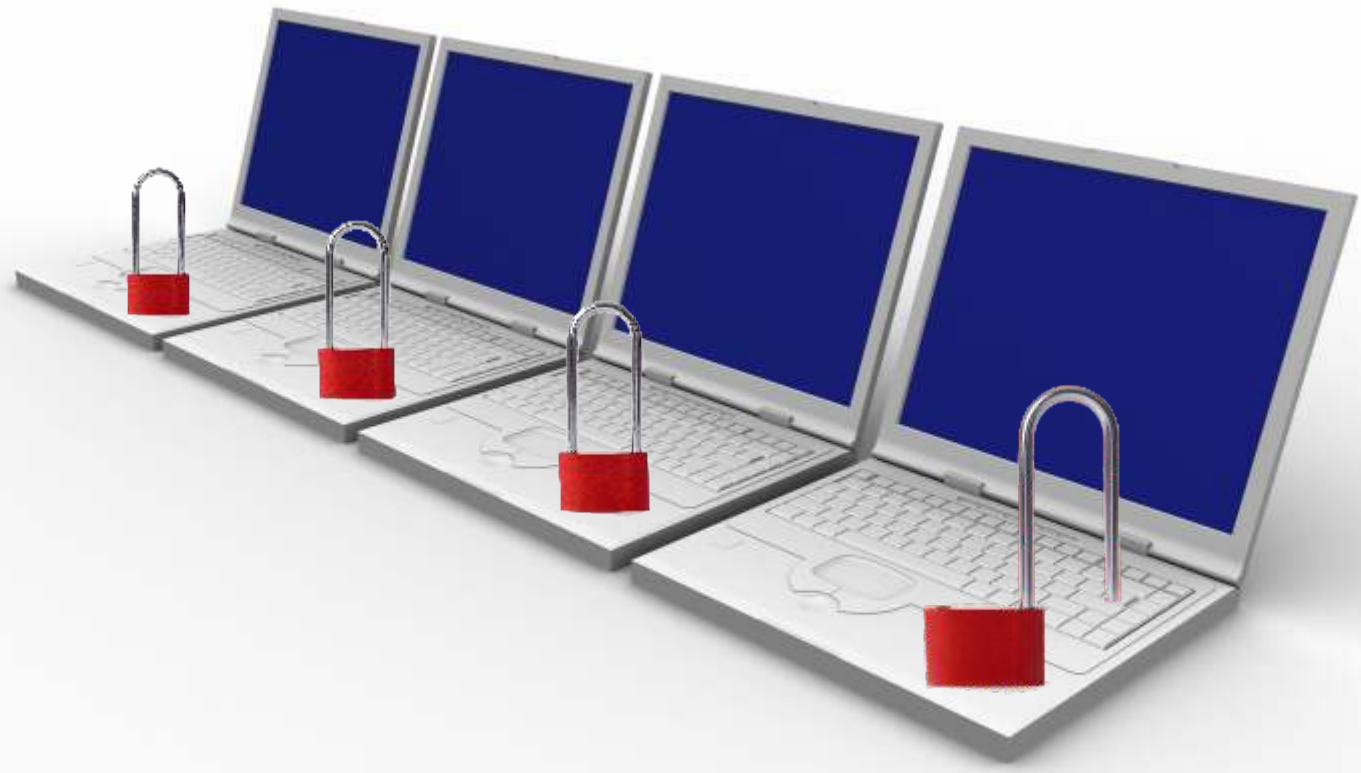
ANCOM
Autoritatea Naţională pentru Administrare
şi Reglementare în Comunicaţii

RAPORT
privind incidentele care au afectat securitatea și integritatea rețelelor și serviciilor de comunicații electronice în anul 2015



Data publicării: 21.06.2016

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 urma analizei incidentelor raportate de furnizorii de rețele și servicii de comunicații electronice, s-a constatat că în 2015 nu au existat incidente care să se încadreze în pragurile stabilite în 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: https://resilience.enisa.europa.eu/article-13/guideline-for-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 2015

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 2015 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 2015 au fost raportate 281 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:

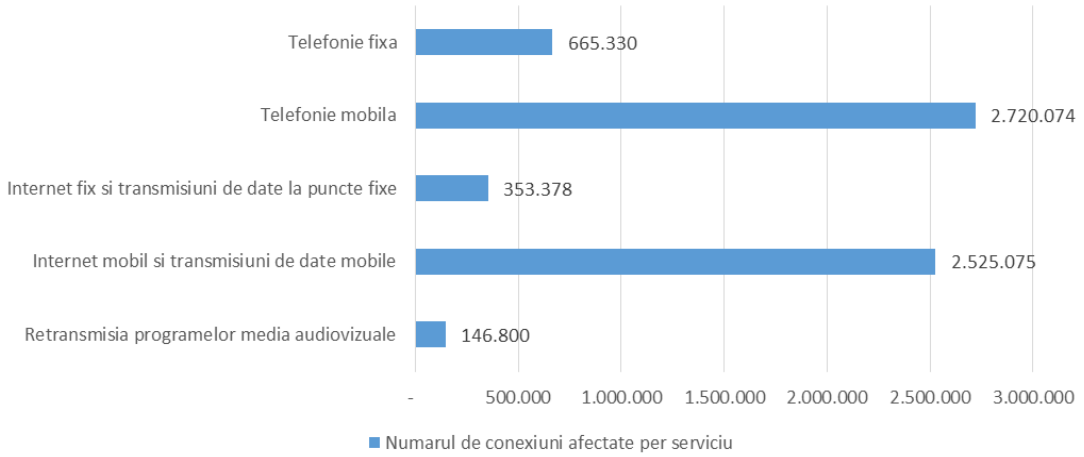
1. Impactul asupra serviciilor și utilizatorilor;
2. Impactul asupra resurselor afectate;
3. Cauzele incidentelor raportate;
4. Durata incidentelor și durata de descoperire,
5. Impactul asupra apelurilor de urgență.

3.1 Impactul asupra serviciilor și utilizatorilor

Numărul total de conexiuni afectate de cele 281 de incidente cu impact asupra principalelor servicii de comunicații electronice în anul 2015 este reprezentat în graficul de mai jos.

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

Fig.1 Numărul de conexiuni afectate per serviciu



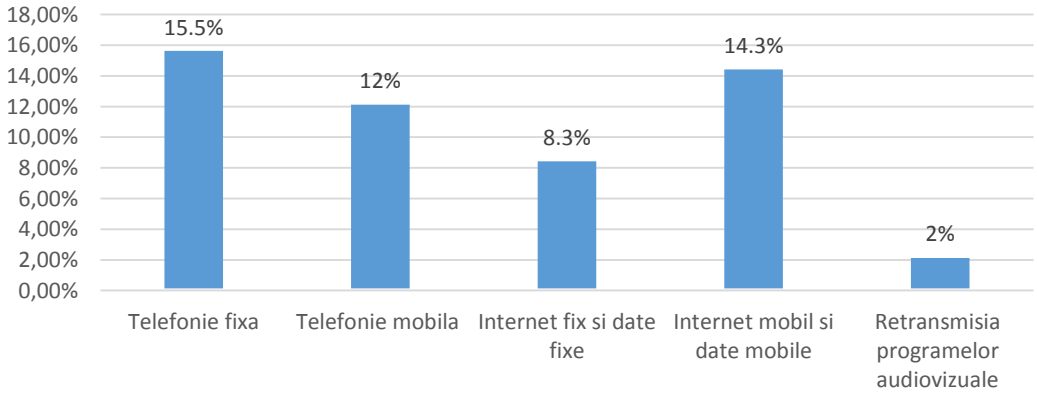
Conform Deciziei 512/2013, în cazul serviciilor furnizate prin intermediul unor rețele publice mobile terestre, furnizorul estimează numărul de conexiuni afectate. Conform instrucțiunilor de completare a formularului de raportare, metoda de estimare a numărului de cartele SIM afectate ia în calcul *traficul 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 2015 cele mai afectate au fost serviciile de telefonie mobilă (2.720.074 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 faptul că serviciile de telefonie fixă și serviciile de internet fix și transmisiuni de date la puncte fixe au fost afectate în mică măsură (665.330 conexiuni, respectiv 353.378 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.

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



* Conform Raportului privind datele statistice, semestrul I 2015, care poate fi accesat la următoarea adresă: https://statistica.ancom.org.ro:8000/sscpds/public/files/100_ro

[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.

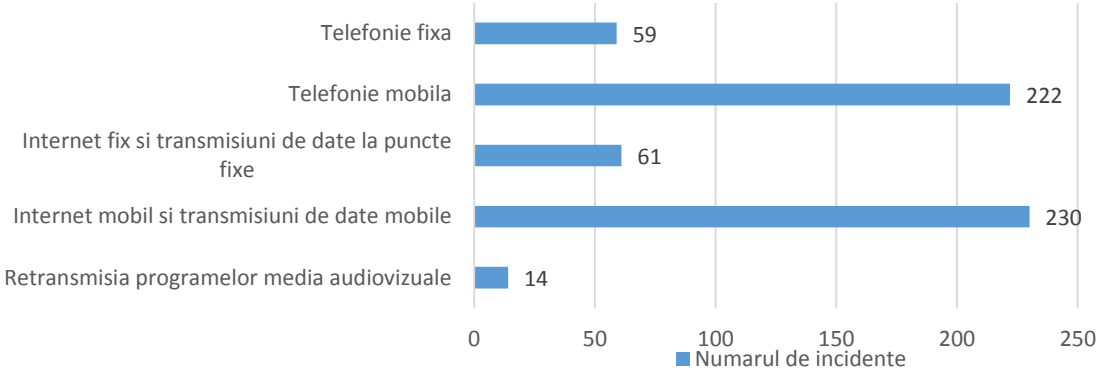
[6] Traficul total înregistrat la nivelul rețelei se consideră a fi suma traficului din toate celulele din rețea în intervalul de timp respectiv, în săptămâna anterioară.

De precizat faptul că procentele din graficul de mai sus sunt calculate ținând cont de numărul total de conexiuni afectate per serviciu. Altfel spus, procentele au fost obținute împărțind numărul conexiunilor afectate de incidentele din 2015 la numărul total de conexiuni raportate de furnizori.

Deși în Fig.1 se observă că numărul conexiunilor afectate în cazul serviciilor de telefonie fixă este mic comparativ cu numărul conexiunilor afectate în cazul serviciului de telefonie mobilă și al celui de internet și date mobile, în Fig.2 se poate observa că în cazul în care raportarea se face la numărul total de conexiuni, serviciile de telefonie fixă au fost afectate într-un procent mai mare față de celelalte servicii.

Figura de mai jos reprezintă numărul de incidente care au afectat fiecare serviciu în anul 2015.

Fig.3 Impactul asupra serviciilor



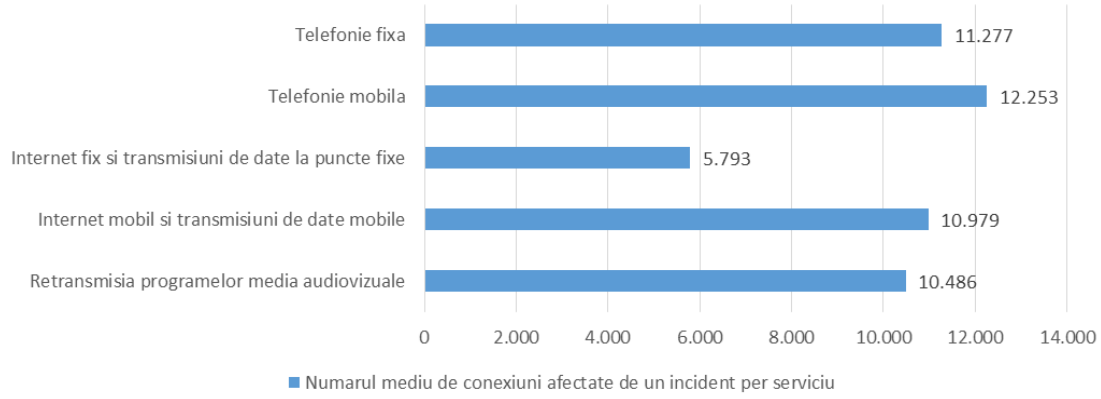
În Fig. 3 se observă că cele mai multe dintre incidentele raportate în 2015 au afectat serviciile de acces la internet mobil și transmisiuni de date la puncte mobile și serviciile de telefonie mobilă (230, respectiv 222 incidente). În ceea ce privește serviciile de acces la internet fix și transmisiuni la puncte fixe și serviciile de telefonie fixă, acestea au fost afectate în cazul a 61, respectiv 59 de incidente raportate în 2015.

De precizat faptul că suma incidentelor pentru fiecare tip de serviciu afectat diferă față de numărul total al incidentelor datorită faptului că 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 2015 este de 22.773 conexiuni. Această medie include toate conexiunile afectate, indiferent dacă a fost afectat un serviciu sau mai multe.

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



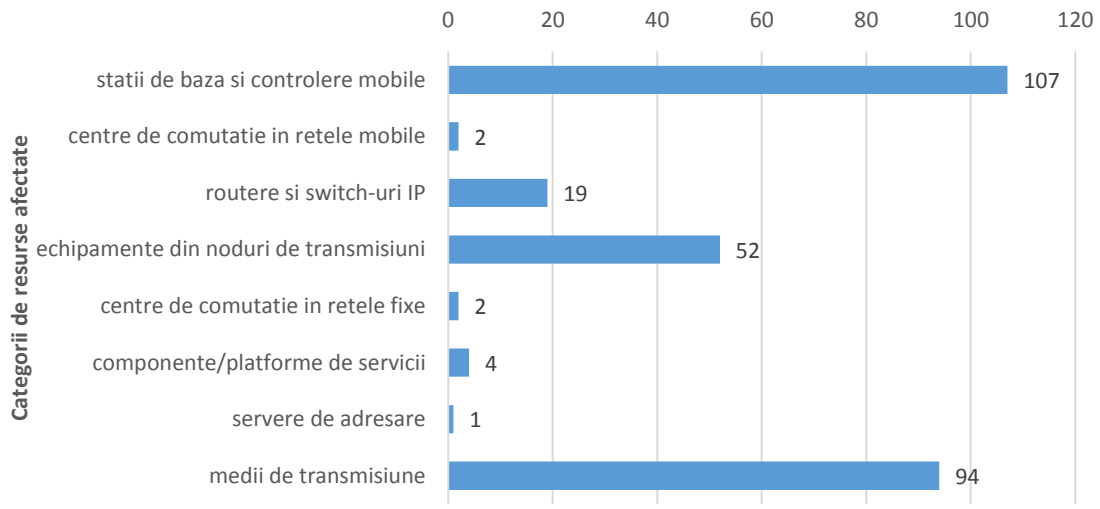
Se poate observa că, deși numărul incidentelor care au afectat serviciile de telefonie fixă (59 incidente) este mai mic decât numărul incidentelor înregistrate în cazul serviciilor de internet mobil si date mobile (230 incidente), numărul mediu de conexiuni afectate de un incident în cazul serviciului de telefonie fixă (11.277 conexiuni) este mai mare decât în cazul serviciului de internet mobil și transmisiuni de date mobile (10.979 conexiuni).

Numărul mediu de conexiuni afectate în cazul serviciilor de telefonie mobilă este de aproximativ 12.253, iar cele mai mici valori aparțin serviciilor de acces la internet fix și transmisiuni de date la puncte fixe (5.793 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.

Fig.5 Număr incidente per resurse afectate



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). 95 din cele 107 de incidente care au afectat categoria Stații de bază și controlere mobile s-au datorat lipsei alimentării cu energie electrică, în cadrul acestora fiind afectate aproximativ 340BTS (2G), 244NodeB (3G)și 8eNodeB (4G).

În cazul a 94 dintre incidente, resursa afectată face parte din categoria Medii de transmisiune, iar 27 dintre acestea fac parte din categoria cauză externă/eroare umană și au constat în ruperea fibrei optice în urma lucrărilor efectuate de terți. 27 dintre incidentele care au afectat resursele din categoria Medii de transmisiune s-au datorat unor erori de comunicare intervenite la nivelul rețelelor partenere, în urma cărora în majoritatea cazurilor au fost afectate stații 3G. Restul incidentelor în care a fost afectată categoria Medii de transmisiune s-au mai datorat tentativelor de furt, alunecărilor de teren și rozătoarelor. În cele mai multe cazuri, afectarea acestei resurse a avut drept consecință izolarea mai multor echipamente care fac parte din categoriile Routere și switchuri IP și Echipamente din noduri de transmisiune.

[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

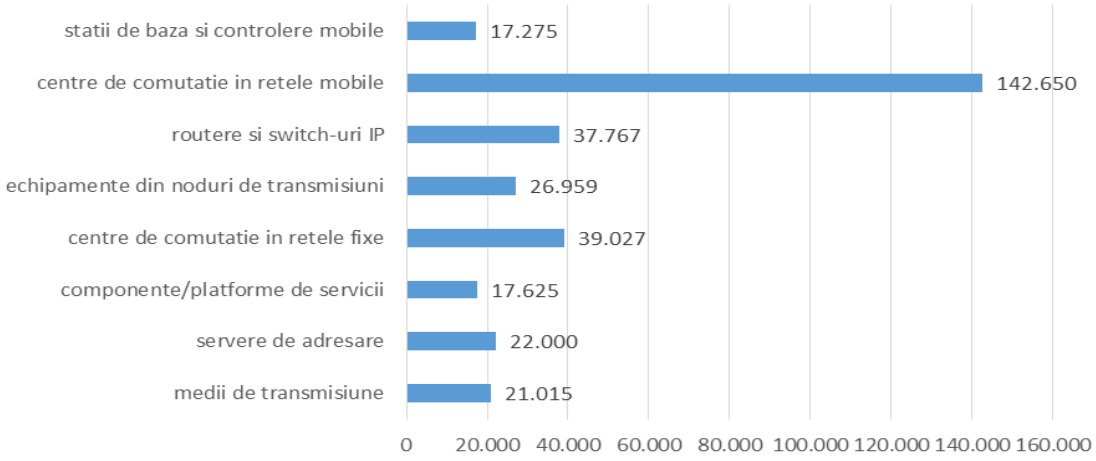
Un astfel de incident cu impact semnificativ, care s-a datorat secționării cablului de fibră optică a fost înregistrat în data de 18.10.2015, când furnizarea serviciilor de comunicații electronice a fost afectată în întreg orașul Năvodari. ANCOM a solicitat operatorilor din zonă informații cu privire la incidentele înregistrate la acea dată în zonă. Conform răspunsurilor acestora, incidentul a afectat rețelele mai multor operatori, în total fiind afectate 25.184 de conexiuni, cea mai lungă durată a incidentului înregistrată de un operator fiind de 3h45min. Acțiunile de răspuns la incident au constat în principal în intervenția echipelor tehnice responsabile pentru repararea fibrei optice iar în cazul unuia operatori, a fost solicitată intervenția poliției.

Dintre operatorii prezenți în zonă, doar în cazul unuia au fost atinse pragurile care definesc un incident ca fiind cu impact semnificativ. Conform raportării acestuia, au fost afectate 17.300 conexiuni, timp de 1h45min, tipul cauzei incidentului fiind din categoria acțiune rău intenționată. Apelarea serviciului de urgență a fost afectat în acest caz.

În cazul a 52 dintre incidente, resursa afectată face parte din categoria Echipamente din noduri de transmisiune, iar în cazul a 19 dintre incidente, resursa afectată face parte din categoria Routere și switch-uri IP. Într-o măsură mai mică au fost afectate resursele din categoriile Componente/platforme de servicii (4 incidente), Centre de comutație în rețele fixe (două incidente), Centre de comutație în rețele mobile (două incidente), Servere de adresare (1 incident).

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 poate observa faptul că resursele din categoriile Centre de comutație mobilă reprezintă resurse critice, afectarea acestora având de fiecare dată un impact major asupra conexiunilor. Astfel, numărul mediu de conexiuni afectate în acest caz a înregistrat valoarea cea mai mare (142.650 conexiuni).

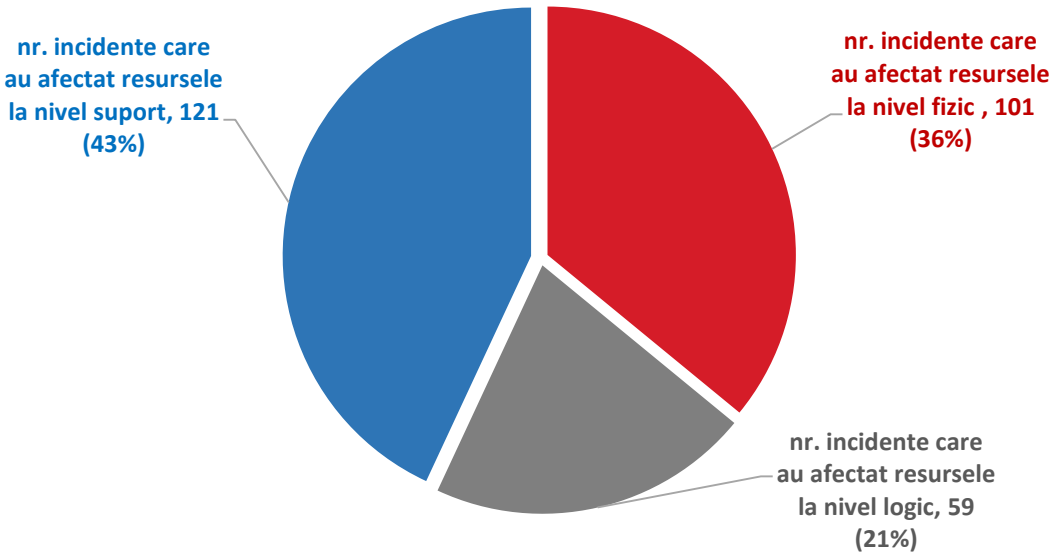
Ținând cont de gradul de complexitate al diferitelor tipuri de resurse (unele pot fi constituite din mai multe componente), afectarea acestora poate avea implicații la nivele diferite. Se disting, astfel, trei nivele la care se vor raporta statisticile privind resursele afectate în urma producerii incidentelor 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.

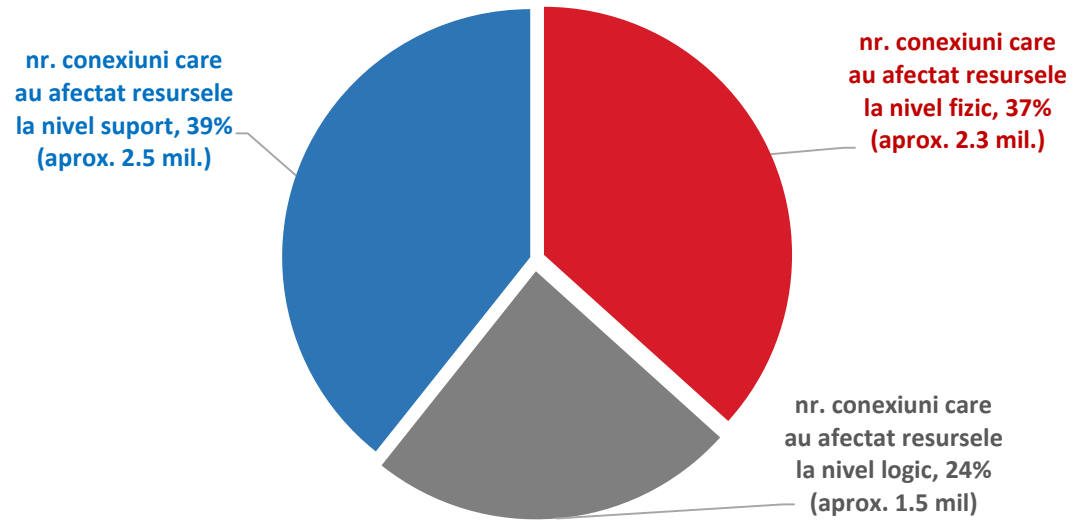
În graficul următor este reprezentat impactul celor 281 de incidente asupra resurselor în funcție de cele trei nivele enunțate mai sus.

Fig.7 Ponderea incidentelor pe tipuri de nivele afectate



În graficul de mai jos este reprezentat impactul 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 în acest caz, o pondere mare a incidentelor este echivalent cu un impact major asupra serviciilor. Astfel, de exemplu, în cazul incidentelor care au afectat resursele la nivel suport se poate observa faptul că ponderea mare a acestora (43%) a însemnat în același timp și un impact major al acestora asupra rețelelor și serviciilor

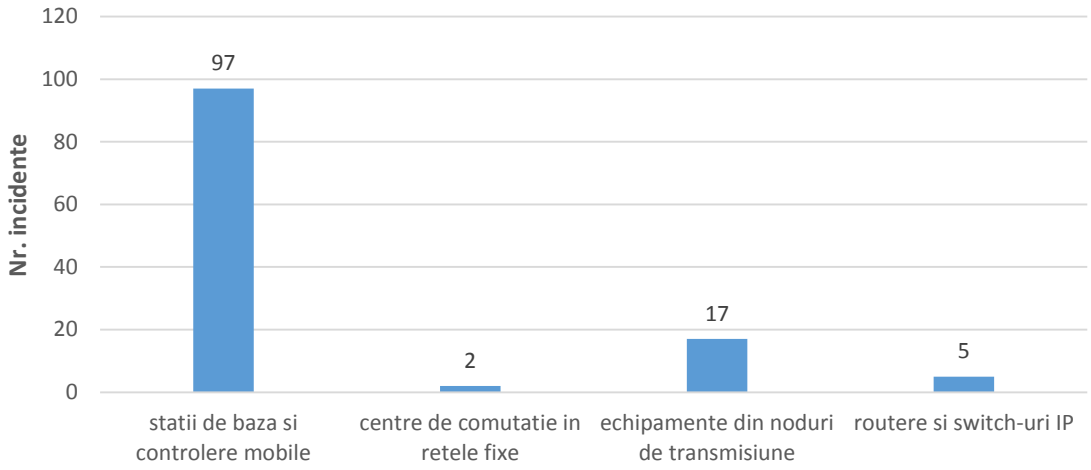
de comunicații electronice, numărul conexiunilor care au afectat resursele la nivel suport fiind cel mai mare (2.5 mil).

Fiecare dintre aceste nivele este analizat în cele ce urmează.

Nivelul suport

În graficul de mai jos sunt reprezentate resursele afectate la nivel suport.

Fig.9 Resurse afectate la nivel suport



În 2015 au fost raportate 121 de incidente care au afectat resursele la nivel suport.

112 dintre acestea (reprezentând aproximativ 40% din totalul incidentelor raportate) fac parte din categoria cauză externă și s-au produs din cauza problemelor apărute la furnizorul de energie electrică. În cazul acestor incidente au fost raportate întreruperi ale alimentării cu energie electrică, avarii înregistrate la furnizorul de energie electrică și șocuri de energie electrică, în urma cărora au fost scoase din funcțiune diferite echipamente (prin blocarea acestora, ori prin pierderea configurației). În unele cazuri, aceste cauze au fost coroborate cu alte cauze subsecvente precum autonomia scăzută a bateriilor, sau lipsa combustibilului din generatorul electric.

Restul incidentelor care au afectat resursele la nivel suport s-au datorat defectării unor echipamente ale furnizorilor (de ex. redresoare, echipamente de climatizare, incendierea grupului electrogen fix)

Resursele afectate la nivel suport fac parte în principal din categoria stații de bază și controlere mobile (97 incidente). Alte resurse afectate sunt din categoriile: echipamente din noduri de transmisiune (17 incidente), routere și switch-uri IP (5 incidente) și centre de comutație în rețelele fixe (2 incidente).

Statistica evidențiază vulnerabilitatea resurselor care fac parte din categoria stații de bază și controlere mobile în cazul problemelor de alimentare cu energie electrică.

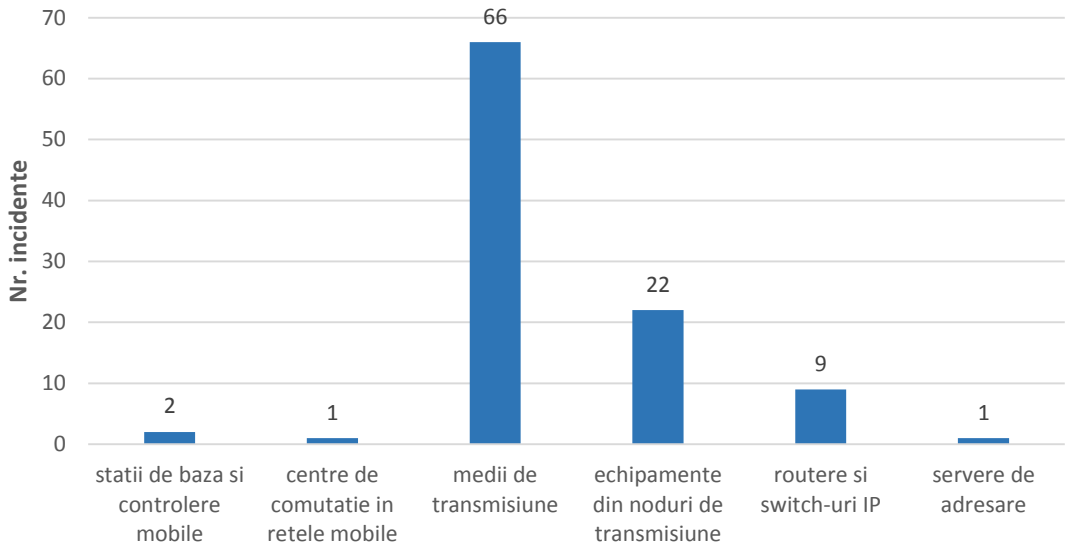
Ca și în anul precedent, având în vedere numărul mare de incidente care se datorează problemelor de alimentare cu energie electrică, precum și impactul considerabil al acestora asupra rețelelor și serviciilor de comunicații electronice (aproximativ 2.000.000 de conexiuni afectate în incidentele raportate), ANCOM recomandă furnizorilor găsirea unor soluții viabile în vederea diminuării acestei probleme. În acest sens, furnizorii pot avea în vedere încheierea unor contracte cu grad de

disponibilitate ridicată din partea furnizorilor de energie electrică, montarea de baterii și generatoare etc.

Nivelul fizic

Statistica privind resursele afectate la nivel fizic este reprezentată în graficul de mai jos.

Fig.10 Resurse afectate la nivel fizic



La nivel fizic, cea mai afectată resursă este fibra optică (încadrată în categoria medii de transmisiune). Din cele 66 de incidente care au afectat la nivel fizic această categorie de resurse în 27 dintre aceste cazuri, incidentele se datorează lucrărilor efectuate de terți, iar în 8 cazuri incidentele s-au datorat acțiunilor rău-intenționate (în principiu aceste acțiuni reprezentând tentative de furt). 7 incidente care au afectat fibra optică la nivel fizic s-au datorat fenomenelor naturale (de ex. fibra a fost ruptă ca urmare a condițiilor meteorologice nefavorabile sau în urma surpării malurilor, ori datorită rozătoarelor). În cazul celorlalte incidente care au afectat mediile de transmisiune la nivel fizic este vorba de întreruperea comunicării între diverse echipamente din cauza vremii nefavorabile (în acest caz fiind afectate linkurile radio). În aproximativ 50% din cele 66 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. Alte măsuri întreprinse în acest sens fiind verificarea periodică a legăturilor pe anumite trasee, deratizarea etc.

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 (rafale de vânt, ploi, viscol și ninsori abundente), fie în urma infiltrării apei la nivelul diverselor echipamente (de ex. PDH) în urma căreia stațiile de bază agregate în acesta au devenit neoperaționale.

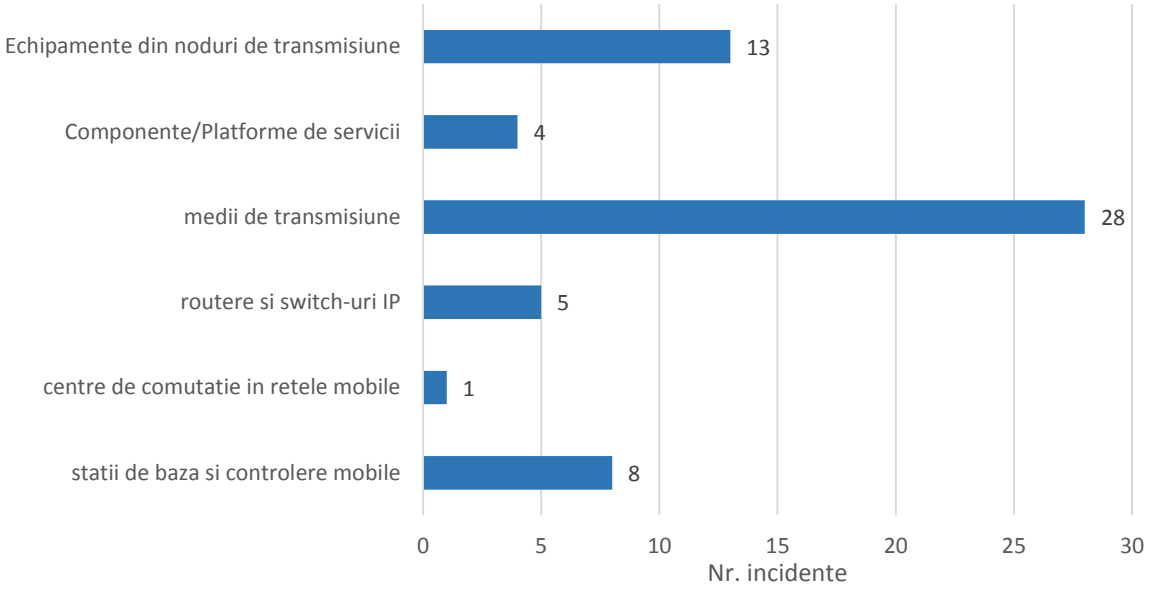
Nivelul logic

În urma raportărilor furnizorilor, s-au înregistrat 59 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, ori erorilor apărute în urma actualizării versiunilor software ale unor echipamente. Resursele afectate în cea mai mare măsură fac parte din categoriile Medii de transmisiune (28 incidente), respectiv Echipamente din noduri de transmisiune (13 incidente). Incidentele în cazul cărora a fost afectată categoria Medii de transmisiune s-au datorat unor probleme intervenite pe linii închiriate contractate de la un alt furnizor.

În acest caz, pentru furnizorul care a raportat, incidentul s-a manifestat printr-o eroare de comunicare între anumite echipamente la nivel de legătură de date.

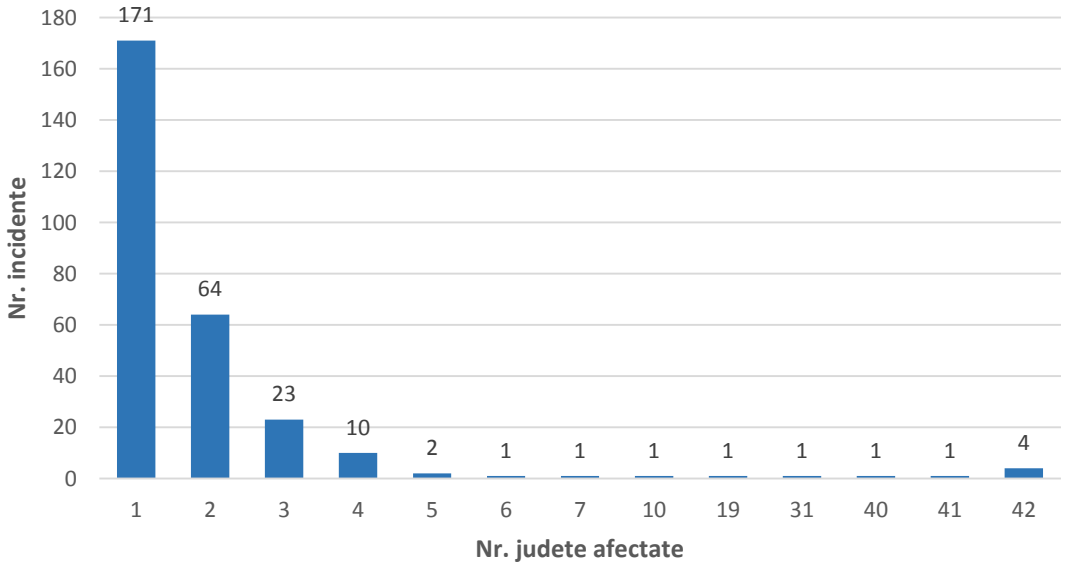
Statistica realizată în acest caz este reprezentată în figura 11.

Fig.11 Resurse afectate la nivel logic



În ceea ce privește regiunea geografică afectată de incidente, în cele mai multe cazuri (171), incidentele raportate au afectat un singur județ, 64 de incidente au avut impact asupra două județe, iar în cazul a 4 incidente, furnizorii au raportat că impactul a fost la nivel național. În acest ultim caz, echipamentele afectate sunt localizate la nivelul rețelei centrale și fac parte din categoriile Centre de comutație în rețele mobile și Componente/Platforme, durata medie a acestora fiind de 156 minute.

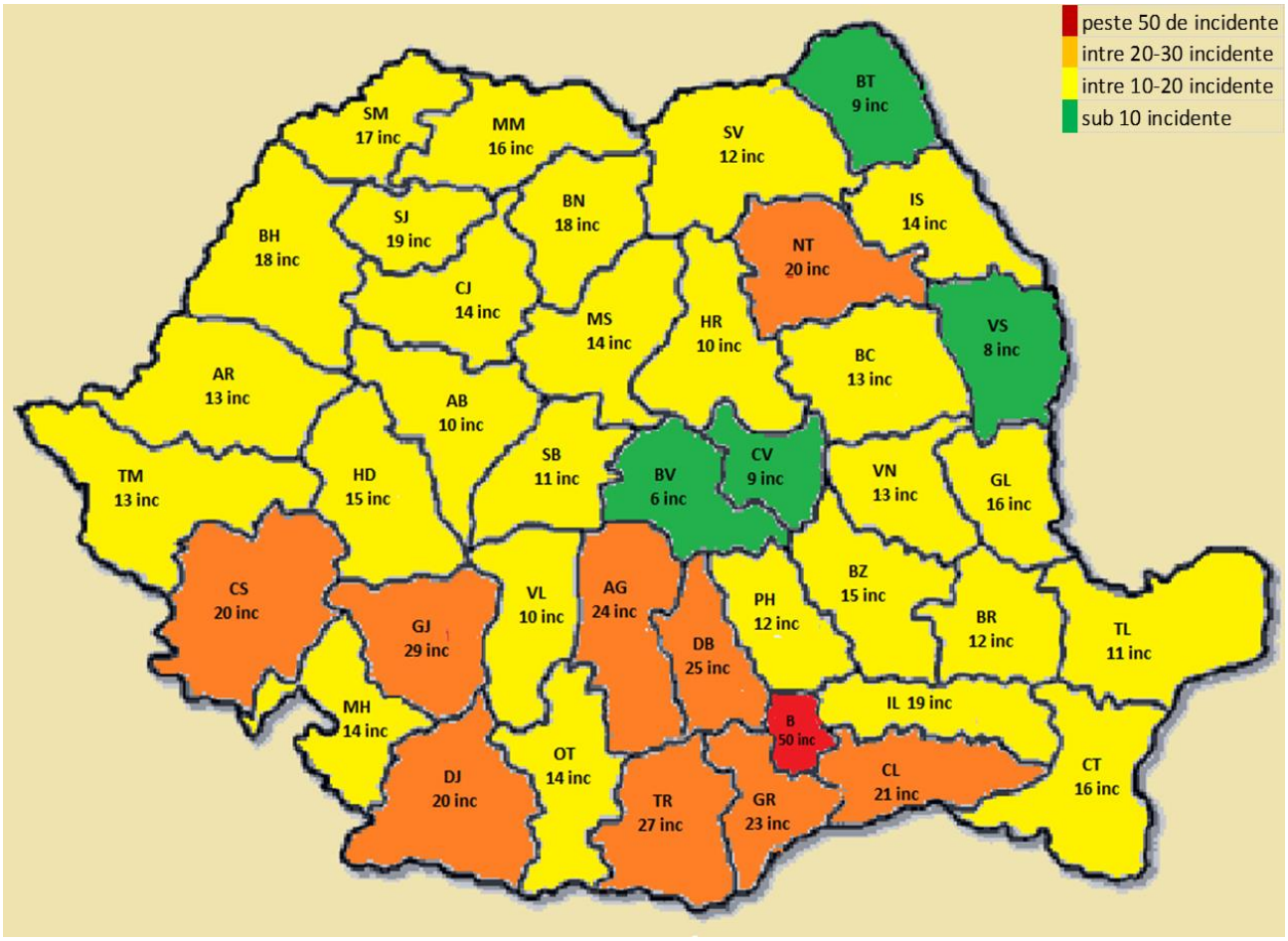
Fig.12 Impactul incidentelor asupra regiunilor geografice efectuate



Analiză geografică

Pentru o imagine mai clară a numărului de incidente care a afectat fiecare județ în parte, această situație este prezentată în figura de mai jos.

Fig.13 Situația incidentelor la nivel național



De precizat faptul că numărul incidentelor însumate la nivel național nu coincide cu numărul de incidente raportate în 2015 (281 incidente) pentru că în cazul a 110 incidente, acestea au avut impact asupra cel puțin a două județe.

Conform raportărilor, cele mai multe incidente au avut loc în București (50 incidente). În Fig. 12 se poate observa că zona cea mai afectată de incidente este partea sudică a țării, aici regăsindu-se majoritatea județelor care au înregistrat cel puțin 20 de incidente.

Județele cel mai puțin afectate sunt Brașov, Vaslui, Covasna și Botoșani

.

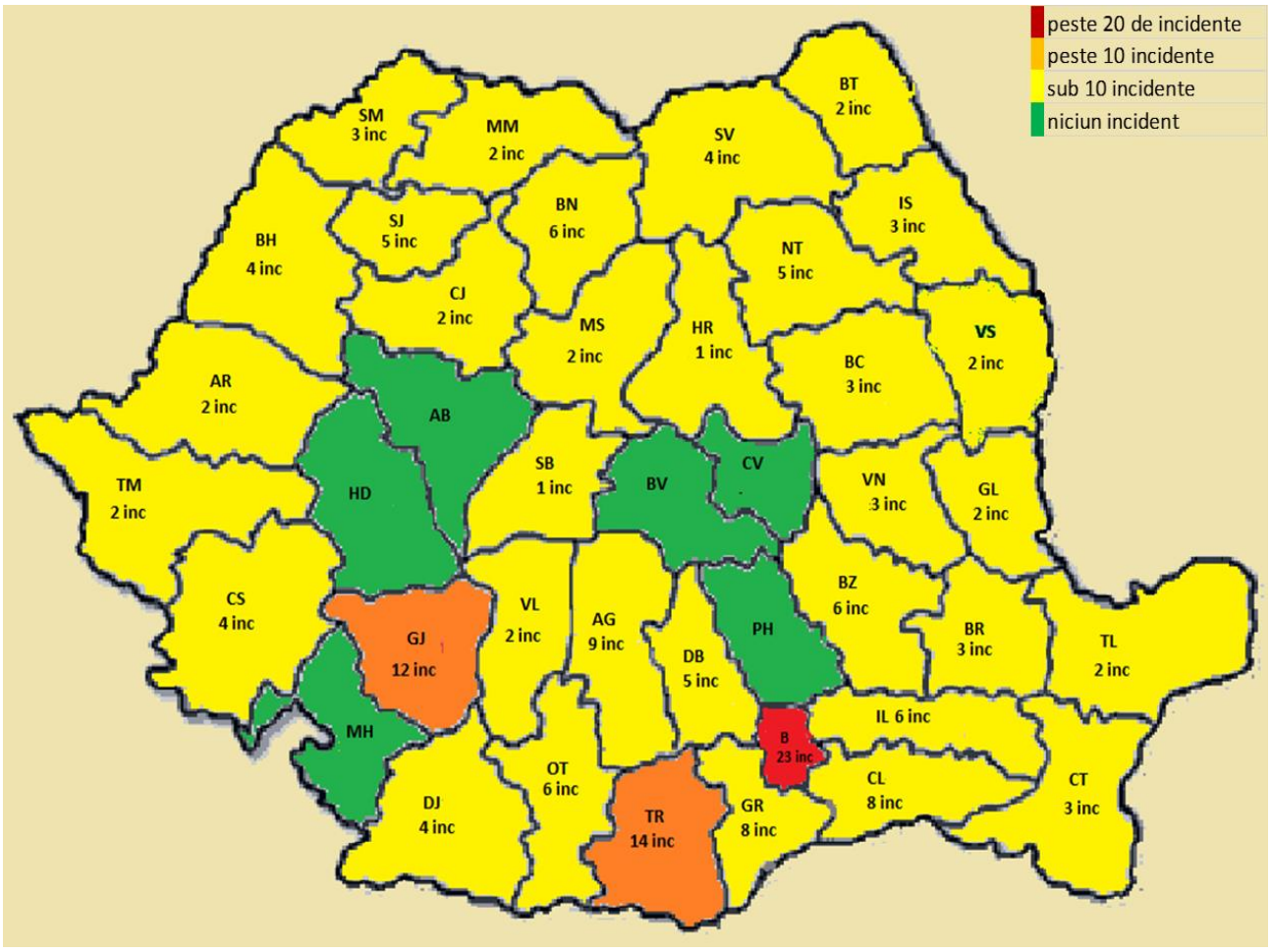
Precizam faptul că în urma raportărilor, s-a putut face distincție între numărul incidentelor înregistrate în București și numărul incidentelor care au afectat județul Ilfov (în ultimul caz fiind vorba de 16 incidente).

Menționăm faptul că în cazul unui incident, furnizorul în cauză a raportat ca fiind afectată jumătatea de sud a țării, fără a mai enumera (nominaliza) județele afectate.

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.

Situația privind incidentele care au avut drept cauză problemele de alimentare cu energie electrică la nivel național, se prezintă astfel:

Fig.14 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 (23 incidente), Teleorman (14 incidente) și Gorj (12 incidente).

În Fig. 14 se poate observa faptul că majoritatea județelor au înregistrat un număr mai mic de 10 incidente datorate problemelor de alimentare cu energie electrică, în 6 cazuri (Brașov, Covasna, Prahova, Mehedinți, Hunedoara, Alba) neexistând probleme de această natură.

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, modificarea procedurilor, verificarea funcționării alarmei care semnalează lipsa combustibilului la generatorul electric etc.

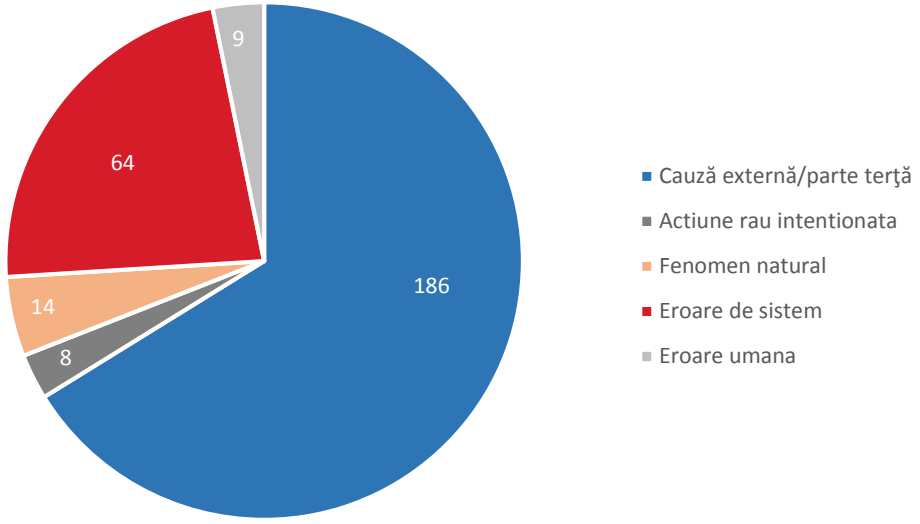
3.3 Cauzele incidentelor raportate

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.

Situația incidentelor în funcție de cauză este prezentată mai jos.

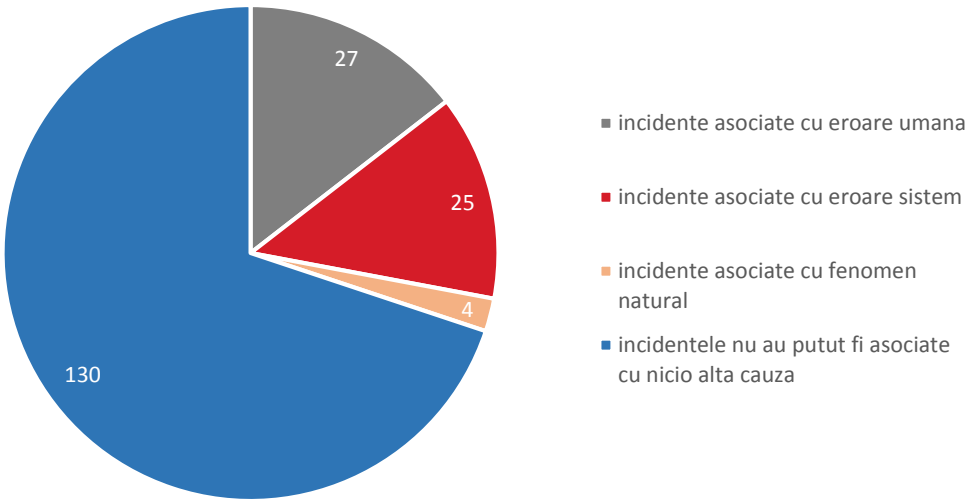
Fig.15 Situația incidentelor în funcție de cauză



Așa cum se poate vedea în Fig. 15, majoritatea incidentelor din 2015 fac parte din categoria cauză externă/parte terță (186 incidente, reprezentând 66% din totalul de incidente raportate în 2015). 64 dintre incidente fac parte din categoria eroare de sistem, 14 de incidente fac parte din categoria fenomen natural, 8 dintre incidente fac parte din categoria acțiune rău – intenționată și doar 9 incidente au fost încadrate în categoria eroare umană.

Incidentele din categoria cauză externă pot fi corelate cu una din celelalte 4 categorii de cauze.

Fig.16 Asocierea cu alte cauze a incidentelor care fac parte din categoria cauză externă/parte terță

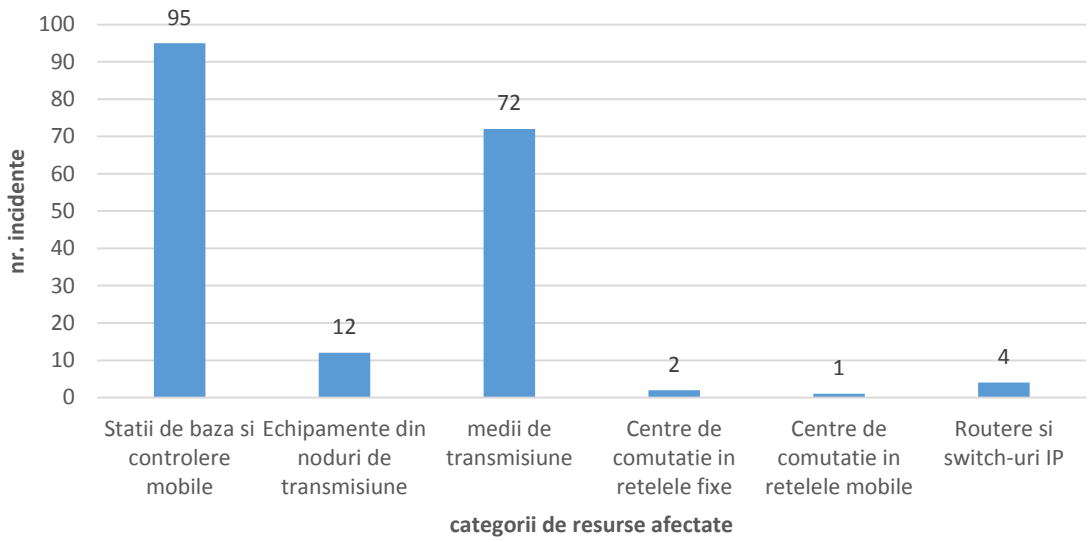


Astfel, dintre cele 186 incidente încadrate în această categorie, 27 au fost asociate cu eroare umană, 25 incidente au fost asociate cu eroare de sistem și 4 incidente au fost asociate cu fenomen natural.

130 de incidente din categoria cauză externă/parte terță nu au putut fi asociate cu nicio altă cauză dintre cele menționate în cadrul Deciziei 512. Acestea s-au datorat în cea mai mare parte defectării unor echipamente din rețelele partenere (28 de incidente). O altă cauză a producerii acestor incidente a fost ruperea (din cauze necunoscute sau neraportate de către furnizori) a fibrei optice, iar în 86 dintre cazuri, incidentele s-au datorat întreruperii alimentării cu energie electrică de către furnizorul de energie electrică.

Întrucât principalele cauze pentru producerea incidentelor raportate în 2015 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.17 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, Centre de comutație în rețelele fixe și Centre de comutație în rețelele mobile.

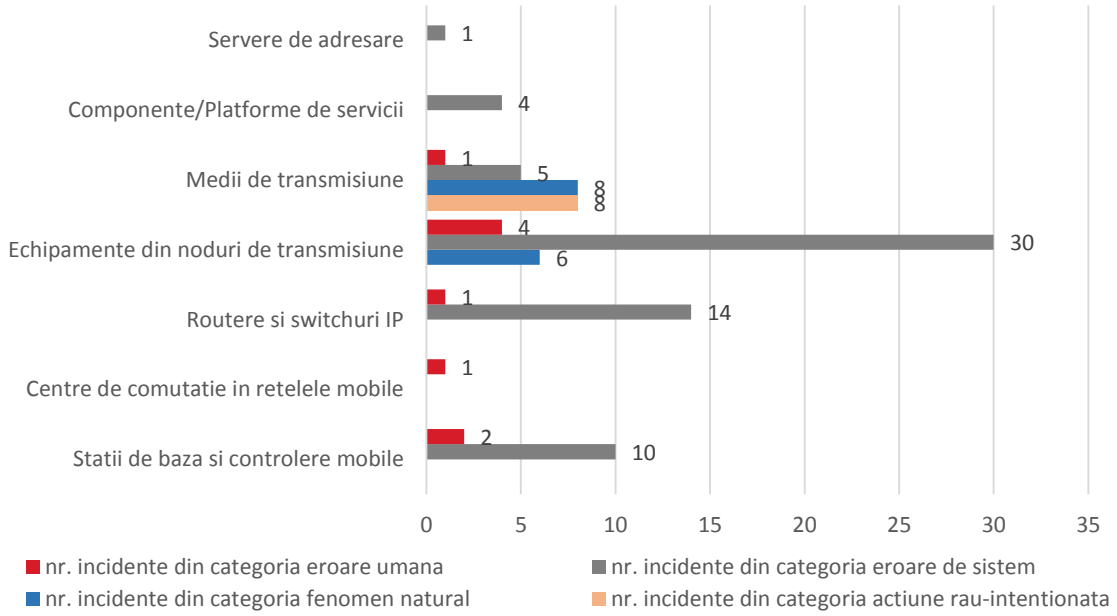
Conform raportărilor, marea majoritate a incidentelor din categoria cauză externă care au afectat resursele din categoria Stații de bază și controlere mobile se datorează problemelor de alimentare cu energie electrică (respectiv întreruperi ale energiei electrice furnizată de rețelele de distribuție națională).

Mediile de transmisiune au fost afectate în principal în urma lucrărilor efectuate de terți, ori din cauze necunoscute de către furnizorii de rețele și servicii de comunicații electronice.

Tot în cazul incidentelor din categoria cauză externă, echipamentele din categoria Centre de comutație în rețelele fixe și categoria Routere și switch-uri au fost afectate în principal din cauza șocurilor de energie electrică. De asemenea, incidentele care au afectat echipamentele din categoria Echipamente din noduri de transmisiune și care fac parte din categoria cauză externă s-au datorat lipsei de alimentare cu energie electrică, cumulată cu autonomia scăzută a bateriilor.

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



Se poate observa faptul că resursele din categoriile Echipamente din noduri de transmisiune, Routere și switchuri IP și Stații de bază și controlere mobile 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 din categoria Medii de transmisiune și se datorează condițiilor meteorologice nefavorabile (rafale de vânt, ploaie, viscol, ninsori abundente) în urma cărora anumite echipamente au fost afectate la nivel fizic. De asemenea, tot în urma fenomenelor naturale (surparea pământului, alunecări de teren), fibra optică a fost întreruptă. Se poate observa că cele mai afectate resurse în cazul incidentelor din categoria acțiune rău intenționată sunt mediile de transmisiune. Aceste incidente s-au datorat tentativelor de furt, distrugerii, respectiv vandalizării cablurilor de fibră optică. Aceste acțiuni au avut în cele mai multe cazuri drept urmare afectarea/izolarea altor categorii de resurse (switch-uri de distribuție, routere, echipamente de transmisiuni etc.). În ceea ce privește incidentele din categoria eroare umană, acestea au afectat în principal resursele din categoria Echipamente din noduri de transmisiune (constând în configurarea eronată a unor echipamente de transmisiuni), restul incidentelor din categoria eroare umană datorându-se erorilor de configurare a diferitelor echipamente, ori secționării din greșeală a fibrei optice.

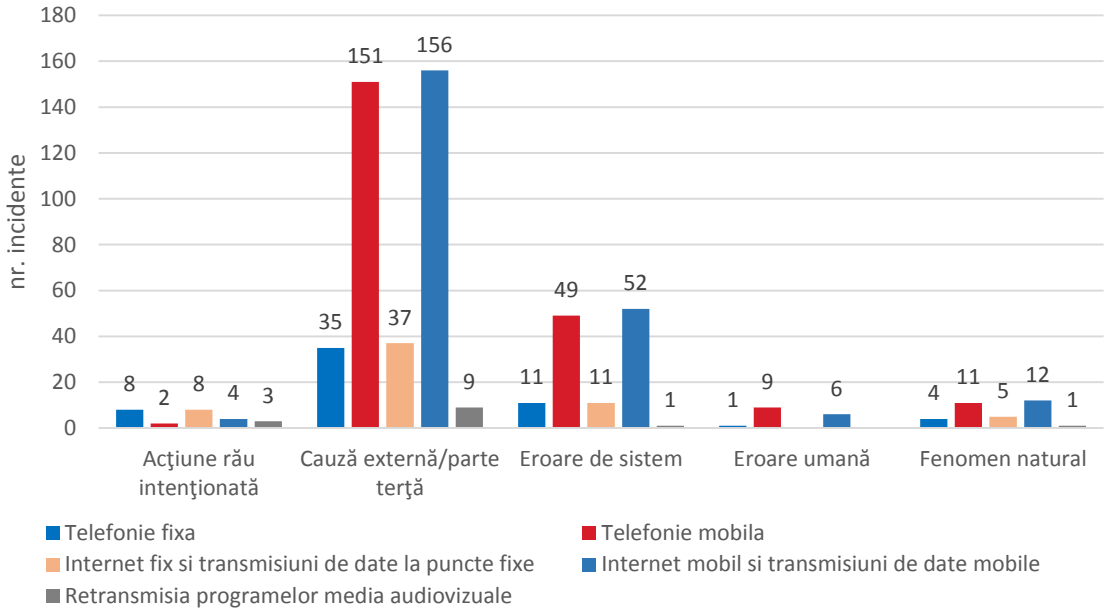
Făcând o analiză a categoriilor de resurse afectate pentru fiecare tip de cauză, din raportările furnizorilor s-a constatat faptul că în cazul incidentelor încadrate în cele 4 categorii de cauze, Stațiile de bază și controlerele mobile au fost afectate în principal din cauza unor erori software apărute, ori datorită configurării greșite a unor echipamente.

Conform raportărilor, resursele din categoria medii de transmisiune au fost afectate fie în urma tentativelor de furt, fie în urma lucrărilor efectuate de terți, fie ca urmare a fenomenelor meteorologice nefavorabile (surpări de mal, alunecări de teren). Afectarea fibrei optice a dus la izolarea anumitor echipamente (routere, switch-uri) și în câteva cazuri ducând la întreruperea furnizării serviciilor unui anumit furnizor în câteva localități (Hațeg, Năvodari).

Echipamentele din categoria Routere și switch-uri au fost afectate în urma defectării anumitor echipamente (switch-uri), problemelor de natură software, ori configurării greșite a unor clase de IP-uri.

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

Fig.19 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.19) diferă de numărul total al incidentelor per tip de cauză (reprezentat în Fig.15) deoarece un incident poate afecta mai multe servicii simultan.

Din Fig.19 se observă că în cazul incidentelor care alcătuiesc majoritatea categoriilor de cauze (cauză externă, eroare de sistem, eroare umană și fenomen natural), cele mai afectate servicii sunt serviciile de acces la internet mobil și transmisiuni de date mobile și serviciile de telefonie mobilă. Cele mai multe incidente care au afectat aceste servicii fac parte din categoria cauză externă. 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 și care au afectat serviciile de acces la internet mobil și transmisiuni de date mobile și serviciile de telefonie mobilă s-au produs în principal datorită problemelor apărute la nivelul furnizorului de energie electrică, ori datorită problemelor apărute la nivelul rețelelor partenere.

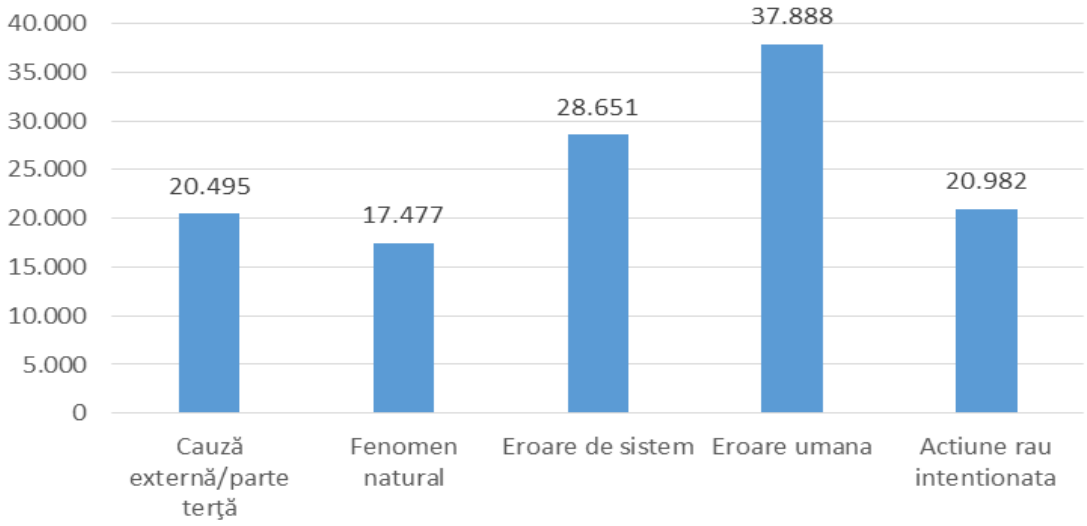
În cazul incidentelor care fac parte din categoriile eroare de sistem și fenomen natural și care au afectat serviciile de acces la internet mobil și transmisiuni de date mobile și serviciile de telefonie mobilă, acestea s-au produs în principal datorită defecțiunilor software sau hardware ale unor echipamente, respectiv datorită condițiilor meteorologice nefavorabile.

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 și au avut impact asupra unui singur județ. Aceste acțiuni au avut ca urmare afectarea/izolarea altor categorii de echipamente (routere, switch-uri, echipamente din noduri de transmisiuni).

Serviciile de retransmisie a programelor audiovizuale au fost afectate în principal în cazul incidentelor care fac parte din categoria cauză externă/parte terță (9 incidente). Acestea s-au datorat în mare parte avariilor la nivelul fibrei optice.

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

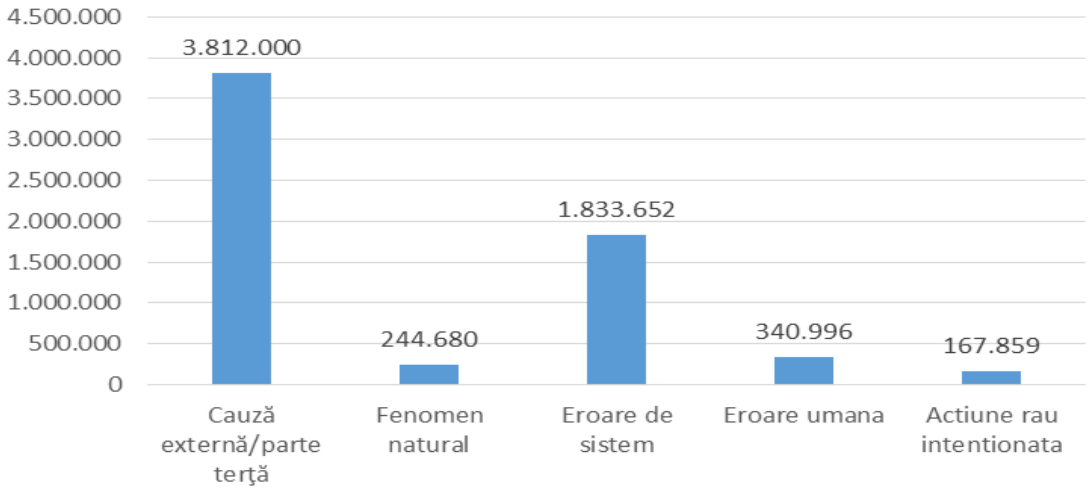
Fig.20 Numărul mediu de conexiuni per tip de cauză



În graficul de mai sus se poate observa faptul că în cazul incidentelor care fac parte din categoriile eroare umană și eroare de sistem a fost afectat în medie cel mai mare număr de conexiuni. Incidentele din categoria fenomen natural au afectat în medie cel mai mic număr de conexiuni (17.477).

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

Fig.21 Numărul de conexiuni afectate în funcție de cauză



Analiza ultimelor două grafice (Fig.20 și Fig.21) susțin situații deja prezentate în acest raport care se referă la numărul de incidente în funcție de fiecare tip de cauză.

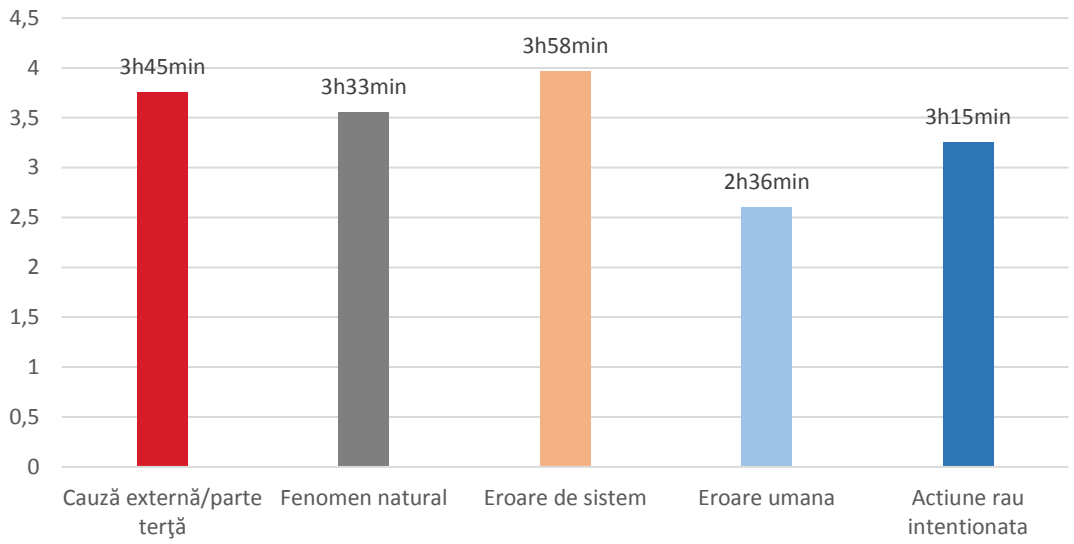
3.4 Durata incidentelor și durata de descoperire a incidentelor

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 2015 este de 1.050 ore, durata medie a unui incident fiind de aproximativ 4 ore (3h44).

În figura de mai jos este ilustrată durata medie a unui incident în funcție de cauza incidentului.

Fig.22 Durata medie a incidentelor în funcție de cauză

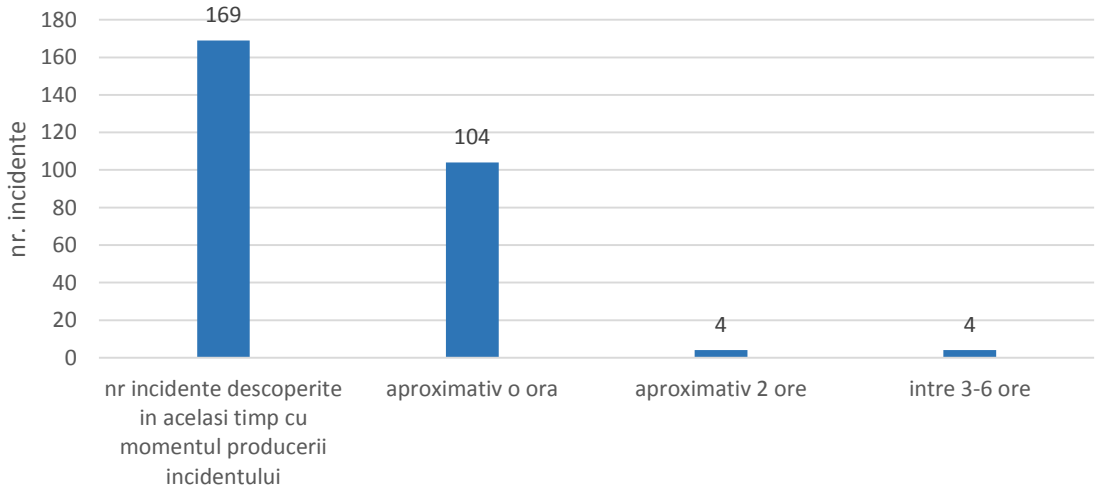


Valoarea cea mai mare a duratei medii aparține categoriei de cauze eroare de sistem (3h58minute).

În Fig.22 se observă că valorile duratei medii ale incidentelor care fac parte din categoriile cauză externă, fenomen natural, eroare de sistem și acțiune rău intenționată sunt comparabile.

Situația privind numărul de incidente și durata în care au fost descoperite este prezentată mai jos.

Fig.23 Numărul de incidente și durata în care au fost descoperite

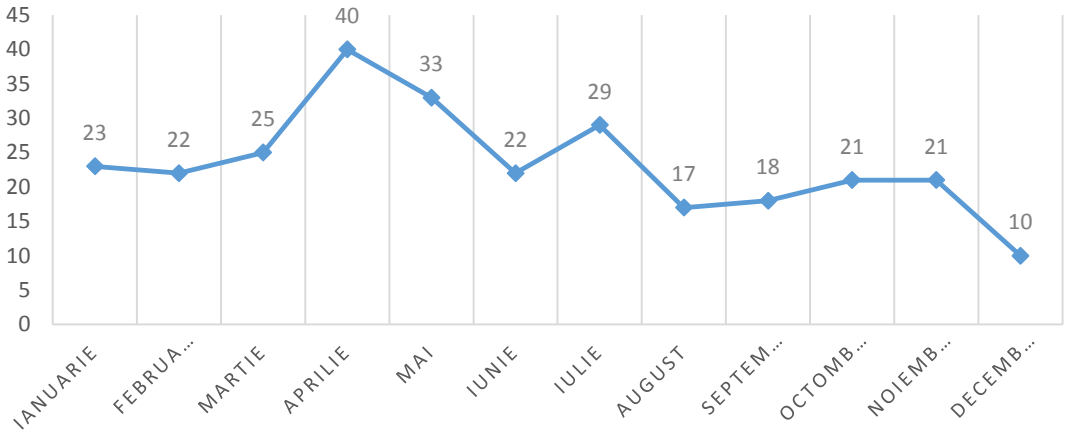


Din Fig.23 se poate observa că cele mai multe incidente (169) au fost descoperite în momentul producerii lor, 104 de incidente au fost descoperite într-o oră, iar 4 incidente au fost descoperite până în 6 ore.

Din informațiile primite de la furnizori, aceste întârzieri în detectarea incidentelor pot avea o justificare prin faptul că, deși furnizorii sunt înștiințați prin alarme exact în momentul la care se produce un incident, acesta nu este introdus în sistem decât după ce alarma respectivă este verificată și validată.

Figura de mai jos reprezintă distribuția incidentelor raportate pe luni în anul 2015.

Fig.24 Numărul incidentelor înregistrate pe luni



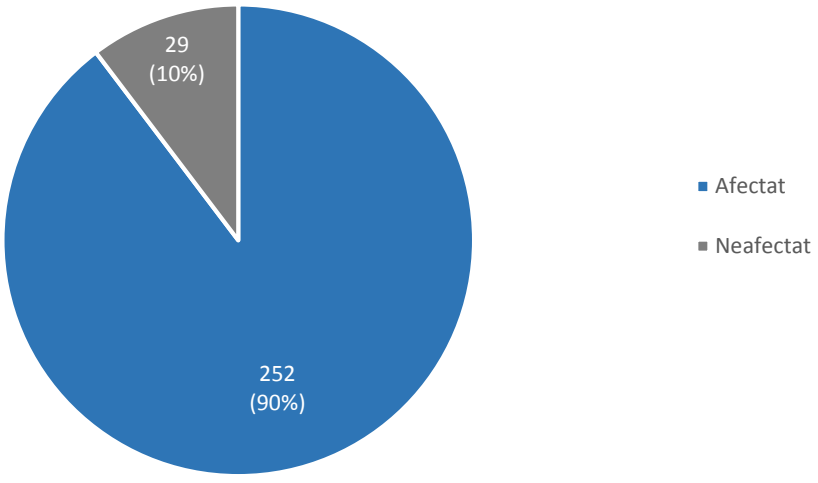
Se poate observa că luna aprilie și mai sunt perioadele în care s-au raportat cele mai multe dintre incidente (40, respectiv 33). Acestea s-au datorat în cea mai mare parte cauzelor externe și majoritatea dintre acestea au fost cauzate de probleme de alimentare cu energie electrică.

3.5 Impactul asupra apelurilor de urgență

90% dintre incidentele raportate în anul 2015 au avut un posibil impact asupra efectuării apelurilor de urgență.

Această statistică este prezentată în figura de mai jos.

Fig.25 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 2015, 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;
- Modificarea procedurilor de restaurare a serviciilor;
- Implementarea unui filtru în sistemul de monitorizare a alarmelor apărute în rețea;
- Revizuirea procedurii de configurare a echipamentelor de interconectare;
- Implementarea de mecanisme în scopul detectării problemelor de configurare IP;
- Stabilirea unor reguli noi privind lucrările programate realizate de producătorii de echipamente;
- Asigurarea redundanței căilor de transmisiune.

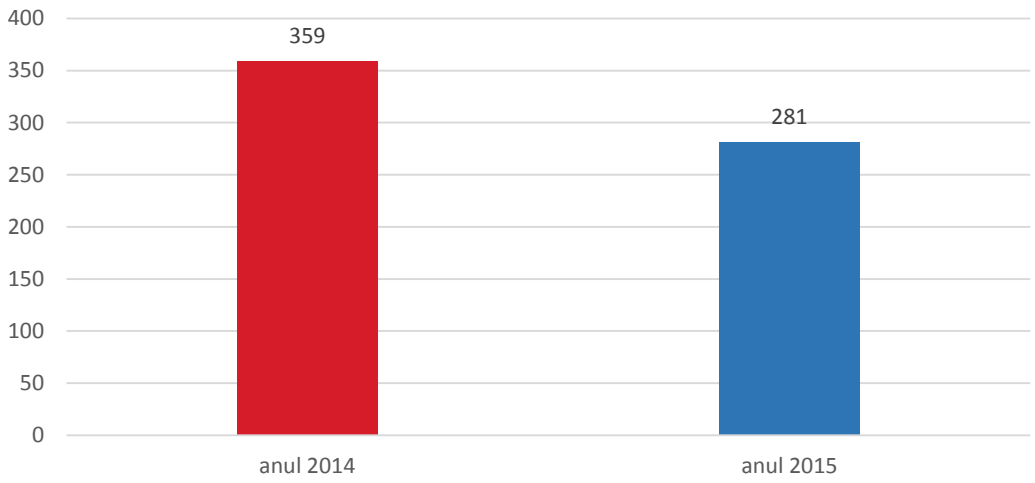
Menționăm faptul că în cazul majorității incidentelor raportate în 2015, câmpul aferent măsurilor luate sau planificate pentru a împiedica producerea unui incident similar nu a fost completat cu informații relevante sau concrete. Acest fapt se poate datora unei deficiențe de raportare, dar și faptului 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 2014 și 2015

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 2014 și 2015.

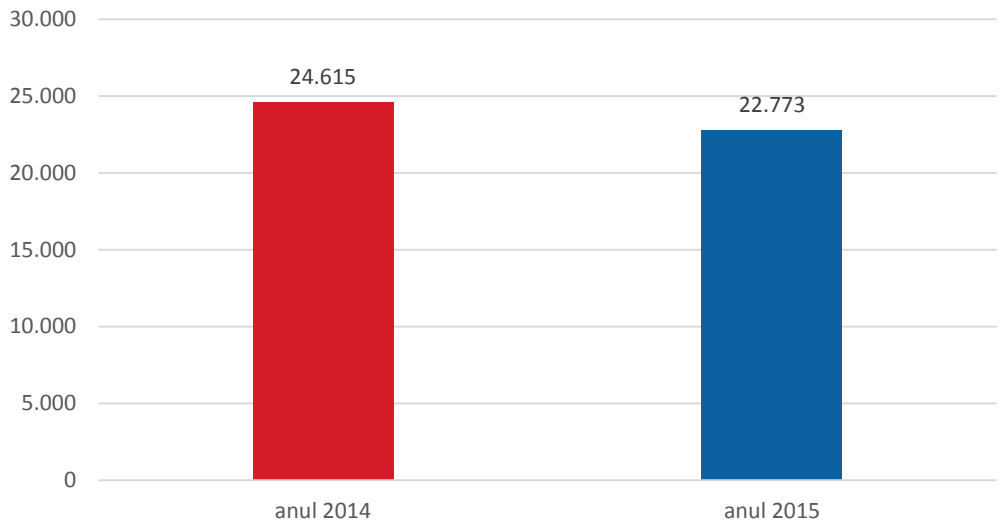
Situația incidentelor în 2015 comparativ cu anul precedent, este prezentată în figura de mai jos.

Fig.26 Numărul incidentelor pentru anii 2014 și 2015



Situația în ceea ce privește numărul mediu de conexiuni afectate înregistrat în 2014 și 2015 este prezentată în figura de mai jos.

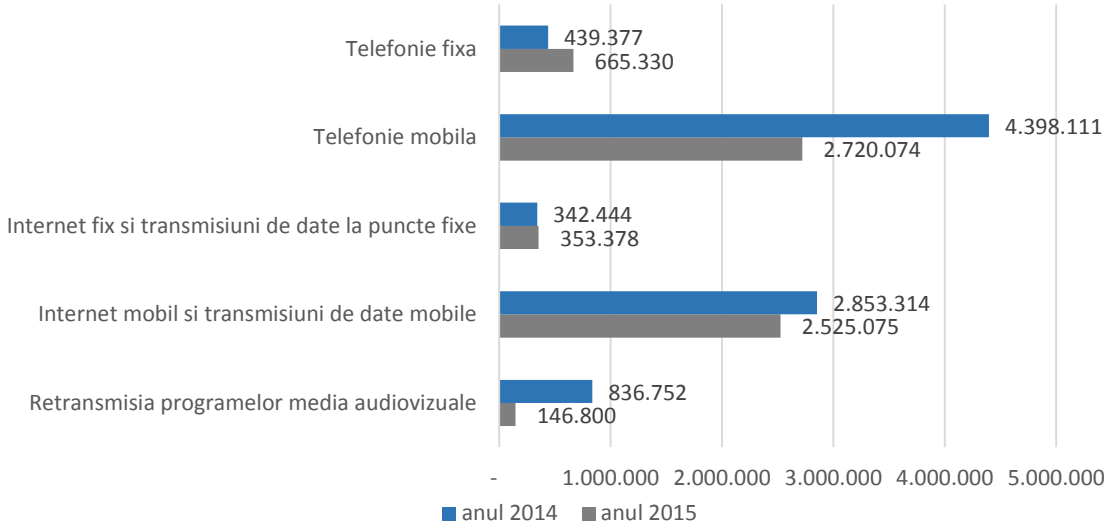
Fig.27 Numărul mediu de conexiuni afectate



Se poate observa astfel că în 2015, valoarea medie a numărului de conexiuni afectate a scăzut față de anul precedent.

În figura de mai jos este reprezentat numărul de conexiuni afectate per serviciu pentru anii în discuție.

Fig.28 Numărul de conexiuni afectate per serviciu

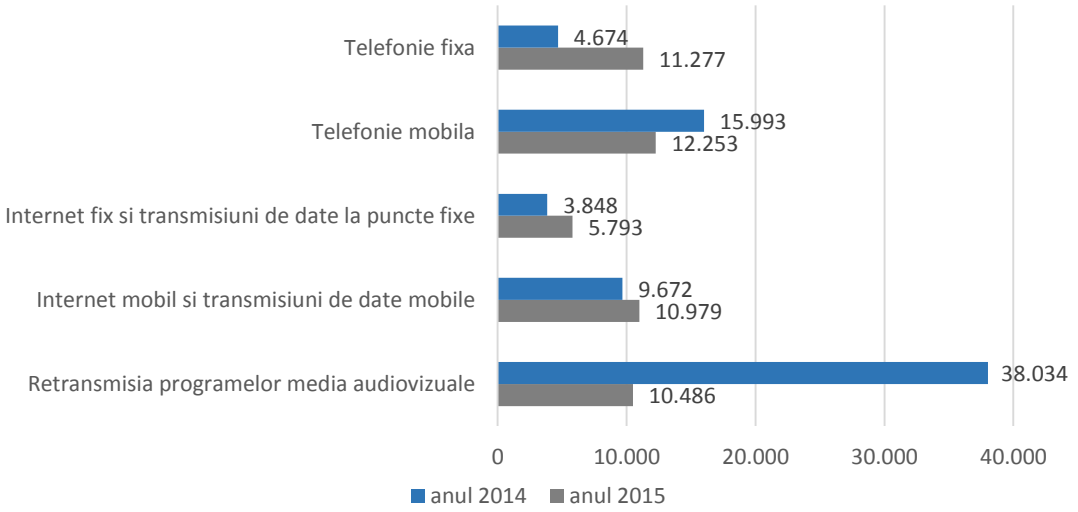


În Fig.28 se poate observa faptul că serviciile de telefonie mobilă și serviciile de internet mobil și transmisiuni de date mobile au fost cele mai afectate atât în 2014, cât și în 2015.

În ceea ce privește serviciile fixe, numărul conexiunilor afectate în acest caz au înregistrat ușoare creșteri în 2015. În schimb, o diferență semnificativă se poate observa în cazul serviciilor de retransmisie a programelor media audiovizuale, pentru care numărul conexiunilor afectate în 2015 a înregistrat o valoare de aproximativ 6 ori mai mica față de anul precedent.

Graficul de mai jos reprezintă situația privind numărul mediu de conexiuni afectate de un incident per serviciu.

Fig.29 Numărul mediu de conexiuni afectate de un incident per serviciu

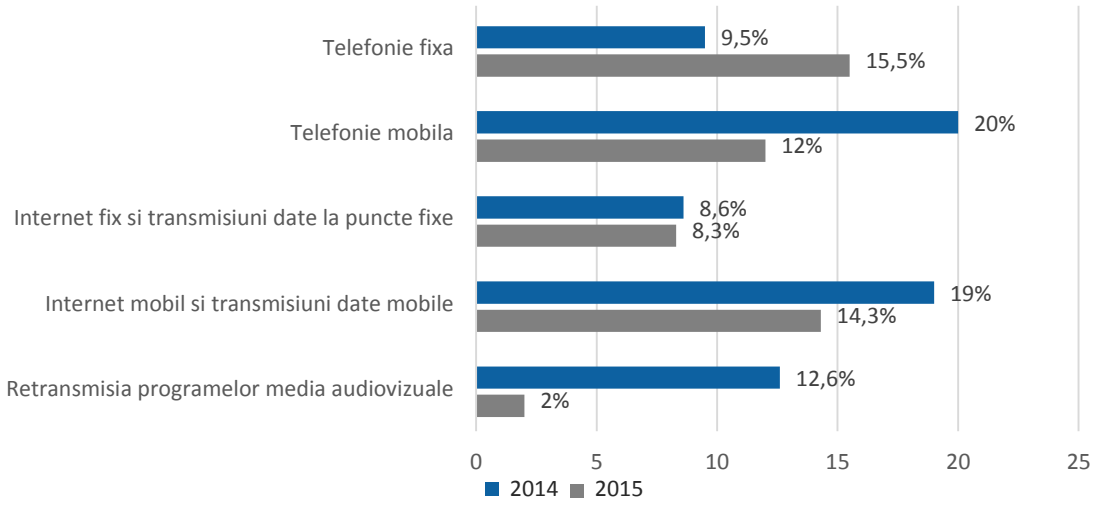


În graficul de mai sus se poate observa că în cazul serviciilor de telefonie fixă, valorile privind numărul mediu de conexiuni afectate de un incident înregistrate în 2015 sunt de cel puțin două ori mai mari față de cele din 2014. De asemenea, valori mai mari față de 2014 ale numărului mediu de conexiuni afectate de un incident per serviciu au fost înregistrate și în cazul serviciilor de internet fix

și transmisiuni de date la puncte fixe și serviciul de internet mobil și transmisiuni de date mobile. În schimb, situația privind serviciile de retransmisie a programelor media audiovizuale este cu mult mai bună în 2015, când valoarea numărului mediu de conexiuni afectate de un incident per serviciu este de cel puțin 3 ori mai mică față de anul precedent.

În ceea ce privește situația conexiunilor afectate în raport cu numărul total de conexiuni per serviciu, aceasta este prezentată în figura de mai jos.

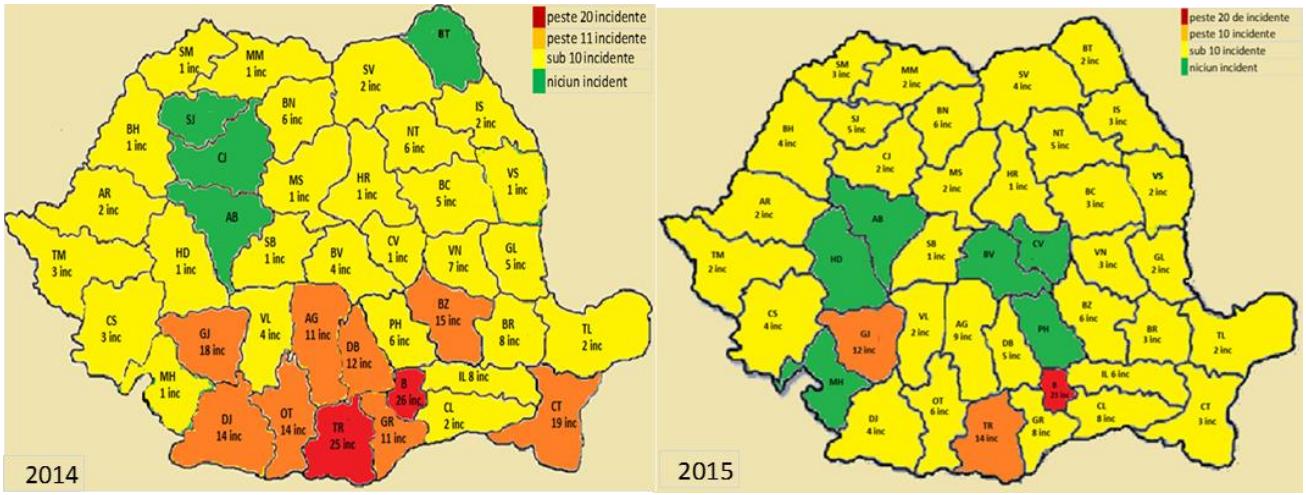
Fig.30 Procentul de conexiuni afectate în raport cu numărul total de conexiuni per serviciu



Se poate observa faptul că doar în cazul serviciilor de telefonie fixă, impactul incidentelor la nivel național este mai mare în 2015 comparativ cu 2014. În cazul celorlalte servicii, situația privind procentul de conexiuni afectate în raport cu numărul total de conexiuni per serviciu este cu mult mai bună în 2015.

Situația la nivel național din 2014 și 2015 a incidentelor care s-au datorat problemelor de alimentare cu energie electrică este prezentată mai jos.

Fig.31 Situația la nivel național din 2014 și 2015 a incidentelor care s-au datorat problemelor de alimentare cu energie electrică

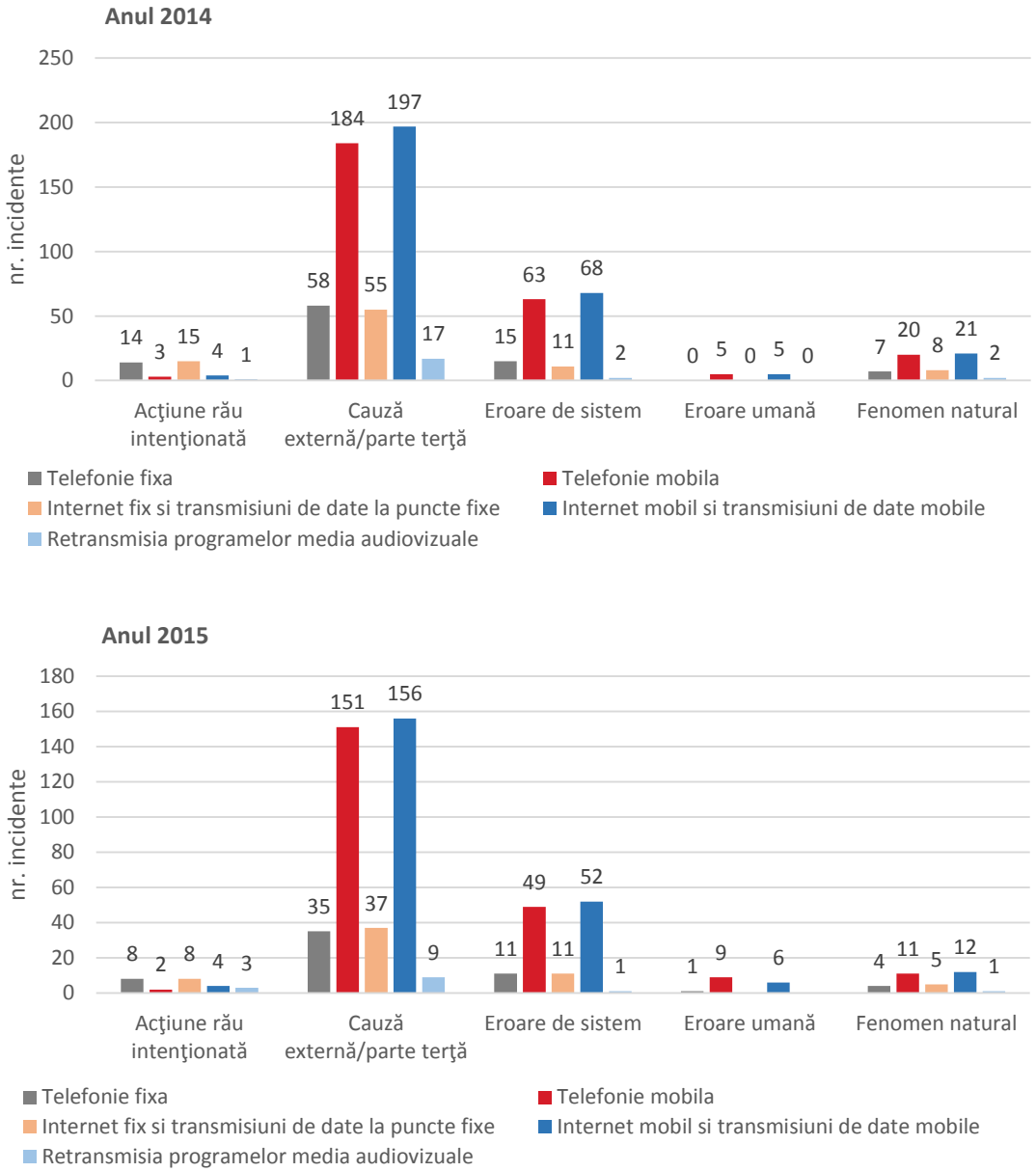


Având în vedere că numărul incidentelor care s-au datorat problemelor de alimentare cu energie electrică au reprezentat în 2014 aproximativ 45% din totalul incidentelor raportate, situația în această privință s-a îmbunătățit în 2015, întrucât procentul acestora a scăzut (40% din totalul de incidente raportate). În plus, în Fig.31 se poate observa faptul că în 2015 a crescut numărul județelor

la nivelul cărora nu s-a înregistrat nici un incident datorat problemelor de alimentare cu energie electrică, iar zona sudică a fost afectată într-o măsură mai mică în comparație cu 2014.

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.32 Numărul incidentelor pentru toate tipurile de servicii afectate în funcție de cauză în anii 2014, respectiv 2015



Se poate observa că situațiile din anii 2014 și 2015 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.

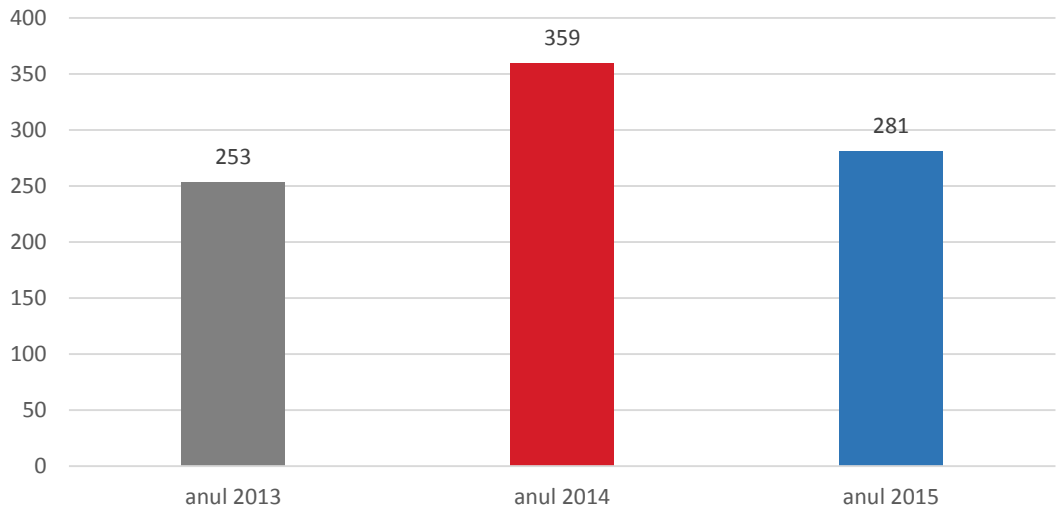
Datele privind incidentele sunt fundamentale pentru dezvoltarea unei înțelegeri clare a naturii și amplorii provocărilor existente la adresa securității și integrității rețelelor și serviciilor prin analiza amenințărilor și vulnerabilităților la adresa securității și integrității rețelelor și serviciilor 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 281 de incidente cu impact semnificativ raportate de către 7 furnizori de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului, pentru anul 2015, se pot desprinde următoarele concluzii:

- analizând situația privind numărul de incidente cu impact semnificativ raportate în ultimii 3 ani, nu se poate identifica deocamdată o direcție majoră de evoluție a acestui parametru. Figura de mai jos este ilustrativă în acest sens:

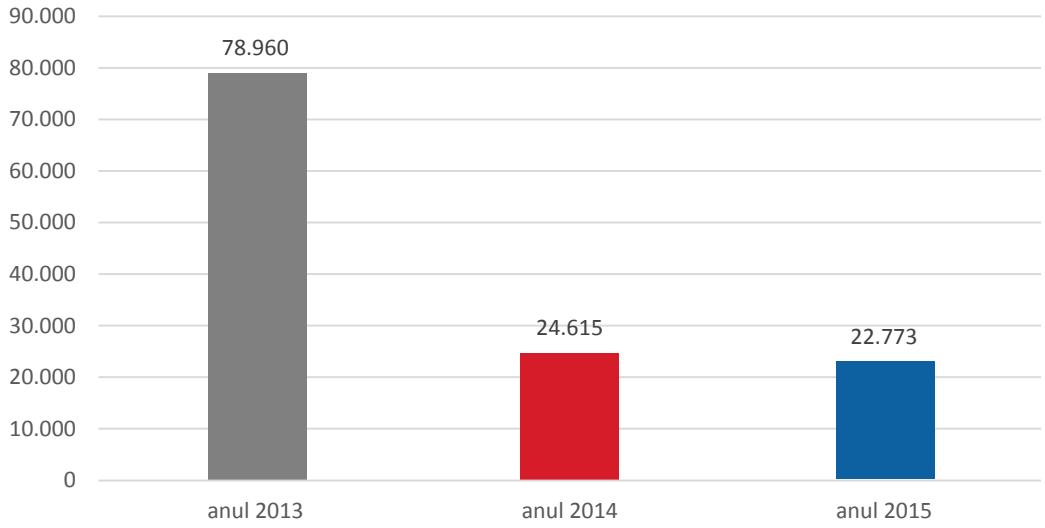
Fig. 33 Comparație 2013, 2014, 2015 privind numărul de incidente raportate



- din punct de vedere al numărului de conexiuni afectate, cea mai afectată categorie de servicii de comunicații electronice au fost serviciile de telefonie mobilă (2.720.074 conexiuni afectate); totodată, raportat la numărul total de conexiuni la nivel național aferente fiecărei categorii de servicii, cele mai afectate au fost serviciul de telefonie fixă (15,5%) și serviciul de acces la internet mobil și date mobile (14,3%);
- din perspectiva numărului de incidente, cele mai multe dintre incidentele raportate în 2015 au afectat serviciile de acces la internet mobil și date mobile (230 incidente) și serviciile de telefonie mobilă (222 incidente);
- numărul mediu de conexiuni afectate de un incident în 2015 este de 22.773; statistica pe ultimii trei ani relevă faptul că valoarea acesteia este în scădere, în 2015

înregistrându-se o valoare cu aproximativ 71% mai mică decât anul 2013. Această situație este prezentată în figura de mai jos:

Fig.34 Comparație 2013, 2014, 2015 privind numărul mediu de conexiuni afectate



- cele mai afectate resurse fac parte din categoria Stații de bază și controlere mobile (107 incidente);
- aproximativ 40% din totalul incidentelor s-au datorat problemelor de alimentare cu energie electrică;
- aproximativ 61% dintre incidente au avut impact asupra unui singur județ;
- doar în cazul a 4 incidente, impactul s-a resimțit la nivel național;
- 66% 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 date mobile;
- în 2015 durata medie a unui incident raportat a fost de 3h44min;
- incidentele din categoria Eroare de sistem au înregistrat cea mai mare durată medie (3h58min);
- aproximativ 97% dintre incidente au fost descoperite în același timp, ori în primele 30 de minute de la momentul producerii lor;
- cele mai multe incidente s-au înregistrat în luna aprilie (40 incidente);
- 90% 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 2015, 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 problemă de ordin general în raportarea incidentelor o reprezintă raportarea greșită a resurselor afectate. De cele mai multe ori, resursa afectată este încadrată într-o categorie greșită, ori sunt raportate mai multe tipuri de resurse aparținând mai multor categorii.

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*).

Comparând modul de raportare al incidentelor din 2015 cu anul precedent, s-a constatat faptul că deficiențele de raportare se mențin, fapt care duce la concluzia privind interesul scăzut al furnizorilor de a îmbunătăți acest aspect.

Subliniem încă o dată importanța unei raportări care să cuprindă informații corecte și (cât mai) complete astfel încât imaginea privitoare la situația incidentelor cu impact semnificativ să reflecte realitatea.

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 a publicat în 2016 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

Analizând incidentele cu impact semnificativ raportate în ultimii ani se poate extrage concluzia că situația în această privință s-a îmbunătățit în 2015, având în vedere că în acest an a fost raportat un număr mai mic de incidente comparativ cu 2014, iar valorile numărului mediu de conexiuni afectate, precum și cea a numărului de conexiuni afectate în raport cu cele existente pe piață sunt în scădere față de anii precedenți.

Pe de altă parte, discrepanța foarte mare între numărul de incidente raportate de fiecare furnizor reprezintă un aspect care a atras atenția și va fi evaluat de către ANCOM. Un alt aspect remarcat îl constituie o anumită neglijență a furnizorilor în completarea raportărilor incidentelor cu informații corecte și de calitate, fapt care se reflectă în menținerea deficiențelor de raportare de la un an la următorul.

Pentru a avea o imagine cât mai completă a situației privind securitatea și integritatea rețelelor și serviciilor de comunicații electronice cât și pentru o îmbunătățire a situației raportării incidentelor cu impact semnificativ, ANCOM a lansat în luna aprilie, 2016, un chestionar[8] adresat furnizorilor, ce vizează analiza/evaluarea stadiului de implementare a măsurilor de securitate în domeniul managementului incidentelor.

[8] Chestionarul este disponibil la adresa: http://www.ancom.org.ro/chestionare_4950