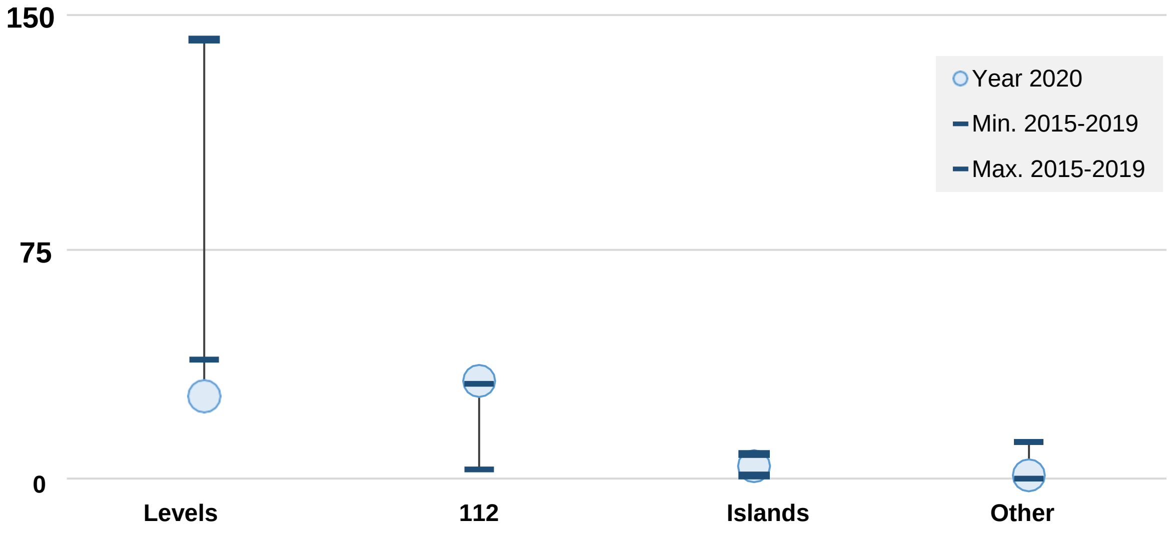
2020 was noteworthy for the occurrence of security incidents directly impacting services provided to customers, subparagraph a), and those related to 112 Service Centre call delivery, subparagraph b).

3.1 Distribution of reported incidents

Graph 9 distributes the incidents reported, with a comparison against the maximum and minimum in the period of 2015-2019.

[2] 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.

Graph 9 – Security incidents notified in 2020 per circumstance, compared to the period of 2015-2019.



Unit: Number of security incidents

Source: ANACOM

Of the 64 incidents in 2020, “effect on the delivery to Public Security Service Posts (112 Service Centres)” recorded 32 incidents, accounting for 50%, while the circumstance related to the “number of subscribers/accesses affected and respective duration of significant impact” (“Levels”) recorded 27 incidents, accounting for 42%.

3.2 Subscribers or accesses affected (Levels)

Table 1 shows the circumstance that matches the number of subscribers or accesses affected with the duration of significant impact. This criterion is subdivided into 6 levels (I to VI). Level I corresponds to the highest number of subscribers/accesses affected and level VI to the lowest.

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

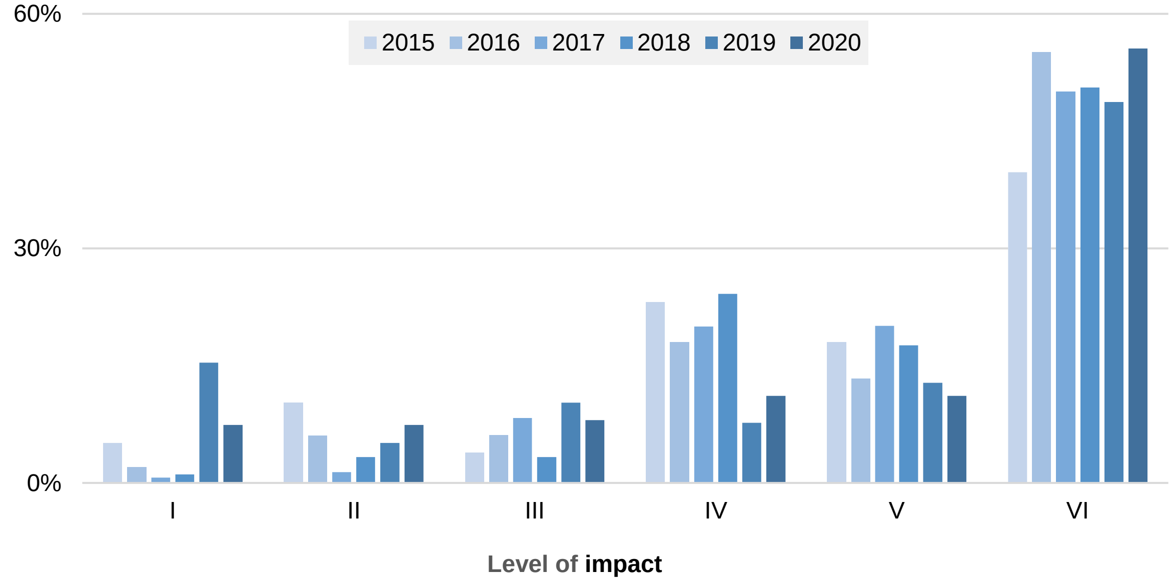
Graph 10 shows the number of security incidents notified relating to the 2015-2020 period, distributed over each of the above-mentioned levels.

Table 1 – Impact levels on subscribers/accesses.

Duration and	Number of subscribers or accesses affected (or, pursuant to [3e] of this article, geographic area affected)	Level
≥ 30 minutes	number of subscribers or accesses affected ≥ 500,000 (or, pursuant to Point I [4e], geographic area affected ≥ 3,000 km2)	**I**
≥ 1 hour	500,000 > number of subscribers or accesses affected ≥ 100,000 (or, pursuant to Point I [4e], 3,000 km2 > geographic area affected ≥ 2,000 km2)	**II**
≥ 2 hours	100,000 > number of subscribers or accesses affected ≥ 30,000 (or, pursuant to Point I (4e), 2,000 km2 > geographic area affected ≥ 1,500 km2)	**III**
≥ 4 hours	30,000 > number of subscribers or accesses affected ≥ 10,000 (or, pursuant to Point I [4e], 1,500 km2 > geographic area affected ≥ 1,000 km2)	**IV**
≥ 6 hours	10,000 > number of subscribers or accesses affected ≥ 5,000 (or, pursuant to Point I [4e], 1,000 km2 > geographic area affected ≥ 500 km2)	**V**
≥ 8 hours	5,000 > number of subscribers or accesses affected ≥ 1,000 (or, pursuant to Point I [4e], 500 km2 > geographic area affected ≥ 100 km2)	**VI**

Source: ANACOM, Security Regulation no. 303/2019

Graph 10 – Security incidents notified per level of impact subscribers/accesses, proportion, 2015-2020.



Unit: % of security incidents

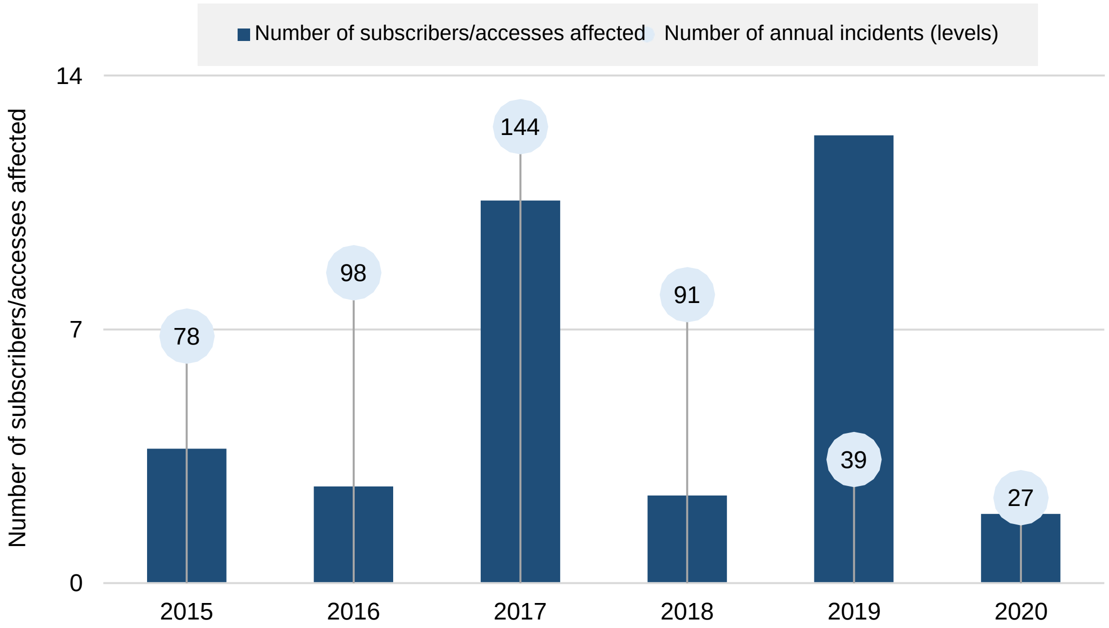
Source: ANACOM

In 2020, the level of the number of subscribers/accesses affected, corresponding to the lowest level of seriousness (level VI), was the most common among security incidents notified, totalling 15.

Note the relative weight of the number of incidents associated with the lower levels IV, V and VI, which had an annual average of 83% in the period of 2015-2020.

Graph 11 shows the number of security incidents due to the circumstance of the number of affected subscribers/accesses and the total annual number of subscribers/accesses affected in 2015-2020.

Graph 11 – Security incidents notified due to the circumstance of the number of subscribers/accesses affected (levels), 2015-2020.



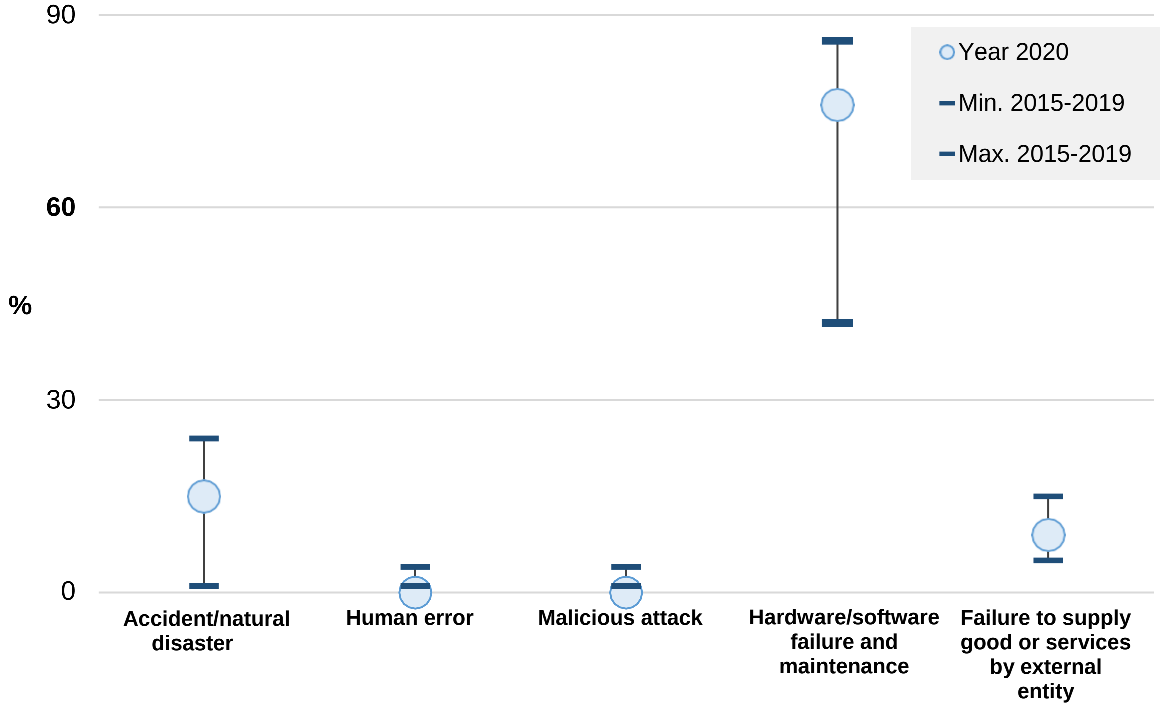
Unit: Number of subscribers/accesses affected (million) and number of annual incidents (level)

Source: ANACOM

Comparing 2020 with the previous year, we observe that the total number of security incidents due to the number of subscribers/accesses affected (levels) fell from 39 to 27 (a reduction of nearly 31%), with a simultaneous decrease in the total number of subscribers/accesses affected from nearly 12.4 million to a total of around 2 million (down around 85%).

Graph 12 shows the root causes giving rise to the number of subscribers/accesses affected, compared to the maximums and minimums from 2015-2019.

Graph 12 – Percentage of the number of subscribers/accesses affected per root cause in 2020, compared to the period of 2015-2019.



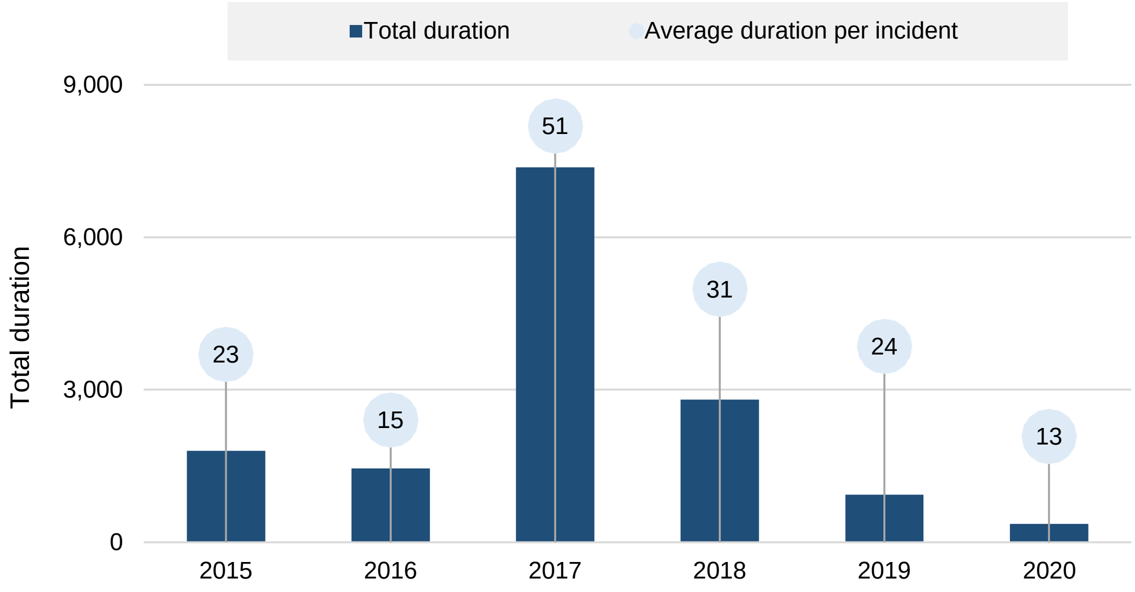
Unit: Number of security incidents and number of subscribers/accesses

Source: ANACOM

The graph highlights the root cause of hardware/software failure and maintenance as giving rise to incidents impacting 76% of all subscribers/accesses affected in 2020, corresponding to nearly 1.5 million, compared to around 8 million in 2019.

Besides the total number of subscribers/accesses affected each year, it is also important to analyse the cumulative annual duration of the impact caused by security incidents occurred in that year (annual impact duration) and the average duration of security incidents during that year (average annual impact duration). This last figure gives an approximate idea of the recovery time for security incidents. Graph 13 shows the figures from these six years.

Graph 13 – Annual impact duration and average annual impact duration, 2015-2020.



Unit: Hours

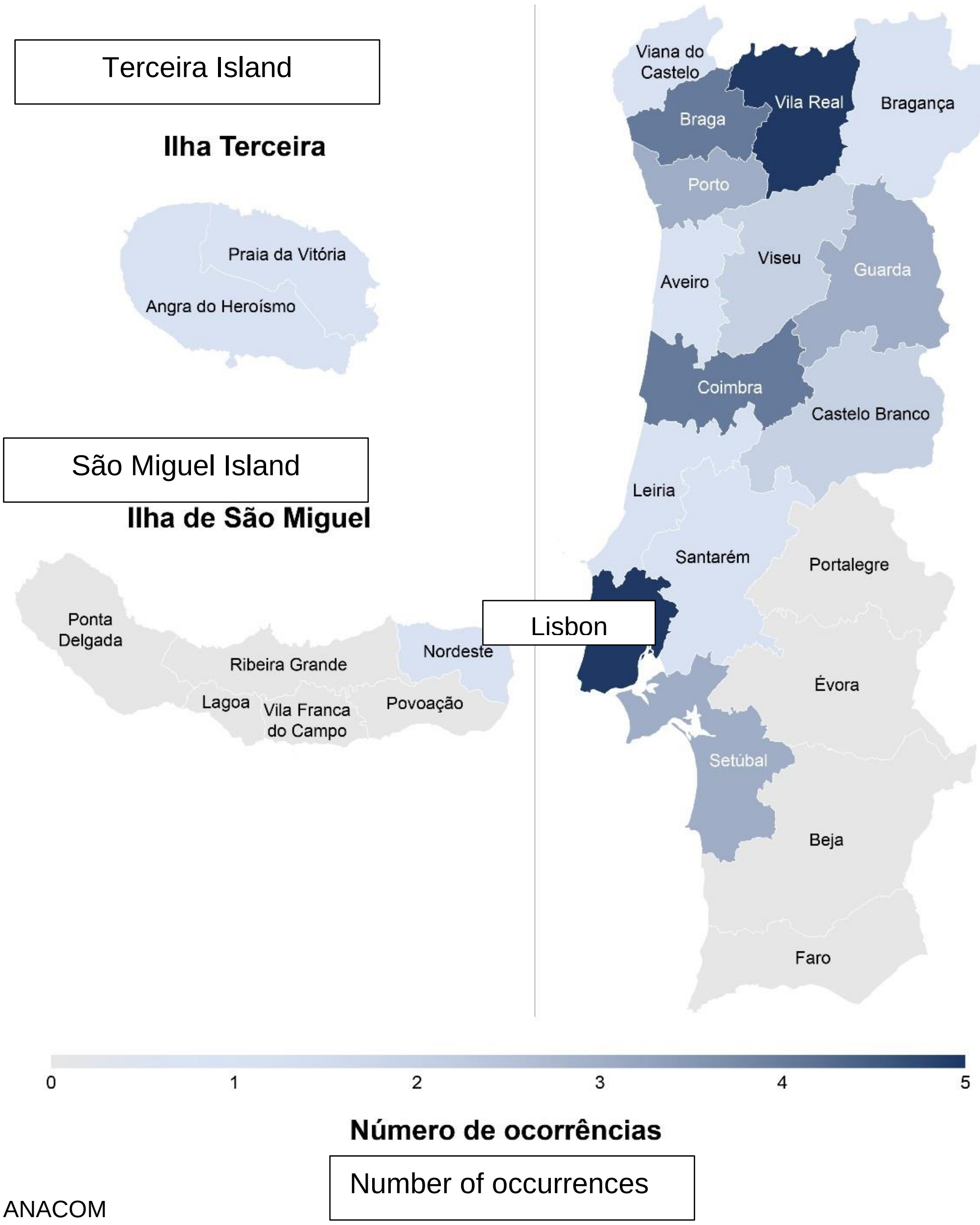
Source: ANACOM

In 2020, the total impact duration was 360 hours. In 2019, this figure was 937 hours, which corresponds to a 62% reduction. In 2017 and 2018 alike, there have been long-lasting security incidents resulting in a high annual impact duration for these years. Such a situation has not yet been recorded in 2019 or in 2020.

Consequently, as regards the average annual impact duration, 2020 was down 46% compared to 2019, from 24 to 13 hours.

Four of the 27 security incidents were national in scope, while the rest had a significant impact on networks and services in the districts of mainland Portugal and the municipalities of the Autonomous Region of the Azores shown in Figure 1.

Figure 1 – Identification of districts on mainland Portugal and municipalities of the Autonomous Region of the Azores affected by incidents of non-national scope notified in 2020.



Source: ANACOM

3.3 Calls to 112 emergency number

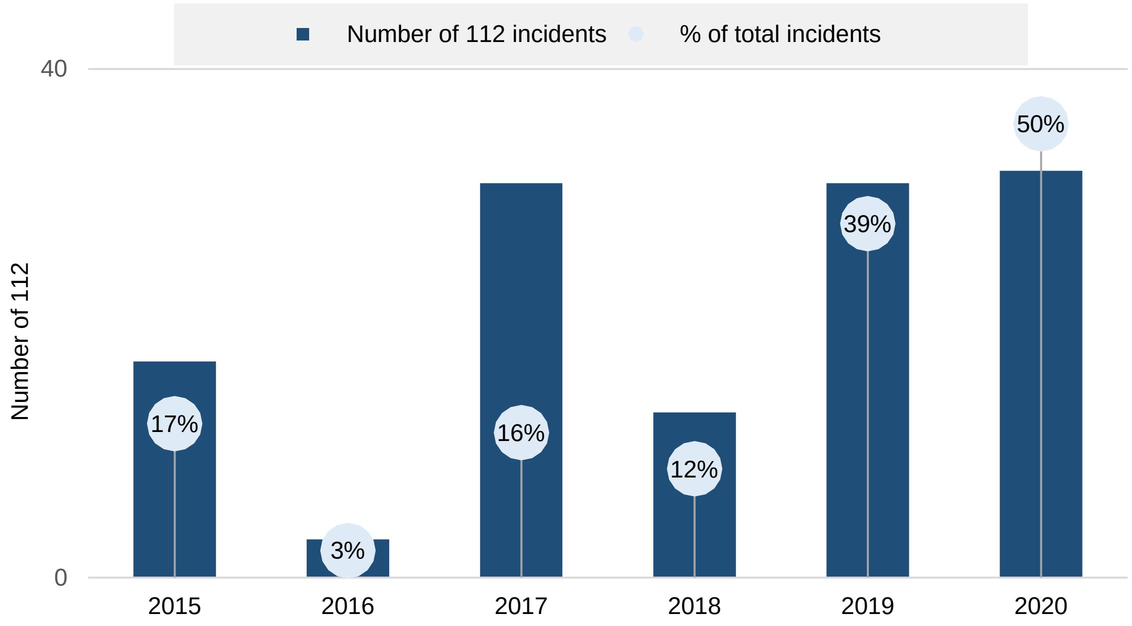
Pursuant to Article 21 (2b) of Security Regulation no. 303/2019 of 1 April, companies must notify ANACOM of security incidents directly or indirectly affecting delivery to Public Security Service Posts (112 Service Centres) of calls to the single European emergency number 112 for a period equal to or greater than 15 minutes.

It should be noted that here it is a question of distinguishing access to 112 by those who have the telephone service but are unable to access the Public Security Service Posts, from those who do not have a telephone service and thus cannot make any successful calls, either to 112 emergency or any other number.

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".

Graph 14 shows the security incidents notified in relation to the circumstance of calls to 112 and to the total.

Graph 14 – Security incidents notified relating to the 112 circumstance, 2015-2020.



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

Source: ANACOM

In 2020, of the 64 security incidents notified, 32 recorded an impact on the Public Security Service Posts (112 Service Centres), i.e. on the ability of users to contact the emergency call centres affected by using the 112 emergency number.

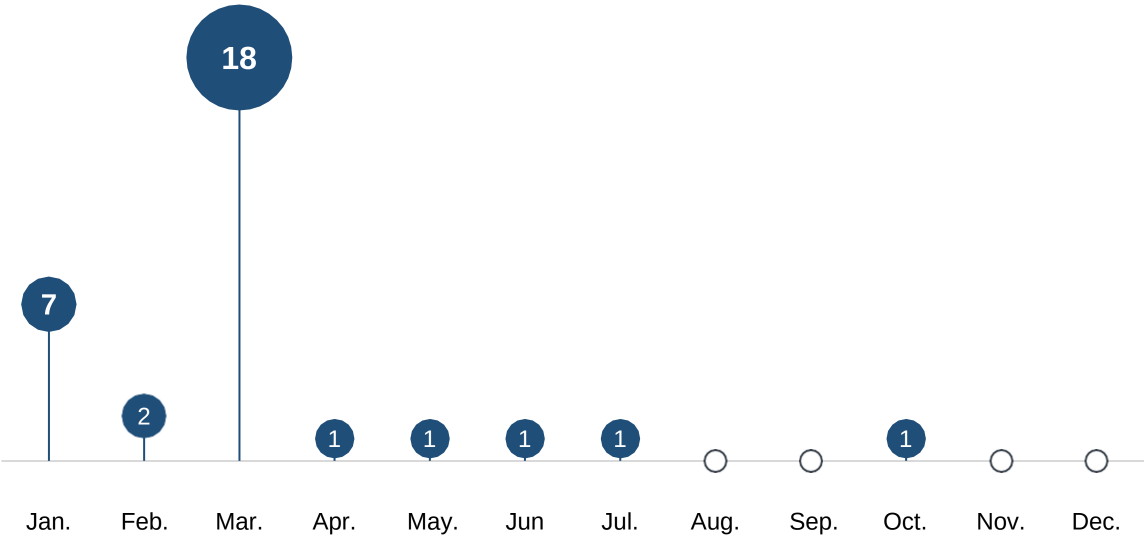
It is confirmed that the figure for security incidents notified increased from 2019 to 2020, in absolute numbers from 31 to 32 and, principally, in percentage terms from 39% to 50%.

Graph 15 shows the monthly figures for the 32 security incidents involving 112 calls. The maximum occurred in March, with 18 incidents.

Having found, in the analysis of 2019 notifications, a problem in accessing the South Operational Centre (COSUL), ANACOM issued letters in early March 2020 to the Minister for Internal Administration and to MEO with a view to analysing the problem in detail and resolving it.

As can be seen in Graph 15, beginning in May 2020, work performed on COSUL's internal systems on 26 May resulted in improvements to COSUL's performance, as demonstrated by the mere three incidents occurring over the remaining seven months of the year.

Graph 15 – Security incidents notified monthly relating to 112 calls, in 2020.



Unit: Number of security incidents

Source: ANACOM

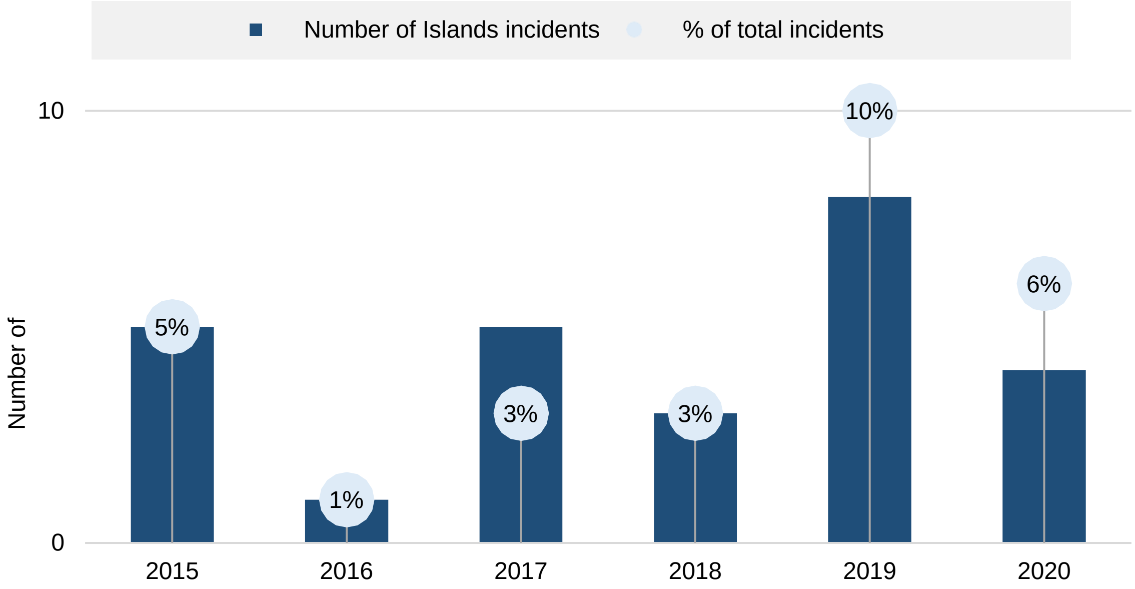
3.4 Islands (“Isolated”)

Pursuant to Article 21 (2e) of Security Regulation no. 303/2019 of 1 April, companies must notify ANACOM of security incidents impacting the supply from 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, provided that they have a duration of 30 minutes or more, regardless of the number of subscribers, number of accesses or geographic area affected.

An “isolated” Island incident means all of the customers of a given operator were unable to access the electronic communications service within the confined territory of one island.

Graph 16 shows four special island situations occurring in the months of March, May, July and September, accounting for 6% of all incidents recorded in 2020.

Graph 16 – Security incidents notified relating to the Islands circumstance, 2015-2020.

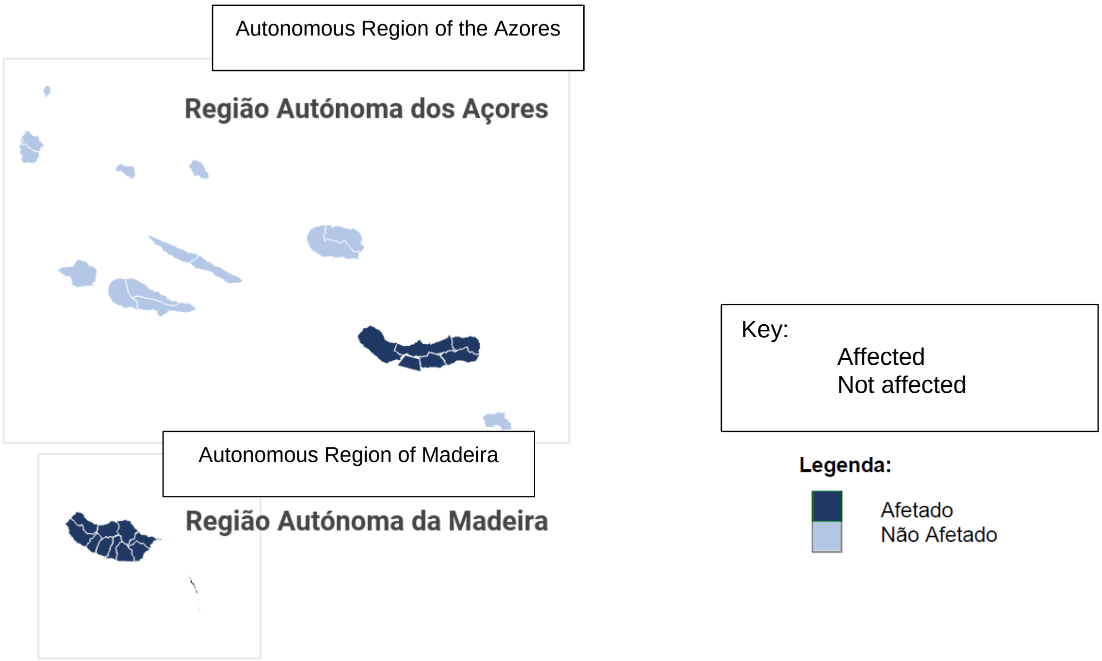


Unit: Number of security incidents and percentage of total incidents (%)

Source: ANACOM

Figure 2 identifies the islands with security incidents that impacted the supply from all networks and services offered by a company in the entire territory of one island in the Autonomous Region of the Azores or the Autonomous Region of Madeira.

Figure 2 – “Isolated” islands of the Autonomous Regions of the Azores and Madeira due to security incidents, in 2020.


Autonomous Region of the Azores
Região Autónoma dos Açores
Autonomous Region of Madeira
Região Autónoma da Madeira
Key:
Affected
Not affected
Legenda:
Afetado
Não Afetado

Source: ANACOM

3.5 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 no. 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.

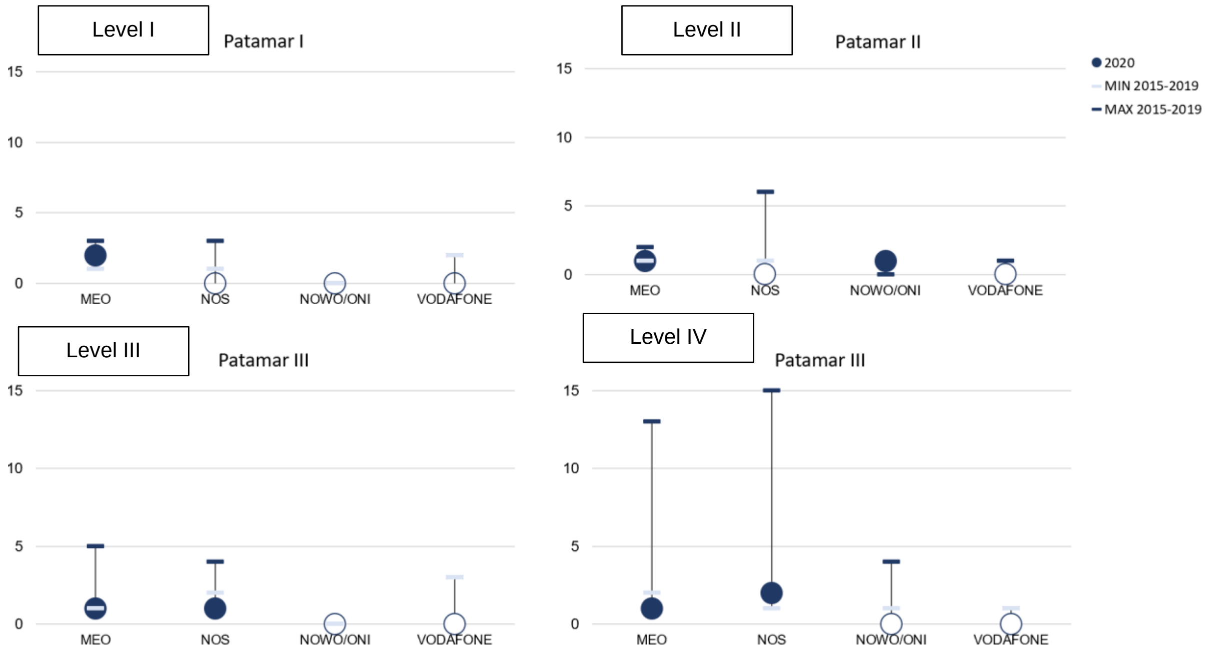
Duration and	Number of subscribers or accesses affected (or, pursuant to [2e] of this article, geographic area affected)	Level
≥ 30 minutes	number of subscribers or accesses affected ≥ 500,000 (or, pursuant to Point I [4e], geographic area affected ≥ 3,000 km$_2$)	**I**
≥ 1 hour	500,000 > number of subscribers or accesses affected ≥ 100,000 (or, pursuant to Point I [4e], 3,000 km$_2$ > geographic area affected ≥ 2,000 km$_2$)	**II**
≥ 2 hours	100,000 > number of subscribers or accesses affected ≥ 30,000 (or, pursuant to Point I [4e], 2,000 km$_2$ > geographic area affected ≥ 1,500 km$_2$)	**III**
≥ 4 hours	30,000 > number of subscribers or accesses affected ≥ 10,000 (or, pursuant to Point I [4e], 1,500 km$_2$ > geographic area affected ≥ 1,000 km$_2$)	**IV**

Source: ANACOM, Security Regulation no. 303/2019

In most cases, information on a given security incident is not only important to the subscribers directly affected, but also to all other users who were unable to communicate with them.

Of the 27 security incidents received in 2020 falling within the levels, nine had the obligation of information to the public, including two at level I, two at level II, two at level III and three at level IV. A comparison of the results with the maximum and minimum of the 2015-2019 period is shown in Graph 17.

Graph 17 – Security incidents covered by the obligation of disclosure to the public by companies in 2020, compared to the period of 2015-2019.



Unit: Security incidents

Source: ANACOM

Pursuant to Article 24 (1c) of Security Regulation no. 303/2019, the information must be provided as soon as possible, within a maximum of four hours following the initial notification to ANACOM.

The means by which companies must provide information to the public should be, at minimum, the websites employed in their relationship with the users of their networks and services, through a link, immediately visible and identifiable without scrolling, posted at the website's homepage, pursuant to (1b). Furthermore, this information must remain publicly accessible for 20 working days following the end date of the security breach or loss of integrity. Note that this information has been duly provided by the companies to the public.

In the case of Public Security Service Posts, no information is provided to the public from the website, since 112 Service Centers are the responsibility of the Ministry of Internal Administration (MAI).

ANACOM AUTORIDADE NACIONAL DE COMUNICAÇÕES

anacom.pt

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

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

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

Public attendance
800206665
info@anacom.pt