ANCOM
National Authority for Management and
Regulation in Communications of Romania

2 Delea Noua Street, Bucharest 3, 030925,Romania
Phone: +40 372 845 400 / +40 372 845 454. Fax: +40 372 845 402
E-mail: ancom@ancom.org.ro. Website: www.ancom.org.ro

# Report
# on the incidents that affected the security and the integrity of the electronic communications networks and services in 2012

**Contents**

## 1. Introduction

For the purpose of ensuring a reliable and safe communications system by means of electronic communications networks, according to the provisions of Art. 46 of the Government Emergency Ordinance no. 111/2011 on electronic communications approved, with amendments and completions, by law no. 140/2012, the providers of public electronic communications networks or of publicly available electronic communications services must adopt and implement all the adequate technical or organizational measures, for the purpose of managing the risks related to the security and integrity of electronic communications networks and services. For the purpose of this report, the security and integrity of electronic communications networks and services means the ability of a network or electronic communication service to resist accidental events or malicious actions that can compromise the continuity of the provision of networks and services, at a performance level equivalent to that preceding the occurrence of the event.

Moreover, according to the provisions of Art. 47(1) of the Government Emergency Ordinance no. 111/2011, "*(1) The providers of public electronic communications networks or of publicly available electronic communications services have the obligation to notify ANCOM, within the shortest term, on all the breaches of security or loss of integrity that have a significant impact on the provision of networks or services*".

The data regarding the incidents are fundamental to the development of a clear understanding of the nature and extent of the existing challenges to network and services security and integrity. Having analyzed the incidents, ANCOM may follow the effectiveness of the security measures adopted by the providers, as well as of their response to incident occurrence, may collect data regarding the types of threats and vulnerabilities to be used within a furthered analysis of the network and service security, constituting a basis for the issuance of recommendations and best practice guidelines.

## 2. Reporting incidents that affected the security and integrity of electronic communications networks and services in 2012

For the purpose of evaluating the incidents that affected the security and integrity of the networks or services, in January 2013, ANCOM transmitted to the providers of electronic communications networks and services a questionnaire regarding the incidents with significant impact on the security and integrity of electronic communications networks and services in 2012. An incident with significant impact is an incident that affects a number higher than 5,000 connections for at least an hour. The questionnaire is included in Annex 1 to this report and was sent to all the providers reporting the provision of a number of connections higher than 5,000 connections, as of 30 June 2012.

Thus, ANCOM requested information regarding:

- date and hour when the incident occurred, respectively when the incident was detected;
- the service/services whose provision was affected by the incident;
- total number of connections affected by the incident, by service;
- resources/equipment affected by the incident;
- incident duration;
- geographical region affected by the incident;
- impact on emergency calls;
- incident description;
- type of incident cause;
- further cause-related information;
- response actions;
- steps taken or planned in order to prevent a similar incident/remove the incident cause;
- other providers of electronic communications networks and services affected.

44 providers of electronic communications networks and services answered the ANCOM request (totaling more than 90% of the electronic communications market in terms of the revenues registered in 2012). 10 providers reported 165 incidents that affected a number of connections higher than 5,000 for at least 60 minutes in 2012 and 34 providers reported not having registered incidents that would match the specified terms.

## 3. Analysis of the reported incidents

The 165 incidents reported by the 10 providers of public electronic communications networks or of publicly available electronic communications services have been consolidated, itemized and subsequently analyzed from 4 standpoints:

1. Impact on services and users:
   - Connections affected,
   - Services affected,
   - Resources affected.
2. Causes of the reported incidents,
3. Duration of incidents and duration until the detection of the incident,
4. Impact on emergency calls.

Most reported incidents belong to the category external cause/third party. Most of the 64 incidents in this category were caused by the interruptions in the electricity supply network and to the accidental sectioning of cables by third parties.

61 incidents belong to the category „System failure”, and were caused mainly by software errors and hardware failures that affected BTS, servers, switch centers etc.

13 of the reported incidents were caused by malicious actions. All these are owed to copper cable theft and to fiber optic vandalizing. In most cases, these incidents affected the fixed telephone services and the internet access through permanent connections provided at fixed locations.

In 2012, 22 incidents caused by natural phenomena that triggered interruptions in the electricity supply were reported.

### 3.1Impact on services and users

The average number of connections affected by an incident, in 2012, is 72,224.

Figure 1 shows the number of connections affected per service. One can notice the fact that SMS data transmission services were the most affected in 2012.

We must emphasize the fact that the figures regarding the affected connections are estimations, since some providers either did not provide exact data regarding the number of connections affected, specifying only that certain services were affected, or specified that more than 5,000 connections were affected.

**Figure 1 Number of affected connections per service**

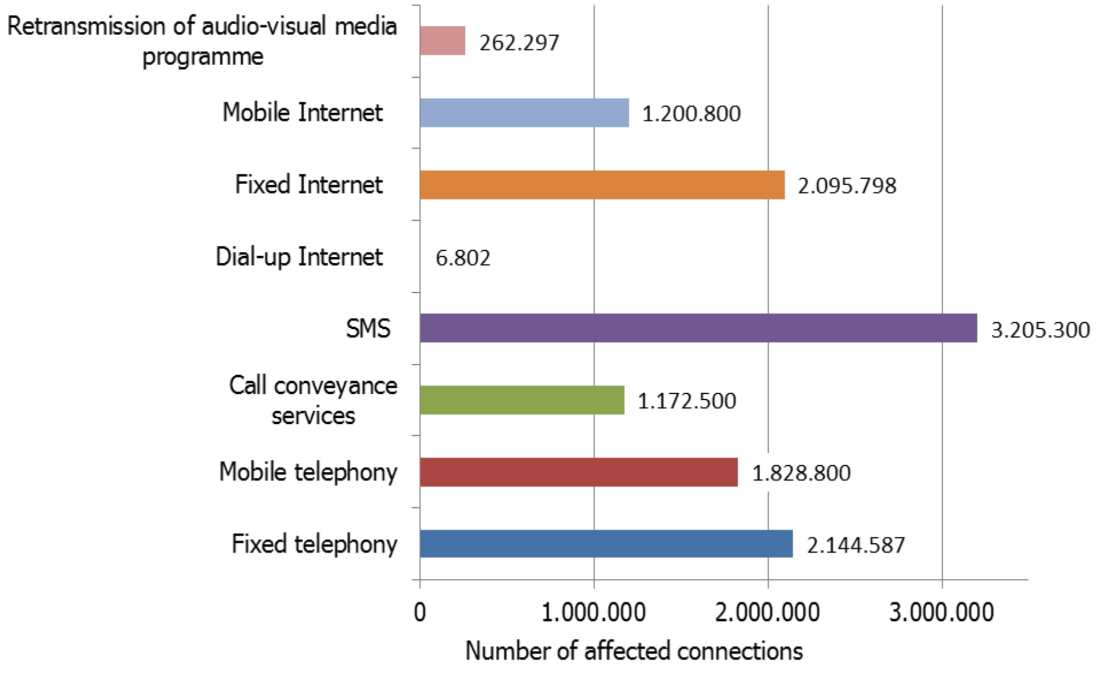


Figure 2 shows the number of incidents that affected each service. Note: some incidents affect one or several services.

**Figure 2 Impact on services**

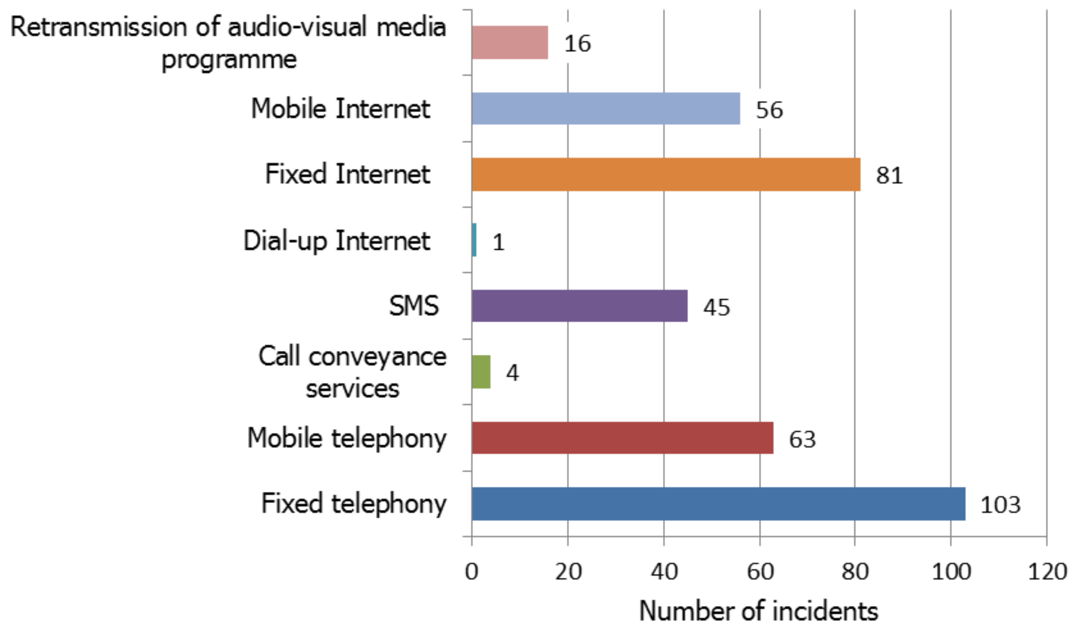
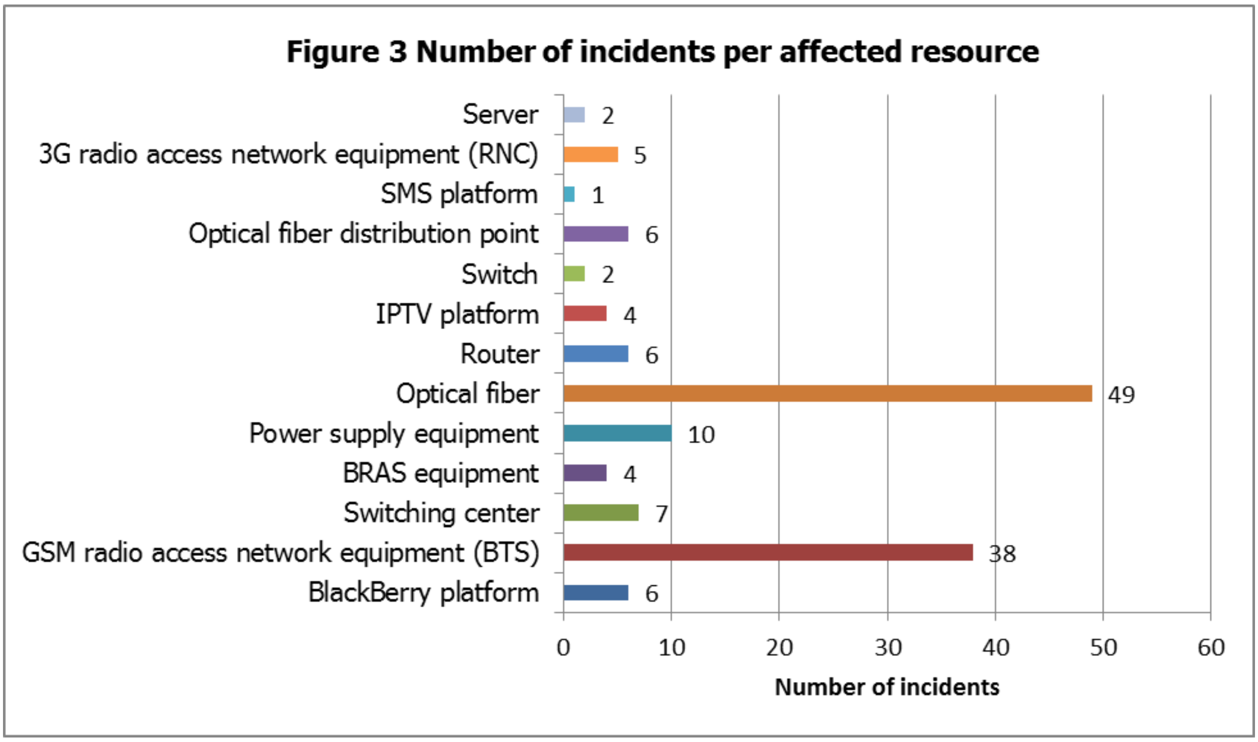


Figure 3 shows the impact of 2012 incidents on resources. The graph presents the number of incidents per affected resource.



In case of 25 incidents, there is no information regarding the affected resources, due to the providers' incomplete reporting.

### 3.2 Causes of reported incidents

The cause of an incident is the event or factor that triggers the incident. ANCOM identified 5 causes of the incidents that affect the security and integrity of electronic communications networks and services: external cause/third party, system failure, malicious attack, natural phenomenon and human error.

Incidents triggered by third parties were caused by the destruction of equipment and cables following construction works and by shortcomings in the electricity supply network caused by third parties.

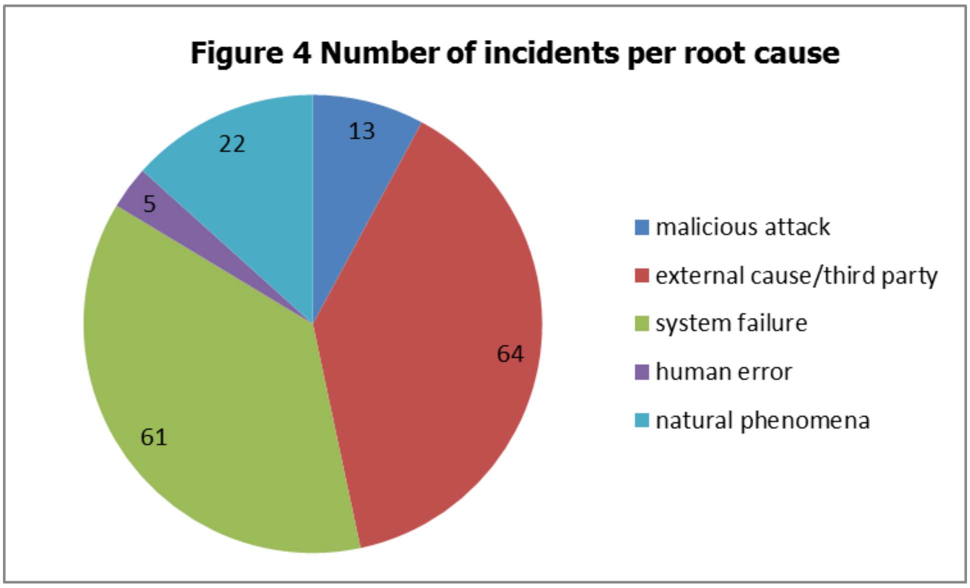
System failure incidents belonged to the categories of software errors, blocked or out-of-order hardware devices, configuration errors, network congestions etc.

In the category malicious attack, there were incidents caused by actions committed on purpose (e.g.: cooper cable theft, fiber optic cable sectioning).

The incidents caused by natural phenomena are owed, mainly, to massive snowfalls during the winter months. These include cases where rodents destroyed a number of cables.

The category human error includes incidents caused by faulty operation and configuration of equipment, systems and utilities.

Figure 4 presents the number of incidents reported for the year 2012, itemized by cause.

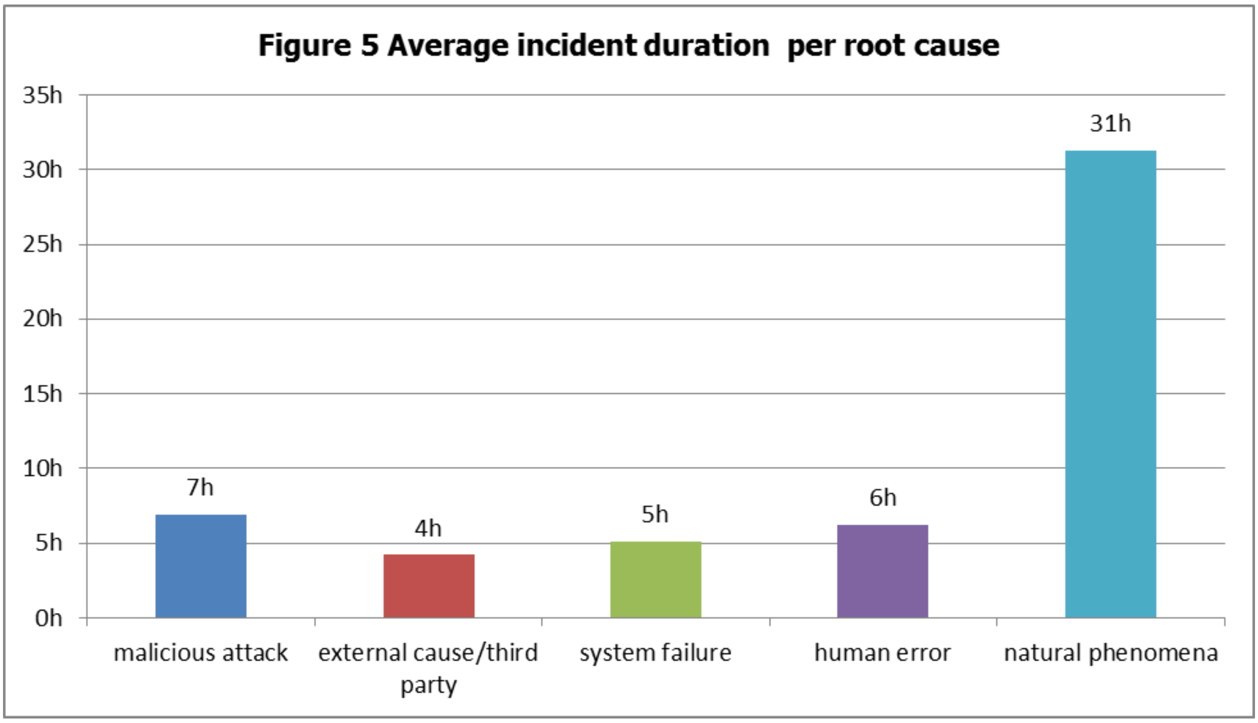


Most incidents were caused by third parties and by system failures.

### 3.3 Duration of incidents and duration until the detection of the incident

The total duration of incidents reported in 2012 is of 1,428 hours and the average duration of an incident is of 8.65 hours.

Figure 5 presents the average duration of an incident, by the initial cause. One can see that the incidents caused by natural phenomena last longer than any other type of incident. This is due mainly to the massive snowfalls during the winter months, which determine access to the affected sites to take longer or prevent access to them, for a certain period.



Out of the 165 incidents reported in 2012:

- 123 incidents were detected at the moment of their occurrence,
- 39 were detected within 1 to 32 minutes,
- 2 incidents were detected in approximately 2 hours and
- 1 incident was detected in approximately 7 hours from the moment of its occurrence.

The situation is illustrated in Figure 6.

**Figure 6 Number of incidents and duration of detection**

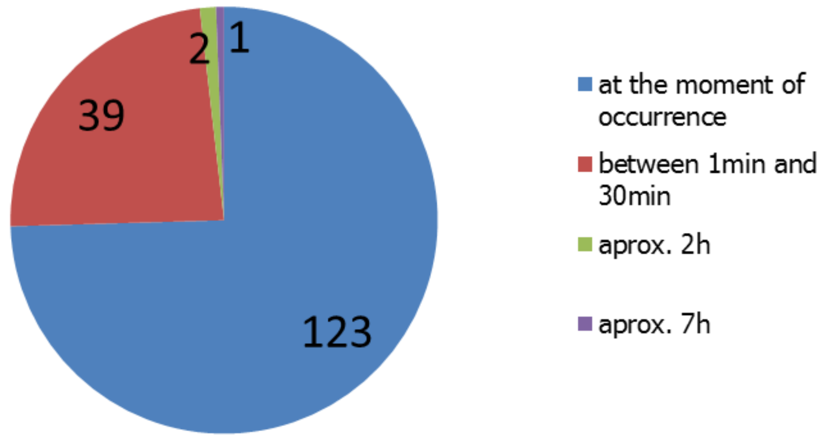


Figure 7 presents the graph of the 39 incidents that were detected within 1 and 32 minutes.

**Figure 7 Graph of the 39 incidents that were detected within 1 and 32 minutes**

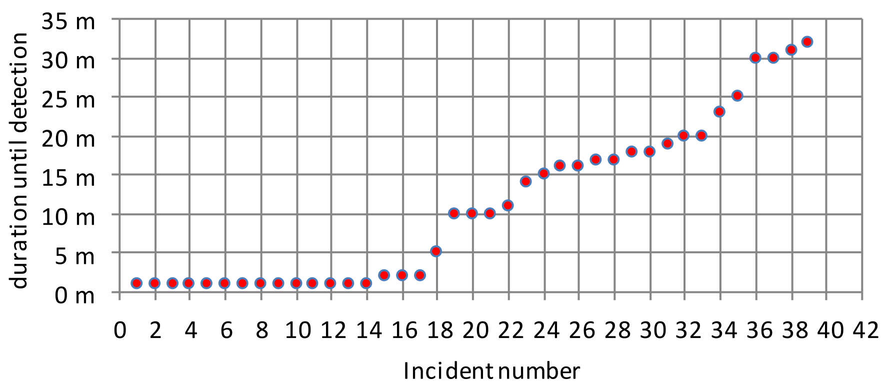


Figure 8 presents the distribution of incidents by the months of 2012. One can see that, in January, there were registered the most incidents. 26 out of the 165 incidents reported for 2012 occurred in January, due to weather conditions.

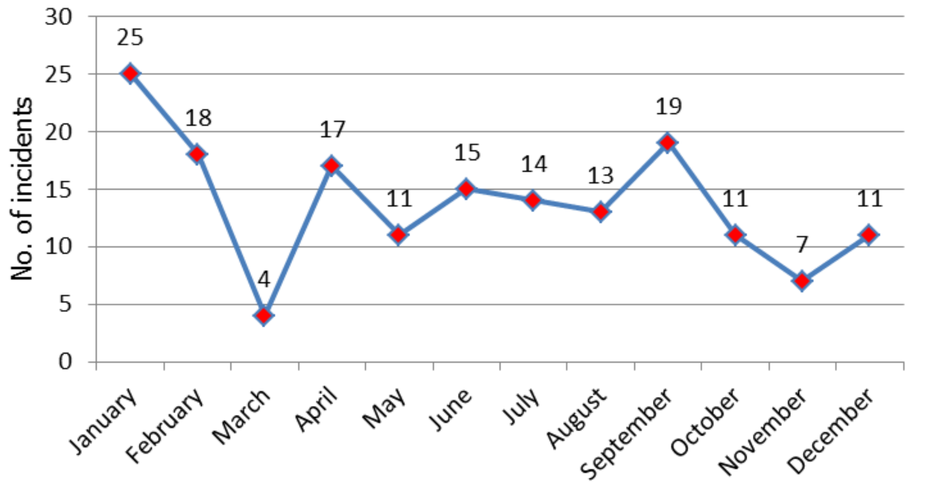


**Figure 8 Number of incidents per months in 2012**

### 3.4 Impact on emergency calls

55.49% of the incidents reported in 2012 had a possible impact on performing emergency calls. Figure 9 presents the percentage of incidents that had a possible impact on emergency calls.

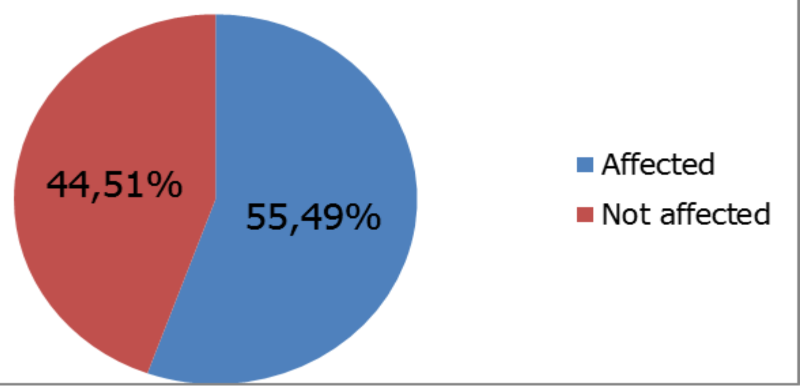


**Figure 9 Impact on emergency calls (%)**

The high rate of incidents that affected the fixed telephone and the mobile telephone services determine a high percent of incidents with impact on emergency calls. One must add that, in the case of mobile networks, when an incident that affected service provision occurs, a user may call the single number of emergency calls if the area where he/she resides is covered by another mobile telephony provider.

## 4. Incident response actions

Remedying the problems raised by the incidents and resuming service to the end-users involves a prompt answer from the providers. Thus, under normal conditions, the providers try to remedy the respective problems within the shortest term, so that they could fulfill their contractual obligations to customers.

The response actions performed for the purpose of remedying the problems raised by incidents consisted of:

- repairing the physical infrastructure by replacing the stolen or destroyed equipment,
- reconnecting the transmission equipment to electricity supply by means of a power unit,
- restoring and troubleshooting actions,
- equipment reconfiguration and restarting etc.

The security measures represent means of managing risk (which can be of administrative, technical, management, or legal nature) including policies, actions, plans, equipment, facilities, procedures, techniques etc. meant to prevent and minimize the risks posed to security or integrity of electronic communications networks or services.

The goal of security measures is to ensure security of the networks and continuity of the services provided over the networks. The security measures apply to all assets, when breached and or failing, can have a negative impact on the security or continuity of the electronic communication networks.

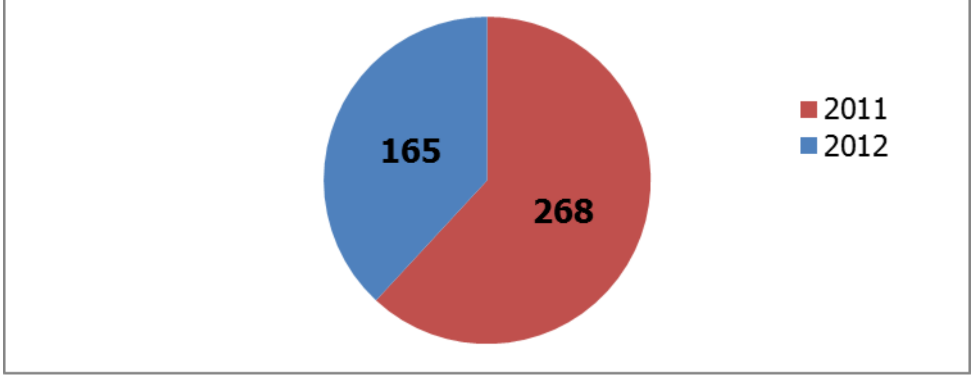
Implementing a suitable set of security measures, including policies, processes, procedures, organizational structures and software and hardware functions, the provider eliminates or reduces the risks regarding the security or integrity of electronic communications networks or services. These measures need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security, integrity and business objectives of the provider are met.

Such measures may be implemented for the purposes of prevention, correction or detection. Preventive measures reduce vulnerabilities and the occurrence probability of an incident, their implementation determining, for example, the failure of a potential attack. Corrective measures reduce the impact/effects of an incident and restore the functioning/operation in normal conditions. Detection measures assess incidents/attacks and activate preventive or corrective measures. Each incident must be analyzed by the provider and the security measures must be periodically updated in order to prevent and minimize the impact of security incidents.

## 5. Comparison between the reporting of incidents in 2012 and the reporting of incidents in 2011

Figure 10 presents the total number of incidents reported in 2012, in comparison to the total number of incidents reported in 2011.

Figure 10 Number of incidents reported in 2011 and 2012



In 2012, one may see a decrease in the number of significant incidents reported by the providers. This may be due to certain deficiencies in reporting stricter security measures implemented by the providers.

Figure 11 presents a comparison between the number of incidents in 2011 and in 2012, itemized by cause.

**Figure 11 Comparison of 2011 and 2012 incidents per root cause**

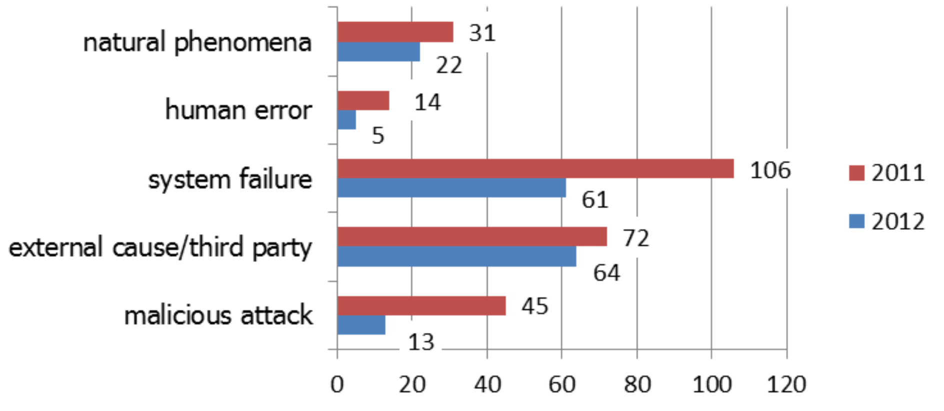
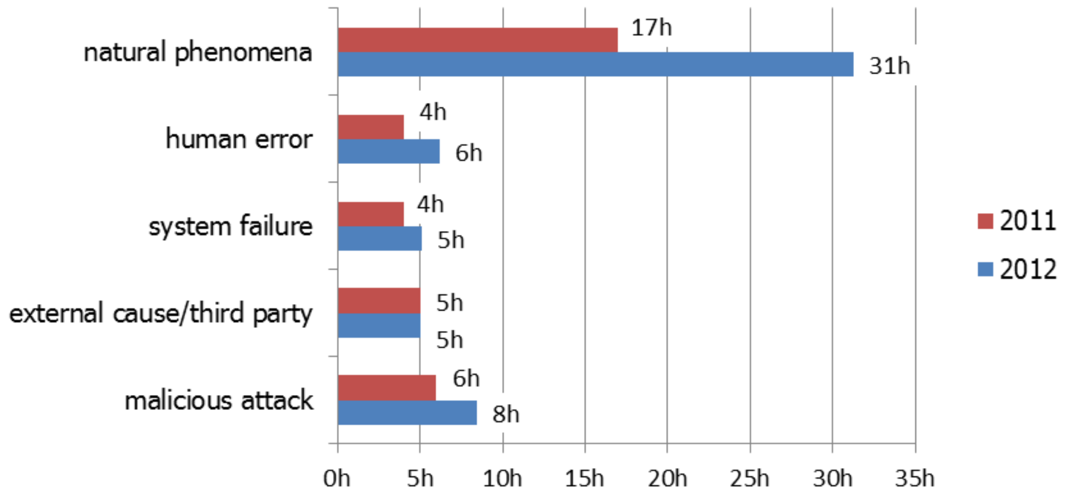


Figure 12 presents a comparison between the average duration of an incident in 2011 and 2012, itemized by cause. One may notice the fact that the average duration of an incident caused by natural phenomena doubled in 2012, compared to 2011.

**Figure 12 Comparison between the average duration on an incident in 2011 and 2012**



## 6. Conclusions

Having analyzed the incidents with significant impact on the electronic communications networks and services, ANCOM may identify the incident cause, may monitor the steps taken by the provider involved for the purpose of restoring the networks and services to an adequate level and may evaluate the security level of the electronic communications networks and services. The statistical analyses of the incidents are, as well, an effective instrument of tracking the trends.

The data regarding the incidents are fundamental for achieving a clear understanding of the nature and extent of the challenges to the security and integrity of the networks and services, by analyzing the vulnerabilities and threats to the security and integrity of networks and services by identifying best practices based on the lessons learned during the incident management process.

## 6.1 Conclusions regarding incident analysis

This report is an overall view on the incidents reported in 2012. Following the consolidation, classification and analysis of the 165 incidents reported by the 10 providers of public electronic communications networks or of publicly available electronic communications services, we can draw the conclusions below:

- Most incidents affected the telephone services provided by means of fixed public networks or of limited mobility networks (103 incidents) and internet access services by permanent connections at a fixed location (81 incidents).
- The most affected service, from the standpoint of the number of connections, is the data transmission service – SMS (approximately 3,205,300 connections affected).
- The most affected resources were fiber optic cablings and BTSs of mobile networks (49 incidents on fiber optic cablings and 38 incidents where BTSs were temporarily inactive).
- 39% of the incidents were due to external causes/third parties and 37% of the incidents were caused by system failures.
- The incidents caused by natural phenomena persist longer than any other incident type (an average duration of 31 hours).
- 75% of the incidents were detected instantly, while the rest of 25% were detected subsequent to their occurrence. Thus, 39 incidents were detected within 1 - 32 minutes and only 3 incidents were detected after a longer period, respectively in 2 hours, 2 hours and 12 minutes and 7 hours.
- The month of January registered the most incidents (15% of the incidents).
- In 55.5% of the cases, the incidents affected totally or partially the performance of emergency calls.

## 6.2 Conclusions regarding reporting deficiencies

The main purpose of reporting is receiving complete, accurate and comparable information on the incidents with a significant impact on the security and integrity of electronic communications networks and services.

Following the analysis of all the 165 forms completed by the providers who reported incidents during 2012, several deficiencies were assessed.

One of the most important deficiencies was failure to fill in the number of connections affected for each affected service. By filling in only one figure under ”Number of connections affected by an incident, per service” the respondents did not clarify whether the respective figure is the total amount of connections affected, for all the services, or the same number of connections were affected for each of the services.

Several of the providers did not estimate the number of connections affected specifying either the affected service only, or the fact that more than 5,000 connections were affected (5,000 affected connections was the reporting threshold).

The format of filling in the date by the affected provider made difficult, in certain cases, the reported data consolidation (the providers used either the format dd.mm.yyyy or the format mm.dd.yyyy without specifying the format).

Regarding the affected resources, some of the answers are too specific and others are too general. Thus, ANCOM will review the form filling instructions, in order to define more clearly the elements to be filled in by the reporting providers).

Most providers did not fill in the fields regarding the steps taken or planned in order to prevent a similar incident/remove the incident cause. We emphasize the fact that the analysis of incidents must trigger a provider to review, update and improve the security measures implemented, in order to eliminate or reduce the risks of occurrence of similar incidents in the future.

According to the draft decision of the President of the National Authority for Management and Regulation in Communications regarding the establishment of the minimum security measures to be taken by the providers of electronic communications networks and services and the reporting of incidents with significant impact on the provision of electronic communications networks and services, the providers have the obligation to report incidents with significant impact (affecting a number of connections larger than 5,000, for at least one hour) on the security and integrity of electronic communications networks and services, including by identifying the incident cause, as well as of the response actions, of the steps taken or planned in order to hinder the occurrence of other similar incidents or to remove the incident cause. Thus, for a reporting as accurate as possible, there must be a permanent monitoring of the providers' reporting, including by applying sanctions where the information requested by ANCOM regarding the incidents with significant impact on the provision of electronic communications networks and services are not fully and accurately provided.