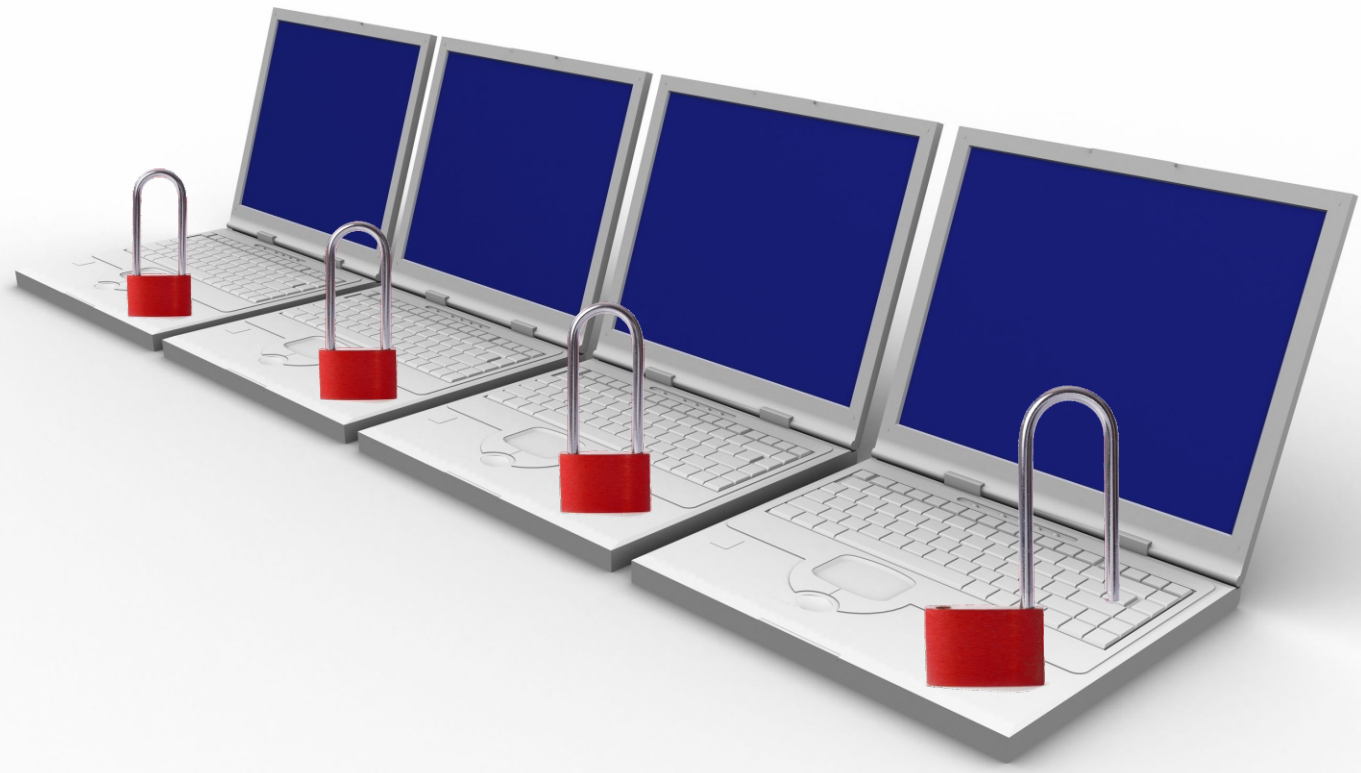
ANCOM
Autoritatea Naţională pentru Administrare
şi Reglementare în Comunicaţii

# RAPORT
# privind incidentele care au afectat securitatea și integritatea rețelelor și serviciilor de comunicații electronice în anul 2013



Data publicării: 21.07.2014

## CUPRINS

## 1. Introducere

În vederea asigurării unui sistem de comunicații fiabil și sigur prin intermediul rețelelor de comunicații electronice, potrivit dispozițiilor art. 46-48 din Ordonanța de urgență a Guvernului nr. 111/2011 privind comunicațiile electronice aprobată, cu modificări și completări, prin Legea nr. 140/2012, furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului trebuie să adopte și să implementeze toate măsurile adecvate, de ordin tehnic sau organizatoric, în vederea administrării riscurilor la adresa securității și integrității rețelelor și serviciilor de comunicații electronice. De asemenea, potrivit acelorași dispoziții, furnizorii au obligația de a notifica ANCOM cu privire la orice încălcare a securității sau pierdere a integrității care are un impact semnificativ asupra furnizării rețelelor sau a serviciilor.

Obligațiile prevăzute la art. 46-48 din Ordonanța de urgență a Guvernului nr. 111/2011 au fost detaliate în Decizia[1] nr. 512/2013 privind stabilirea măsurilor minime de securitate ce trebuie luate de către furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului și raportarea incidentelor cu impact semnificativ asupra furnizării rețelelor și serviciilor de comunicații electronice. Conform Deciziei 512/2013, *securitatea și integritatea rețelelor și serviciilor de comunicații electronice reprezintă capacitatea unei rețele sau a unui serviciu de comunicații electronice de a rezista evenimentelor, accidentale sau rău-intenționate, care pot compromite sau afecta continuitatea furnizării rețelelor și serviciilor la un nivel de performanță echivalent cu cel anterior producerii evenimentului*.

Articolul 4 al aceleiași Decizii impune furnizorilor obligația de a notifica ANCOM cu privire la existența unui incident cu impact semnificativ asupra securității și integrității rețelelor și serviciilor de comunicații electronice. În cadrul Deciziei 512/2013, incidentul cu impact semnificativ este definit ca fiind *acel incident care afectează un număr mai mare de 5.000 de conexiuni, timp de cel puțin 60 de minute.*

Conform art. 47 alin. (4) din Ordonanța de urgență a Guvernului nr. 111/2011 privind comunicațiile electronice, *„ANCOM transmite anual un raport succint Comisiei Europene și Agenției Europene pentru Securitatea Rețelelor Informatice și a Datelor cu privire la notificările primite potrivit alin. (1) și măsurile adoptate în aceste cazuri*."

Astfel, în vederea îndeplinirii obligației autorității de transmitere a informațiilor relevante către Comisia Europeană și ENISA (Agenția Europeană pentru Securitatea Rețelelor Informatice și a Datelor), în urma analizei incidentelor raportate de furnizorii de rețele și servicii de comunicații electronice în 2013, ANCOM a transmis un raport succint conform cu ghidul[2] ENISA de raportare a incidentelor. Pe baza rapoartelor furnizate de statele membre ale Uniunii Europene, ENISA publică[3] anual un raport privind incidentele de securitate ce au avut loc în anul precedent.

[1] Textul integral al acestei decizii este disponibil la următoarea adresă: http://www.ancom.org.ro/uploads/forms_files/decizie_2013_5121381320491.pdf

[2] Disponibil la adresa http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/Technical%20Guidelines%20on%20Incident%20Reporting/incidents-reporting-to-enisa/technical-guideline-on-incident-reporting

[3] Rapoartele ENISA sunt disponibile la următoarea adresă: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports

## 2. Raportarea incidentelor care au afectat securitatea și integritatea rețelelor și serviciilor de comunicații electronice în anul 2013

Având în vedere faptul că Decizia nr. 512 a fost emisă în cursul anului 2013, furnizorii au avut obligația ca până la data de 15 octombrie 2013 să raporteze toate incidentele cu impact semnificativ care au avut loc în anul 2013 până la data intrării în vigoare a acestei Decizii (respectiv, 1 octombrie 2013).

Începând cu data de 1 octombrie 2013, raportarea cu privire la existența unui astfel de incident cuprinde două etape. Prima constă în transmiterea unei notificări inițiale până cel târziu ora 13 a zilei lucrătoare următoare celei în care a fost detectat incidentul, iar cea de-a doua constă în completarea și transmiterea în termen de două săptămâni de la detectarea incidentului cu impact semnificativ a formularului-tip prevăzut în anexa nr. 2 a Deciziei 512/2013.

În cadrul notificării finale, furnizorii trebuie să raporteze informații referitoare la:

- data și ora la care s-a produs incidentul, respectiv la care s-a descoperit incidentul;
- serviciul/serviciile a căror furnizare a fost afectată de incident;
- numărul total de conexiuni afectate de incident, separat pentru fiecare serviciu afectat;
- resursele/echipamentele afectate de incident;
- durata incidentului;
- regiunea geografică afectată de incident;
- impactul asupra apelurilor de urgență;
- descrierea incidentului;
- tipul cauzei incidentului;
- mai multe informații despre cauza incidentului;
- acțiuni de răspuns la incident;
- măsurile luate sau planificate pentru a împiedica producerea unui incident similar/ eliminarea cauzei incidentului;
- alți furnizori de rețele și servicii de comunicații electronice afectați.

Începând cu 1 ianuarie 2014, transmiterea notificării finale privind existența unui incident cu impact semnificativ asupra securității și integrității rețelelor și serviciilor de comunicații electronice se realizează exclusiv prin intermediul unei aplicații disponibile pe pagina[4] de internet a ANCOM.

## 3. Analiza incidentelor raportate

În anul 2013 au fost raportate 253 de incidente de către 6 furnizori de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului. Acestea au fost centralizate, catalogate și apoi analizate din mai multe puncte de vedere:

1. Impactul asupra serviciilor și utilizatorilor:
    - Conexiuni afectate,
    - Servicii afectate,
    - Resurse afectate,
    - Aria/răspândirea geografică.

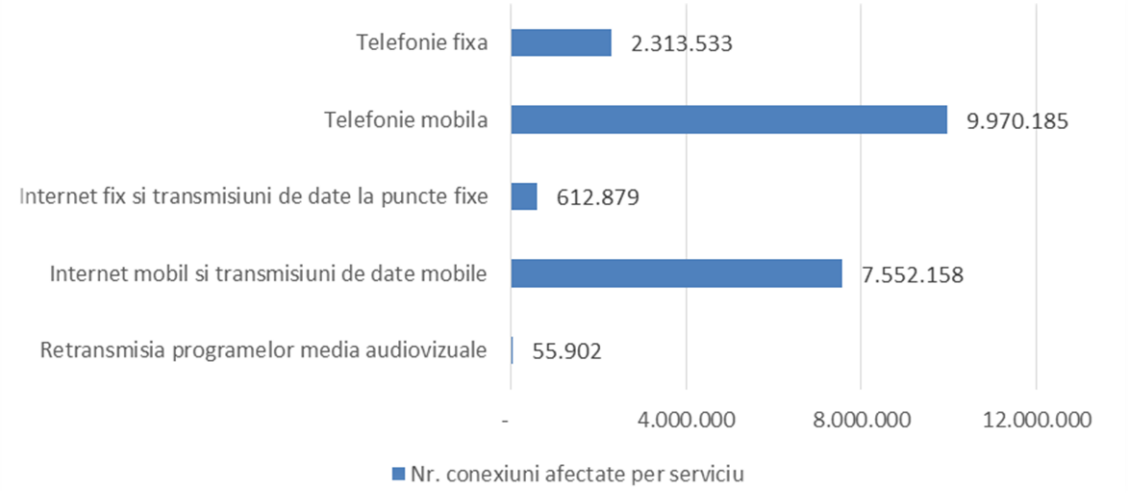
[4] Aplicația poate fi accesată la următorul link: https://statistica.ancom.org.ro:8000/sscpds/public/categories/communications

2. Cauzele incidentelor raportate,
3. Durata incidentelor și durata de descoperire,
4. Impactul asupra apelurilor de urgență.

## 3.1 Impactul asupra serviciilor și utilizatorilor

Numărul total de conexiuni afectate de cele 253 de incidente cu impact asupra principalelor servicii de comunicații electronice în anul 2013 este reprezentat în graficul de mai jos.

**Fig.1 Numărul de conexiuni afectate per serviciu**




Această statistică are la bază o estimare a numărului de conexiuni afectate, întrucât unii furnizori nu au raportat date exacte în această privință. Conform Deciziei 512/2013, în cazul serviciilor furnizate prin intermediul unor rețele publice mobile terestre, furnizorul estimează numărul de conexiuni afectate. Conform instrucțiunilor de completare a formularului de raportare, metoda de estimare a numărului de cartele SIM afectate ia în calcul *traficul total pierdut la nivelul tuturor celulelor afectate*[5] pe fiecare serviciu (voce și date), *traficul total înregistrat la nivelul rețelei*[6] și numărul de cartele SIM active pe respectivul serviciu la nivelul furnizorului. În plus, și în cazul serviciilor de telefonie furnizate prin intermediul unor rețele publice fixe, datorită naturii unor incidente, numărul de conexiuni afectate nu a putut fi precizat cu exactitate.

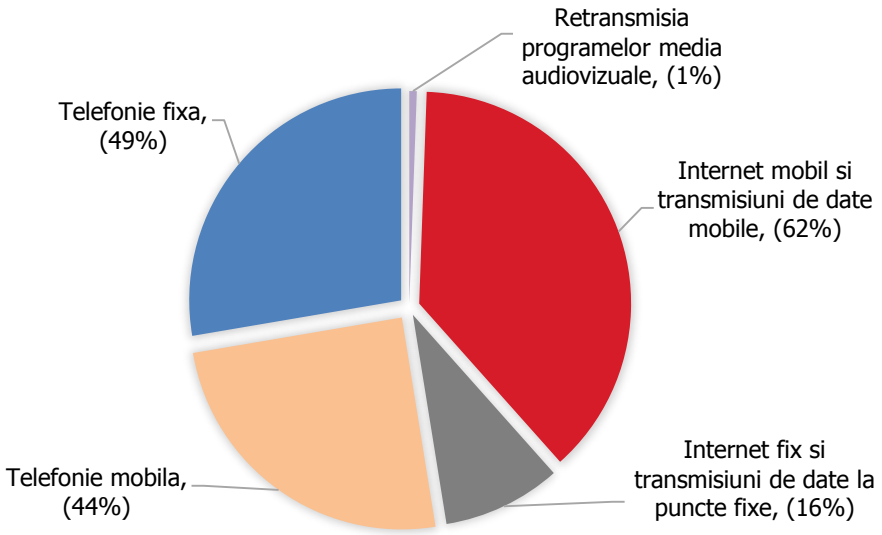
În 2013 cele mai afectate au fost serviciile de telefonie mobilă (9.970.185 conexiuni afectate). De precizat faptul că în cazul incidentelor care au afectat serviciile de telefonie mobilă, au fost afectate implicit și serviciile de transmisiuni de date - SMS. Din figura 1 se poate observa că incidentele au afectat într-o mică măsură retransmisia serviciilor de programe media audiovizuale. În principal, acest fapt se datorează structurii rețelelor care permit retransmisia serviciilor de programe audiovizuale și a modului în care acestea sunt operate. Acest tip de rețele cuprinde sisteme de recepție și distribuție colectivă, menite să deservească zone mici (un cartier, un oraș etc.). Tocmai datorită caracterului distributiv al acestor rețele, în cazul producerii unui incident, numărul de conexiuni afectate ar fi mic.

[5] Traficul total pierdut la nivelul tuturor celulelor afectate se consideră a fi traficul înregistrat săptămâna anterioară, în același interval de timp în care a avut loc incidentul, la nivelul acelor celule

[6] Traficul total înregistrat la nivelul rețelei se consideră a fi suma traficului din toate celulele din rețea în intervalul de timp respectiv, în săptămâna anterioară.

Pentru o imagine mai clară în privința impactului pe care incidentele l-au avut asupra serviciilor, în figura 2 este reprezentat procentajul conexiunilor afectate raportat la numărul total de conexiuni de pe piață, pentru fiecare tip de serviciu.

**fig.2 Procentul de conexiuni afectate in 2013 in raport cu numarul total de conexiuni per serviciu* (%)**



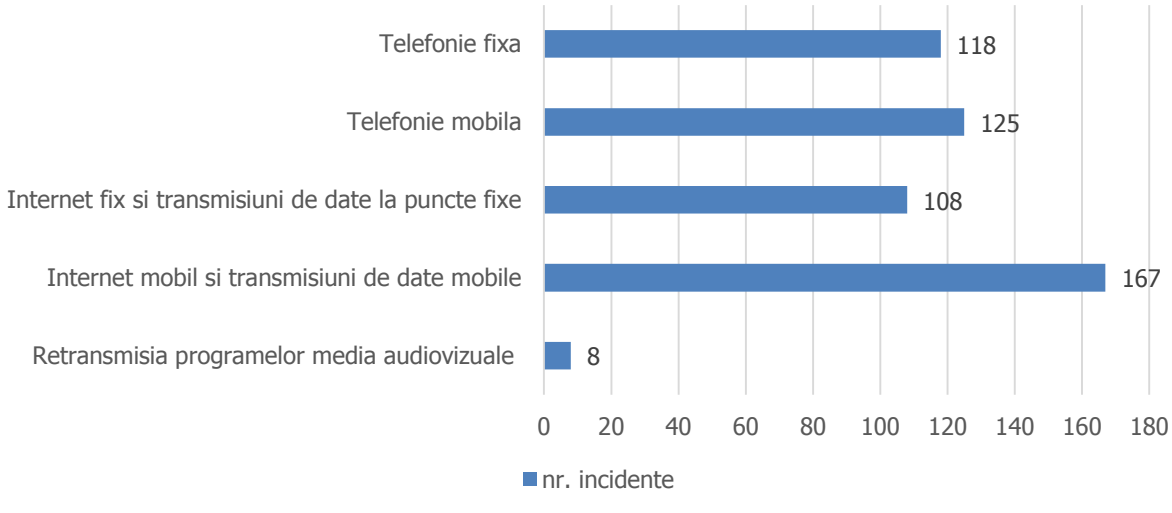

* Conform Raportului privind datele statistice care poate fi accesat la următoarea adresă: https://statistica.ancom.org.ro:8000/sscpds/public/alldocuments/report

De precizat faptul că procentele din graficul de mai sus sunt calculate ținând cont de numărul total de conexiuni afectate per serviciu. Altfel spus, conexiunile luate în calcul nu sunt afectate doar de un singur incident.

Se poate observa că, deși serviciile de telefonie mobilă au avut cel mai mare număr de conexiuni afectate (Fig.1), atunci când raportarea se face la numărul total de conexiuni, serviciul cel mai afectat este cel de internet mobil și transmisiuni de date mobile.

Figura de mai jos reprezintă numărul de incidente care au afectat fiecare serviciu în anul 2013. Se poate observa că majoritatea incidentelor au afectat serviciile de acces la internet pe mobil și serviciile de transmisiuni de date mobile (167 incidente).

**Fig.3 Impactul asupra serviciilor**

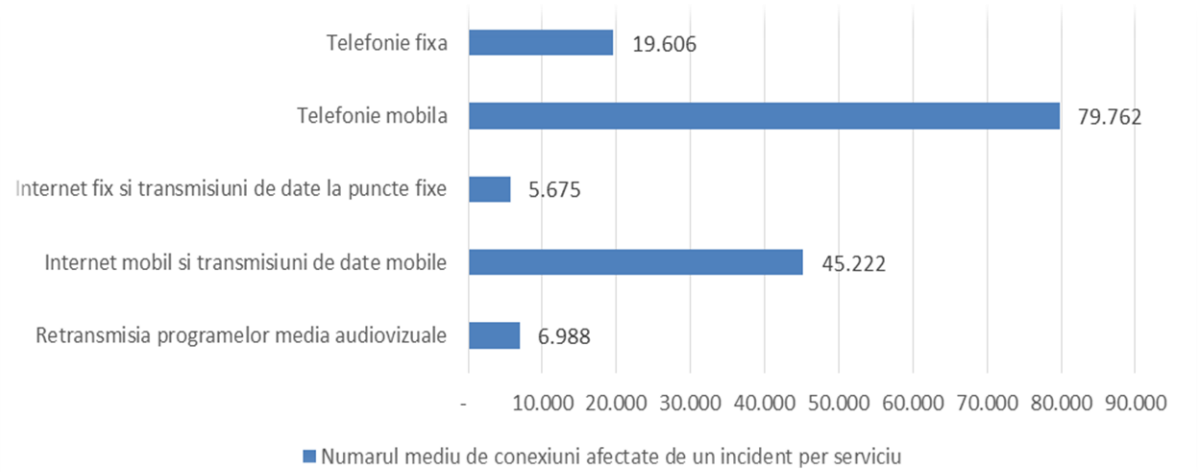


De precizat faptul că suma incidentelor pentru fiecare tip de serviciu afectat diferă față de numărul total al incidentelor datorită faptului că un incident poate afecta mai multe tipuri de servicii simultan.

Conform datelor raportate de către furnizori, numărul mediu de conexiuni afectate de un incident în 2013 este de 78.960. Această medie include toate conexiunile afectate, indiferent de tipul de serviciu afectat (inclusiv pe cele în cazul cărora au fost afectate mai multe servicii simultan).

Figura de mai jos reprezintă numărul mediu de conexiuni afectate de un incident per serviciu.

**Fig.4 Numărul mediu de conexiuni afectate de un incident per serviciu**

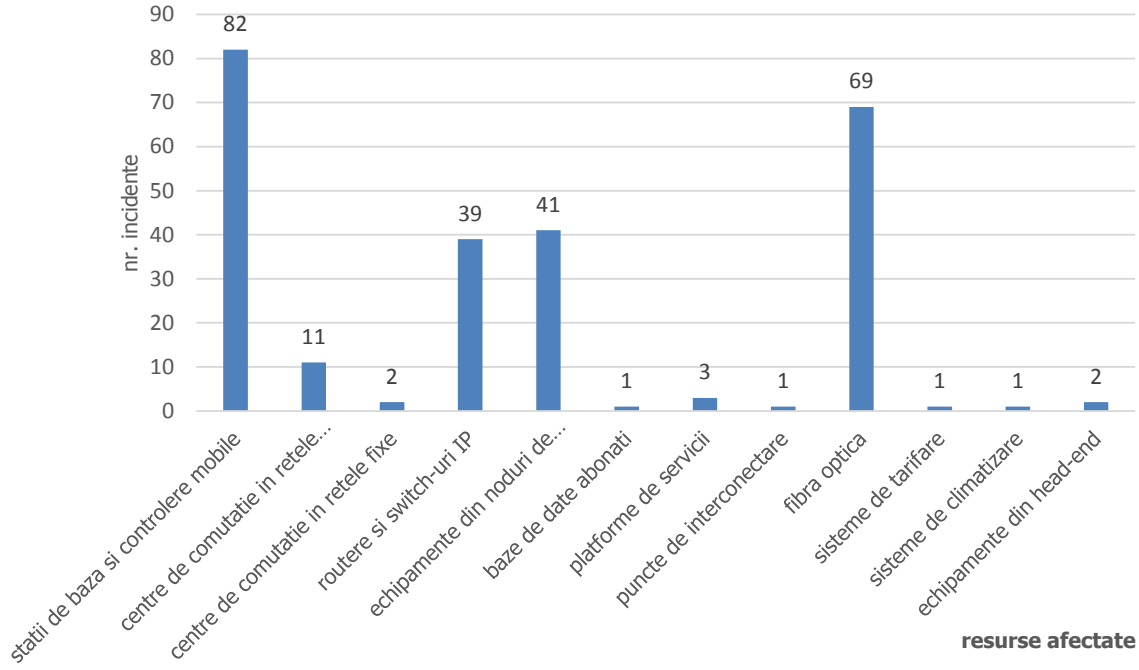



Din figura 4, se poate observa faptul că în cazul serviciului de telefonie mobilă au fost afectate în medie 79.762 de conexiuni, iar în cazul serviciilor de internet mobil și transmisiuni de date mobile, au fost afectate în medie 45.222 de conexiuni. Spre comparație, următorul cel mai afectat serviciu, cel de telefonie fixă, a înregistrat un număr mediu de 19.606 conexiuni afectate. Astfel, un incident care a afectat serviciile mobile e mult mai probabil să afecteze un număr semnificativ de utilizatori, decât un incident care a vizat oricare alt serviciu.

## 3.2 Impactul asupra resurselor afectate

Pentru determinarea impactului incidentelor asupra resurselor (echipamente/sisteme de comunicații etc.), toate resursele afectate, menționate de furnizori în raportări, au fost încadrate în mai multe categorii. Astfel, graficul următor evidențiază numărul de incidente ce au afectat fiecare categorie de resurse în parte.

**Fig.5 Numar de incidente per categorie de resurse afectate**



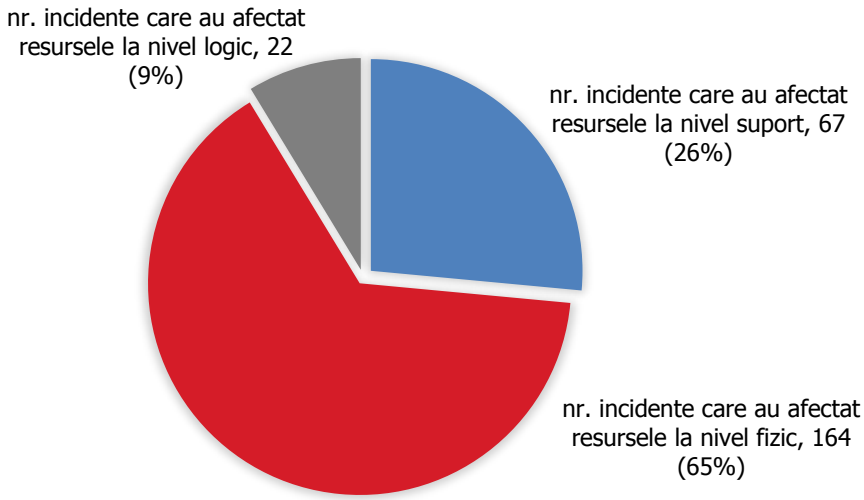

În cazul celor mai multe incidente, resursele afectate fac parte din categoriile stații de bază și controlere mobile și fibra optică.

Având în vedere faptul că anumite resurse prezintă mai multe componente, afectarea acestora poate avea implicații la nivele diferite. Se disting, astfel, trei nivele la care se vor raporta statisticile privind resursele afectate în urma producerii incidentelor cu impact semnificativ în 2013:

- Nivelul suport, care face referire la componentele suport ale echipamentelor, precum cele necesare alimentării cu energie electrică;
- Nivelul fizic, care face referire la componentele hardware ale echipamentelor;
- Nivelul logic, care face referire la componentele software ale echipamentelor.

Graficul următor reprezintă impactul celor 253 de incidente asupra resurselor în funcție de cele trei nivele enunțate mai sus.

**Fig.6 Impactul incidentelor asupra resurselor pe diferite nivele**



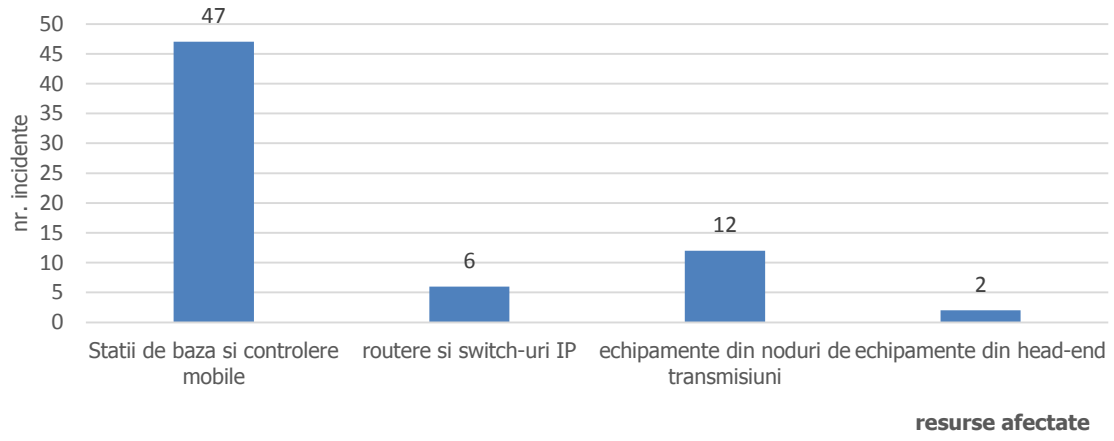
Fiecare dintre aceste nivele este analizat în cele ce urmează.

**Nivelul suport**

Din totalul incidentelor cu impact semnificativ raportate în 2013, 67 dintre acestea (aproximativ 26%) s-au produs din cauza problemelor de alimentare cu energie electrică. Astfel de probleme s-au datorat faptului că au existat fluctuații de tensiune înregistrate în rețeaua furnizorului de energie electrică (ce au condus la defectarea unor echipamente ori descărcarea bateriilor), sau furtului bateriilor și acumulatorilor de alimentare cu energie electrică, ori faptului că alimentarea cu energie electrică a fost întreruptă pentru un timp îndelungat, caz în care rezervele cu combustibil (sau alte resurse de alimentare cu energie electrică) s-au epuizat.

Resursele afectate din cauza problemelor de alimentare cu energie electrică sunt reprezentate în figura de mai jos.

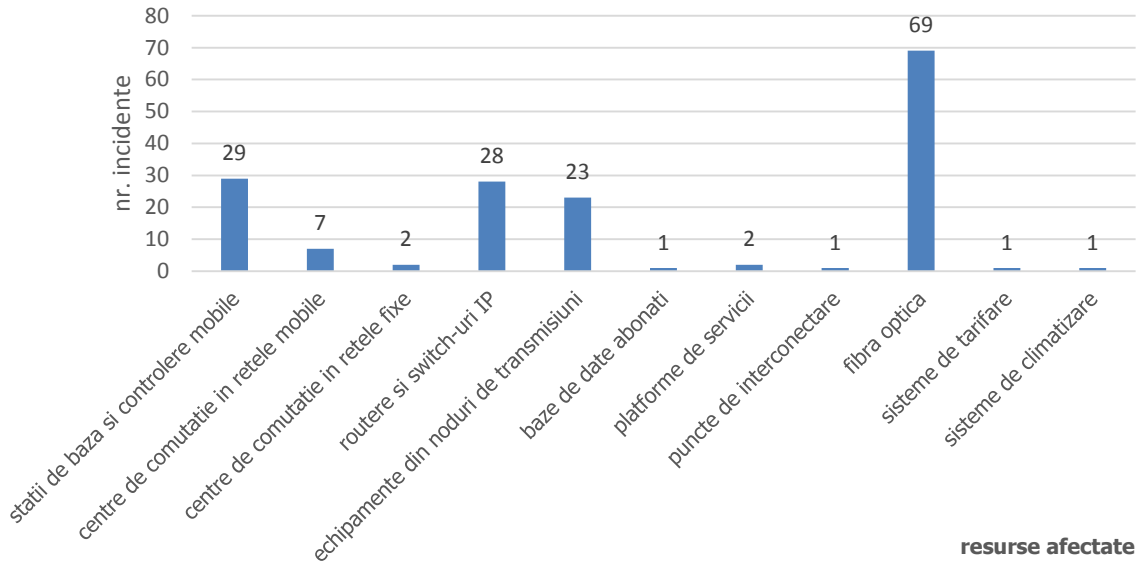
**Fig.7 Resurse afectate la nivel suport**




Astfel, în cazul a 47 de incidente produse din cauza problemelor de alimentare cu energie electrică (aproximativ 70% din incidentele care au afectat resursele la nivel suport), resursele afectate fac parte din categoria stații de bază și controlere mobile, în cazul a 12 incidente având aceeași cauză, resursele afectate au fost echipamente din noduri de transmisiuni. Se desprinde astfel concluzia că echipamentele din rețelele mobile (stații de bază etc.) sunt cele mai vulnerabile la întreruperile în alimentarea cu energie electrică.

**Nivelul fizic**

**Fig.8 Resurse afectate la nivel fizic**



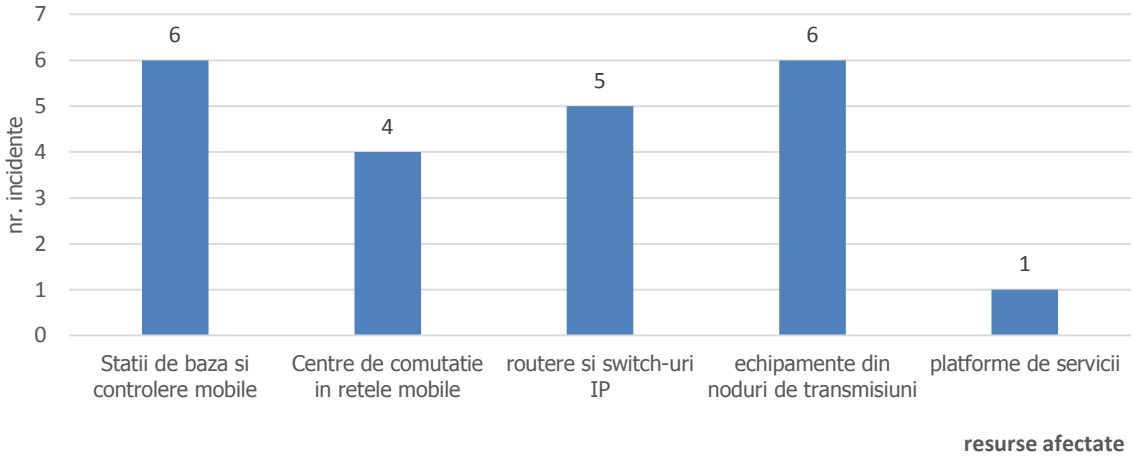
Conform raportărilor pe 2013, s-au înregistrat 164 de incidente (aproximativ 65% din incidentele raportate în 2013) care au afectat componentele hardware ale echipamentelor. Statistica privind resursele afectate la nivel fizic este reprezentată în graficul de mai jos.

Din figura 8 se poate observa că la nivel fizic, cea mai afectată resursă este fibra optică. Cele 69 de incidente care au vizat afectarea la nivel fizic a fibrei optice (aproximativ 42% din incidentele care au afectat resursele la nivel fizic), s-au datorat în principiu accidentelor cauzate de terțe părți, acțiunilor rău-intenționate sau rozătoarelor.

**Nivelul logic**

În urma raportărilor furnizorilor, s-au înregistrat 22 de incidente care au afectat resursele la nivel logic. Statistica realizată în acest caz este reprezentată în figura 9.

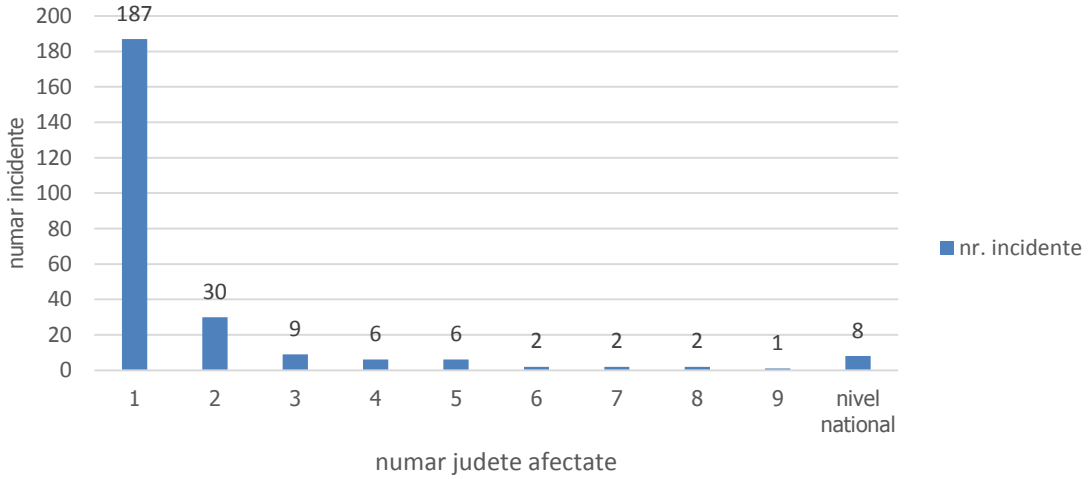
**Fig.9 Resurse afectate la nivel logic**




Incidentele care au afectat resursele la nivel logic s-au datorat unor erori apărute la nivelul diferitelor echipamente sau configurării greșite a acestora.

În ceea ce privește regiunea geografică afectată de incidente, în cele mai multe cazuri, incidentele raportate au afectat un singur județ. În cazul a 8 incidente, furnizorii au raportat că impactul a fost la nivel național.

**Fig.10 Impactul incidentelor asupra regiunilor geografice afectate**



În cazul incidentelor cu impact la nivel național, resursele afectate fac parte din categoriile routere și switch-uri IP, puncte de interconectare, sisteme de tarifare, baze de date abonați, platforme de servicii și centre de comutație în rețele mobile.

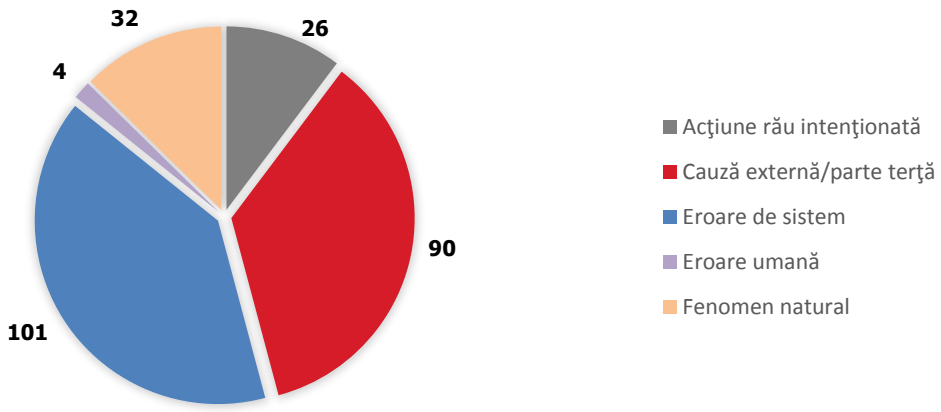
### 3.3 Cauzele incidentelor raportate

Cauza unui incident reprezintă evenimentul sau factorul care declanșează incidentul.

Conform Deciziei 512/2013, au fost identificate 5 cauze ale incidentelor care afectează securitatea și integritatea rețelelor și serviciilor de comunicații electronice: cauză externă/parte terță, eroare de sistem, acțiune rău intenționată, fenomen natural și eroare umană.

Așa cum se poate vedea în figura de mai jos (Fig. 11), majoritatea incidentelor din 2013 face parte din categoriile eroare de sistem și cauză externă/parte terță.

**Fig.11 Numarul de incidente in functie de cauza**




Incidentele cauzate de erori de sistem au fost de tipul erori software, defecțiuni hardware, congestii în rețea.

*Exemplu: un incident din această categorie a vizat o problemă software a sistemului de tarifare, serviciile de date mobile fiind afectate timp de aproximativ două ore. Impactul incidentului a fost la nivel național.*

Din categoria acțiune rău-intenționată fac parte incidentele cauzate de acțiuni efectuate în mod deliberat (de exemplu: secționarea sau furtul unor segmente de cablu de fibră optică, furtul bateriilor de alimentare cu energie electrică, vandalizarea unor echipamente, atac de tip DoS[7]).

*Un exemplu de incident din această categorie: furtul unui segment de fibră optică a afectat serviciul de telefonie fixă și cel de acces la internet fix timp de 15 ore.*

Incidentele cauzate de fenomene naturale se datorează în principal fenomenelor meteorologice (precipitații abundente, descărcări electrice, zăpezi), care au afectat diverse echipamente și care au împiedicat în unele cazuri accesul echipelor de intervenție în vederea restabilirii serviciilor. Din această categorie mai fac parte incidentele cauzate de rozătoare, câini etc.

[7] Denial of Service

*Exemplu: datorită infiltrațiilor cu apă, 5 stații de bază au devenit nefuncționale. Serviciile de telefonie mobilă au fost afectate timp de aproximativ 3 ore.*

În categoria eroare umană au fost încadrate incidentele care au avut drept cauză configurarea și operarea greșită a echipamentelor.

*Exemplu: ca urmare a configurării greșite a unui echipament, serviciile de telefonie și acces la internet au fost afectate timp de aproximativ 5 ore. Un alt incident care a vizat configurarea greșită a unui echipament a afectat serviciile de date mobile timp de 90 de minute și a avut impact asupra 5 județe.*

Incidentele raportate având drept cauză părți terțe au fost provocate în principal de probleme privind alimentarea cu energie electrică și de secționarea accidentală a fibrei optice, în cadrul lucrărilor realizate de terți.

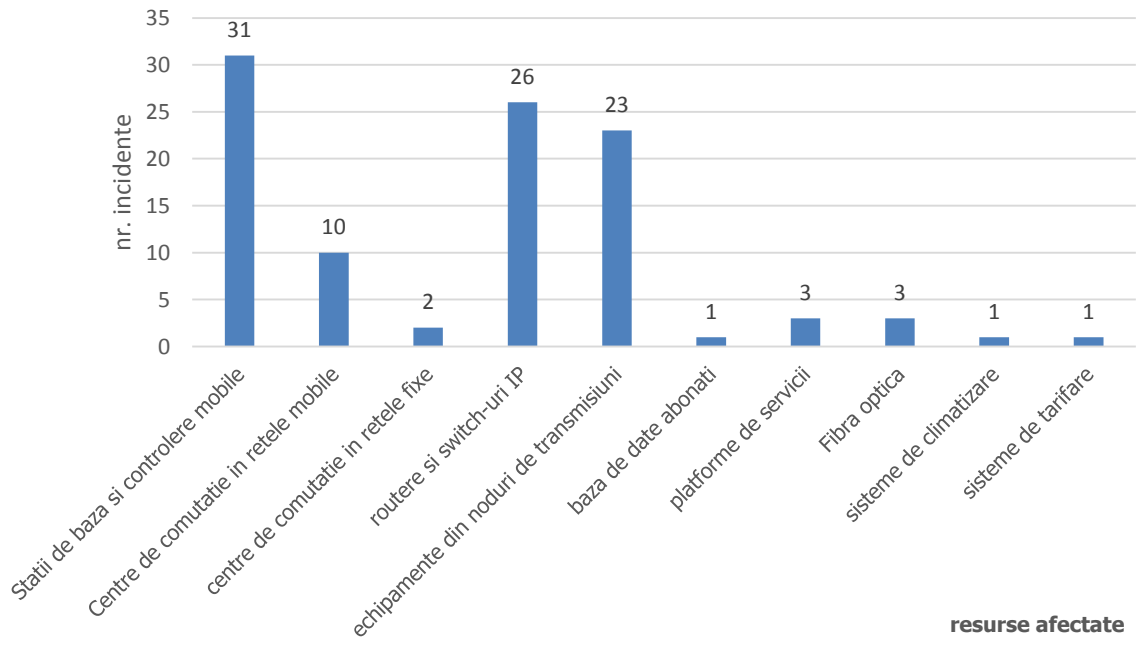
*Exemplu: din cauza lucrărilor executate de o parte terță, au fost secționate segmente de fibră optică, fapt ce a afectat serviciile de telefonie fixă și de acces la internet fix timp de aproximativ 8 ore.*

În principiu, categoria cauză externă/parte terță poate fi corelată cu una din celelalte 4 cauze. Astfel, din cele 90 de incidente care fac parte din categoria cauză externă/parte terță, se disting 11 incidente pentru care au fost raportate astfel de corelări.

Astfel, în cazul a 8 dintre incidente, cauza principală a fost corelată cu fenomen natural, în cazul a două dintre incidente cauza principală a fost corelată cu eroare de sistem, iar pentru un incident, cauza principală a fost corelată cu acțiune rău-intenționată. Pentru 79 dintre incidente nu au fost menționate astfel de corelări.

Întrucât principalele cauze pentru producerea incidentelor raportate în 2013 fac parte din categoria eroare de sistem și cauză externă/parte terță, este relevantă identificarea resurselor afectate în fiecare din aceste cazuri. Figura 12 ilustrează numărul de incidente cauzate de erori de sistem per categorie de resurse afectate.

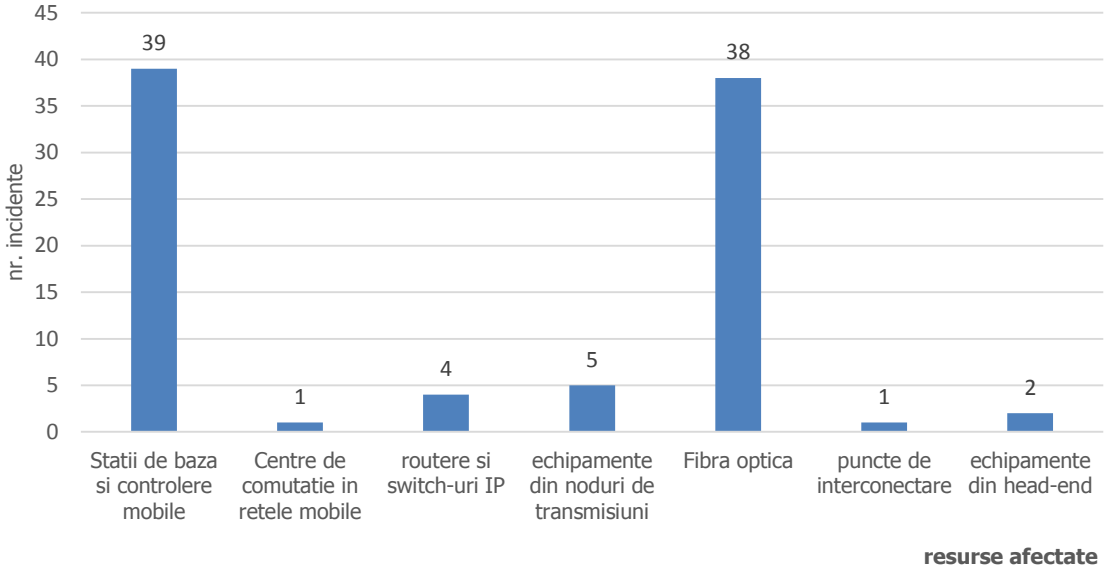
**Fig.12 Resurse afectate in cazul incidentelor avand drept cauza eroare de sistem**



Se poate observa că cele mai afectate categorii de resurse în cazul incidentelor cauzate de erori de sistem au fost stații de bază și controlere mobile, routere și switch-uri IP și echipamente din noduri de transmisiuni.

În figura 13 este reprezentat numărul de incidente cauzate de părți terțe, per categorie de resurse afectate.

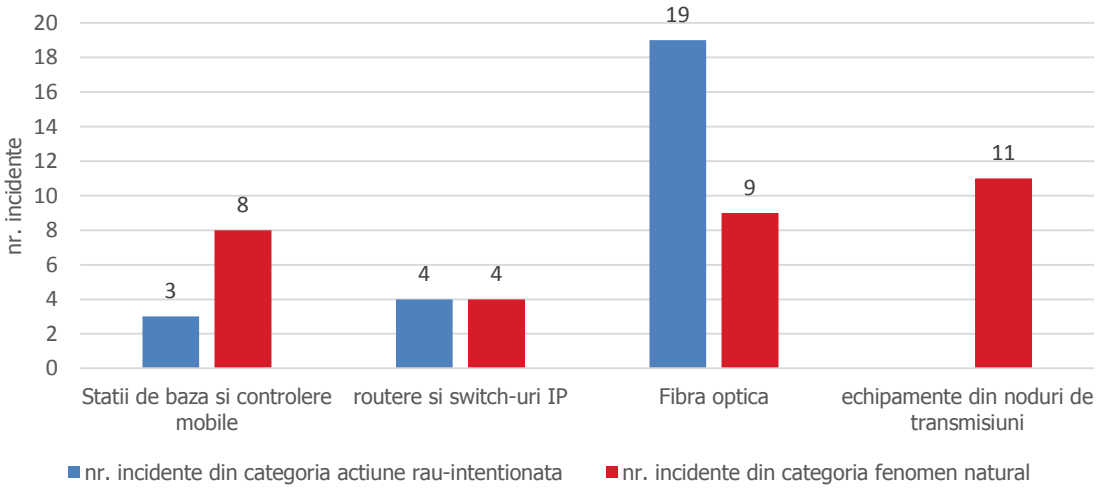
**Fig.13 Resursele afectate in cazul incidentelor care fac parte din categoria cauza externa**




Se poate observa, astfel, că pentru incidentele care fac parte din categoria cauză externă, resursele cele mai afectate sunt stații de bază și controlere mobile și fibra optică.

Statistica incidentelor care fac parte din categoriile acțiune rău-intenționată și fenomen natural per categorie de resurse afectate este reprezentată în figura următoare.

**Fig.14 Resursele afectate in cazul incidentelor care fac parte din categoriile actiune rau-intentionata si fenomen natural**

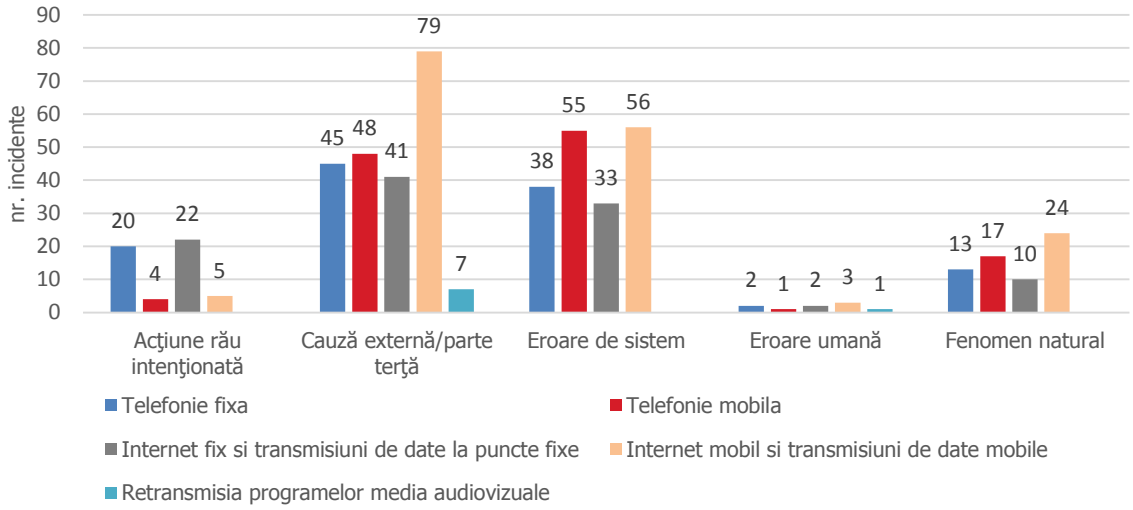


Astfel, se poate observa faptul că cea mai afectată resursă în cazul incidentelor din categoria acțiune rău-intenționată este fibra optică. În principiu, acest lucru s-a datorat acțiunilor de furt și distrugere a unor segmente de cablu de fibră optică.

De precizat că în cazul incidentelor care fac parte din categoria eroare umană, resursele afectate au fost stații de bază și controlere mobile, echipamente din noduri de transmisiuni și routere și switch-uri IP.

Situația privind numărul incidentelor pentru toate tipurile de servicii afectate, în funcție de cauză este prezentată în figura 15.

**Fig.15 Numarul incidentelor pentru toate tipurile de servicii afectate, in functie de cauza**




De precizat faptul că în acest caz suma incidentelor pentru toate tipurile de servicii afectate, în funcție de cauză (Fig.15) diferă de numărul total al incidentelor per tip de cauză (reprezentat în Fig.11) deoarece un incident poate afecta mai multe servicii simultan.

Figura 15 reflectă faptul că fiecare sistem de comunicații prezintă diverse vulnerabilități. Astfel, rețelele care folosesc cablul ca suport pentru transportul semnalelor în scopul furnizării serviciilor prezintă vulnerabilitatea că acest suport poate fi afectat la nivel fizic (secționat, furat etc.). Acest lucru este confirmat și de statistica din figura 15, din care se observă că în cazul incidentelor din categoria acțiune rău-intenționată, care au vizat furtul sau distrugerea cablurilor de fibră optică, cele mai afectate servicii au fost cele de telefonie fixă și cele de acces la internet fix și transmisiuni de date fixe.

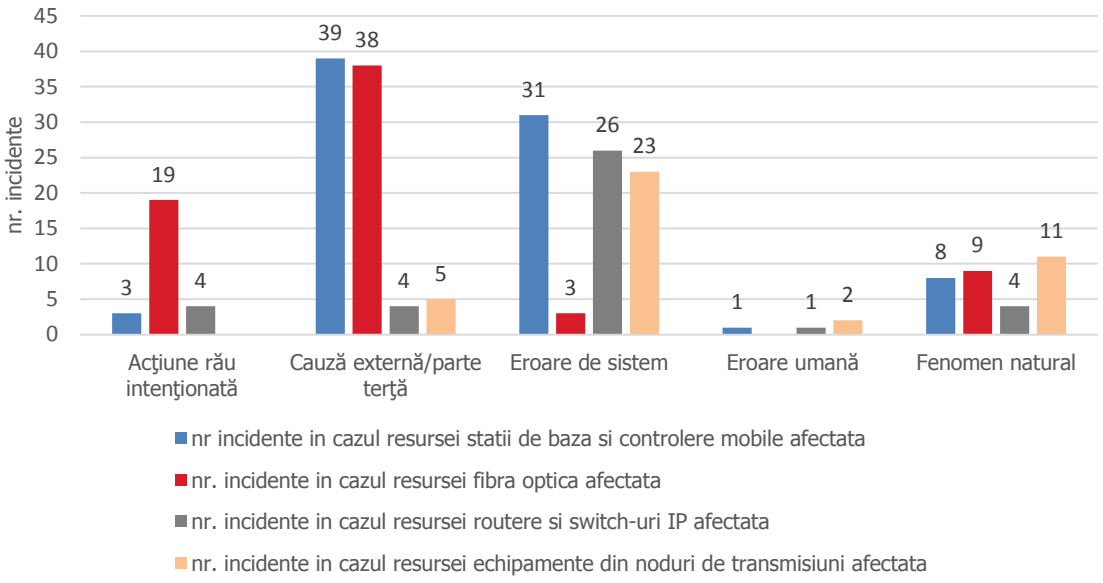
Rețeaua prin intermediul căreia sunt furnizate serviciile mobile prezintă vulnerabilitatea că alimentarea cu energie electrică, necesară funcționării unora dintre componentele rețelei, nu este (în multe cazuri) sub controlul furnizorului de servicii de comunicații electronice. Acest fapt este confirmat și de figura 15, din care se observă că cele mai multe incidente (79) care fac parte din categoria cauză externă/parte terță și care s-au datorat în principal problemelor de alimentare cu energie electrică, au afectat serviciile de internet mobil și transmisiuni de date mobile. În această situație, cele mai afectate au fost stațiile de bază și controlerele mobile.

În cazul incidentelor din categoria fenomen natural care au afectat serviciile de internet mobil și transmisiuni de date mobile, cele mai afectate au fost echipamentele din nodurile de transmisiune, stațiile de bază și controlerele mobile.

Incidentele care s-au datorat erorii umane au afectat în cea mai mică măsură serviciile de comunicații electronice.

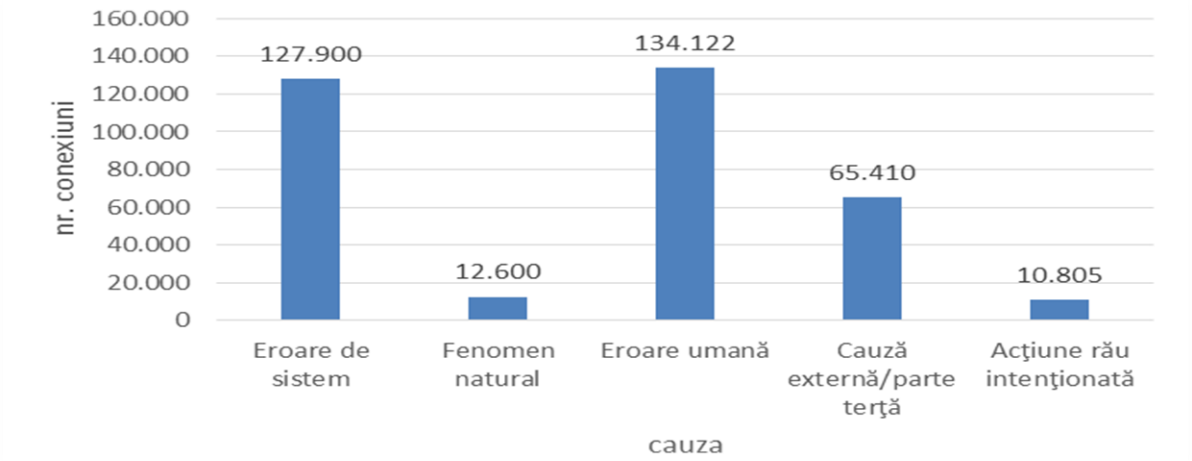
Având în vedere resursele afectate în cazul celor mai multe dintre incidentele petrecute în 2013 (Fig.5), este relevantă statistica privind numărul de incidente care au implicat aceste resurse, în funcție de cauză. Graficul de mai jos prezintă situația în acest sens.

**Fig.16 Numarul incidentelor pentru cele mai afectate resurse in functie de cauza**




În figura de mai jos este reprezentată statistica privind numărul mediu de conexiuni afectate în funcție de cauză.

**Fig.17 Numărul mediu de conexiuni per tip de cauză**




Din graficul de mai sus, se poate observa că incidentele din categoria eroare umană au afectat în medie cel mai mare număr de conexiuni. Cu toate că incidentele din această categorie sunt puține, impactul lor e justificat prin faptul că numărul conexiunilor afectate este foarte mare.

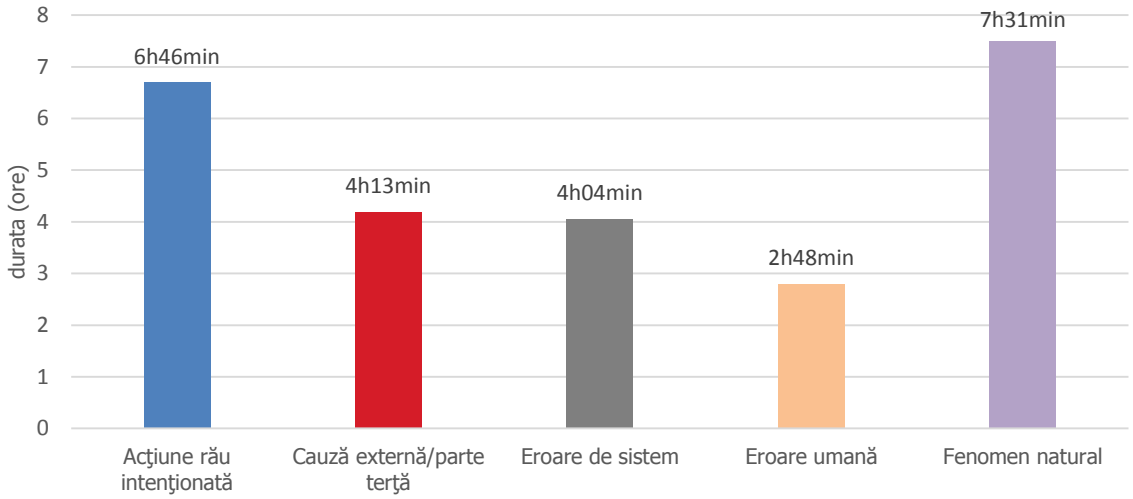
## 3.4 Durata incidentelor și durata de descoperire a incidentelor

Durata unui incident reprezintă intervalul de timp dintre momentul în care serviciul începe să se degradeze sau s-a întrerupt, până în momentul în care acesta este restabilit la parametrii inițiali.

Durata totală a incidentelor raportate pe anul 2013 este de 1.218 ore și durata medie a unui incident este de aproximativ 5 ore.

În figura 18 este ilustrată durata medie a unui incident în funcție de cauza inițială.

**Fig.18 Durata medie a unui incident in functie de cauza initiala**




Cele mai mari valori ale duratei medii a unui incident se regăsesc în cazul categoriilor de cauze fenomen natural, respectiv acțiune rău-intenționată. Aceasta se datorează în principal caracterului greu previzibil al apariției fenomenelor naturale nefavorabile, care au îngreunat totodată accesul echipelor tehnice în vederea restaurării serviciilor, cât și al furtului de echipamente de nivel suport (baterii, acumulatori) sau secționării cablurilor de fibră optică.

Dintre cele 253 de incidente raportate în anul 2013, 201 au fost descoperite în același timp cu momentul producerii incidentului, 33 de incidente au fost descoperite în aproximativ o oră, 15 incidente au fost descoperite până în 5 ore, iar 4 incidente au fost descoperite peste 6 ore de la momentul producerii lui. Durata cea mai lungă raportată până la descoperirea unui incident a fost de aproximativ 13 ore de la momentul producerii lui.

**Fig.19 Numarul de incidente si durata in care au fost descoperite**

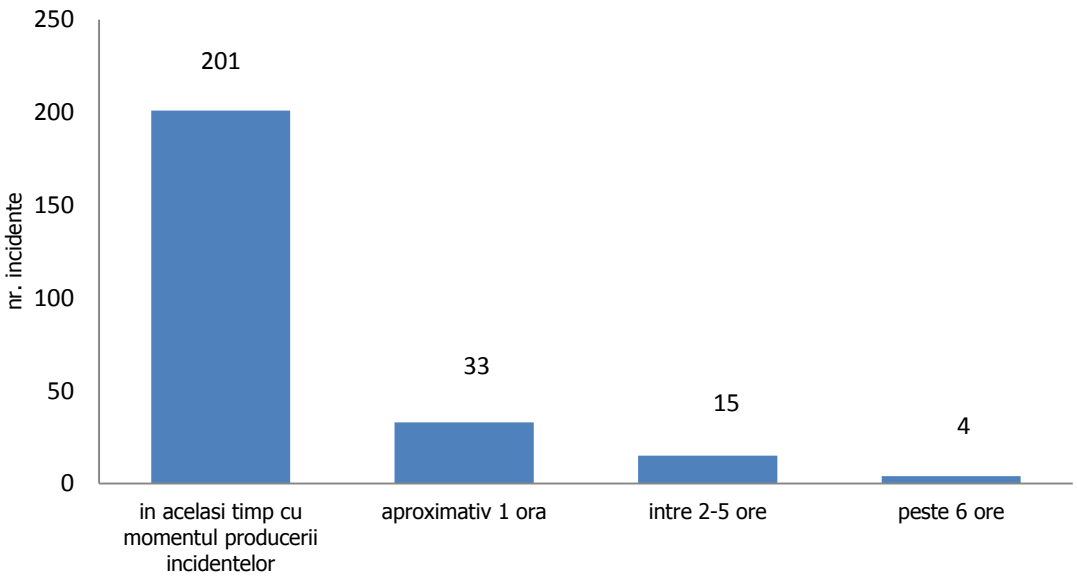
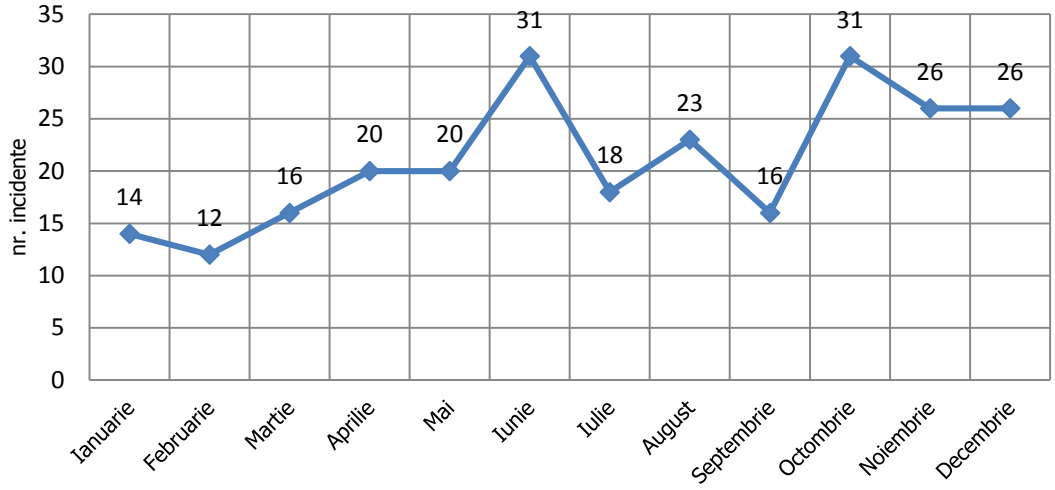


Figura de mai jos reprezintă distribuția incidentelor raportate pe luni în anul 2013.

**Fig.20 Numarul incidentelor inregistrate pe luni in anul 2013**



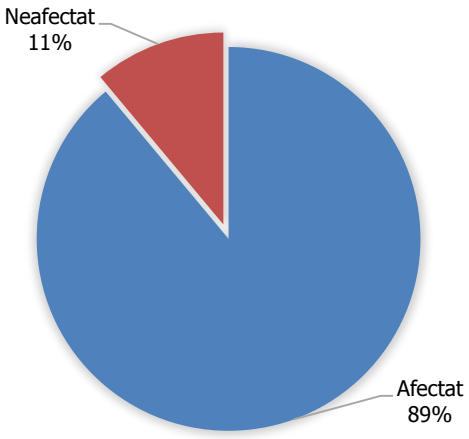

Se poate observa că lunile în care s-au raportat cele mai multe dintre incidente sunt iunie și octombrie. Cauzele producerii incidentelor din aceste perioade fac parte în principal din categoriile fenomene naturale, eroare de sistem și cauză externă/parte terță.

## 3.5 Impactul asupra apelurilor de urgență

89% dintre incidentele raportate în anul 2013 au avut un posibil impact asupra efectuării apelurilor de urgență.

Această statistică este prezentată în figura de mai jos.

**Fig.21 Impactul asupra apelurilor de urgenta**




Având în vedere faptul că incidentele din 2013 au avut un impact mare asupra serviciilor de telefonie (fixă și mobilă), această statistică este predictibilă, deoarece atunci când serviciile de telefonie sunt afectate, în mod implicit este afectat și serviciul de urgență 112.

De menționat faptul că, deși incidentele au avut impact asupra apelurilor de urgență, în principiu, utilizatorii serviciilor de telefonie mobilă au putut apela numărul unic pentru apeluri de urgență dacă zona din care s-a inițiat apelul era acoperită de alt furnizor de telefonie mobilă sau de alte stații de bază din rețea, neafectate de incident.

## 4. Acțiunile de răspuns la incident

Acțiunile de răspuns la incident au cuprins atât măsuri preventive de securitate implementate în vederea minimizării riscului apariției incidentelor, cât și acțiuni întreprinse și măsuri adoptate în scopul de a restabili serviciul la parametrii inițiali.

Conform raportărilor furnizorilor, în scopul remedierii problemelor apărute, printre acțiunile de răspuns întreprinse se numără următoarele:

- Repararea/înlocuirea echipamentului afectat (măsură luată în cazul defectării componentelor hardware ale echipamentelor);
- Redirecționarea traficului (în cazul unor incidente care fac parte din categoria eroare de sistem);
- Refacerea infrastructurii fizice prin înlocuirea cablurilor și echipamentelor sustrase sau deteriorate (în cazul incidentelor care fac parte din categoria cauză externă/parte terță sau acțiuni rău-intenționate);
- Contactarea furnizorului de echipamente în vederea soluționării problemei (în cazul unor incidente din categoria eroare de sistem);
- Reconfigurarea și reinițializarea echipamentelor (în cazul unor incidente din categoria eroare de sistem sau eroare umană).

Măsurile de securitate reprezintă mijloace (de natură administrativă, tehnică, managerială sau juridică) de management al riscurilor, incluzând politici, acțiuni, planuri, echipamente, facilități, proceduri, tehnici etc. menite să elimine sau să reducă riscurile privind securitatea și integritatea rețelelor sau a serviciilor de comunicații electronice.

Privitor la măsurile luate sau planificate pentru a împiedica producerea unui incident similar sau eliminarea cauzei incidentului produs, raportările furnizorilor au cuprins:

- Stabilirea/revizuirea procedurilor;
- Achiziționarea unor echipamente de backup;
- Asigurarea mentenanței periodice a echipamentelor;
- Asigurarea redundanței căilor de transmisiune;
- Achiziționarea echipamentelor care să asigure alimentarea cu energie electrică pentru un timp mai îndelungat;
- Creșterea securității locațiilor în care s-au înregistrat acțiuni rău intenționate (în cazuri de furt/distrugere resurse fizice);
- Adoptarea de metode care să garanteze buna funcționare a echipamentului indiferent de condițiile meteorologice (degivrare). Aceste metode vizează în principal incidentele care fac parte din categoria fenomen natural.

Menționăm faptul că în cazul mai multor incidente nu a fost completat câmpul referitor la măsurile luate sau planificate pentru a împiedica producerea unui incident similar/eliminarea cauzei incidentului. Acest lucru este datorat unor deficiențe de raportare, dar și faptului că unele incidente au fost cauzate de părți terțe (de ex. lucrări efectuate de terți), situație care nu necesită neapărat implementarea unor măsuri de securitate. Totuși, este recomandabil ca organizația să analizeze

periodic informațiile despre incidente pentru a identifica tendințele acestora și domeniile ce necesită atenție specială și pentru a analiza măsurile ce pot fi luate pentru prevenirea unor incidente similare.

Datele privind măsurile de securitate adoptate de furnizori, precum și măsurile luate sau planificate pentru a împiedica producerea unui incident similar sau eliminarea cauzei incidentului produs, sunt necesare pentru urmărirea lecțiilor învățate în urma măsurilor de detectare, răspuns și de recuperare luate înainte, în timpul și după incident.

# 5. Concluzii

Prin analiza incidentelor cu impact semnificativ asupra rețelelor și serviciilor de comunicații electronice, ANCOM este informată cu privire la cauzele incidentului, poate urmări acțiunile furnizorului în vederea remedierii rețelelor și serviciilor la un nivel corespunzător și poate evalua nivelul de securitate al rețelelor și serviciilor de comunicații electronice. Analiza statistică a incidentelor constituie, de asemenea, un instrument eficient de a urmări tendințele acestora.

Datele privind incidentele sunt fundamentale pentru dezvoltarea unei înțelegeri clare a naturii si amplorii provocărilor existente la adresa securității si integrității rețelelor și serviciilor prin analiza amenințărilor si vulnerabilităților la adresa securității si integrității rețelelor și serviciilor si prin identificarea de bune practici bazate pe lecțiile învățate în procesul de management al incidentelor.

## 5.1 Concluzii în urma analizei incidentelor

În urma centralizării și analizării celor 253 de incidente raportate de către cei 6 furnizori de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului, pentru anul 2013, se pot desprinde următoarele concluzii:

- Serviciul cel mai afectat din punct de vedere al numărului de conexiuni este serviciul de telefonie mobilă (9.970.185 conexiuni afectate);
- În cazul serviciilor de acces la internet mobil și transmisiuni de date mobile, incidentele au afectat 62% din totalul conexiunilor existente pe piață;
- Marea majoritate a incidentelor a afectat serviciile de acces la internet mobil și serviciile de transmisiuni de date mobile (167 incidente);
- Numărul mediu de conexiuni afectate de un incident din 2013 este de 78.960;
- Resursele cele mai afectate au fost stațiile de bază, controlerele mobile și fibra optică;
- 67 dintre incidente s-au produs din cauza problemelor de alimentare cu energie electrică;
- Aproximativ 74% dintre incidente au avut impact asupra unui singur județ;
- Aproximativ 40% dintre incidente fac parte din categoria eroare de sistem, iar 35% au avut cauze externe/părți terțe;
- În cazul incidentelor având drept cauză eroare de sistem, cele mai afectate resurse au fost din categoria stații de bază și controlere mobile, iar în cazul incidentelor din categoria cauză externă, cele mai afectate resurse au fost stațiile de bază și controlerele mobile și fibra optică;
- Cele mai multe incidente care au afectat serviciile de acces la internet mobil fac parte din categoria cauză externă;
- Incidentele cauzate de fenomene naturale și de acțiuni rău intenționate au afectat rețelele și serviciile de comunicații electronice pentru un timp mai îndelungat decât incidentele care fac parte din celelalte categorii de cauze (7h31min, respectiv 6h46min);

- Aproximativ 80% dintre incidente au fost descoperite în momentul producerii; 15 incidente au fost descoperite până în 5 ore, iar 4 incidente au fost descoperite după 6 ore de la momentul producerii lor. Cea mai lungă durată a unui incident a înregistrat aproximativ 13 ore;
- Cele mai multe incidente (25%) s-au înregistrat în lunile iunie și octombrie;
- 89% dintre incidente au avut impact asupra apelurilor de urgență.

## 5.2 Concluzii privind deficiențele de raportare

Pentru a avea o imagine clară și corectă a situației privind incidentele de securitate raportate în anul 2013, este esențial ca raportările furnizorilor să conțină informații complete, corecte și comparabile.

În urma analizei informațiilor cuprinse în raportările transmise de furnizori, s-au constatat mai multe deficiențe de raportare.

Una dintre acestea este necompletarea numărului de conexiuni afectate, furnizorii specificând în acest caz doar tipurile de servicii și proporția în care acestea au fost afectate (de ex. *în proporție de peste 50%*).

În unele cazuri, furnizorii nu au specificat cu exactitate resursele afectate, câmpul aferent resurselor afectate fiind completat cu o denumire generică (de ex. *power*, *switching, transmisiuni*). Acest lucru a îngreunat procesul încadrării incidentelor respective în categorii de resurse.

Există, de asemenea, deficiențe de raportare în ceea ce privește cauza producerii incidentului. Astfel, în câteva cazuri, informațiile aferente acestui câmp lipsesc, sau sunt incorecte. Având în vedere că unele incidente pot avea o cauză inițială și una subsecventă, în urma studierii incidentelor, s-a constatat că în raportare nu s-a făcut distincție între aceste două tipuri de cauze. Deși trebuie raportată cauza inițială, în unele cazuri, furnizorii au completat câmpul aferent cu cauza subsecventă sau cu ambele tipuri de cauze corelate (de ex. *fenomen natural/eroare de sistem*).

O mare parte dintre furnizori nu a completat câmpurile privind acțiunile de răspuns la incident și măsurile luate sau planificate pentru a împiedica producerea unui incident similar/eliminarea cauzei incidentului. În câteva cazuri, câmpul privind acțiunile de răspuns la incident a fost completat cu informația irelevantă *Conform procedurilor interne*.

Pentru asigurarea calității procesului de raportare, ANCOM are în vedere luarea măsurilor necesare astfel încât să se asigure că informațiile solicitate referitoare la incidentele cu impact semnificativ asupra furnizării rețelelor și serviciilor de comunicații electronice sunt transmise în mod complet și corect.

De asemenea, în vederea clarificării unor detalii tehnice privind procedura de identificare și raportare a incidentelor de securitate, ANCOM are în vedere elaborarea unui ghid de raportare a incidentelor de securitate ce au afectat securitatea și integritatea rețelelor publice de comunicații electronice și servicii de comunicații electronice destinate publicului. Ghidul se adresează furnizorilor de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului în scopul transmiterii către ANCOM de informații cât mai corecte, complete și comparabile asupra incidentelor care au un impact semnificativ asupra securității și integrității rețelelor și serviciilor de comunicații electronice.

*Autoritatea Naţională pentru Administrare şi Reglementare în Comunicaţii (ANCOM) este instituţia care protejează interesele utilizatorilor de comunicaţii din România, prin promovarea concurenţei pe piaţa de comunicaţii, administrarea resurselor limitate, încurajarea investiţiilor eficiente în infrastructură şi a inovaţiei. Pentru mai multe detalii despre activitatea ANCOM vizitaţi www.ancom.org.ro, www.portabilitate.ro şi www.veritel.ro.*