REPORT ON SECURITY BREACHES OR LOSS OF INTEGRITY 2019

ANACOM
AUTORIDADE NACIONAL DE COMUNICAÇÕES

REPORT ON SECURITY BREACHES OR LOSS OF INTEGRITY

2019

ANACOM
AUTORIDADE NACIONAL DE COMUNICAÇÕES

ANACOM AUTORIDADE NACIONAL DE COMUNICAÇÕES

Annual Report

of

Security Breaches or Losses of Integrity

for

.

2019

1 Introduction

This report presents an aggregated analysis of the information contained in notifications of security breaches or losses of integrity with a significant impact (hereinafter called "notifications", thus encompassing initial, end-of-significant impact and final notifications sent by companies which offer public communications networks or publicly accessible electronic communications services to the Autoridade Nacional de Comunicações (ANACOM) in 2019. It also plots the evolution seen since 2015, and sometimes since 2018.

The main aspects that we should highlight from the analysis of the 2019 data are:

- **The total number of security incidents notified was 80, while in 2018 there were 113 incidents;**
- **A total of 12.4 million affected subscribers/accesses were recorded, compared to 2.4 million in 2018. In March, May and October 2019, the monthly amount exceeded 2 million;**
- **The baseline for the number of affected subscribers/accesses, corresponding to the lowest level of severity, was the most common among the reported security incidents (19), while the baseline relating to the highest level was the second (6).**
- **The average annual duration for the impact of security incidents relating to the affected subscribers/accesses was 24 hours;**
- **15 security incidents were covered by the obligation of disclosure to the public;**
- **The number of security incidents notified in relation to access to Public Security Service Points (112 Service Centres) was 31, corresponding to 39%;**
- **ANACOM reported 8 security incidents to ENISA which exceeded the EU-wide threshold, based on the duration of an incident and the relative number of affected subscribers/accesses.**

In terms of the provisions of article 54-B of Law 5/2004 of 10 February, in its current wording (hereinafter "Electronic Communications Law"), all companies which 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.

For this purpose, through its determination[1] of 12 December 2013, ANACOM approved measures that defined the circumstances, the format and the procedures applicable to the requirements for communicating security breaches or losses of integrity (hereinafter "security incident") with a significant impact on the functioning of networks and services (ANNEX A) and disclosure to the public by companies of security incidents on their networks and services (ANNEX B). This determination sets the criteria and respective impact thresholds that companies, if a security incident occurs, should consider when sending the respective notifications, for example: regarding the combination between, on the one hand, the number of subscribers/accesses affected or the size of the affected geographic area and, on the other hand, the duration of the impact[2] or regarding the duration of the period for which the delivery to the Public Security Service Points (112 Service Centres) of calls to the single European emergency number 112 is directly or indirectly affected.

This determination remained in force in 2019; however, on 1 April of that year, in Series II of the Official Gazette, Regulation 303/2019 was published on the security and integrity of electronic communications, approved by ANACOM's final decision of 14 March 2019. Under article 37 of the same, ANACOM's 2013 decision, mentioned above, is only revoked on 1 April 2020.

As in previous years, in 2019, 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[3].

Also in 2019, ANACOM reported 8 security incidents to ENISA, which exceeded the EU-wide threshold, based on the duration of an incident and the relative number of affected subscribers/accesses, compared with 5 security incidents in 2018.

[1] As per the determination of 12 December 2013, ANACOM's Board of Directors approved the decision regarding the circumstances, the format and the procedures applicable to the requirements for communicating security breaches or losses of integrity with a significant impact on the functioning of networks and services by companies which offer public communications networks or publicly accessible electronic communications services (article 54-C (2) and article 54-B of the Electronic Communications Law (ECL)), and also disclosure to the public by companies which offer public communications networks or publicly accessible electronic communications services, of security breaches or losses of integrity with a significant impact on the functioning of networks and services (article 54-E (b) of the ECL). Available at https://www.anacom.pt/render.jsp?contentId=1185455.

[2] Regarding these two criteria, the respective impact thresholds are divided into a set of levels. One is sufficient for the company to proceed with sending the respective notifications to ANACOM.

[3] 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

2 Analysis

As a result of the 2019 activity analysis, we highlight the occurrence of security incidents that exceeded the highest significant impact threshold established by point I (3a) of Annex A to the ANACOM Determination, together with incidents that directly or indirectly affected the delivery to the Public Security Service Points (112 Service Centres) of calls to the single European emergency number 112.

Additionally, we highlight the main trends over the 2015-2019 period, in terms of 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.

It was also highlighted that, with regard to communications security supervisory actions, ANACOM in 2019 held meetings for a more detailed analysis with teams from each of the companies that notified it of security breaches or losses of integrity during 2018 and 2019 in order to obtain supplementary information and improve information processes.

2.1 Number of Security Incidents Notified

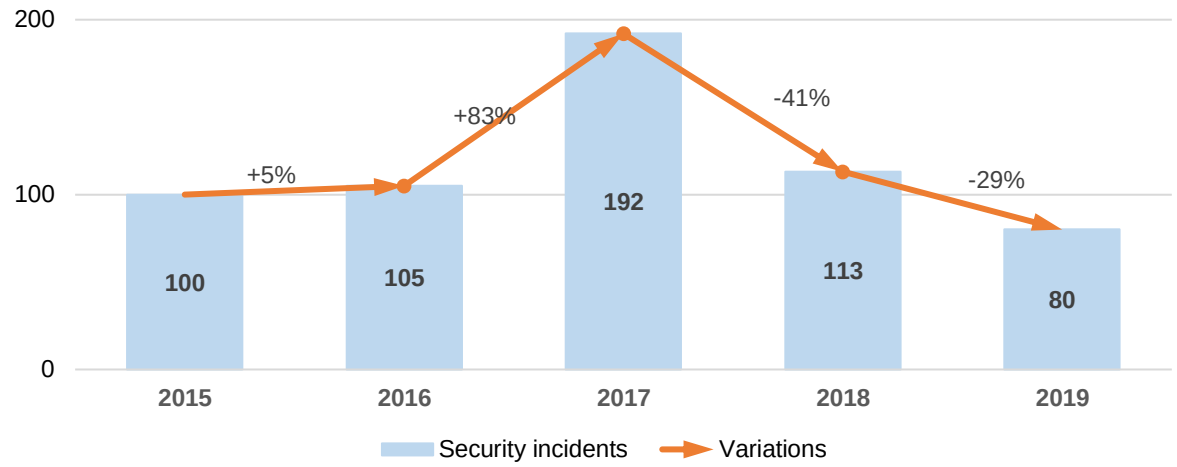
In 2019, the companies, as a whole, notified ANACOM of 80 security incidents.

This was the lowest figure recorded since 2015. During the 2015-2019 period, the companies notified a total of 590 security incidents, recording: 100 incidents in 2015, 105 in 2016, 192 in 2017, 113 in 2018 and, as stated, 80 in 2019 (graph 1).

Graph 1 clearly shows that there was an initial rising trend in the annual number of security incidents notified. The peak was reached in 2017 (the year in which the devastating forest fires struck Portugal). A sharp fall has been recorded in the last two years.

More precisely, a reduction of 41% was recorded in 2018 compared to 2017 and a reduction of 29% in 2019 compared to 2018.

Graph 1 – Annual number of security incidents notified during the 2015-2019 period.

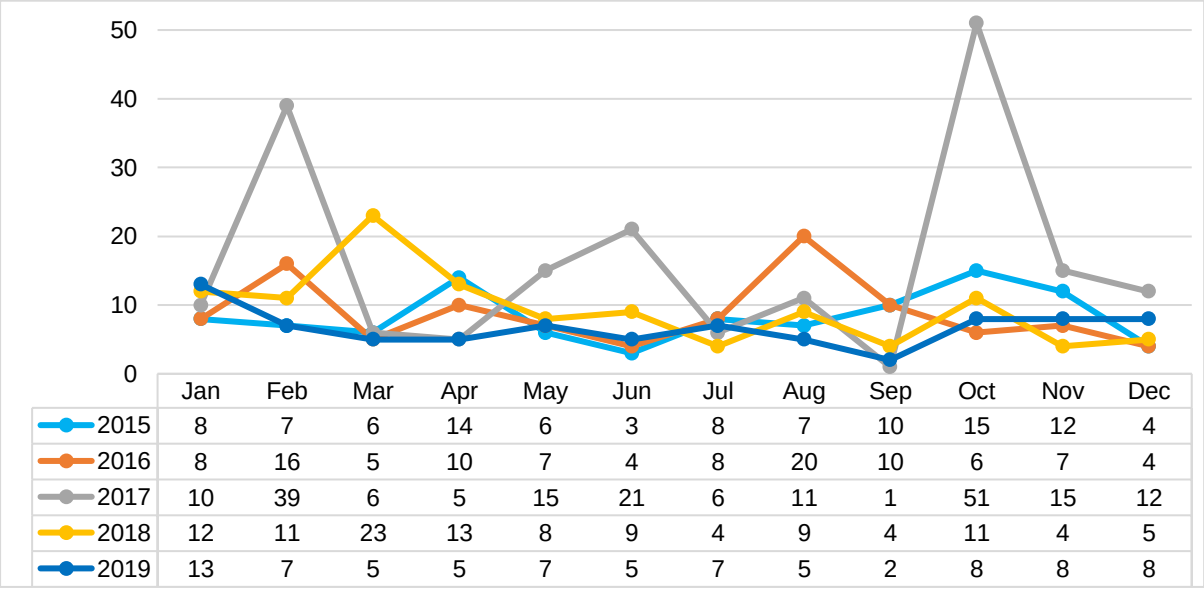


Unit: number of security incidents

Source: ANACOM

Besides the annual figure for security incidents which were notified to ANACOM, it is also important to consider the monthly figures recorded in each of these years in order to identify aspects relating to seasonality, in particular due to natural phenomena, which can be seen in graph 2 and in Tables 1 and 2.

Graph 2 – Monthly figures for security incidents notified in the 2015-2019 period.



	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
2015	8	7	6	14	6	3	8	7	10	15	12	4
2016	8	16	5	10	7	4	8	20	10	6	7	4
2017	10	39	6	5	15	21	6	11	1	51	15	12
2018	12	11	23	13	8	9	4	9	4	11	4	5
2019	13	7	5	5	7	5	7	5	2	8	8	8

Unit: number of security incidents

Source: ANACOM

Thus in 2019, the highest figure was recorded in January, with 13 incidents, while the lowest was in September, with 2 incidents. As indicated above, the highest figures for security

incidents notified were recorded in 2017, with 39 notifications in February, 21 in June and 51 in October.

From these data, we created two tables, Table 1 and Table 2, in which the quarterly figures are aggregated. Table 1 corresponds to the 2015-2019 period and Table 2 refers to 2019.

Table 1 – Quarterly figures for number of security incidents notified in the 2015-2019 period.

2015-2019	1Q	2Q	3Q	4Q
Quarterly Total	176	132	112	170
% of Incidents reported per Quarter	30	22	19	29

Unit: number of security incidents
Source: ANACOM

Table 2 – Quarterly figures for number of security incidents notified in 2019.

2019	1Q	2Q	3Q	4Q
Quarterly Total	25	17	14	24
% of Incidents reported per Quarter	31	21	18	30

Unit: number of security incidents
Source: ANACOM

It was also confirmed that, during the 2015-2019 period, the 1st quarter (176; 30%) and the 4th quarter (170; 29%) had the highest number of security incidents notified, corresponding to 59% of all security incidents notified.

In particular, in 2019, the 1st and 4th quarters combined corresponded to 61% of the security incidents notified.

In summary, the figures for the number of security incidents shows aspects of seasonality with higher figures in the 1st and 4th quarters and lower figures in 2nd and 3rd quarters.

2.2 Root cause

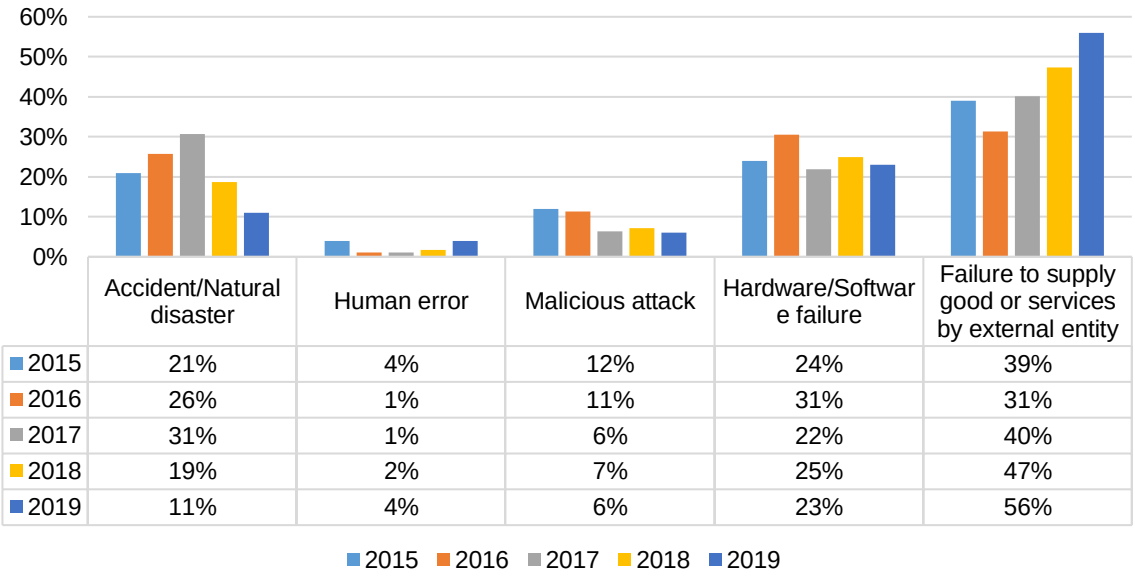
The root causes established by ANACOM's 2013 determination are as follows:

- 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 – due to technical system failure, in its physical (hardware) and/or logical (software) components;
- Failure in the supply of goods or services by an external entity – due to a break in the supply of goods or services, such as the supply of electricity or leased lines.

Graph 3 details, in percentage terms and by root cause, the security incidents that were notified in the five years under analysis. Failure in the supply of goods or services by an external entity was the main root cause.

Graph 3 – Security incidents notified during the 2015-2019 period by root cause.



	Accident/Natural disaster	Human error	Malicious attack	Hardware/Software failure	Failure to supply good or services by external entity
2015	21%	4%	12%	24%	39%
2016	26%	1%	11%	31%	31%
2017	31%	1%	6%	22%	40%
2018	19%	2%	7%	25%	47%
2019	11%	4%	6%	23%	56%

Unit: % of security incidents

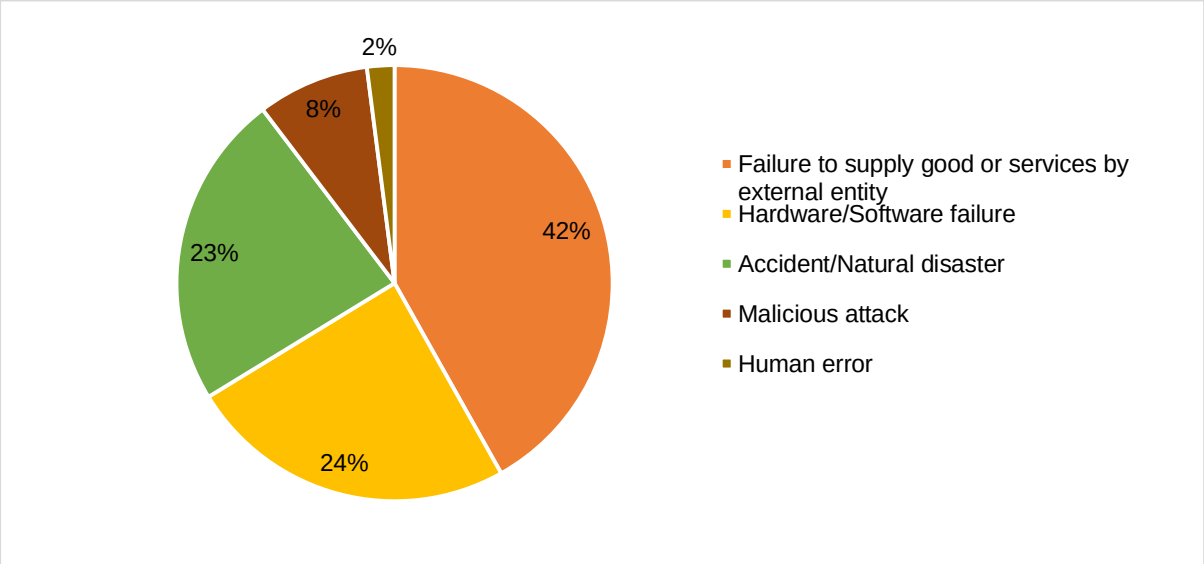
Source: ANACOM

As in recent years, in 2019, it was observed that most security incidents recorded were due to failure in the supply of goods or services by an external entity. The majority were failures in electricity supply, some of which, in turn, were the consequence of adverse weather phenomena. These same phenomena also resulted in incidents with the accident/natural disaster root cause, in third place this year. We should also highlight hardware/software failures, which represented almost a quarter of the total security incidents notified.

Regarding the root cause – Malicious attacks showed a slight fall. However, there was a slight increase in the number of security incidents with human error as their root cause compared to recent years. The number of incidents caused by accident/natural disaster fell considerably.

In these five years, the three main root causes were, in descending order (graph 4): failure in the supply of goods or services by an external entity, especially failures in electricity supply (42%, corresponding to 247 security incidents with this root cause from a total of 590 security incidents notified during this period), hardware/software failure (24%, 144 of 590) and accident/natural disaster, especially storms or forest fires (23%, 138 of 590).

Graph 4 – Percentage of number of security incidents notified in the 2015-2019 period for each root cause.



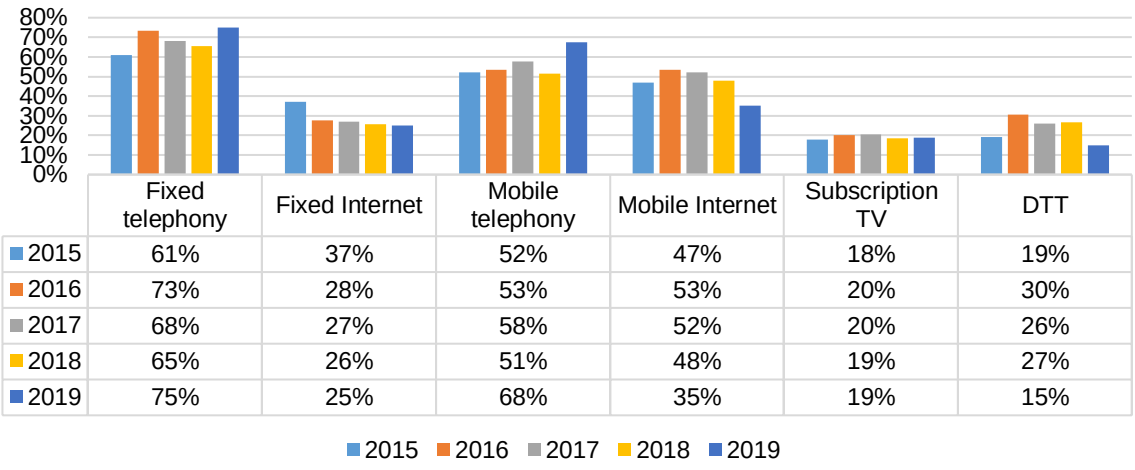
Unit: % of security incidents

Source: ANACOM

2.3 Impact on service

For the purposes of analysing the security incidents in terms of the respective impact on electronic communication services, namely: fixed and mobile telephony, fixed and mobile Internet, subscription television and digital terrestrial television (DTT), the situation in graph 5 shows the details in percentage terms of security incidents notified by service affected during the last five years.

Graph 5 – Percentage of security incidents notified for each type of service affected in the 2015-2019.



	Fixed telephony	Fixed Internet	Mobile telephony	Mobile Internet	Subscription TV	DTT
2015	61%	37%	52%	47%	18%	19%
2016	73%	28%	53%	53%	20%	30%
2017	68%	27%	58%	52%	20%	26%
2018	65%	26%	51%	48%	19%	27%
2019	75%	25%	68%	35%	19%	15%

Unit: % of security incidents

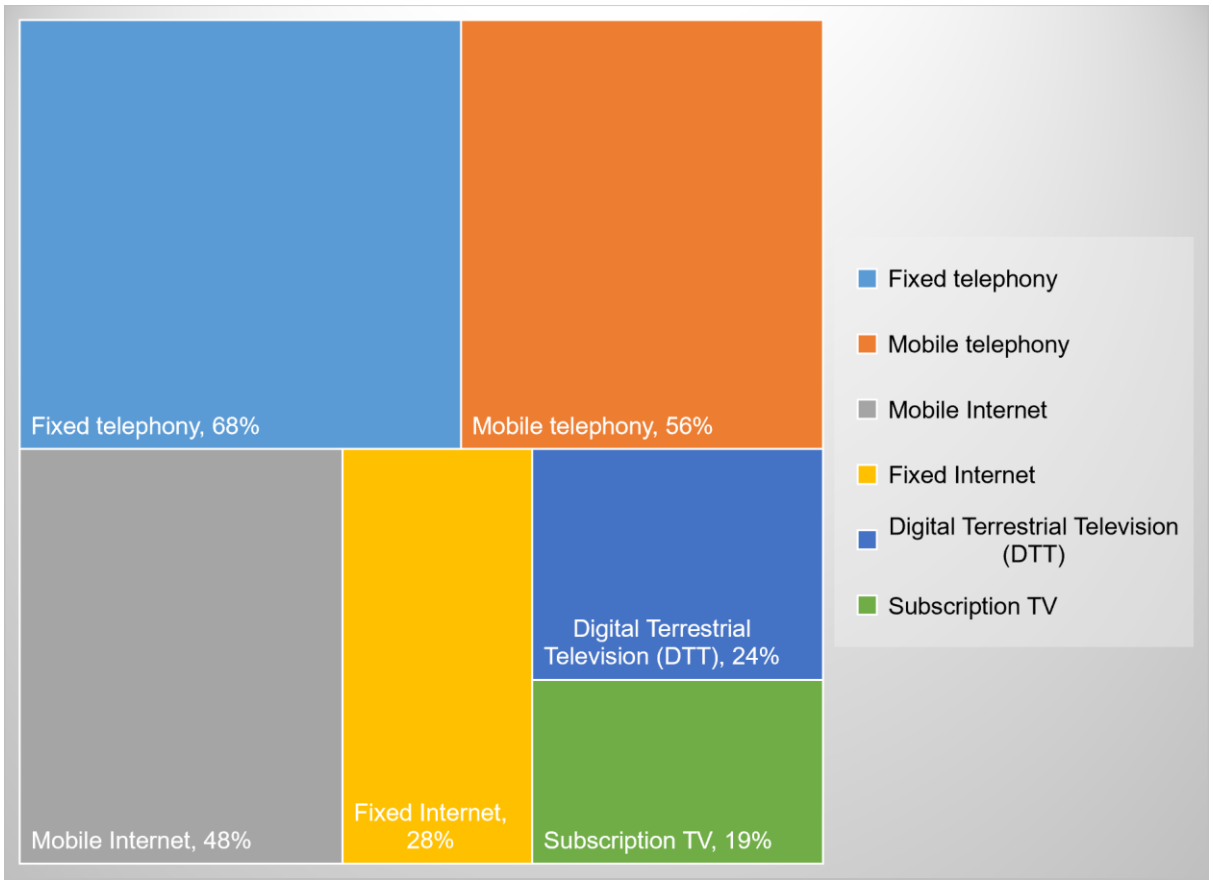
Source: ANACOM

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

It should be noted that the majority of notifications had an impact on two or more publicly available electronic communications services, with the result that the annual sum of percentages for each of the affected services was over 100%. In 2019, we thus had: for fixed Telephony **–** 75%, for fixed Internet **–** 25%, for mobile Telephony **–** 68%, for mobile Internet **–** 35%, for subscription TV **–** 19% and, finally, for Digital Terrestrial Television (DTT) **–** 15%.

According to the notifications 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 2019, this service was affected in 75% of the security incidents notified.

Graph 6 – Average percentage of security incidents notified in the 2015-2019 period for each type of service affected.



Unit: % of security incidents

Source: ANACOM

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

In these five years, the three services most affected were, in descending order (graph 6): fixed telephony (68%), mobile telephony (56%) and mobile Internet (48%). Fixed Internet, DTT and subscription TV services were respectively affected in 28%, 24% and 19% of the notifications received.

2.4 Circumstances and respective impact

In accordance with the 2013 determination, the circumstances which gave rise to the security incidents notified were, *inter alia*, the following:

a) Number of subscribers/accesses affected and respective duration of significant impact, a criterion that is subdivided into 6 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;

c) Effect on the supply from all networks and services offered by a company in the entire territory of an island in the Autonomous Regions of the Azores or Madeira, with a duration of 30 minutes or more.

Table 3 shows in absolute and percentage terms the security incidents notified in 2018 and 2019 by the circumstances which gave rise thereto.

Table 3 – Absolute and percentage figures for security incidents notified in 2018 and 2019 by circumstance.

	Subscribers/Accesses		112		Islands		Others		Total	
	A.F.	%	A.F.	%	A.F.	%	A.F.	%	A.F.	%
2018	91	81	13	12	3	3	6	5	113	100
2019	39	49	31	39	8	10	2	2	80	100

Unit: number of security incidents in absolute figures (A.F.) and percentage (%)

Source: ANACOM

In 2019, the most common notification circumstance was the number of subscribers/accesses affected, 39 incidents, corresponding to 49%; in 2018, the figure was 91 incidents, corresponding to 81%. The effect on delivery to Public Security Service Posts (112 Service Centres) recorded 31 incidents, corresponding to 39%.

2.4.1 Subscribers or accesses affected

Table 4 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 in terms of a particular minimum impact duration and of an interval between the minimum and maximum number of subscribers or accesses affected.

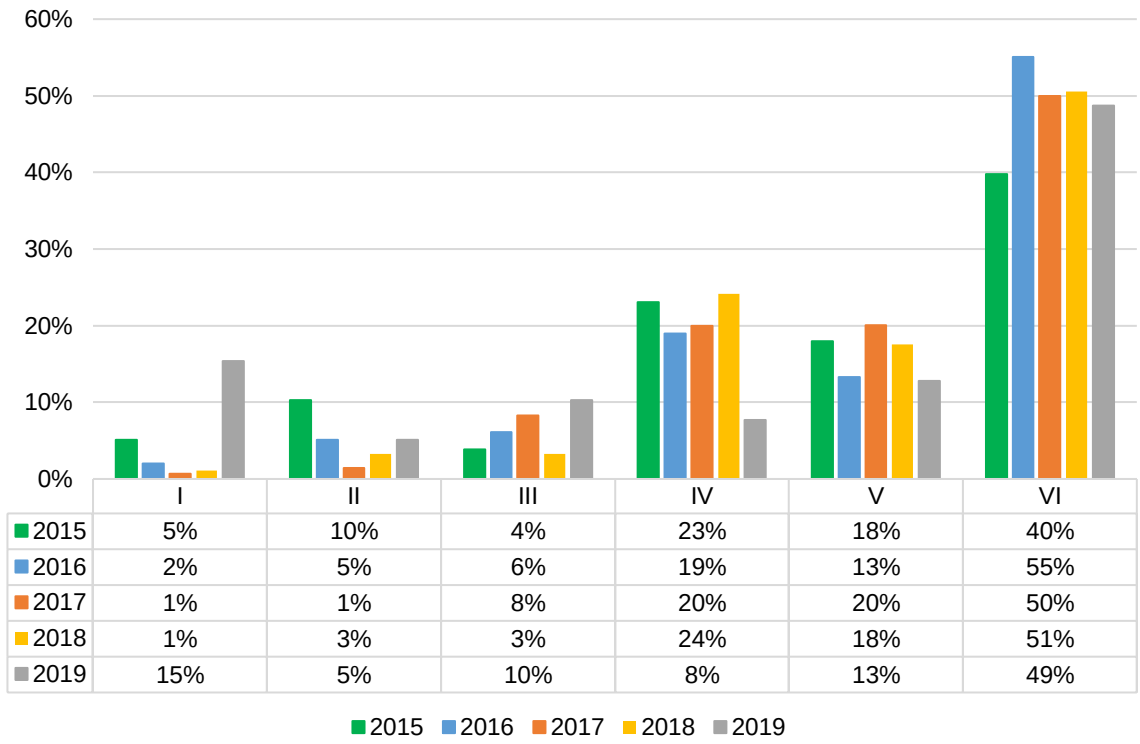
Table 4 – Impact levels on subscribers/accesses.

Level	Duration	Number of subscribers or accesses affected
I	**≥ 30 minutes**	Number of subscribers/accesses ≥ 500,000
II	**≥ 1 hour**	500,000 > Number of subscribers/accesses ≥ 100,000
III	**≥ 2 hours**	100,000 > Number of subscribers/accesses ≥ 30,000
IV	**≥ 4 hours**	30,000 > Number of subscribers/accesses ≥ 10,000
V	**≥ 6 hours**	10,000 > Number of subscribers/accesses ≥ 5,000
VI	**≥ 8 hours**	5,000 > Number of subscribers/accesses ≥ 1,000

Source: ANACOM, 2013 determination

Graph 7 shows the number of security incidents notified relating to the 2015-2019 period, distributed over each of the abovementioned levels. For each level the percentage figure is shown for the security incidents notified in each year due to this circumstance. Table 3 reveals that in 2018 the number of security incidents notified due to the number of subscribers/accesses affected was 91 and in 2019 it was 39.

Graph 7 – Security incidents notified for each level of impact on subscribers/accesses during the 2015-2019 period, in percentages.



	I	II	III	IV	V	VI
2015	5%	10%	4%	23%	18%	40%
2016	2%	5%	6%	19%	13%	55%
2017	1%	1%	8%	20%	20%	50%
2018	1%	3%	3%	24%	18%	51%
2019	15%	5%	10%	8%	13%	49%

Unit: % of security incidents

Source: ANACOM

We highlight the relative weight of the lower levels IV, V and VI because, as expected, these recorded the highest number of notifications (an annual average of 84% of the total notifications at the different levels).

This interpretation of the data may be misleading, however, especially when the affected areas are larger and have lower population densities, which is typical in rural or forest areas frequently affected by forest fires.

In 2019, a significant and unusual rise was seen at level I, with an unprecedented figure of 15%, corresponding to the maximum figure for this criterion, and a slight fall in level IV

compared to the previous years. As we shall see below, the rise at level I was essentially due to security incidents which happened in March, May and October.

The assessment of the impact of the security incidents on the subscribers/accesses is made, under this criterion, by combining the number of subscribers or accesses affected (subscriber/access) and the time from when the impact became significant, to reach one of the levels shown in Table 4.

For each security incident notified the number of subscribers or accesses affected corresponds to the sum of the subscribers or accesses that are affected by the same security incident on the different networks and services, regardless of the duration of the incident.

For each month the number of subscribers or accesses affected in that month corresponds to the sum of the subscribers or accesses that are affected by security incidents notified for which the initial notification was received in that month.

We have designated the accumulated amount as the total number of subscribers/accesses in that month as the monthly figure calculated in accordance with the two preceding paragraphs.

Table 5 shows for each month the number of security incidents due to the circumstance of the number of affected subscribers/accesses and the cumulative monthly figure for the total number of affected subscribers/accesses for 2018 and 2019. As per Table 3, there were 91 in 2018 and 39 in 2019.

Table 5 – Security incidents notified due to the circumstance of the number of subscribers/accesses affected in each month in 2018 and 2019.

	2018		2019	
	Number of security incidents	Number of subscribers/accesses	Number of security incidents	Number of subscribers/accesses
January	9	64,073	3	38,960
February	7	69,928	5	49,943
March	17	91,875	3	2,999,001
April	10	76,519	2	505,000
May	6	734,382	4	2,833,573
June	8	28,268	2	503,380
July	3	453,204	2	5,091
August	8	52,516	4	173,249
September	4	90,024	2	4,561
October	10	652,152	6	4,601,557
November	4	52,895	3	76,917

December	5	46,411	3	574,858
Total	**91**	**2,412,247**	**39**	**12,366,090**

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

Source: ANACOM

In terms of annual variations from 2018 to 2019, we observe that the total number of security incidents due to the number of subscribers/accesses affected fell from 91 to 39 (a reduction of nearly 57%) and, simultaneously, there was an increase in the total number of subscribers/accesses affected from nearly 2.4 million to a total of around 12.4 million (an increase of around 513%).

In fact, in 2019, the figures recorded in March, May and October were due to security incidents which had an impact at the national level. Security incidents took place during these months, some of which are included in level I, the highest impact level for this circumstance, which in these cases were especially due to:

- in March due to a hardware/software failure;
- in May due to human error;
- in October due to a hardware/software failure and malicious attack.

Thus in 2019, for a total number of 39 security incidents notified due to circumstance of the number of subscribers/accesses affected, as per Table 3, the impacts by root cause were as follows (Table 6). Table 6 also shows the figures for 2018:

Table 6 – Number of subscribers/accesses affected by root cause in 2018 and 2019.

	2018		**2019**	
Root cause	**Number of subscribers/accesses**	**%**	**Number of subscribers/accesses**	**%**
Accident/Natural Disaster	574,347	24	157,675	1
Human error	431,500	18	3,315,557	27
Malicious attack	29,052	1	519,721	4
Hardware/software failure	1,004,466	42	7,823,158	63
Failure in the supply of goods or services by external entity	372,882	15	549,979	4
TOTAL	**2,412,247**	**100**	**12,366,090**	**100**

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

In 2019, the security incidents notified due to hardware/software failure root cause had the greatest impact in terms of the number of subscribers/accesses affected, at around 8 million (63%). The corresponding figure for 2018 was 1 million (42%). The security incidents caused by human error in 2019 affected around 3 million (27%), while in 2018 the number was around 432,000 (18%).

Besides the total number of subscribers/accesses affected each year, it is also important to analyse the annual duration of the impact caused by security incidents which occurred in that year (annual impact duration) and the average duration of security incidents during that year (average annual impact duration). This last figure allows us to get an approximate idea of the recovery time for security incidents.

Thus, the annual impact duration is the result of the sum of the period between the beginning of the incident and the end of the impact of the same for all security incidents that occurred during the year due to this circumstance.

The average annual impact duration is calculated from the annual impact duration divided by the number of security incidents in the year.

Table 7 shows the figures for 2018 and 2019 regarding the annual impact duration and average annual impact duration.

Table 7 – Annual impact duration and average annual impact duration.

Year	Annual impact duration (hours)	Average annual impact duration (hours)
2018	2,808	31
2019	937	24

Unit: hours
Source: ANACOM

In 2019, the total impact duration was 937 hours. In 2018, this figure was 2,808 hours, which corresponds to a 67% reduction. In 2018, there were long-lasting security incidents which caused the enormous annual impact duration for that year. Such a situation has not yet been recorded in 2019.

Consequently, as regards the average annual impact duration, the change from 2019 to 2018 was from 31 to 24 hours, which corresponded to a 23% reduction. This change reflected an improvement in recovery time.

Under the provisions of ANNEX B of the 2013 determination, in 2019 15 security incidents were covered by the obligation of disclosure to the public, corresponding to: 6 at level I, 2 at level II, 4 at level III, 3 at level IV. Table 8 shows their distribution by company:

Table 8 – Security incidents covered by the obligation of disclosure to the public.

	Level I	Level II	Level III	Level IV
Altice Portugal	1	1	2	2
NOS Comunicações	3	-	2	1
Vodafone Portugal	2	1	-	-
Total	6	2	4	3

Unit: security incidents

Source: ANACOM

2.4.2 Calls to 112 emergency number

Under the 2013 determination, the companies notified ANACOM of security incidents that directly or indirectly affected the delivery to the Public Security Service Points (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 obviously cannot make any successful calls, either to 112 emergency or any other number.

Table 9 was constructed from Table 3, limiting it to the security incidents notified in relation to the circumstance of calls to 112 and to the total.

Table 9 – Security incidents notified relating to 112 calls.

	112		Total	
	A.F.	%	A.F.	%
2018	13	12	113	100
2019	31	39	80	100

Unit: number of security incidents in absolute figures (A.F.) and percentage (%)

Source: ANACOM

Regarding this circumstance, in 2019, of the 80 security incidents notified, 31 recorded an impact on the Public Security Service Points (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 significantly from 2018 to 2019, in numbers from 13 to 31 and, principally, in percentage terms from 12% to 39%.

3 2019 Summary

In 2019, the analysis of information regarding notifications of security incidents with a significant impact that the companies communicated to ANACOM reveals in summary the following aspects:

- The total number of security incidents notified was 80, corresponding to a fall of 29% compared to 2018 (graph 1);
- The highest number of security incidents notified was 13 in January. The lowest figure was 2, in September (graph 2);
- The 1st and 4th quarters recorded the largest number of security incidents notified, together accounting for 61% (Table 2);
- A failure in the supply of goods or services by external entity is the most common root cause, corresponding to 57% (graph 3);
- Fixed telephony was the service most frequently affected with 75% of the total of security incidents notified. Mobile telephony corresponded to 68% (Note: most incidents notified generally have an impact on more than one service) (graph 5);
- Hardware/software failure is the root cause with the greatest impact in terms of the number of subscribers/accesses affected, corresponding to 63%, followed by human error, which corresponds to 27%;
- The most frequent notification circumstance is the number of subscribers/accesses affected at 39 incidents, corresponding to 49%. In second place was the effect on the delivery of calls to 112 at 31 incidents, corresponding to 39% (Table 3);
- The security incidents notified due to the number of subscribers/accesses at level VI were the most common, corresponding to 49%. However, a significant and unusual rise was seen at level I (level of highest impact), with an unprecedented figure of 15%, which was the second most notified (graph 7);
- The total number of subscribers/accesses affected was close to 12.4 million, while in 2018 this figure was around 2.4 million, corresponding to an increase of 513% (Table 5);

- The figures recorded in March (3 million), May (3 million) and October (4.6 million) were due to security incidents which had an impact at the national level (Table 5);

- The security incidents notified due to hardware/software failure root cause had the greatest impact in terms of the number of subscribers/accesses affected, at around 8 million (63%). In second place were security incidents caused by human error, at around 3 million (27%) (Table 6);

- The annual impact duration was 937 hours. In 2018, this figure was 2,808 hours, which corresponds to a 67% reduction (Table 7);

- 15 security incidents were covered by the obligation of disclosure to the public (Table 8);

- As regards the average annual impact duration, the change from 2019 to 2018 was from 31 to 24 hours, which corresponded to a 23% reduction (Table 9);

- 31 security incidents were notified due to their effect on access to the Public Security Service Points (112 Service Centres), which corresponded to 39% of the total incidents (Table 9);

- ANACOM reported 8 security incidents to ENISA, which exceeded the EU-wide threshold, based on the duration of an incident and the relative number of affected subscribers/accesses, compared with 5 security incidents in 2018;

4 2019 Highlights

Main aspects to highlight from 2019:

- The total number of security incidents notified was 80, while in 2018 there were 113 incidents;
- A total of 12.4 million affected subscribers/accesses were recorded, compared to 2.4 million in 2018. In March, May and October 2019, the monthly amount exceeded 2 million;
- The baseline for the number of affected subscribers/accesses, corresponding to the lowest level of severity, was the most common among the reported security incidents (19), while the baseline relating to the highest level was the second (6).
- The average annual duration for the impact of security incidents relating to the affected subscribers/accesses was 24 hours;
- 15 security incidents were covered by the obligation of disclosure to the public;
- The number of security incidents notified in relation to access to Public Security Service Points (112 Service Centres) was 31, corresponding to 39%;
- ANACOM reported 8 security incidents to ENISA which exceeded the EU-wide threshold, based on the duration of an incident and the relative number of affected subscribers/accesses.

These situations were analysed individually in great detail, resulting in supervisory actions within the scope of ANACOM's powers.

ANACOM

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

Açores
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

Atendimento ao Público
Public Attendance
800206665
info@anacom.pt

www.anacom.pt