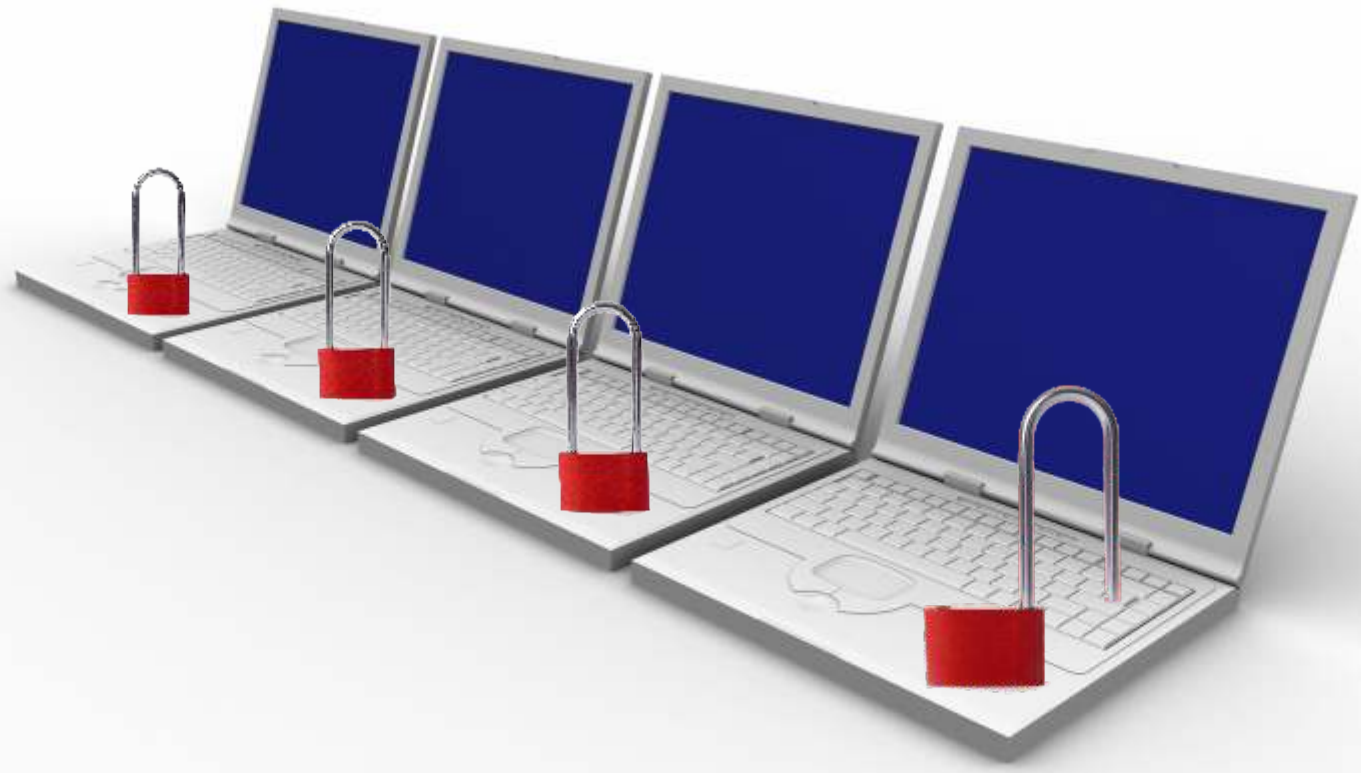
ANCOM
Autoritatea Naţională pentru Administrare
şi Reglementare în Comunicaţii

RAPORT
privind incidentele care au afectat securitatea și integritatea rețelelor și serviciilor de comunicații electronice în anul 2014



Data publicării: 21.05.2015

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, cu modificările și completările ulterioare, 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*."

În vederea îndeplinirii obligației de a transmite informațiile relevante către Comisia Europeană și ENISA (Agenția Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor), în urma analizei incidentelor raportate de furnizorii de rețele și servicii de comunicații electronice în 2014, 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] Varianta integrală a documentului este disponibilă la următoarea adresă: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/Technical%20Guidelines%20on%20Incident%20Reporting

[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 2014

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 etapă constă în completarea electronică, în termen de două săptămâni de la detectarea incidentului cu impact semnificativ, a unei notificări finale prin intermediul unei aplicații disponibile pe pagina[4] de internet a ANCOM.

În cadrul notificării finale, informațiile raportate de furnizori în 2014 se referă 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.

3. Analiza incidentelor raportate

În anul 2014 au fost raportate 359 de incidente de către 7 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:

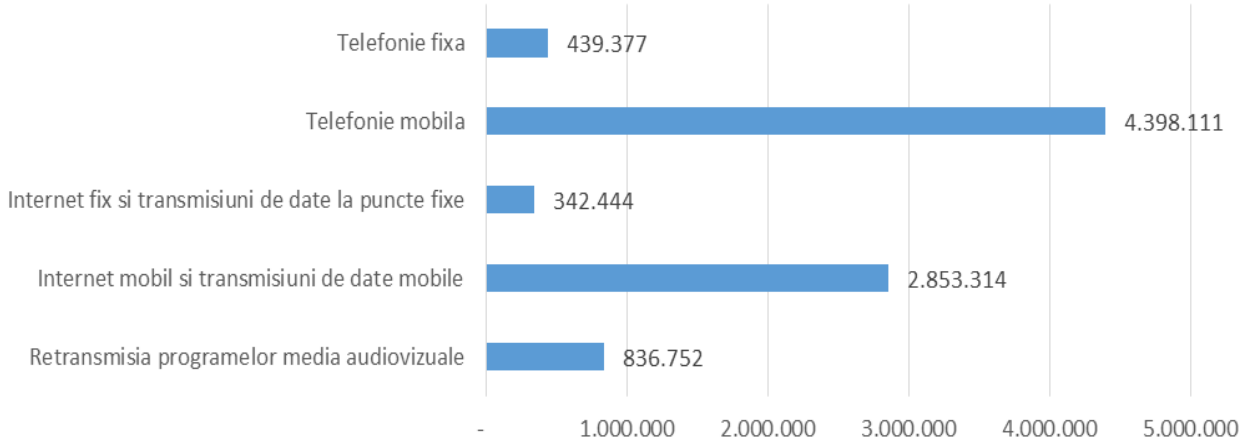
1. Impactul asupra serviciilor și utilizatorilor
    - Conexiuni afectate,
    - Servicii afectate,
    - Resurse afectate,
    - Aria/răspândirea geografică.
2. Cauzele incidentelor raportate
3. Durata incidentelor și durata de descoperire
4. Impactul asupra apelurilor de urgență

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

3.1 Impactul asupra serviciilor și utilizatorilor

Numărul total de conexiuni afectate de cele 359 de incidente cu impact asupra principalelor servicii de comunicații electronice în anul 2014 este reprezentat în graficul de mai jos.

Fig.1 Numărul de conexiuni afectate per serviciu



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.

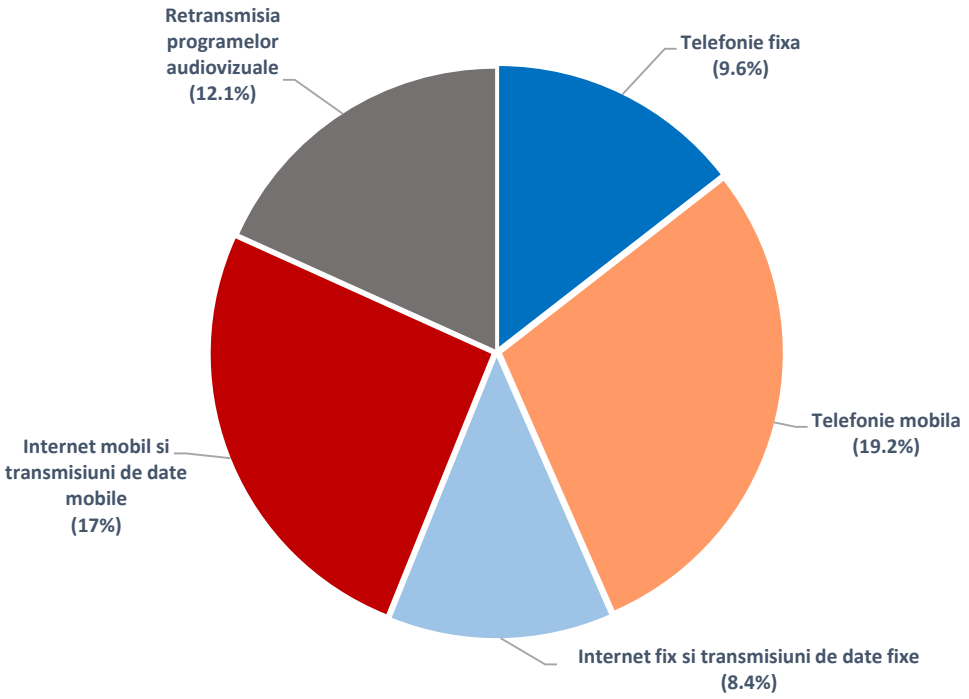
În 2014 cele mai afectate au fost serviciile de telefonie mobilă (4.398.111 conexiuni afectate). Se consideră că în cazul incidentelor care au afectat serviciile de telefonie mobilă, au fost afectate și serviciile de transmisiuni de date – SMS.

În Fig.1 se poate observa că serviciile de telefonie fixă și serviciile de internet fix și transmisiuni de date la puncte fixe au fost afectate în mică măsură (439.377 conexiuni, respectiv 342.444 conexiuni afectate).

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

[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.

Fig.2 Procentul de conexiuni afectate în raport cu numărul total de conexiuni per serviciu*

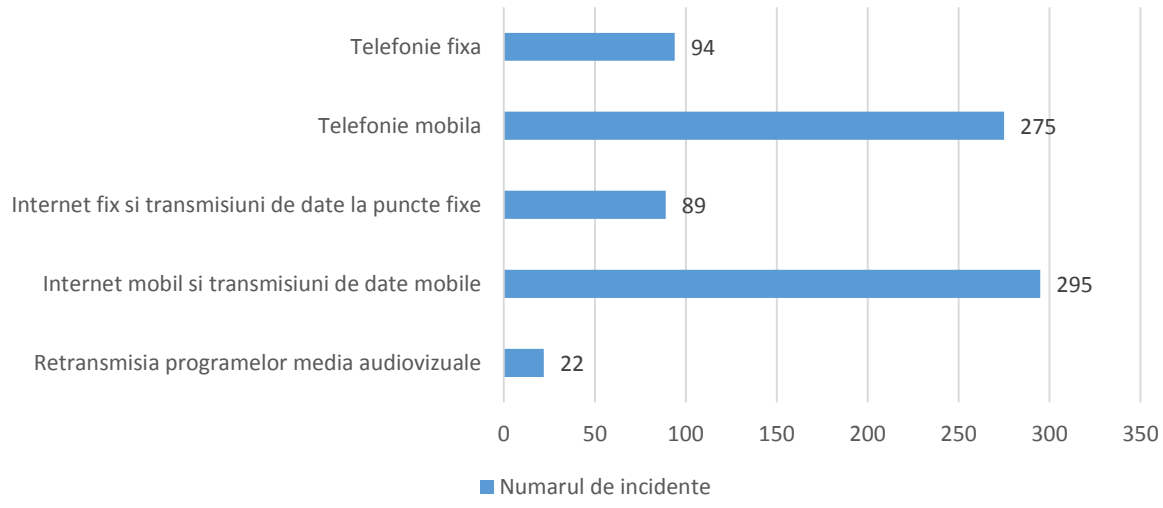


* Conform Raportului privind datele statistice, semestrul II 2014, care poate fi accesat la următoarea adresă: https://statistica.ancom.org.ro:8000/sscpds/public/alldocuments/report

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.

În Fig.2 se poate observa că și în cazul în care raportarea se face la numărul total de conexiuni, serviciile de telefonie mobilă și serviciile de internet mobil și transmisiuni de date mobile au fost afectate într-un procent mai mare față de celelalte servicii.

Fig.3 Impactul asupra serviciilor

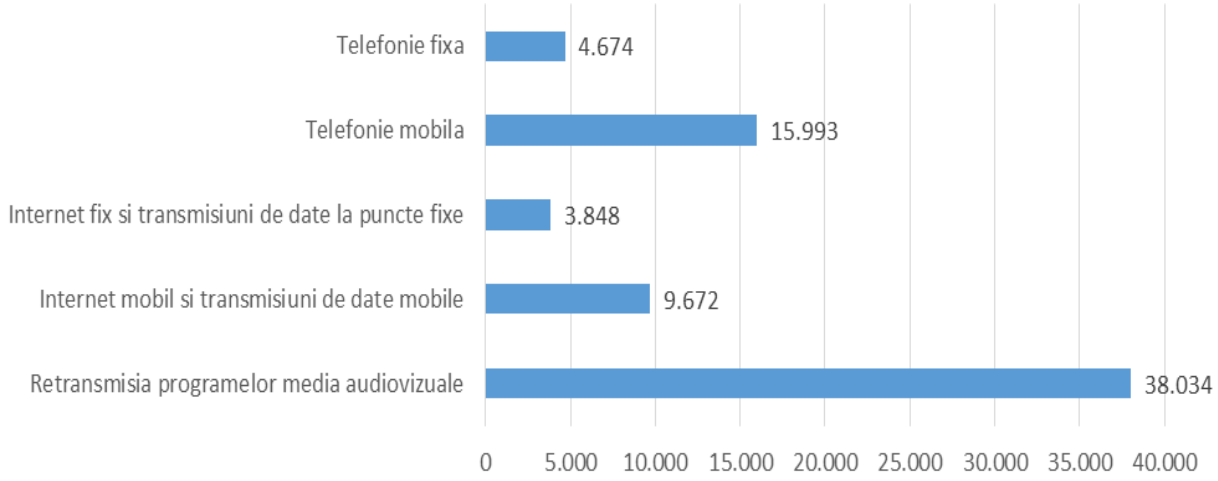


În Fig. 3 se observă că cele mai multe dintre incidentele raportate în 2014 au afectat serviciile de acces la internet mobil și transmisiuni de date la puncte mobile și serviciile de telefonie mobilă (295, respectiv 275 incidente). În ceea ce privește serviciile de telefonie fixă și acces la internet fix și transmisiuni la puncte fixe, acestea au fost afectate de 94, respectiv 89 de incidente raportate în 2014.

De precizat faptul că suma incidentelor pentru fiecare tip de serviciu afectat diferă față de numărul total al incidentelor deoarece un incident afectează în majoritatea cazurilor mai multe tipuri de servicii simultan.

Conform datelor raportate de către furnizori, numărul mediu de conexiuni afectate de un incident în 2014 este de 24.615. 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).

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



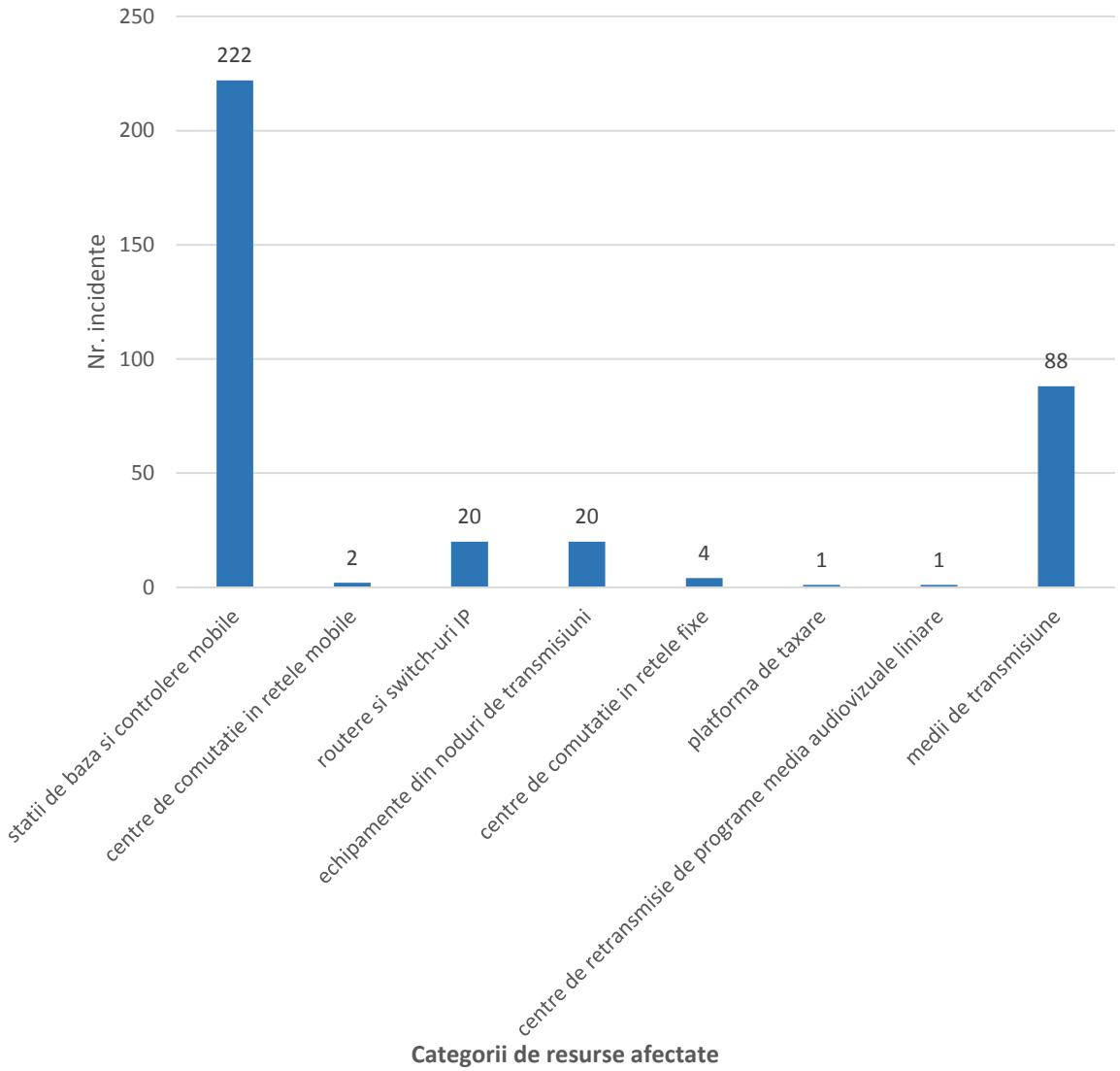
Se poate observa că, deși serviciile de retransmisie a programelor audiovizuale au fost afectate în cazul a 22 de incidente (însemnând aproximativ 6% din totalul incidentelor raportate în 2014), acestea au înregistrat cea mai mare valoare în ceea ce privește numărul mediu de conexiuni afectate de un incident în 2014 (38.034 conexiuni). Numărul mediu de conexiuni afectate în cazul serviciilor de telefonie mobilă este de aproximativ 16.000, iar cele mai mici valori se înregistrează la nivelul serviciilor de telefonie fixă și serviciilor de acces la internet fix și transmisiuni de date la puncte fixe (4.674 conexiuni, respectiv 3.848 conexiuni).

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, conform *Ghidului de raportare a incidentelor*[7], elaborat de ANCOM. Astfel, graficul următor evidențiază numărul de incidente ce au afectat fiecare categorie de resurse în parte.

[7] Textul integral al documentului *Ghid de raportare a incidentelor* este disponibil la următoarea adresă: http://www.ancom.org.ro/uploads/links_files/20141219_GHID_DE_RAPORTARE_A_INCIDENTELOR.pdf

Fig.5 Număr incidente per resurse afectate

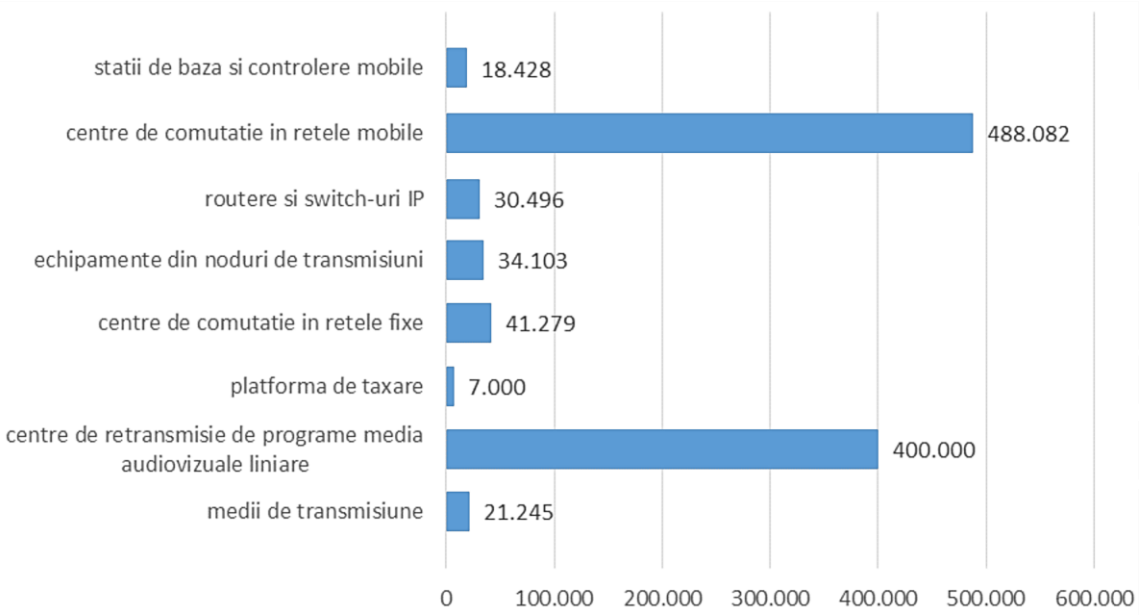


De precizat faptul că în cazul unui incident, au fost afectate concomitent două resurse care fac parte din categoriile Stații de bază și controlere mobile și Echipamente din noduri de transmisiune.

În Fig.5 se poate observa că în cazul celor mai multe incidente, resursele afectate fac parte din categoria Stații de bază și controlere mobile. Acest lucru este explicabil, având în vedere faptul că, din punct de vedere al numărului de conexiuni, cele mai afectate au fost serviciile de telefonie mobilă și serviciile de internet mobil și transmisiuni de date mobile (Fig.1). În cazul a 88 dintre incidente, resursa afectată face parte din categoria Medii de transmisiune (de ex. cablul de fibră optică).

Pentru a evidenția impactul pe care îl poate avea afectarea unei resurse asupra serviciilor de comunicații electronice, în graficul de mai jos este reprezentat numărul mediu de conexiuni afectate pentru toate tipurile de servicii, în funcție de resursele afectate.

Fig.6 Numărul mediu de conexiuni afectate în funcție de resurse



Se observă că resursele din categoriile Centre de comutație mobilă și Centre de retransmisie a programelor media audiovizuale reprezintă resurse critice, afectarea acestora având de fiecare dată un impact major asupra conexiunilor. Astfel, numărul mediu de conexiuni afectate în cele două cazuri a înregistrat valorile cele mai mari (488.082 conexiuni, respectiv 400.000 conexiuni).

Ținând cont de gradul de complexitate a diferitelor tipuri de resurse (unele pot fi constituite din 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 2014:

- Nivelul suport, face referire la componentele suport ale echipamentelor precum cele utilizate pentru alimentarea cu energie electrică, echipamente auxiliare (de alimentare de backup cu energie electrică – Grup electrogen, baterie/UPS, Sisteme de monitorizare și control al temperaturii – cooler, aer condiționat etc.), instalații electrice (cabluri electrice, siguranțe, întrerupătoare, transformatoare etc. deținute de furnizor) etc.;
- Nivelul fizic, care face referire la componentele hardware ale echipamentelor/ resurselor;
- Nivelul logic, care face referire la componentele software ale echipamentelor/ resurselor.

În graficul următor este reprezentat impactul celor 359 de incidente asupra resurselor în funcție de cele trei nivele enunțate mai sus. Menționăm faptul că în cazul a 3 incidente, informațiile raportate de furnizori nu au fost suficiente pentru a putea identifica nivelul la care au fost afectate resursele, fiind vorba în principal de defecțiuni pe liniile de transmisiuni închiriate de la alți furnizori de comunicații electronice.

Fig.7 Ponderea incidentelor pe tipuri de nivele afectate

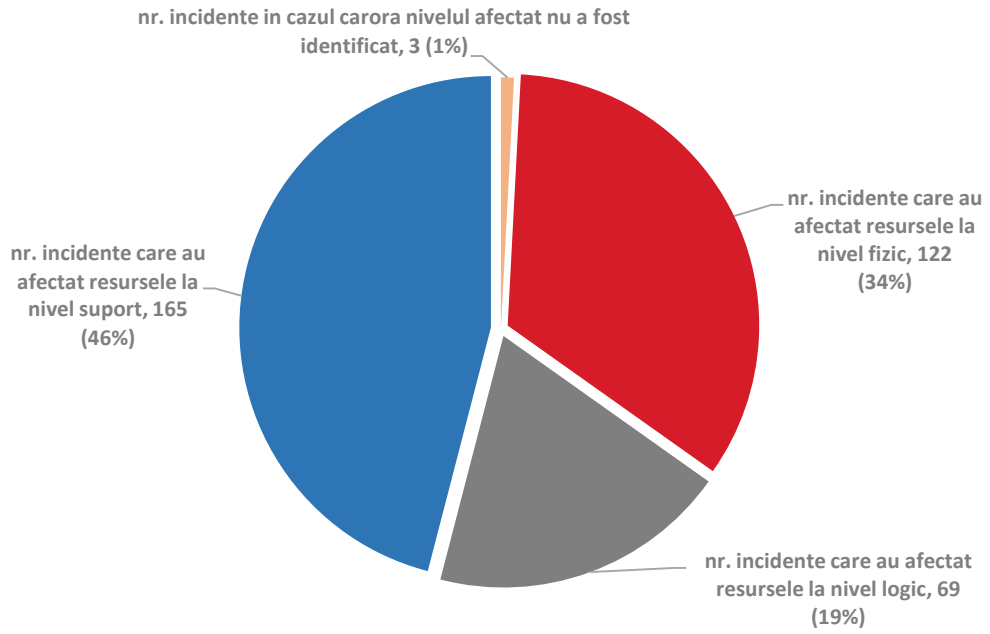
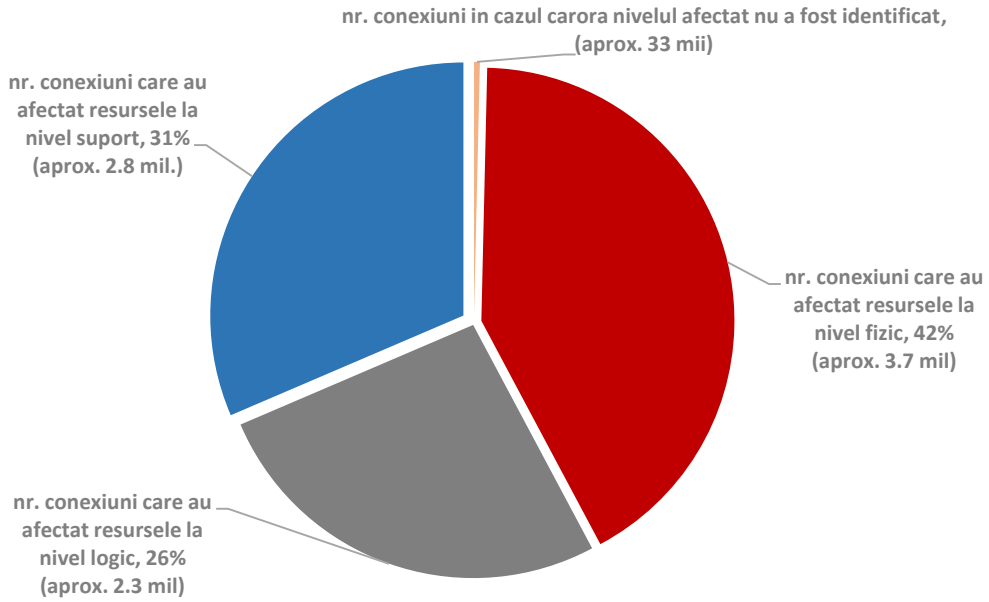


Fig.8 Impactul incidentelor pe tipuri de nivele afectate



Din cele două grafice (Fig.7 și Fig.8) se poate desprinde concluzia că o pondere mare a incidentelor nu are neapărat ca efect un impact major asupra serviciilor. Astfel, în cazul incidentelor care au afectat resursele la nivel suport se poate observa faptul că, deși acestea au înregistrat o pondere mare (46% din totalul incidentelor), numărul conexiunilor afectate este mai mic în comparație cu numărul de conexiuni afectate în cazul incidentelor care au afectat resursele la nivel fizic (a căror pondere este de 34%). Totodată, deși numărul conexiunilor care au afectat resursele la nivel fizic reprezintă 42% din totalul conexiunilor afectate, ponderea incidentelor care au afectat resursele la nivel fizic este de 34%. Fiecare dintre aceste nivele este analizat în cele ce urmează.

Nivelul suport

În 2014 au fost raportate 165 de incidente care au afectat resursele la nivel suport. 163 dintre acestea (reprezentând aproximativ 45% din totalul incidentelor raportate) s-au produs din cauza problemelor de alimentare cu energie electrică. În 139 dintre aceste cazuri, incidentele s-au datorat cauzelor externe, în principal fiind raportate avarii la furnizorul de energie electrică, întreruperi ale alimentării cu energie electrică în urma fenomenelor meteorologice nefavorabile și probleme datorate supratensiunilor și șocurilor de energie electrică, în urma cărora au fost scoase din funcțiune diferite echipamente (prin blocarea acestora, ori prin pierderea configurației). În 24 de cazuri, problemele de alimentare cu energie electrică s-au datorat în principal defectării echipamentului de electro-alimentare, fapt care a condus la întreruperea funcționării unor echipamente.

Celelalte 2 incidente care au afectat resursele la nivel suport includ incidentele produse din cauza problemelor semnalate la nivelul sistemului automat de climatizare.

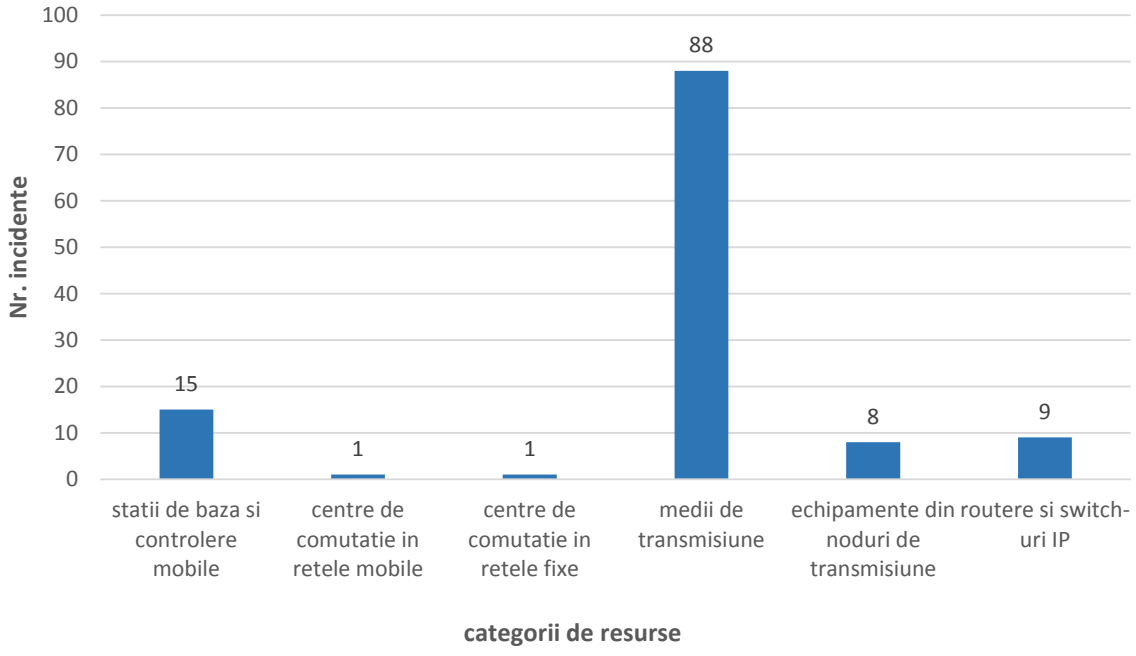
Resursele afectate la nivel suport fac parte în principal din categoria stații de bază și controlere mobile (155 incidente). Alte resurse afectate sunt din categoriile: centre de comutație în rețelele fixe (3 incidente), echipamente din noduri de transmisiune (2 incidente), routere și switch-uri IP (4 incidente). În cazul unui incident, din cauza problemelor de alimentare cu energie electrică au fost afectate concomitent două resurse care fac parte din categoria Stații de bază și controlere mobile și echipamente din noduri de transmisiune.

Această statistică scoate în evidență vulnerabilitatea resurselor care fac parte din categoria stații de bază și controlere mobile la întreruperile în alimentarea cu energie electrică.

Având în vedere numărul mare de incidente care se datorează problemelor de alimentare cu energie electrică, precum și impactul considerabil al acestora asupra rețelelor și serviciilor de comunicații electronice (peste 2.500.000 de conexiuni afectate în incidentele raportate), ANCOM recomandă furnizorilor găsirea unor soluții viabile în vederea diminuării acestei probleme.

Nivelul fizic

Fig.9 Resurse afectate la nivel fizic



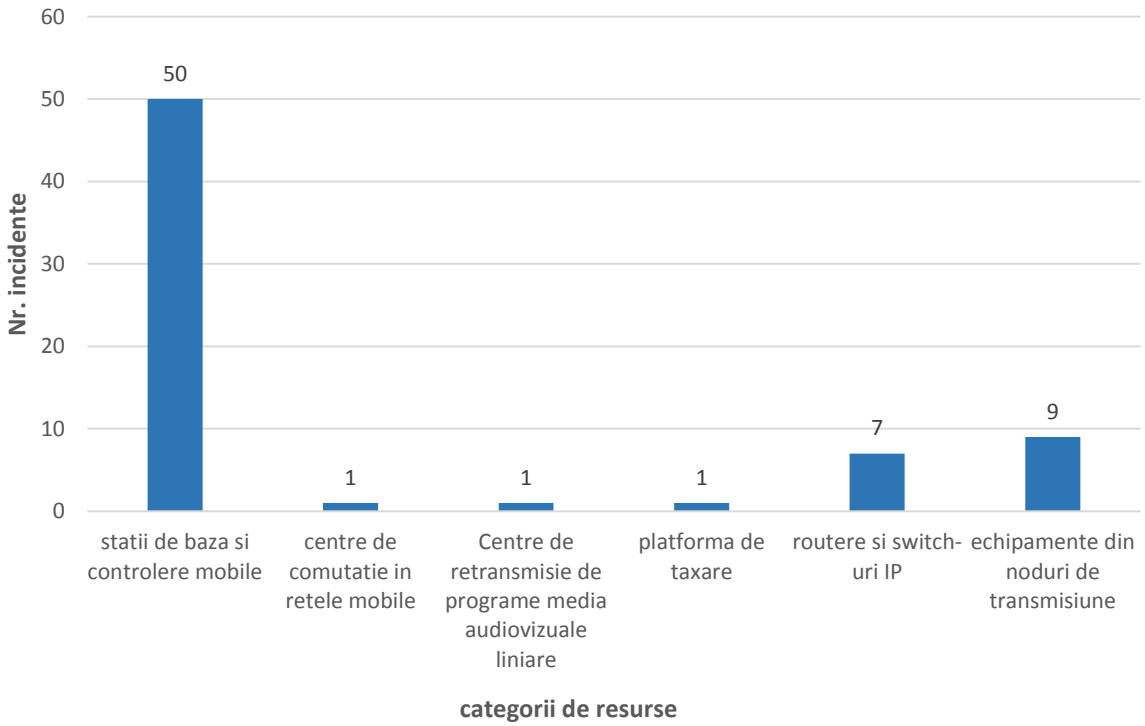
La nivel fizic, cea mai afectată resursă este fibra optică (încadrată în categoria medii de transmisiune). Din cele 88 de incidente care au afectat la nivel fizic acest tip de resursă, în 64 de cazuri incidentele se datorează lucrărilor efectuate de terți, iar în 6 cazuri incidentele s-au datorat fenomenelor naturale (de ex. înghețarea unor joncțiuni, fibra a fost ruptă de furtuni sau în urma surpării malurilor). 18 incidente care au afectat fibra optică la nivel fizic s-au datorat acțiunilor rău-intenționate (în principiu aceste acțiuni reprezentând tentative de furt). În 42 din cele 88 de cazuri, măsura planificată de furnizori pentru a împiedica producerea unor incidente similare o reprezintă creșterea securității în zonele respective care constau în patrulări cu echipe speciale.

În ceea ce privește resursele care fac parte din categoriile Echipamente din noduri de transmisiune și routere și switch-uri IP, acestea au fost afectate la nivel fizic fie în urma fenomenelor naturale (fulger, rafale de vânt, ploi), fie în urma infiltrării apei la nivelul diverselor echipamente (în urma căreia au fost afectate interfețe ale unor routere, ori s-au produs scurtcircuite).

Nivelul logic

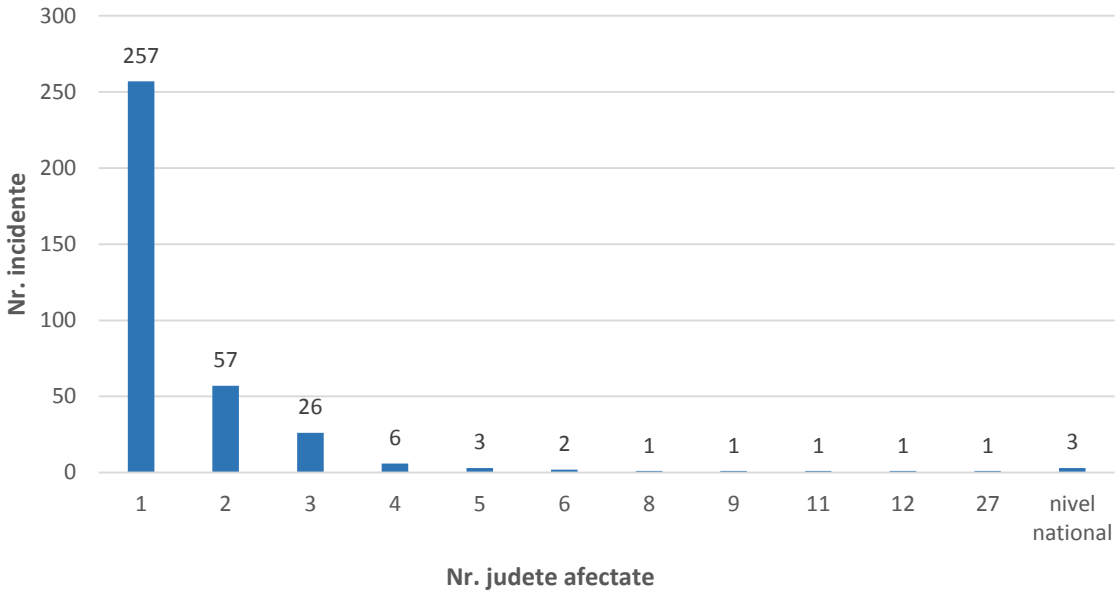
În urma raportărilor furnizorilor, s-au înregistrat 69 de incidente care au afectat resursele la nivel logic. Incidentele care au afectat resursele la nivel logic s-au datorat unor erori apărute în funcționarea software a diferitelor echipamente sau configurării greșite a acestora.

Fig.10 Resurse afectate la nivel logic



În ceea ce privește regiunea geografică afectată de incidente, în cele mai multe cazuri (257), incidentele raportate au afectat un singur județ, 57 de incidente au avut impact asupra două județe, iar în cazul a 3 incidente, furnizorii au raportat că impactul a fost la nivel național.

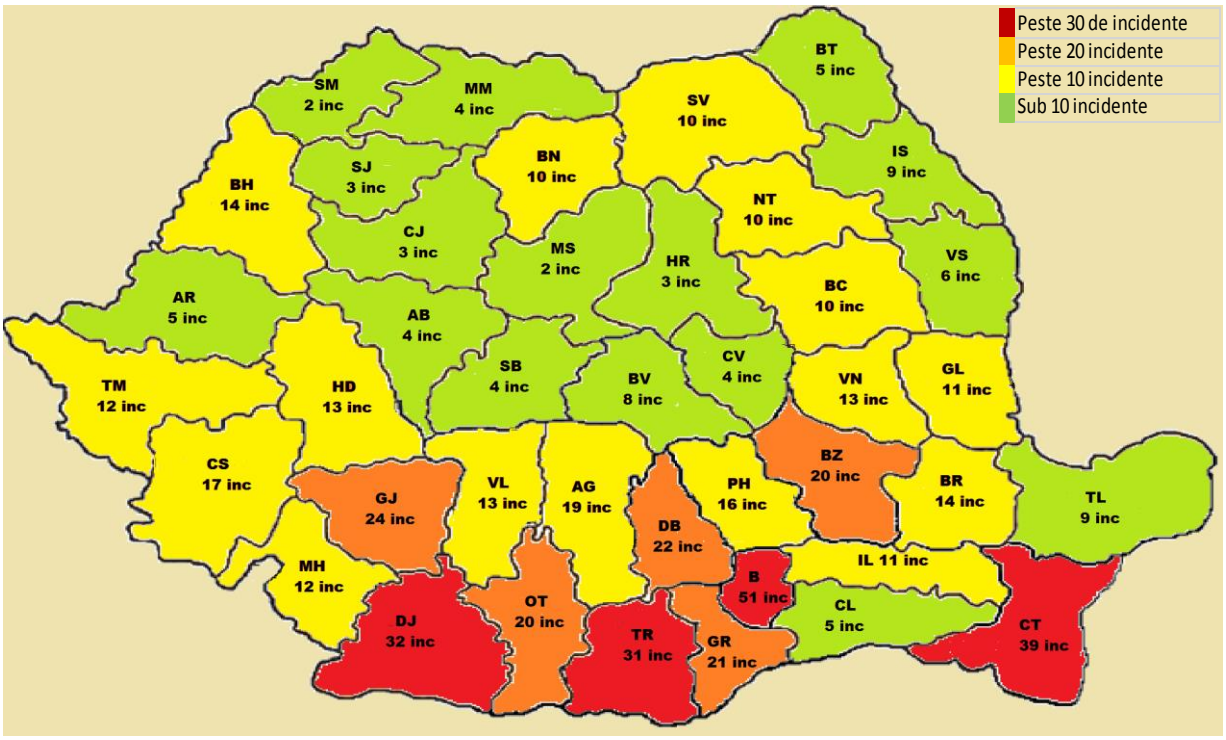
Fig.11 Impactul incidentelor asupra regiunilor geografice efectuate



Analiză geografică

Pentru o imagine mai clară a numărului de incidente care a afectat fiecare județ în parte, prezentăm mai jos situația comparativă la nivel național.

Fig.12 Situația incidentelor la nivel național



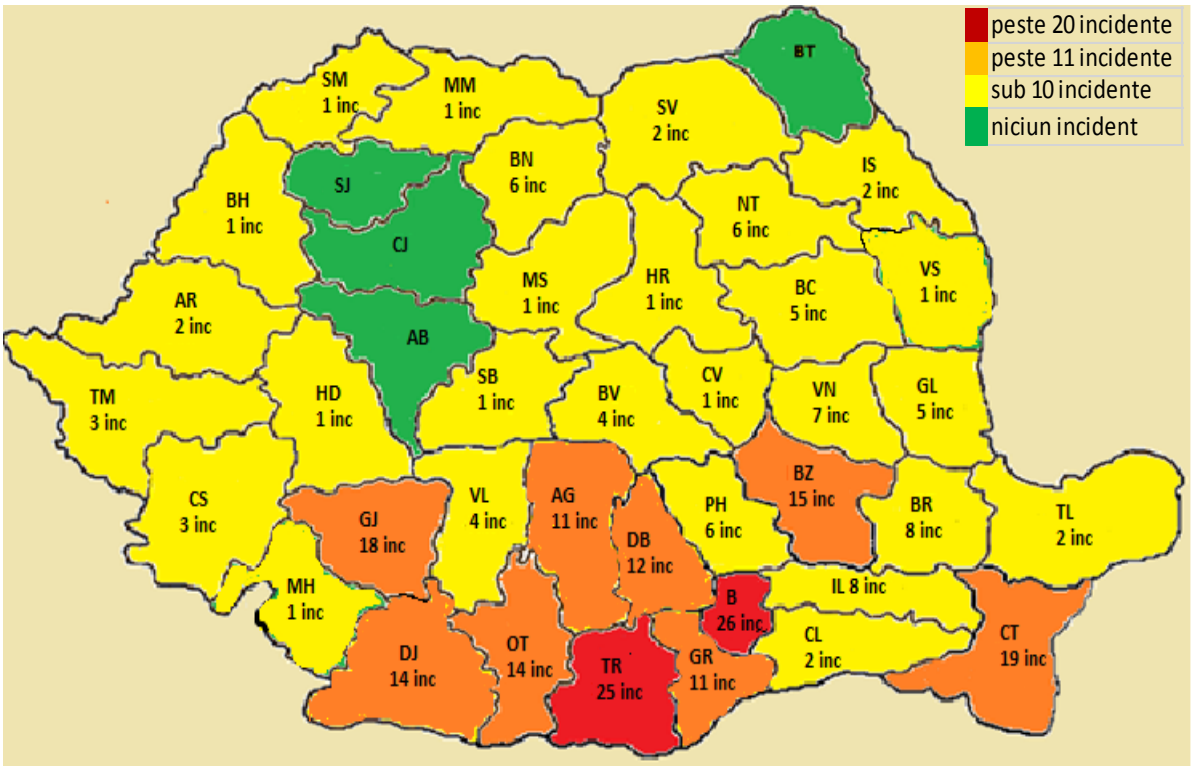
De precizat faptul că numărul incidentelor însumate la nivel național nu coincide cu numărul de incidente raportate în 2014 (359 incidente) pentru că în cazul a 102 incidente, acestea au avut impact asupra cel puțin a două județe.

Conform raportărilor, cele mai multe incidente au avut loc în București (51 incidente) și în Constanța (39 incidente). De asemenea, județele Dolj și Teleorman reprezintă zone foarte afectate la nivelul cărora s-au înregistrat peste 30 de incidente.

Precizam faptul că în urma raportărilor, s-a putut face distincție între numărul incidentelor înregistrate în București și numărul incidentelor care au afectat județul Ilfov (20 incidente).

Având în vedere numărul mare al incidentelor care au avut drept cauză problemele de alimentare cu energie electrică, o situație pe județe în această privință este relevantă.

Fig.13 Situația la nivel național a incidentelor care s-au datorat problemelor de alimentare cu energie electrică



Conform raportărilor furnizorilor, cele mai multe incidente care s-au datorat problemelor de alimentare cu energie electrică s-au înregistrat în București și Teleorman (26 incidente, respectiv 25 incidente).

În cazul județelor Olt, Teleorman și Gorj, incidentele cauzate de probleme cu alimentarea cu energie electrică reprezintă cel puțin 70% din incidentele care au fost raportate în aceste zone.

De remarcat faptul că există 4 zone (Botoșani, Sălaj, Cluj, Alba) în care alimentarea cu energie electrică nu a reprezentat o problemă în 2014.

În cazul întreruperii alimentării cu energie electrică, deși furnizorii dispun de surse de alimentare de backup cu energie, serviciile au fost totuși afectate din cauza autonomiei mici a acestor surse sau din cauză că momentul punerii lor în funcțiune nu a coincis cu momentul producerii

incidentului (pentru activarea lor fiind necesară deplasarea unei echipe de intervenție la locul incidentului, de exemplu în cazul instalării unui grup electrogen, sau a unui generator mobil).

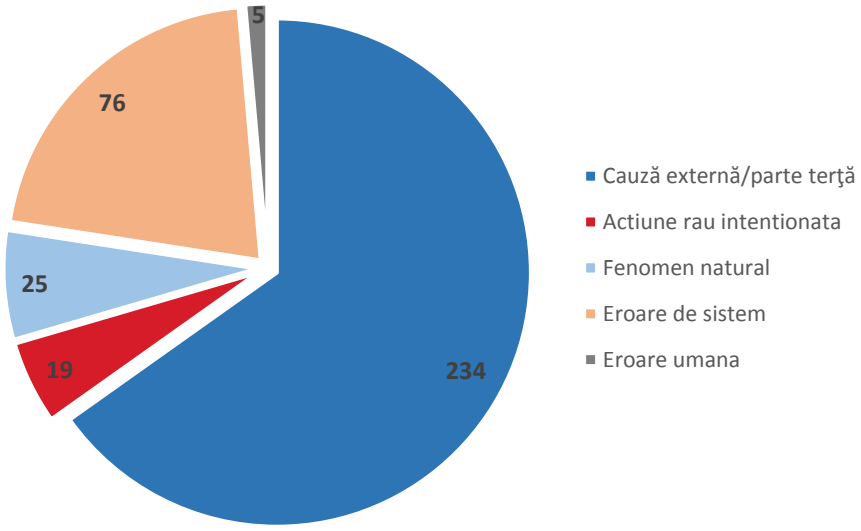
Pentru a împiedica apariția acestui tip de incident, printre măsurile planificate de furnizori se află: schimbarea bateriilor în vederea creșterii autonomiei, montarea unui generator automat, revizii generator etc.

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.

Fig.14 Situația incidentelor în funcție de cauză



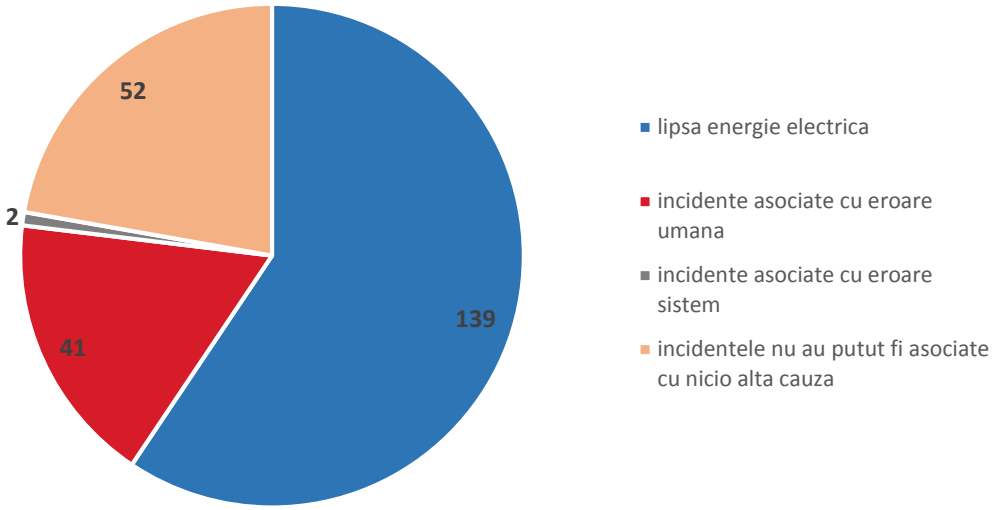
Așa cum se poate vedea în Fig. 14, majoritatea incidentelor din 2014 fac parte din categoria cauză externă/parte terță (234 incidente, reprezentând 65% din totalul de incidente raportate în 2014). 76 dintre incidente fac parte din categoria eroare de sistem, 25 de incidente fac parte din categoria fenomen natural, 19 dintre incidente fac parte din categoria acțiune rău – intenționată și doar 5 incidente au fost încadrate în categoria eroare umană.

Incidentele din categoria cauză externă pot fi corelate cu una din celelalte 4 cauze. Astfel, dintre cele 234 incidente încadrate în această categorie, 41 au fost asociate cu eroare umană și 2 incidente au fost asociate cu eroare de sistem. 139 dintre aceste incidente s-au datorat lipsei energiei electrice.

52 de incidente din categoria cauză externă/parte terță nu au putut fi asociate cu nicio altă cauză. Acestea s-au datorat în cea mai mare parte defectării unor echipamente din rețelele partenere. O altă cauză a producerii acestor incidente a fost ruperea (din cauze necunoscute sau neraportate de către furnizori) a fibrei optice.

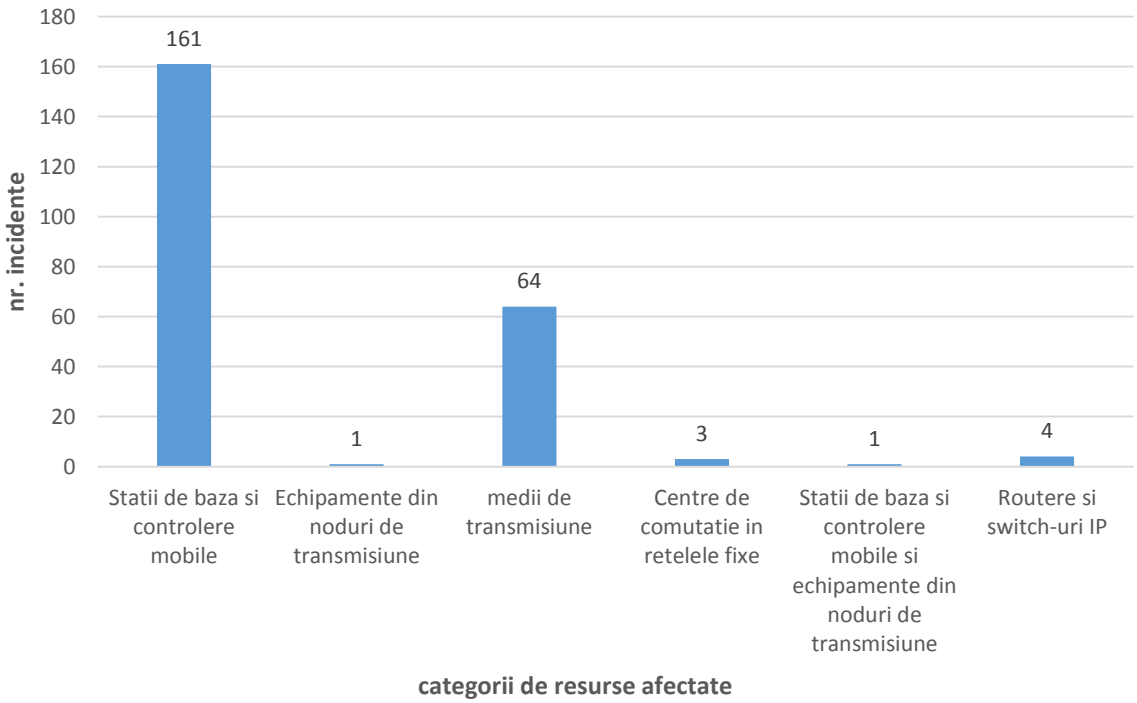
Situația incidentelor care fac parte din categoria cauză externă este prezentată în figura de mai jos:

Fig.15 Asocierea cu alte cauze a incidentelor care fac parte din categoria cauză externă/parte terță



Întrucât principalele cauze pentru producerea incidentelor raportate în 2014 fac parte din categoria cauză externă/parte terță, este relevantă identificarea resurselor afectate în acest caz. Figura de mai jos ilustrează numărul de incidente din categoria cauză externă per categorie de resurse afectate.

Fig.16 Resursele afectate în cazul incidentelor din categoria cauză externă



Se poate observa că în cazul incidentelor din categoria cauză externă cele mai afectate resurse sunt stațiile de bază și controlerele mobile. Categoriile de resurse afectate în mică măsură sunt echipamentele din noduri de transmisiune, Routere și switch-uri IP și centre de comutație în rețelele fixe.

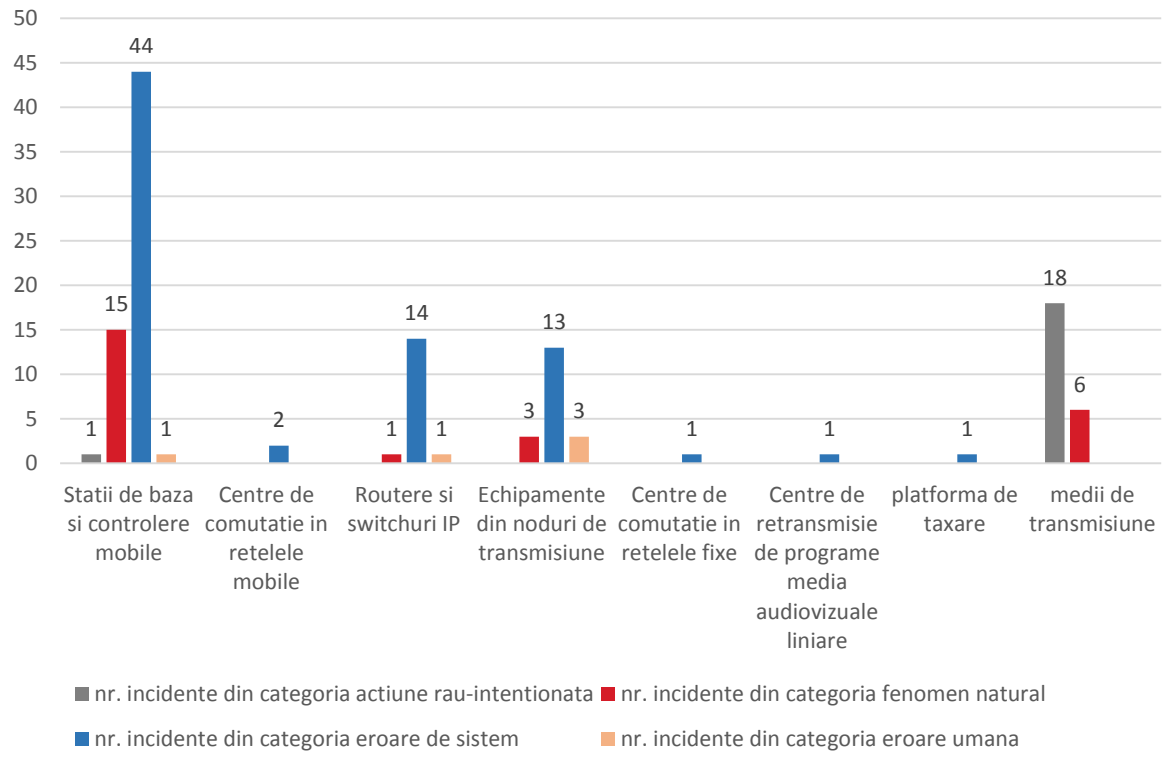
Conform raportărilor, în cazul incidentelor din categoria cauză externă, resursele din categoria Stații de bază și controlere mobile au fost afectate din cauza unor probleme de ordin tehnic intervenite la nivelul rețelelor partenere, ori din cauza problemelor de alimentare cu energie electrică (respectiv întreruperi ale energiei electrice furnizată de rețelele de distribuție națională). Mediile de transmisiune au fost afectate în principal în urma lucrărilor efectuate de terți, ori din cauze necunoscute sau neraportate de către furnizorii de rețele și servicii de comunicații electronice.

Tot în cazul incidentelor din categoria cauză externă, echipamentele din categoria Centre de comutație au fost afectate din cauza șocurilor de energie electrică, în urma cărora centrala de comutație în rețelele fixe a fost scoasă din funcțiune. Conform raportărilor, avariile electrice reprezintă cauza afectării resurselor din categoria Routere și switch-uri.

Întrucât numărul incidentelor încadrate în categoria cauză externă se detașează evident față de numărul celor care vizează celelalte 4 categorii de cauze, acestea din urmă au fost luate în considerare împreună în cazul statisticii privind resursele afectate.

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

Fig.17 Resursele afectate în cazul incidentelor care fac parte din cele 4 categorii de cauze



Se poate observa faptul că resursele din categoriile Stații de bază și controlere mobile, Echipamente din noduri de transmisiune și Routere și switchuri IP au fost cel mai afectate în cazul incidentelor cauzate de erori de sistem. În cazul incidentelor cauzate de fenomene naturale, cele mai

afectate resurse sunt stațiile de bază și controlere mobile. Se poate observa că cele mai afectate resurse în cazul incidentelor din categoria acțiune rău intenționată sunt mediile de transmisiune.

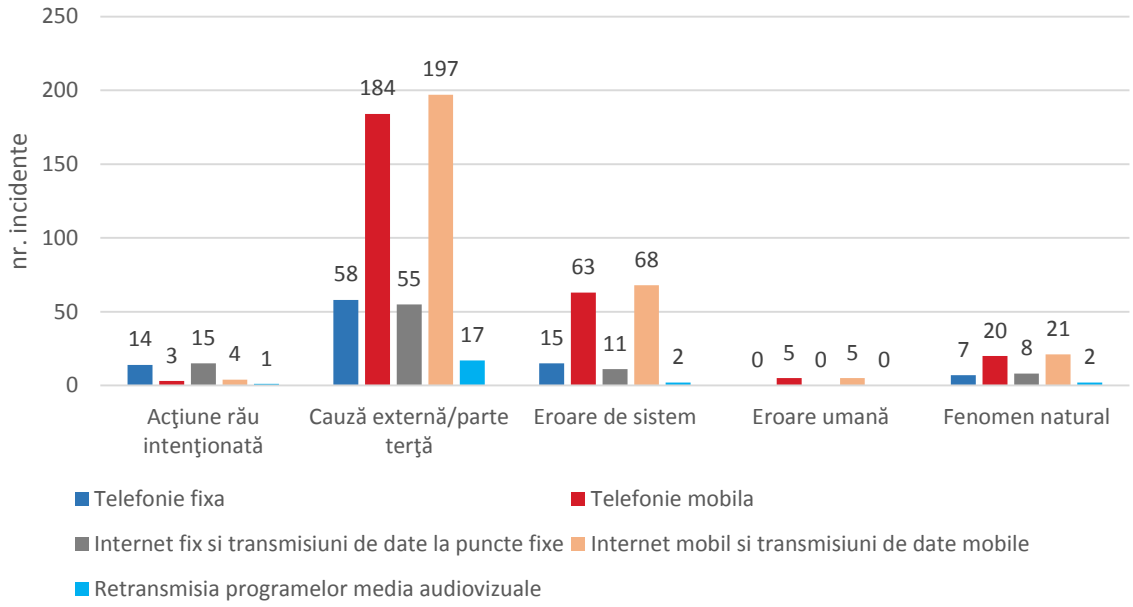
Din raportările furnizorilor s-a constatat faptul că în cazul incidentelor încadrate în cele 4 categorii de cauză, Stațiile de bază și controlerele mobile au fost afectate în principal din cauza unor erori software apărute, ori în urma defectării echipamentelor de electro-alimentare.

Conform raportărilor, resursele din categoria medii de transmisiune au fost afectate fie în urma acțiunilor rău intenționate, fie ca urmare a fenomenelor meteorologice nefavorabile (surpări de mal, vânt puternic, înghețarea unor joncțiuni de fibră optică).

Echipamentele din categoria Routere și switch-uri au fost afectate în urma infiltrării apei la nivelul echipamentelor, blocării porturilor, ori problemelor de natură software.

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

Fig.18 Numărul incidentelor pentru toate tipurile de servicii în funcție de cauză



De precizat faptul că în acest caz suma incidentelor pentru toate tipurile de servicii afectate, în funcție de cauză (Fig.18) diferă de numărul total al incidentelor per tip de cauză (reprezentat în Fig.14) deoarece un incident poate afecta mai multe servicii simultan.

Din Fig.18 se observă că atât în cazul incidentelor care fac parte din categoria cauză externă cât și în cazul celor care fac parte din categoria fenomen natural, cele mai afectate au fost serviciile de acces la internet mobil și transmisiuni de date mobile și serviciile de telefonie mobilă. Această situație este predictibilă ținând cont de vulnerabilitățile ce caracterizează sistemele prin intermediul cărora sunt transmise aceste servicii, anume faptul că alimentarea cu energie electrică necesară funcționării unora din componentele rețelei nu este în totalitate sub controlul furnizorului de servicii de comunicații electronice. Incidentele care fac parte din categoriile cauză externă/parte terță s-au produs în principal datorită problemelor apărute la nivelul furnizorului de energie electrică.

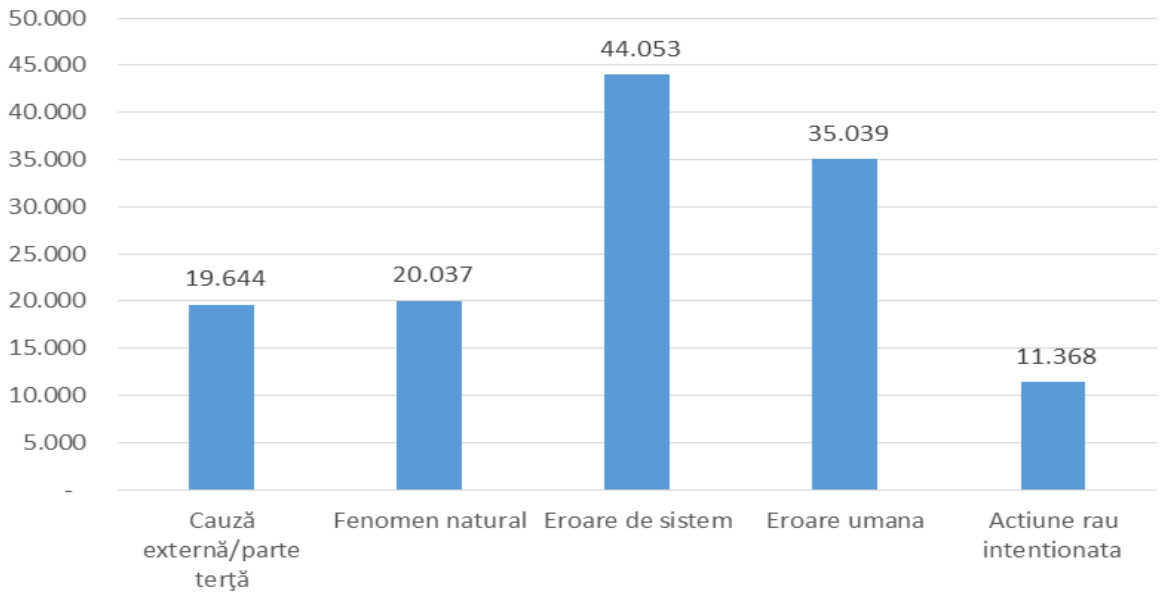
În cazul incidentelor care fac parte din categoria acțiune rău-intenționată, cele mai afectate servicii sunt telefonia fixă și serviciile de acces la internet fix și transmisiuni de date la puncte fixe. Având în vedere că rețelele prin intermediul cărora sunt furnizate aceste servicii folosesc pentru

transportul semnalelor cabluri, și această situație este explicabilă. În acest caz, incidentele s-au datorat în principal tentativelor de furt.

Cele mai multe incidente care au afectat serviciile de retransmisie a programelor audiovizuale (17) fac parte din categoria cauză externă/parte terță. Acestea s-au datorat în mare parte avariilor la nivelul fibrei optice (în urma fenomenelor naturale sau cauzate de efectuarea unor lucrări de terți).

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

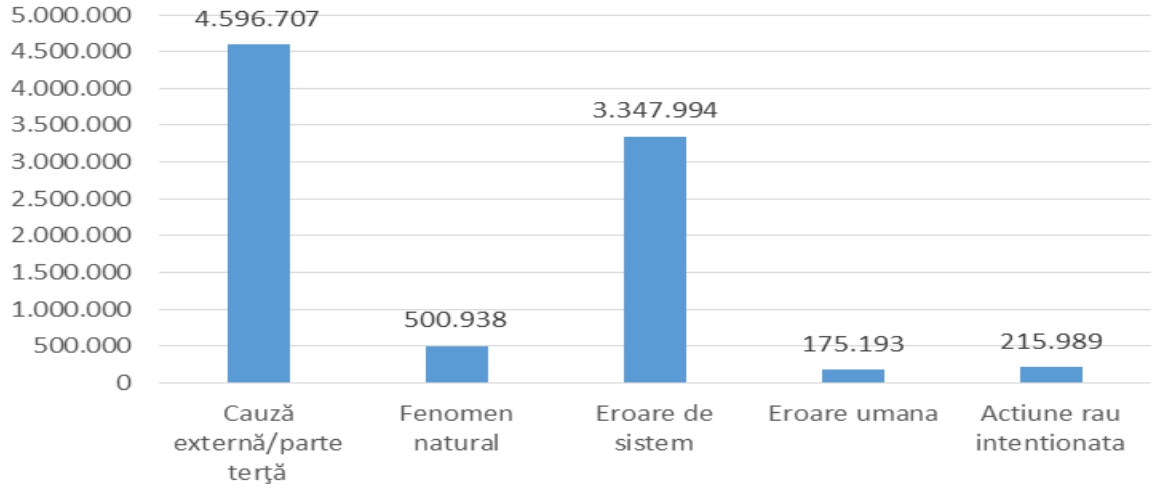
Fig.19 Numărul mediu de conexiuni per tip de cauză



În graficul de mai sus se poate observa faptul că în cazul incidentelor care fac parte din categoriile eroare de sistem și eroare umană a fost afectat în medie cel mai mare număr de conexiuni. Incidentele din categoria acțiune rău-intenționată au afectat în medie cel mai mic număr de conexiuni (11.368).

Statistica privind numărul de conexiuni afectate în funcție de cauză este prezentată mai jos:

Fig.20 Numărul de conexiuni afectate în funcție de cauză



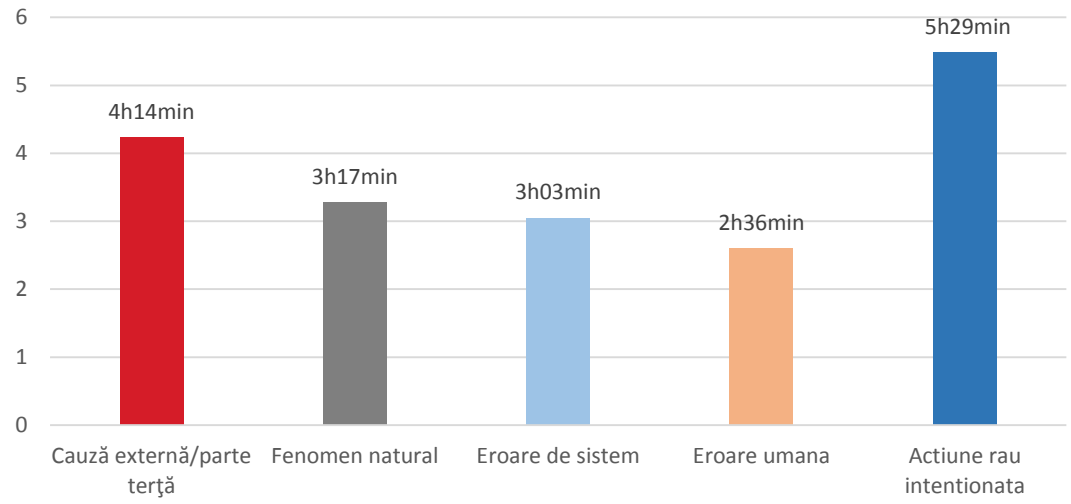
Analiza ultimelor două grafice (Fig.19 și Fig.20) susțin situații deja prezentate în acest raport care se referă la numărul de incidente în funcție de fiecare tip de cauză.

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.

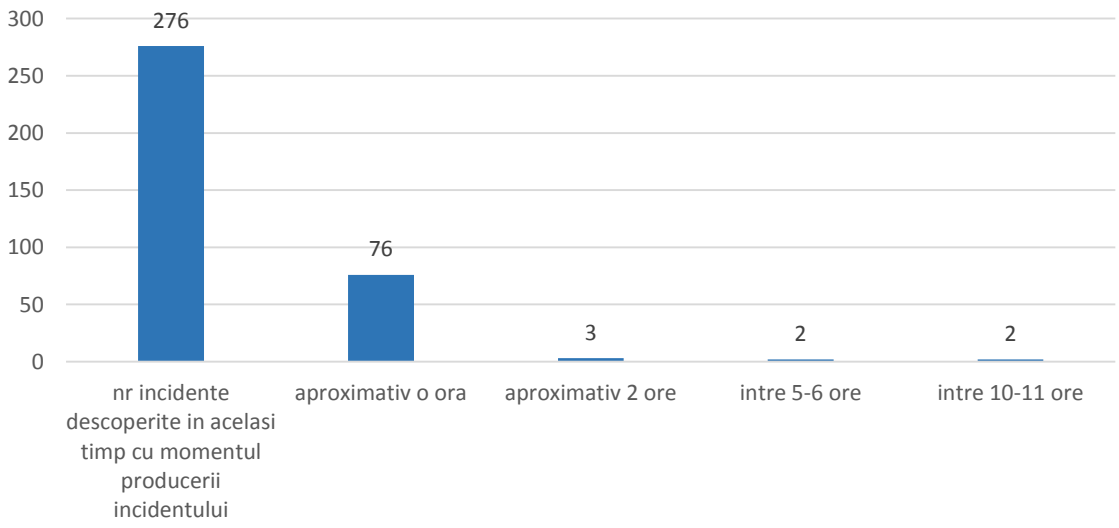
Durata totală a incidentelor raportate pe anul 2014 este de 1.420 ore, durata medie a unui incident fiind de aproximativ 4 ore (3h57).

Fig.21 Durata medie a incidentelor în funcție de cauză



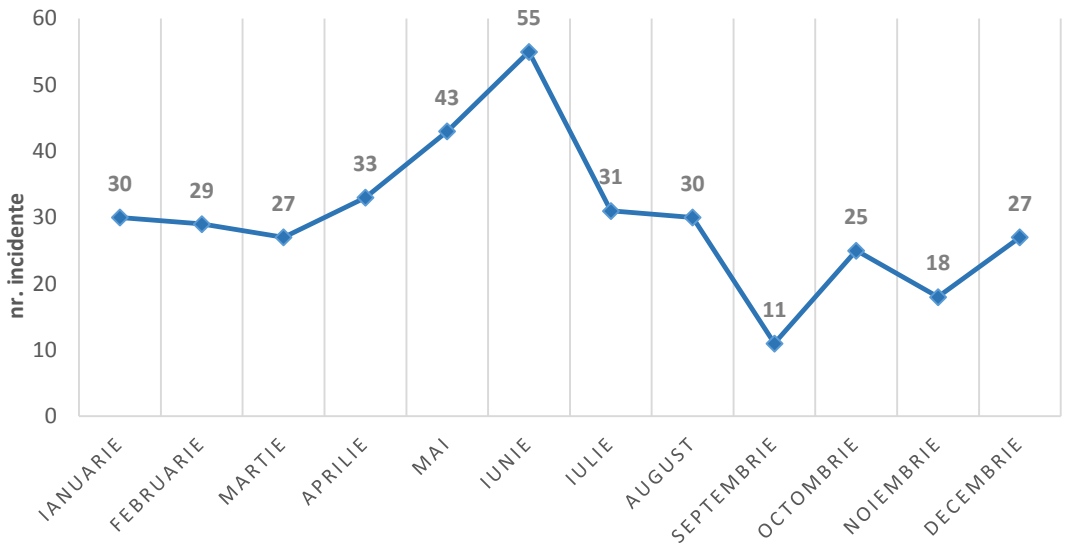
Valoarea cea mai mare a duratei medii aparține categoriei de cauze acțiune rău-intenționată (5h29minute). Având în vedere numărul mic al incidentelor din această categorie (19), statistica din Fig.21 evidențiază impactul major pe care această categorie de incidente l-a avut asupra rețelelor și serviciilor de comunicații electronice. Incidentele generate de terțe părți au înregistrat o durată medie de aproximativ 4 ore. Acest fapt se datorează unei serii de factori care nu sunt în totalitate sub controlul furnizorului de servicii (probleme de alimentare cu energie electrică, secționarea fibrei optice în cadrul lucrărilor efectuate de terți sau din cauze naturale etc.)

Fig.22 Numărul de incidente și durata în care au fost descoperite



Din Fig.22 se poate observa că cele mai multe incidente (276) au fost descoperite în momentul producerii lor, 76 de incidente au fost descoperite într-o oră, iar 2 incidente au fost descoperite până în 6 ore. Incidentele care au fost descoperite în intervalul cel mai mare (peste 10 ore) s-au datorat secționării fibrei optice în mai multe locuri în cadrul unei tentative de furt, respectiv condițiilor meteorologice nefavorabile (vânt puternic și ploaie) care au afectat alimentarea cu energie electrică a unui site.

Fig.23 Numărul incidentelor lunare înregistrate în anul 2014

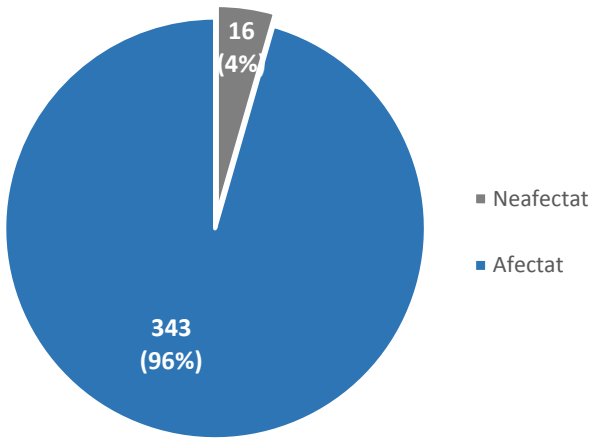


Se poate observa că luna iunie este perioada în care s-au raportat cele mai multe dintre incidente (55). Acestea s-au datorat în cea mai mare parte cauzelor externe, 67% dintre acestea fiind cauzate de probleme de alimentare cu energie electrică.

3.5 Impactul asupra apelurilor de urgență

96% dintre incidentele raportate în anul 2014 au avut un posibil impact asupra efectuării apelurilor de urgență.

Fig.24 Impactul asupra apelurilor de urgență



Impactul potențial major pe care l-au avut incidentele asupra apelurilor de urgență nu este surprinzător având în vedere faptul că cele mai afectate servicii, în 2014, au fost cele de telefonie mobilă (în acest caz fiind afectat implicit 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 acțiuni întreprinse și măsuri adoptate în scopul de a restabili serviciul la parametrii inițiali, cât și măsuri preventive de securitate implementate în vederea minimizării riscului apariției incidentelor.

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

- Notificarea părților responsabile în vederea remedierii defecțiunilor apărute din cauze ce excedă sfera de control a furnizorului de comunicații electronice (în principal în cazul incidentelor cauzate de lipsa energiei electrice);
- Restabilirea tronsonului de fibră optică prin înlocuirea unor segmente de cablu sau prin efectuarea de joncțiuni (în cazul incidentelor în care a fost afectată fibra optică);
- Repornirea echipamentelor sau redirecționarea traficului (în cazul incidentelor din categoria eroare de sistem-erori de tip software);
- Repararea/înlocuirea echipamentelor defectate (în cazul incidentelor datorate defectării componentelor hardware ale echipamentelor).

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:

- Suplimentarea cu surse de alimentare cu energie electrică necesare funcționării echipamentelor din diferite locații;
- Creșterea securității locațiilor în care s-au înregistrat distrugeri la nivel fizic ale diferitelor resurse;
- Asigurarea redundanței căilor de transmisiune.

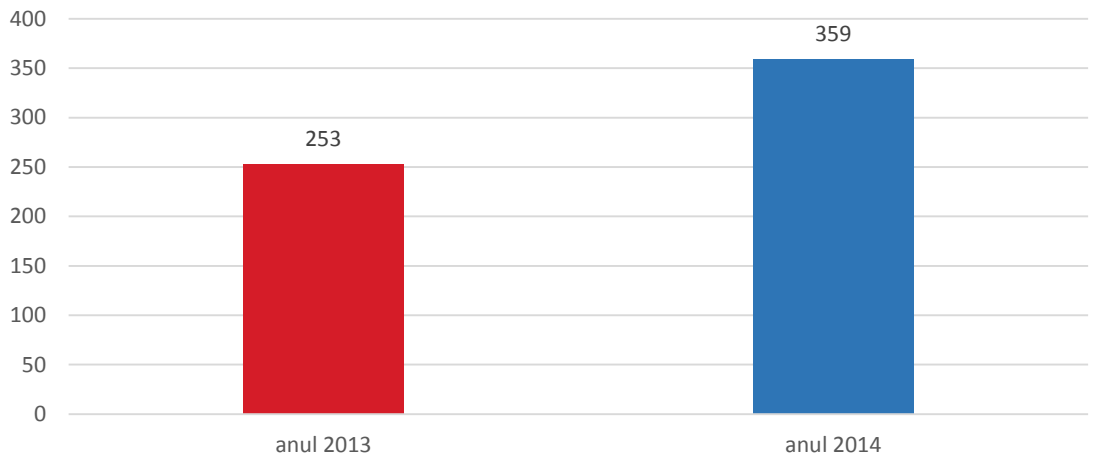
Menționăm faptul că în cazul majorității incidentelor raportate în 2014, câmpul aferent măsurilor luate sau planificate pentru a împiedica producerea unui incident similar nu a fost completat cu informații relevante sau concrete. Acest fapt se poate datora unei deficiențe de raportare, dar și faptului că natura celor mai multe incidente (care fac parte din categoria cauză externă) nu a permis implementarea unor astfel de măsuri.

5. Comparație privind situația incidentelor raportate în 2013 și 2014

Pentru o imagine mai clară a evoluției situației privind incidentele și impactul lor asupra serviciilor și utilizatorilor, în cele ce urmează se vor face comparații între anii 2013 și 2014.

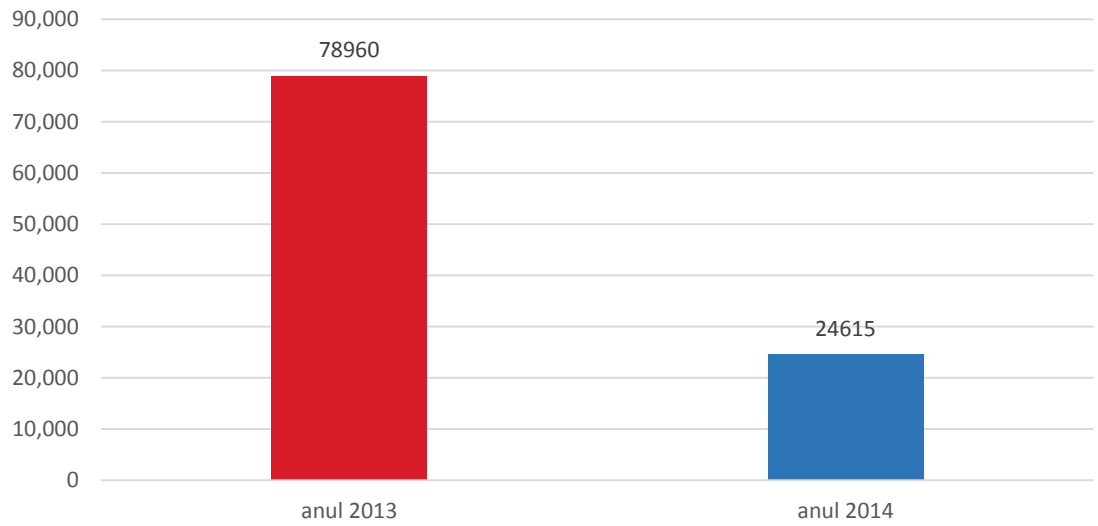
Situația incidentelor în 2014 comparativ cu anul precedent, este prezentată în figura de mai jos.

Fig.25 Numărul incidentelor pentru anii 2013 și 2014



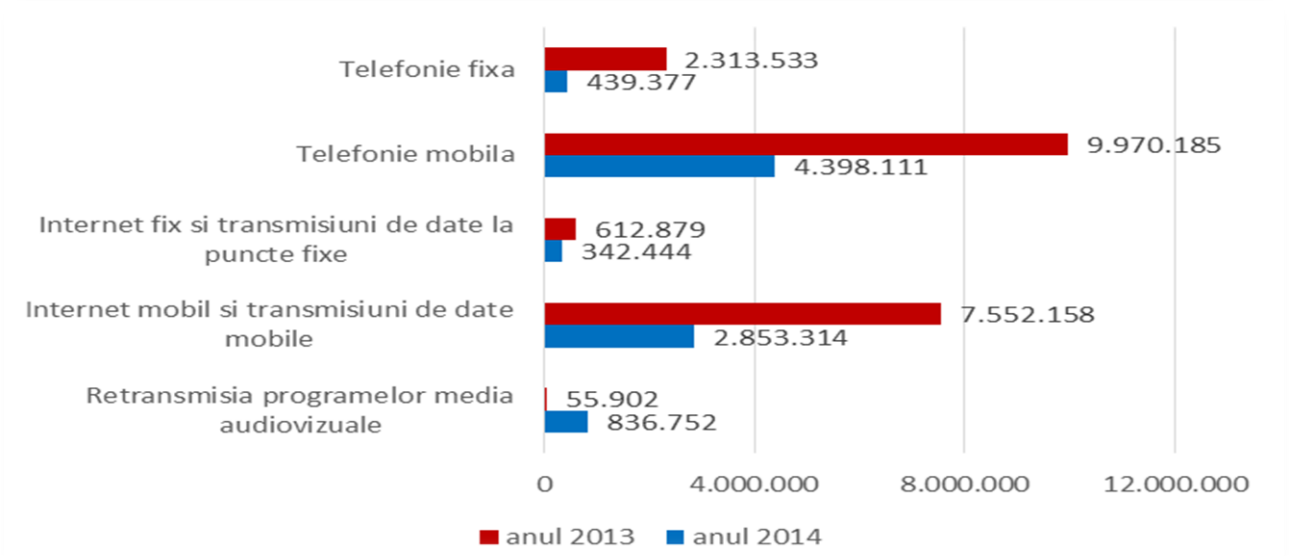
Situația în ceea ce privește numărul mediu de conexiuni afectate înregistrat în 2013 și 2014 este prezentată în figura de mai jos.

Fig.26 Numărul mediu de conexiuni afectate



Se poate observa astfel că, deși numărul incidentelor a crescut, impactul acestora a fost mult mai mic în 2014, numărul mediu de conexiuni afectate înregistrând o valoare de 3 ori mai mică decât în 2013.

Fig.27 Numărul de conexiuni afectate per serviciu

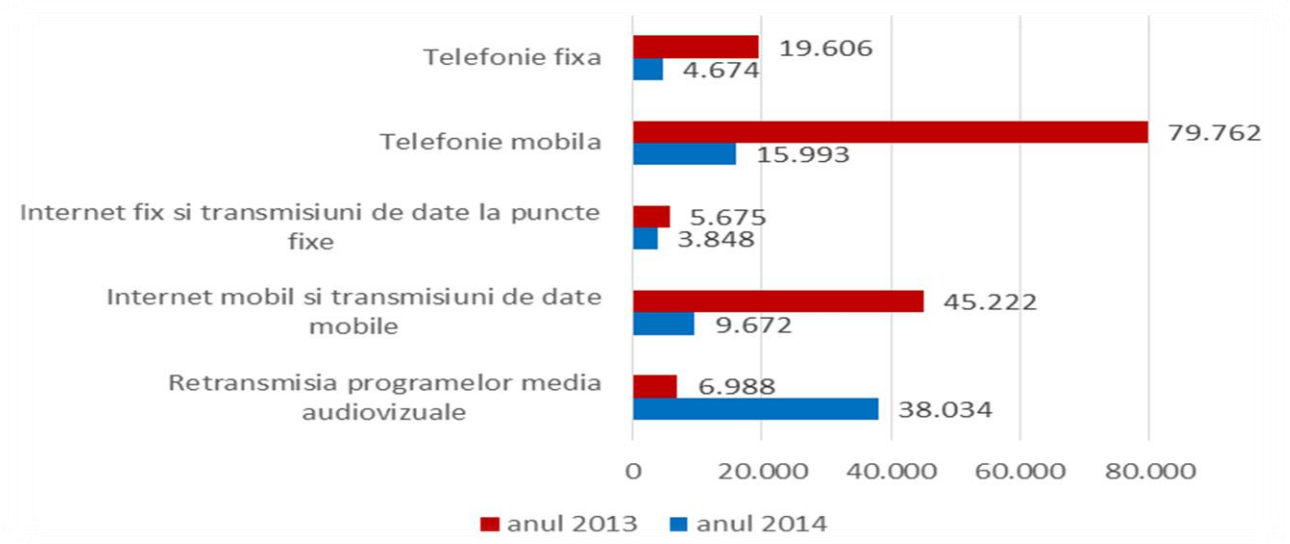


Atât în 2013 cât și în 2014 cel mai afectat serviciu din punct de vedere al numărului de conexiuni afectate a fost serviciul de telefonie mobilă.

Din graficul de mai sus se poate observa că în 2014 s-au înregistrat valori mai mari față de 2013 doar în cazul serviciilor de retransmisie a programelor media audio vizuale.

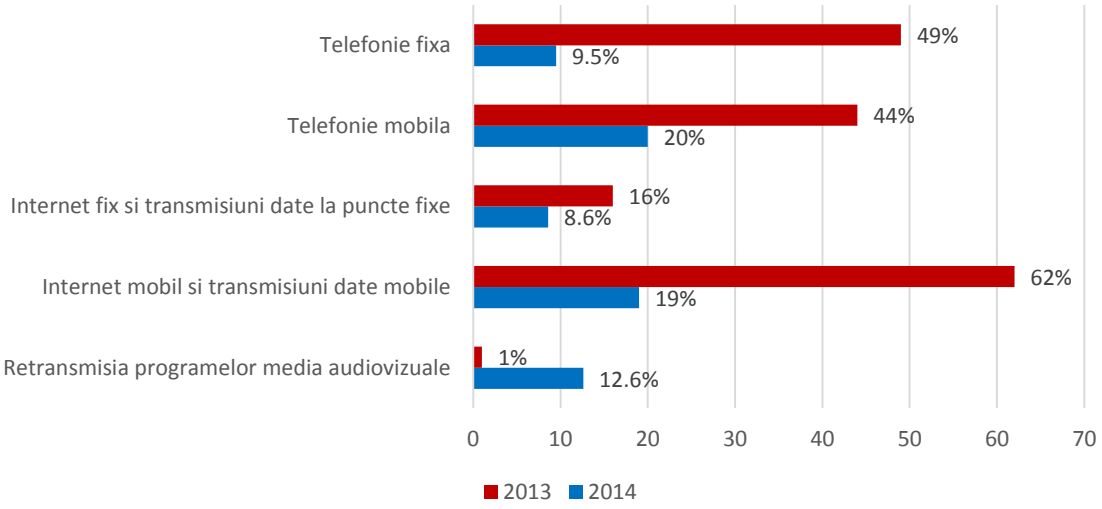
În cazul celorlalte servicii s-au înregistrat valori de câteva ori mai mici comparativ cu anul 2013. Cea mai evidentă diferență este în cazul serviciului de telefonie fixă, unde numărul de conexiuni afectate este de aproximativ cinci ori mai mic în 2014.

Fig.28 Numărul mediu de conexiuni afectate de un incident per serviciu



În graficul de mai sus se poate observa că doar valoarea numărului mediu de conexiuni afectate în cazul serviciilor de retransmisie a programelor media audiovizuale este mai mare în 2014 comparativ cu 2013. Se poate observa că în cazul celorlalte servicii numărul mediu de conexiuni afectate aferent anului 2014 a înregistrat valori cu mult mai mici față de 2013.

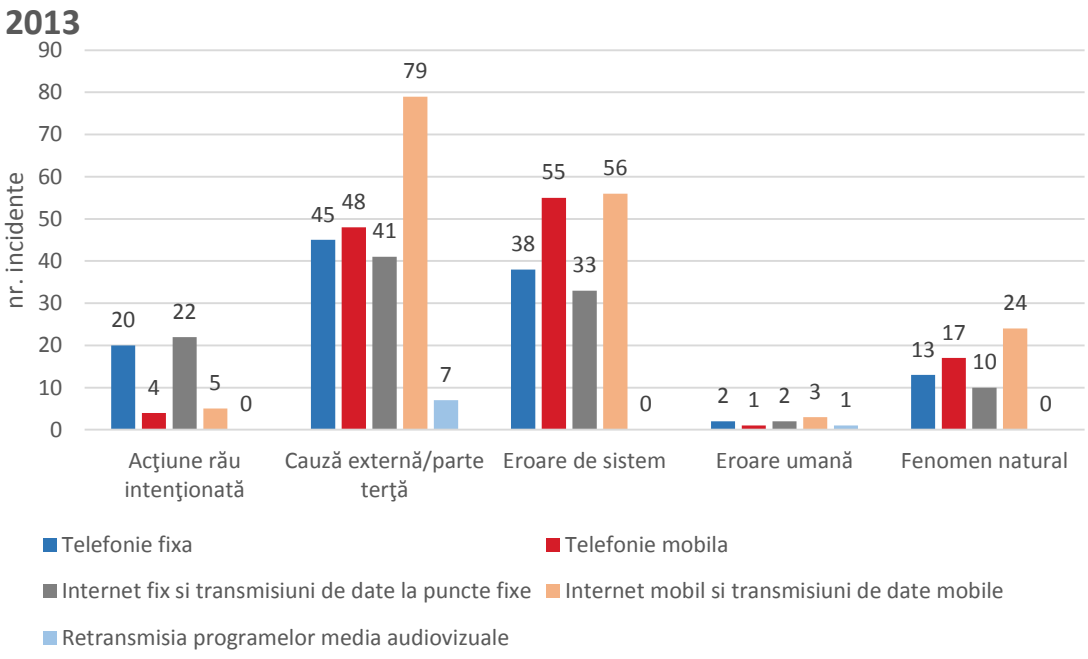
Fig.29 Procentul de conexiuni afectate în raport cu numărul total de conexiuni per serviciu

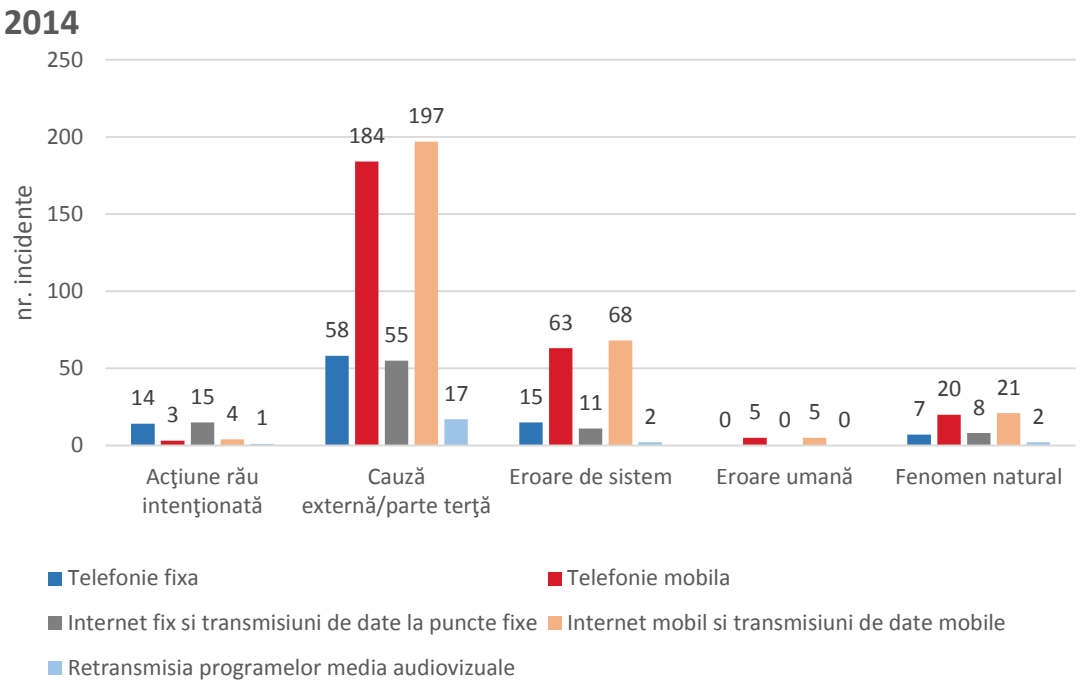


Se poate observa faptul că impactul incidentelor din 2014 asupra serviciilor la nivel național a fost cu mult mai mic comparativ cu anul 2013. În 2014 acestea au afectat până la 20% dintre conexiuni (în cazul serviciului de telefonie mobilă), pe când în 2013, incidentele au afectat până la 62% dintre conexiuni (în cazul serviciilor de acces la internet mobil și transmisiuni de date mobile).

În graficele de mai jos este reprezentat numărul incidentelor pentru toate tipurile de servicii afectate, în funcție de cauză pentru anii 2013 și 2014.

Fig.30 Numărul incidentelor pentru toate tipurile de servicii afectate în funcție de cauză în anii 2013, respectiv 2014





Se poate observa că situațiile din anii 2013 și 2014 privind numărul incidentelor pentru toate tipurile de servicii afectate în funcție de cauză prezintă mai multe similitudini. Astfel, incidentele care au afectat în cea mai mare măsură serviciul de acces la internet mobil și transmisiuni de date mobile fac parte din categoria cauză externă/parte terță. Incidentele care au afectat în cea mai mică măsură serviciile de comunicații electronice fac parte din categoria eroare umană. Cele mai afectate servicii în cazul incidentelor din categoria acțiune rău-intenționată sunt serviciile de telefonie fixă și serviciul de acces la internet fix și transmisiuni de date la puncte fixe. În cazul incidentelor care fac parte din categoria eroare de sistem și fenomen natural, cele mai afectate sunt serviciul de telefonie mobilă și serviciul de acces la internet mobil și transmisiuni de date mobile.

6. 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 și amplorii provocărilor existente la adresa securității și integrității rețelelor și serviciilor prin analiza amenințărilor și vulnerabilităților la adresa securității și integrității rețelelor și serviciilor și prin identificarea de bune practici bazate pe lecțiile învățate în procesul de management al incidentelor.

6.1 Concluzii în urma analizei incidentelor

În urma centralizării și analizării celor 359 de incidente cu impact semnificativ raportate pentru anul 2014 de către 7 furnizori de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului, se pot desprinde următoarele concluzii:

- cele mai afectate au fost serviciile de telefonie mobilă (4.398.111 conexiuni afectate);

- raportat la numărul total de conexiuni la nivel național, cele mai afectate au fost serviciul de telefonie mobilă (20%) și serviciul de acces la internet mobil și date mobile (19%). Aceste valori sunt cu mult mai mici comparativ cu anul 2013;
- cele mai multe dintre incidentele raportate în 2014 au afectat serviciile de acces la internet mobil și transmisiuni de date la puncte mobile (295 incidente) și serviciile de telefonie mobilă (275 incidente);
- numărul mediu de conexiuni afectate de un incident în 2014 este de 24.615, pe când în 2013 valoarea înregistrată fost de aproximativ 3 ori mai mare (78.960 conexiuni);
- cele mai afectate resurse fac parte din categoria Stații de bază și controlere mobile (222 incidente);
- aproximativ 45% din totalul incidentelor au fost generate de probleme de alimentare cu energie electrică;
- aproximativ 71% dintre incidente au avut impact asupra unui singur județ;
- 65% dintre incidentele raportate fac parte din categoria cauză externă/parte terță;
- în cazul incidentelor care fac parte din categoria cauză externă/parte terță, cele mai afectate resurse sunt Stații de bază și controlere mobile;
- cele mai multe incidente din categoria cauză externă/parte terță au afectat serviciile de acces la internet mobil și transmisiuni de date mobile;
- în 2014 durata medie a unui incident a fost de 3h57min; în 2013 s-a înregistrat o durată mai mare (aproximativ 5h);
- incidentele din categoria acțiune rău intenționată au înregistrat cea mai mare durată medie (5h29min);
- aproximativ 77% dintre incidente au fost descoperite în același timp cu producerea lor; cea mai lungă durată a unui incident a înregistrat aproximativ 11 ore;
- cele mai multe incidente s-au înregistrat în luna iunie (55 incidente);
- 96% dintre incidente au avut un potențial impact asupra apelurilor de urgență.

6.2 Concluzii privind deficiențele de raportare

Pentru a avea o imagine clară și corectă a situației privind incidentele de securitate raportate în anul 2014, 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 se referă la cauza producerii incidentelor. Astfel, în câteva cazuri informațiile aferente acestui câmp sunt incorecte. Ca și în anul precedent, s-a constatat faptul că în cazul unor incidente nu s-a făcut distincție între cauza inițială și cea subsecventă. Deși trebuie raportată cauza inițială, în câteva cazuri, furnizorii au completat câmpul aferent cu cauza subsecventă sau cu ambele tipuri de cauze corelate (de ex. eroare de sistem/eroare umană).

O altă deficiență de raportare constă în necompletarea câmpurilor *Acțiuni de răspuns la incident*, respectiv *Măsurile luate sau planificate pentru a împiedica producerea unui incident similar*, eliminarea ori completarea acestor câmpuri cu informații nerelevante (de ex. *Natura incidentului nu a permis adoptarea de măsuri specifice în vederea preîntâmpinării apariției de noi incidente*).

Pentru a preîntâmpina astfel de deficiențe și pentru o raportare cât mai corectă a informațiilor referitoare la incidentele cu impact semnificativ, ANCOM a elaborat și publicat un *Ghid de raportare a incidentelor* , care se adresează furnizorilor de rețele și servicii de comunicații electronice.

În vederea creării unei imagini cât mai clare privind incidentele raportate de furnizori și pentru o evaluare cât mai corectă a impactului acestor incidente asupra rețelelor și serviciilor de comunicații electronice, sunt necesare informații suplimentare. În acest scop, începând cu 1 ianuarie 2015, aplicația de raportare a incidentelor a fost modificată, prin detalierea unor aspecte ce țin de identificarea și localizarea resurselor sau echipamentelor afectate de incidentul raportat, aria geografică afectată de incident și impactul asupra apelurilor de urgență.

Modul de completare a noii aplicații, precum și alte informații utile privind raportarea incidentelor cu impact semnificativ de către furnizori au fost detaliate în cadrul Ghidului de raportare a incidentelor, elaborat de ANCOM.

Întrucât prevenirea incidentelor este de regulă mai puțin costisitoare decât răspunsul/reacția la acestea, ANCOM pune accent pe eforturile proactive în scopul asigurării securității și integrității rețelelor. În acest sens, ANCOM va finaliza în 2015 un Ghid de implementare a măsurilor de securitate în domeniul managementului incidentelor care se adresează furnizorilor de rețele și servicii de comunicații electronice.

Având în vedere potențialul impact al incidentelor asupra propriei organizații și asupra utilizatorilor finali, ANCOM recomandă furnizorilor să accentueze importanța oferită managementului incidentelor.

6.3 Concluzii calitative

Având în vedere că 2014 a fost al doilea an de raportare a incidentelor semnificative ce au afectat securitatea rețelelor și serviciilor de comunicații electronice, 2013 fiind totodată anul emiterii deciziei ANCOM ce stabilește detaliile obligațiilor de raportare, este probabil ca și aceste aspecte să fi avut o contribuție vizavi de diferențele apărute între datele aferente incidentelor raportate în cei doi ani. Sistemul de raportare se află în acest moment într-o fază inițială de calibrare și rodare, atât din perspectiva furnizorilor cât și din perspectiva autorității de reglementare, fapt ce poate induce anumite discrepanțe și neînțelegeri în raportarea și interpretarea datelor. Din acest motiv, eventualele analize și concluzii calitative cu privire la interpretarea datelor obținute pot conține o doză semnificativă de incertitudine și pot conduce la concluzii eronate cu privire la evoluția securității rețelelor și serviciilor de comunicații electronice. În consecință, autoritatea de reglementare se abține de la a analiza și formula, la acest moment, concluzii calitative cu privire la aspectele menționate.

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. Pentru a testa și monitoriza calitatea serviciului de internet, accesați www.netograf.ro.