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 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 2016 au existat 5 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 2016

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 2016 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 2016 au fost raportate 279 de incidente de către 6 furnizori de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului. Acestea au fost centralizate, catalogate și apoi analizate din mai multe puncte de vedere:

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

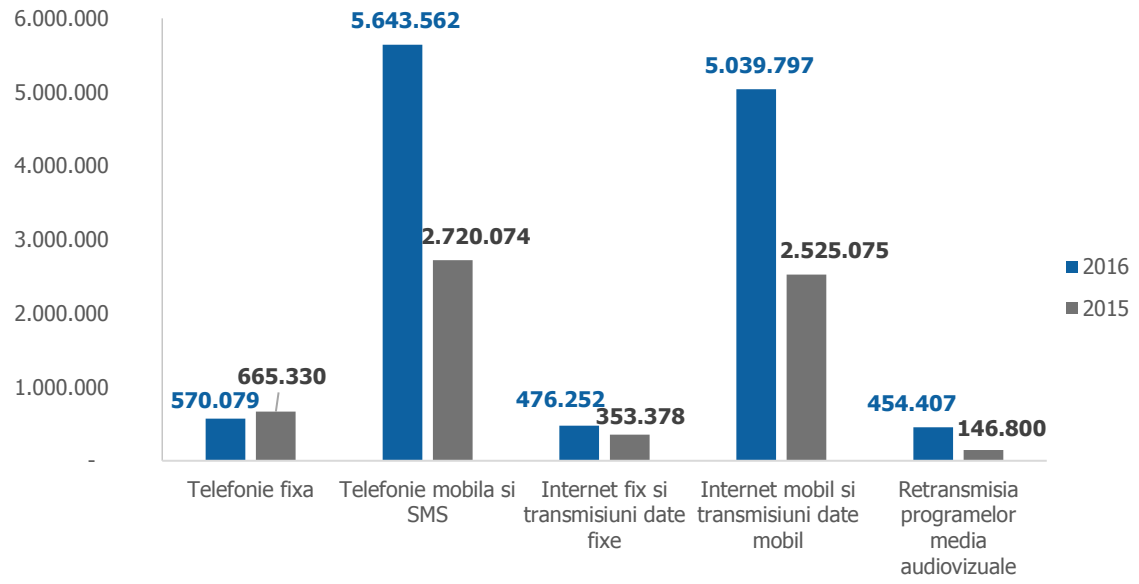
3.1 Impactul asupra serviciilor și utilizatorilor

În 2016 s-au raportat 279 incidente cu impact semnificativ asupra rețelelor și serviciilor de comunicații electronice. Menționăm că în anul 2015 s-au înregistrat 281 de incidente.

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

Numărul total de conexiuni afectate de incidentele cu impact asupra principalelor servicii de comunicații electronice în anul 2016 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.

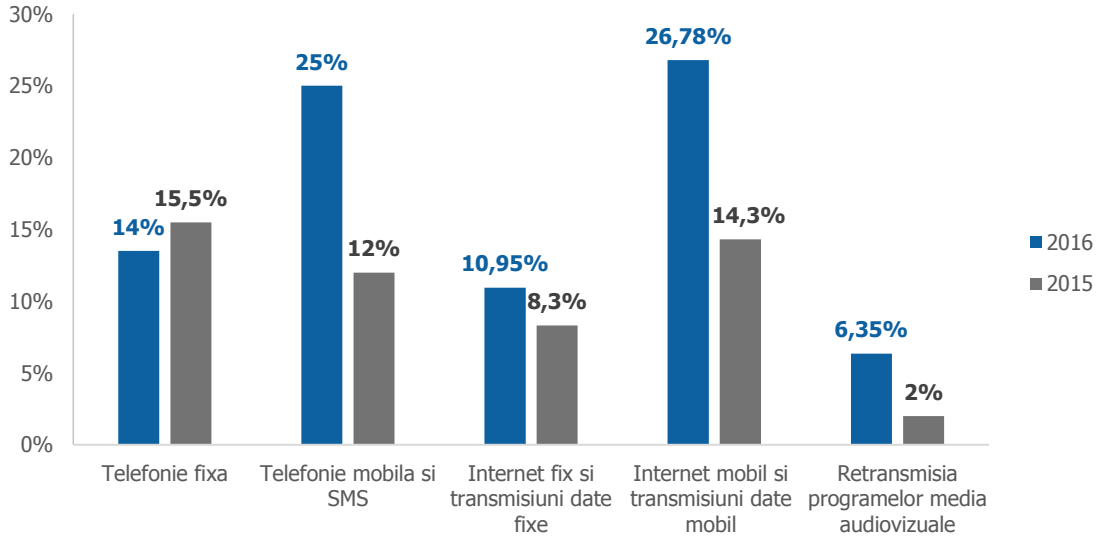
În 2016 cele mai afectate au fost serviciile de telefonie mobilă și SMS (5.643.562 conexiuni afectate). În Fig.1 se poate observa faptul că serviciile de telefonie fixă, serviciile de internet fix și transmisiuni de date la puncte fixe au fost afectate în mică măsură.

Se poate observa o creștere foarte mare a conexiunilor afectate în 2016 în comparație cu 2015 la serviciile mobile.

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 numarul total de conexiuni per serviciu*(%)

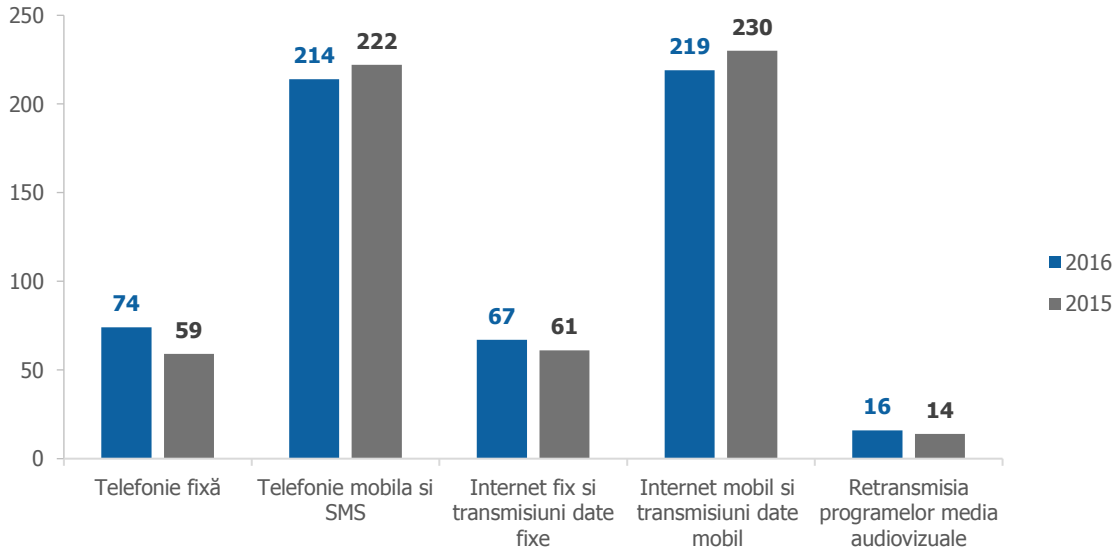


* Conform Raportului privind datele statistice, semestrul I 2016, care poate fi accesat la următoarea adresă: https://statistica.ancom.org.ro:8000/sscpds/public/files/130_ro

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 2016 la numărul total de conexiuni raportate de furnizori.

Figura de mai jos reprezintă numărul de incidente care au afectat fiecare serviciu în anul 2016.

Fig.3 Impactul asupra serviciilor



În Fig. 3 se observă că cele mai multe dintre incidentele raportate în 2016 au afectat serviciile de acces la internet mobil și transmisiuni de date la puncte mobile și serviciile de telefonie mobilă (219, respectiv 214 incidente). Cel mai puțin afectat serviciu este cel de retransmitere a programelor

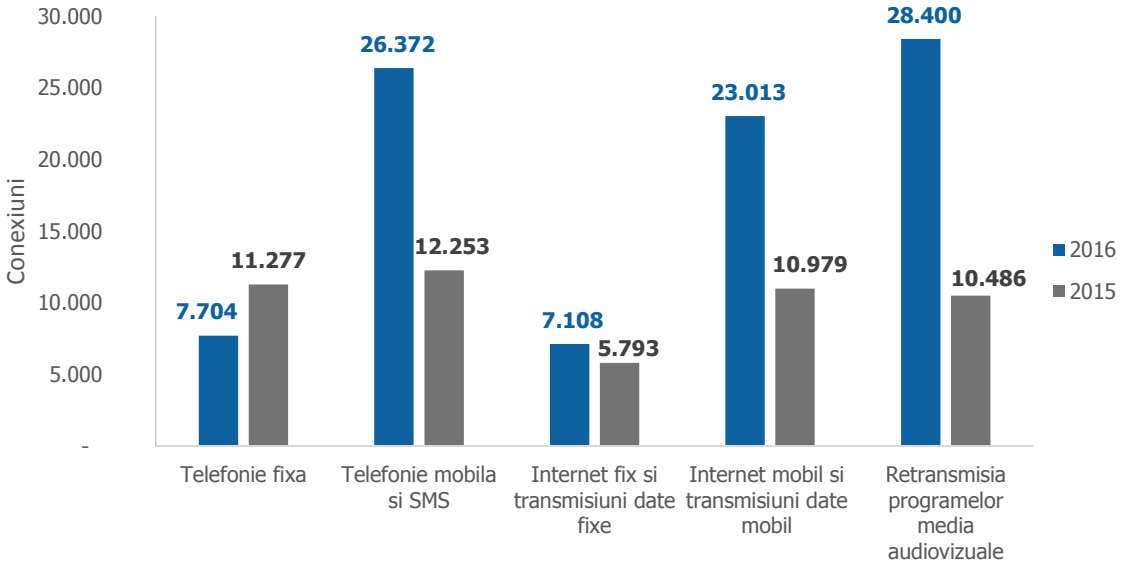
media audiovizuale, 16 incidente afectând acest serviciu în anul 2016. Se poate observa că s-au menținut proporțiile față de anul 2015.

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.

Numărul mediu de conexiuni afectate de un incident în 2016 este de 47.859 conexiuni, în creștere mare față de 2015 (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



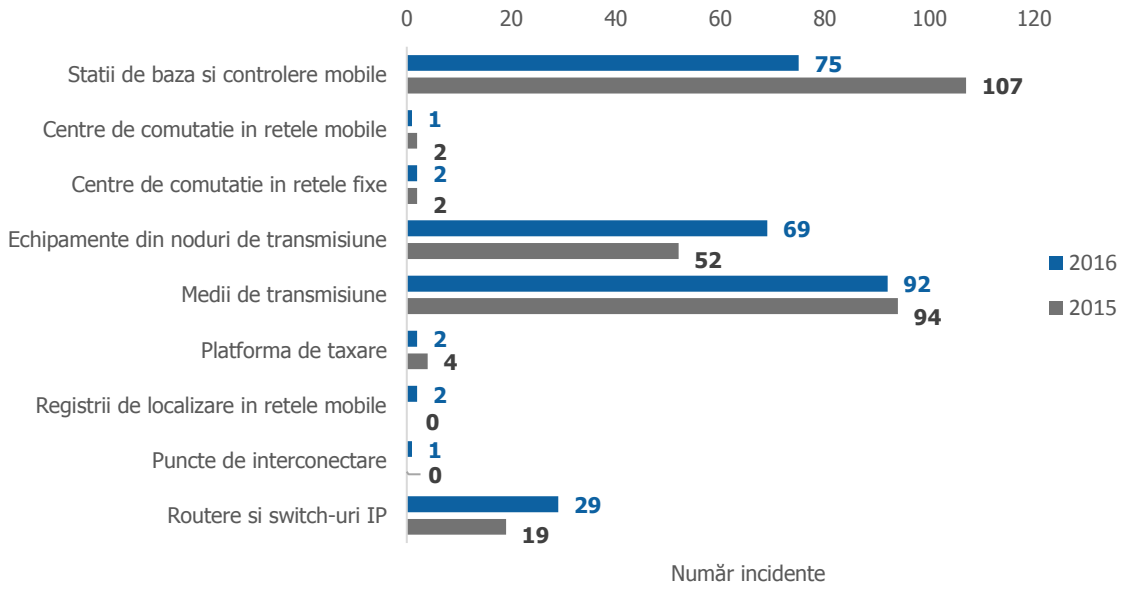
Se poate observa că, deși numărul incidentelor care au afectat serviciile de retransmitere a programelor media audiovizuale (16 incidente) este mai mic decât numărul incidentelor înregistrate în cazul serviciilor de internet mobil și date mobile (219 incidente), numărul mediu de conexiuni afectate de un incident în cazul serviciului de retransmitere a programelor media audiovizuale (28.400 conexiuni) este mai mare decât în cazul serviciului de internet mobil și transmisiuni de date mobile (23.013 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



În Fig.5 se poate observa că în cazul celor mai multe incidente, resursele afectate fac parte din categoria Medii de transmisiune, Stații de bază și controlere mobile și echipamente din noduri de transmisiune.

În cazul a 92 dintre incidente, resursa afectată face parte din categoria Medii de transmisiune, iar 61 dintre acestea fac parte din categoria cauză externă/eroare umană și au constat în ruperea fibrei optice în urma lucrărilor efectuate de terți. 8 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 de bază în rețelele mobile. Restul incidentelor în care a fost afectată categoria Medii de transmisiune s-au 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 switch-uri IP și Echipamente din noduri de transmisiune.

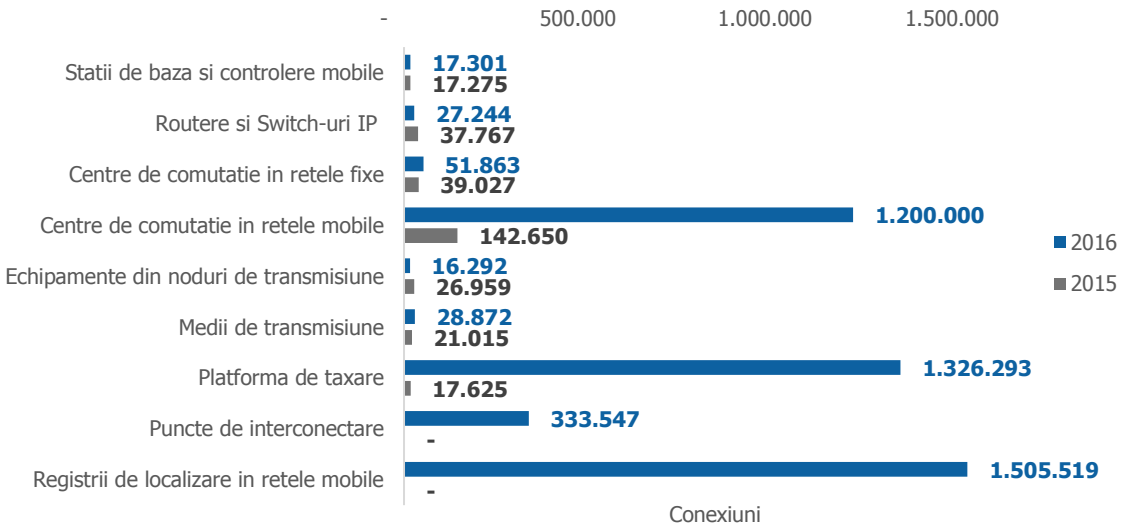
67 din cele 75 de incidente care au afectat categoria Stații de bază și controlere mobile s-au datorat lipsei sau problemelor de alimentare cu energie electrică, în cadrul acestora fiind afectate aproximativ 196 BTS (2G), 260 NodeB (3G) și 51 eNodeB (4G).

În cazul a 69 dintre incidente, resursa afectată face parte din categoria Echipamente din noduri de transmisiune, iar în cazul a 36 dintre incidente, resursa afectată face parte din categoria Routere și switch-uri IP. Într-o măsură mai mică au fost afectate resursele din categoriile Platforma de taxare (2 incidente), Centre de comutație în rețele fixe (2 incidente), Centre de comutație în rețele mobile (1 incident), Regiștrii de localizare (2 incidente).

Se poate observa că numărul echipamentelor afectate din categoria Stații de bază și controlere mobile a scăzut în 2016 față de 2015 dar a crescut numărul de echipamente afectate din noduri de transmisiune, routere și switch-uri IP.

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 Nr. mediu de conexiuni în funcție de resursa afectată



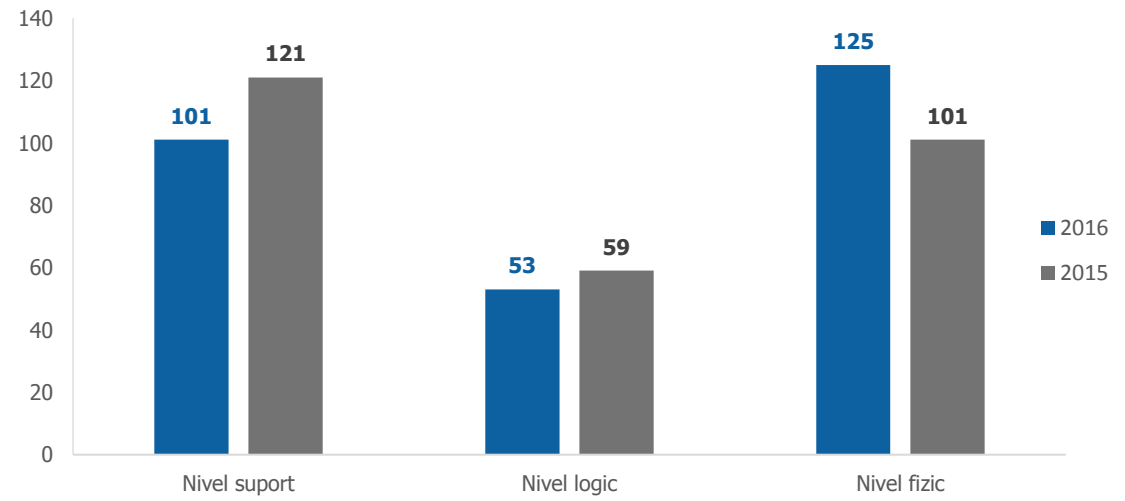
Se poate observa că resursele din cele 3 categorii (registrii de localizare, platforma de taxare și centre de comutație în rețelele mobile) care se evidențiază în figura 6 cu numărul mediu cel mai mare de conexiuni afectate, fac parte din rețeaua centrală. Având în vedere numărul mic de incidente care afectează aceste categorii de resurse, rezultă că acestea sunt afectate rar dar în momentul în care se produce un incident, impactul este considerabil, ajungând să afecteze până la 40% din baza de clienți a unui furnizor.

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 niveluri diferite:

- 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.

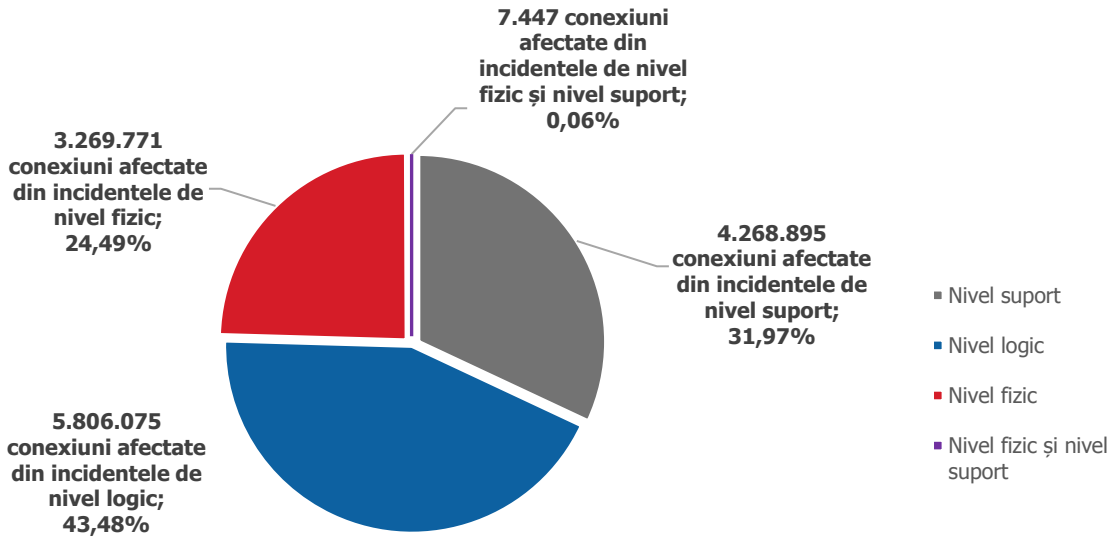
În graficul următor este reprezentat impactul celor 279 de incidente asupra resurselor în funcție de cele trei niveluri enunțate mai sus.

Fig. 7 Ponderea incidentelor pe tipuri de niveluri afectate



În graficul de mai jos este reprezentat impactul incidentelor pe tipuri de niveluri afectate.

Fig.8 Impactul incidentelor pe tipuri de niveluri afectate



Numărul mediu de conexiuni afectate de un incident de nivel:

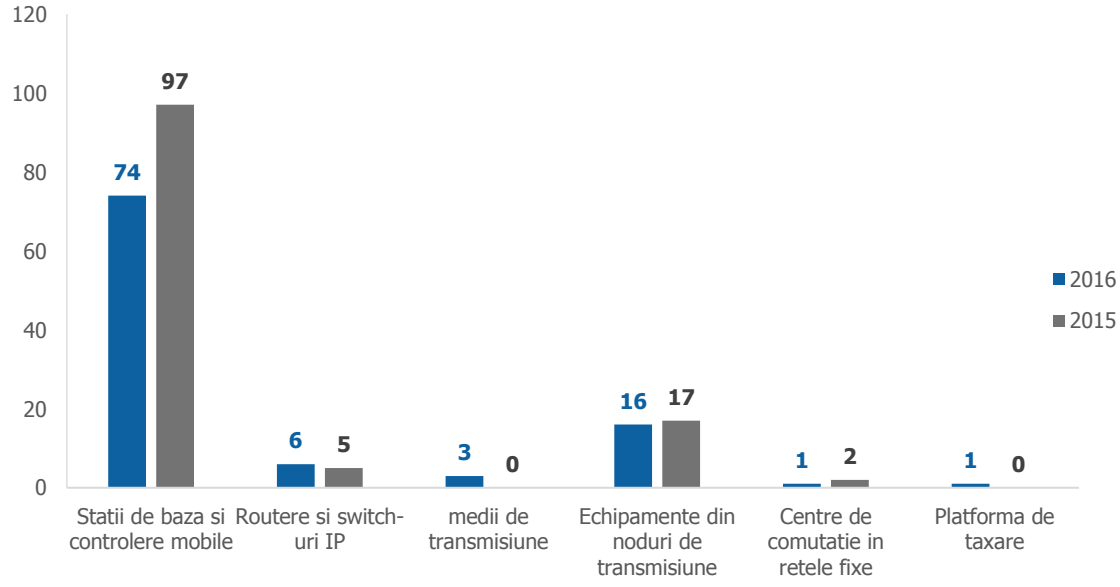
- suport - 42.266 conexiuni
- logic - 109.549 conexiuni
- fizic - 26.369 conexiuni
- fizic și suport - 7.447 conexiuni

Fiecare dintre aceste niveluri 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 2016 au fost raportate 101 incidente care au afectat resursele la nivel suport.

Majoritatea incidentelor (89) 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.

Două incidente care au afectat resursele la nivel suport s-au datorat unor fenomene naturale severe (afectarea structurii metalice pe care era montat echipamentul, infiltrații de apă în panourile electrice).

Restul incidentelor ce au afectat resursele la nivel suport s-au datorat unor erori de sistem ce au afectat redresoare, siguranțe etc.

Resursele afectate la nivel suport fac parte în principal din categoria stații de bază și controlere mobile (74 incidente). Alte resurse afectate sunt din categoriile: echipamente din noduri de transmisiune (16 incidente), routere și switch-uri IP (6 incidente), medii de transmisiune (3 incidente), centre de comutație în rețelele fixe (1 incident) și platforma de taxare (1 incident).

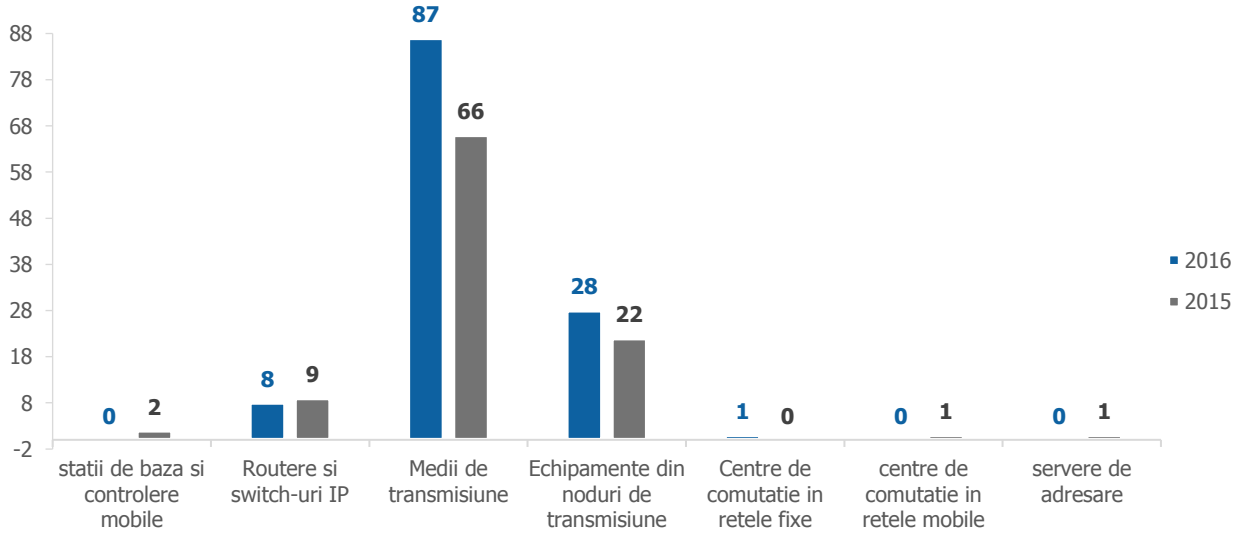
Statistica evidențiază vulnerabilitatea resurselor care fac parte din categoria stații de bază și controlere mobile în cazul problemelor de alimentare cu energie electrică.

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 4.260.000 de conexiuni afectate în incidentele raportate, în creștere mare față de anul precedent), 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 87 de incidente care au afectat la nivel fizic această categorie de resurse în 61 dintre aceste cazuri, incidentele se datorează lucrărilor efectuate de terți, iar în 3 cazuri incidentele s-au datorat acțiunilor rău-intenționate (în principiu aceste acțiuni reprezentând tentative de furt). 5 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 cazul a 12 incidente în care a fost afectată fibra optică la nivel fizic, nu se cunoaște cu exactitate cauza. Astfel, aceste incidente au fost încadrate la Cauza externa/terță parte fără a fi corelată cu altă cauză precum eroare umană sau acțiune rău-intenționată. În aproximativ 50% din 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.

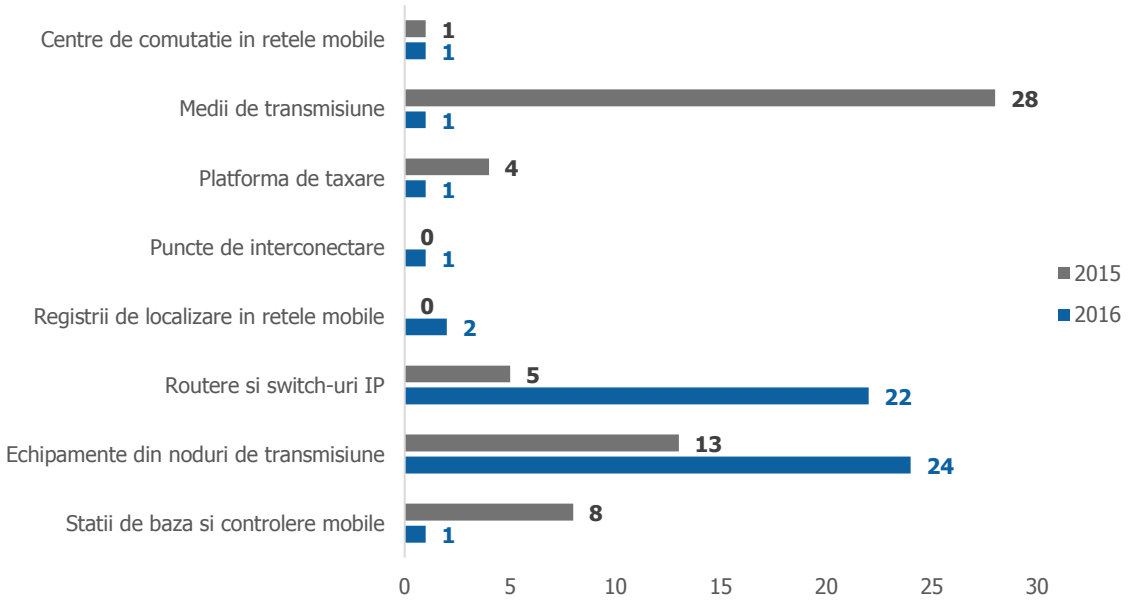
În ceea ce privește resursele care fac parte din categoriile Echipamente din noduri de transmisiune și Routere și switch-uri IP, acestea au fost afectate la nivel fizic, fie în urma fenomenelor naturale (rafale de vânt, ploi, viscol și ninsori abundente), fie în urma unor defecțiuni hardware în urma cărora stațiile de bază agregate în acesta au devenit neoperaționale.

Nivelul logic

În urma raportărilor furnizorilor, s-au înregistrat 53 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 Echipamente din noduri de transmisiune (24 incidente) și Routere și switch-uri (22 incidente).

Statistica realizată în acest caz este reprezentată în figura 11.

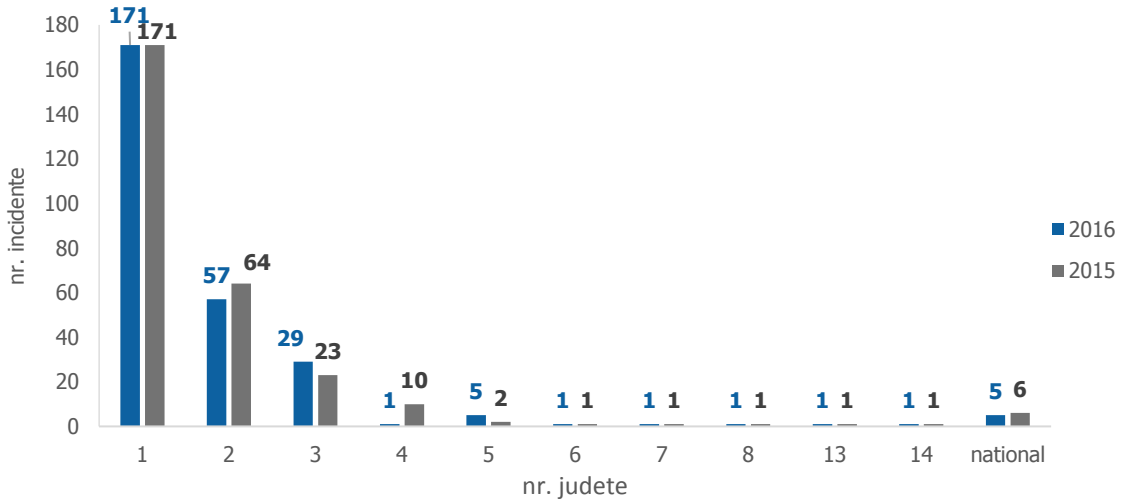
Fig.11 Resurse afectate la nivel logic



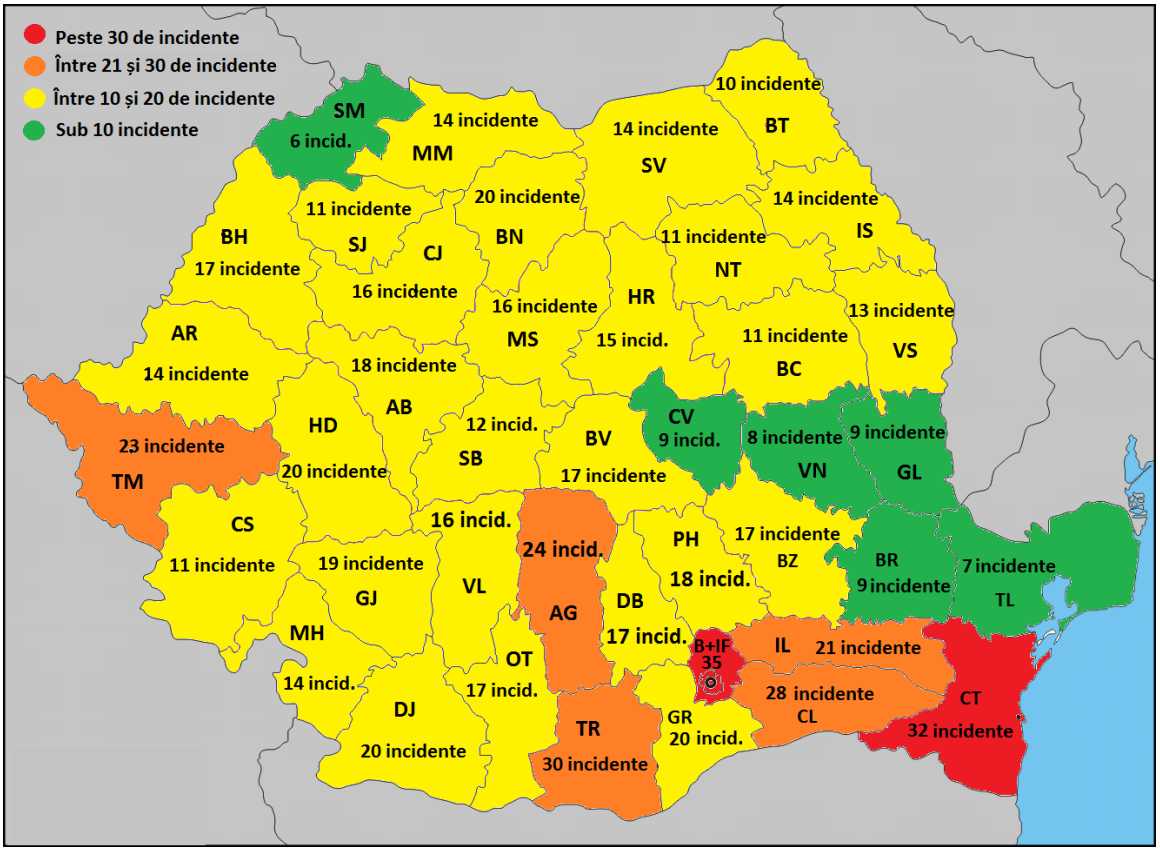
Aria geografică

În ceea ce privește regiunea geografică afectată de incidente, în cele mai multe cazuri (171), incidentele raportate au afectat un singur județ, 57 de incidente au avut impact asupra două județe, 29 de incidente au avut impact asupra 3 județe iar în cazul a 5 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 Registrii de localizare în rețele mobile, Platforma de taxare și Puncte de Interconectare. Durata medie a incidentelor cu impact la nivel național este de 181 de minute.

Fig.12 Impactul incidentelor asupra regiunilor geografice afectate



Pentru o imagine mai clară a numărului de incidente care a afectat fiecare județ în parte, această situație este prezentată în figura 13.



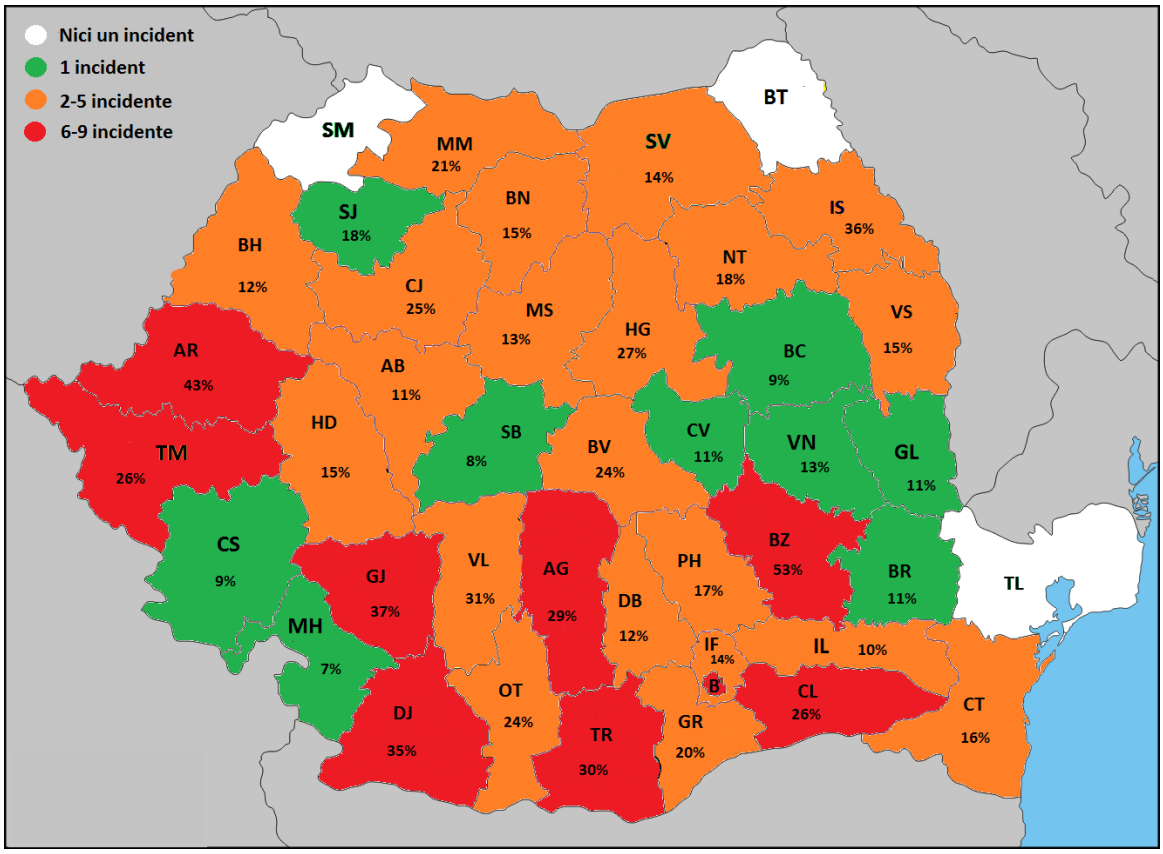
De precizat faptul că numărul incidentelor însumate la nivel național nu coincide cu numărul de incidente raportate în 2016 (279 incidente) pentru că în cazul a 108 incidente, acestea au avut impact asupra cel puțin a două județe.

Conform raportărilor, cele mai multe incidente au afectat județele București și Ilfov (35 incidente).

Județele cel mai puțin afectate sunt Satu Mare, Tulcea, Vrancea, Galați, Brăila și Covasna.

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, sunt prezentate în figura 14, împreună cu procentajul pe care îl reprezintă numărul de incidente cauzate de lipsa alimentării cu energie electrică din totalul incidentelor care au afectat respectivul județ.



Conform raportărilor furnizorilor, cele mai multe incidente care s-au datorat problemelor de alimentare cu energie electrică s-au înregistrat în Teleorman, Buzău (câte 9 incidente), Călărași, Argeș, Gorj, Dolj (câte 7 incidente) și București, Timiș, Arad, (cu câte 6 incidente).

În Fig. 14 se poate observa faptul că toate județele au înregistrat un număr mai mic de 10 incidente datorate problemelor de alimentare cu energie electrică, în 3 cazuri (Satu-Mare, Tulcea și Botoșani) 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.

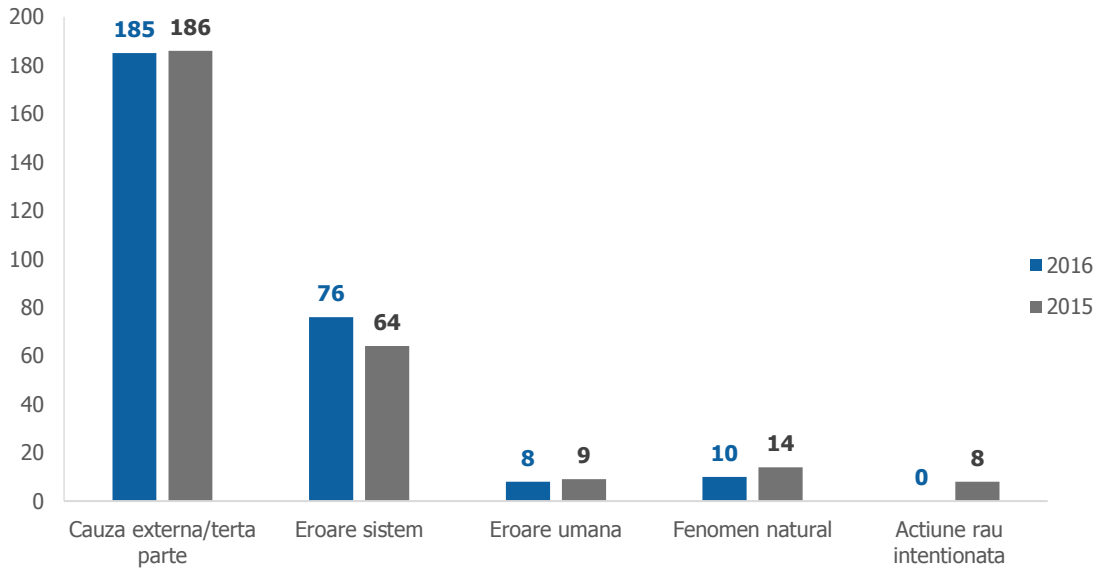
3.3 Cauzele incidentelor raportate

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.

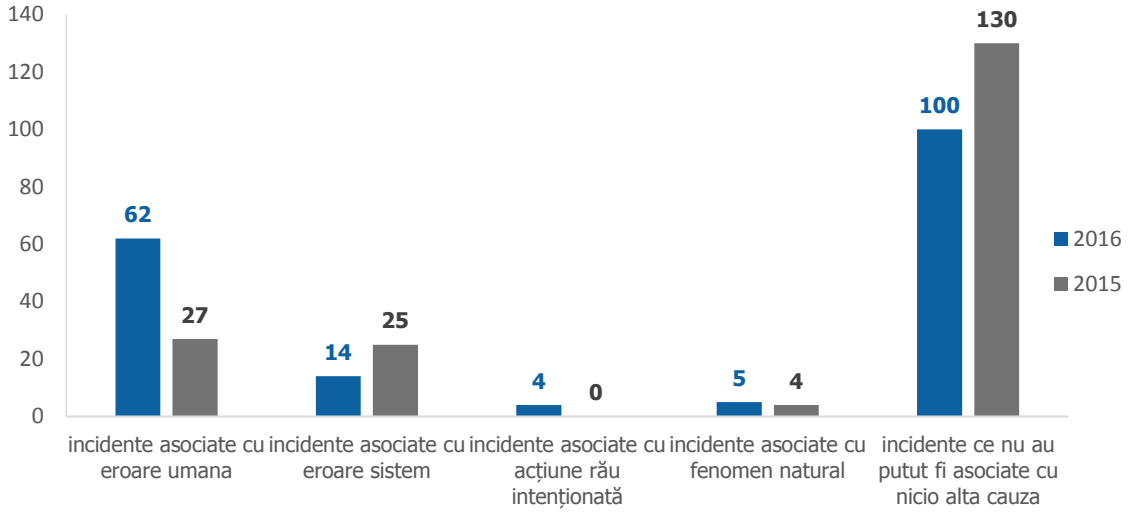
Fig.15 Situația incidentelor în funcție de cauză



Așa cum se poate vedea în Fig. 14, majoritatea incidentelor din 2016 fac parte din categoria cauză externă/parte terță (185 incidente, reprezentând 66% din totalul de incidente raportate în 2016). 76 dintre incidente fac parte din categoria eroare de sistem, 10 de incidente fac parte din categoria fenomen natural și 8 incidente au fost încadrate în categoria eroare umană. În 2016, nu a fost raportat nici un incident cauzat de acțiune rău intenționată fără a fi corelat cu cauză externă/terță parte.

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

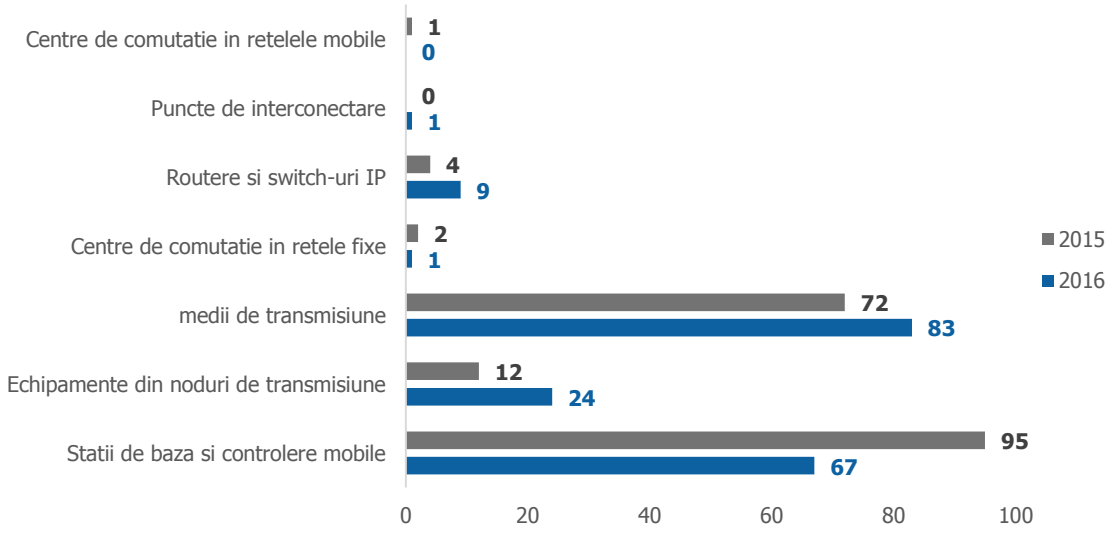


Astfel, dintre cele 185 incidente încadrate în această categorie, 62 au fost asociate cu eroare umană, 14 incidente au fost asociate cu eroare de sistem, 5 incidente au fost asociate cu fenomen natural și 4 incidente au fost asociate cu acțiune rău-intenționată.

100 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 (aprox. 70 de incidente). O altă cauză a producerii acestor incidente a fost ruperea (din cauze necunoscute sau neraportate de către furnizori) a fibrei optice.

Întrucât principalele cauze pentru producerea incidentelor raportate în 2016 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 mediile de transmisiune, stațiile de bază și controlerele mobile și echipamentele din noduri de transmisiune. Categoriile de resurse afectate în mică măsură sunt Routere și switch-uri IP, Centre de comutație în rețelele fixe și Puncte de interconectare.

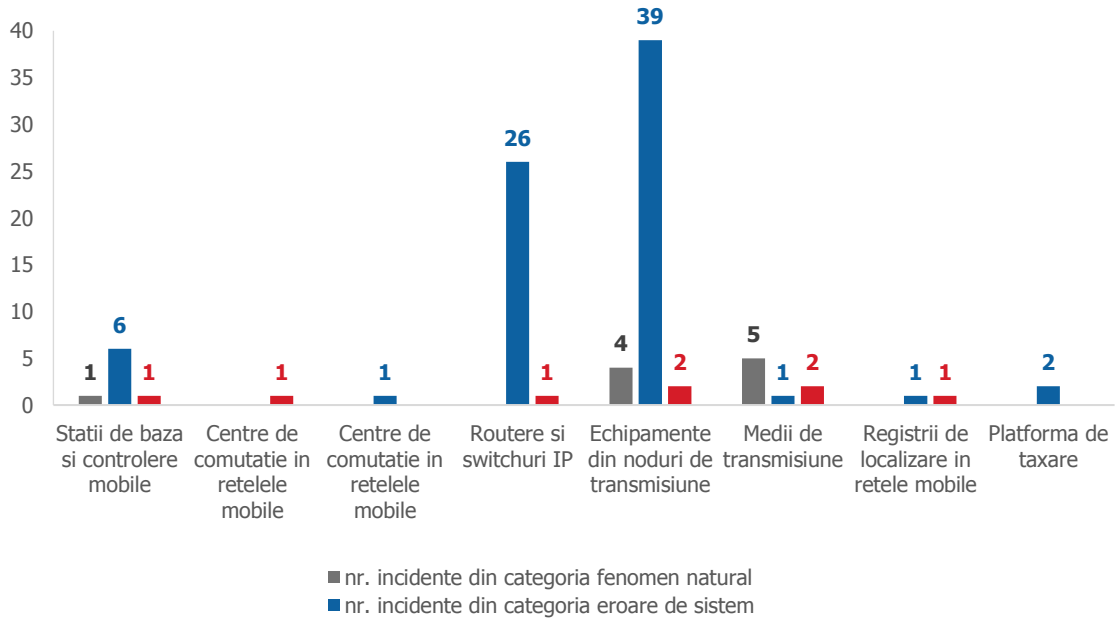
Conform raportărilor, marea majoritate a incidentelor din categoria cauză externă care au afectat resursele din categoria Stații de bază și controlere mobile se datorează problemelor de alimentare cu energie electrică (respectiv întreruperi ale energiei electrice furnizată de rețelele de distribuție 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 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 3 categorii de cauze raportate



Se poate observa faptul că resursele din categoriile Echipamente din noduri de transmisiune și Routere și switch-uri 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 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.

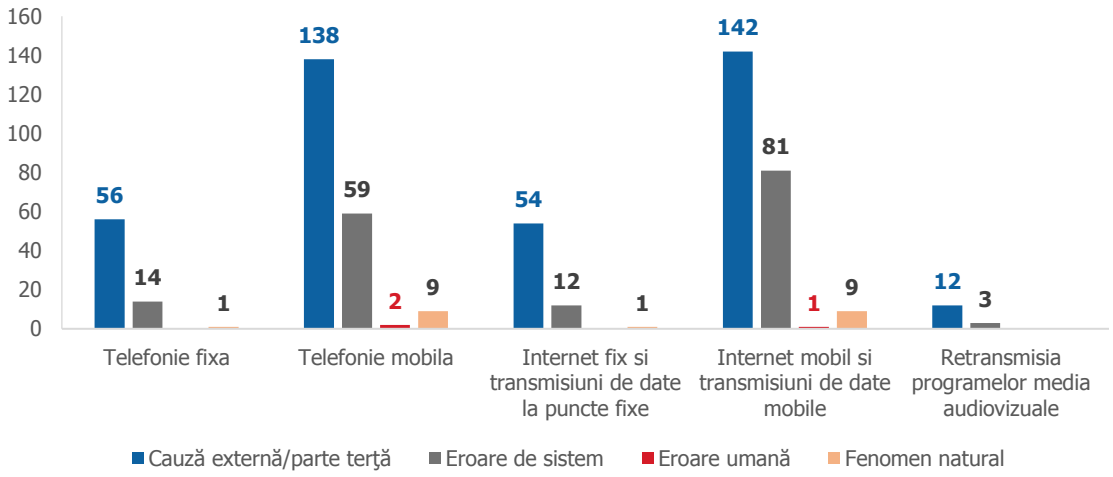
Făcând o analiză a categoriilor de resurse afectate pentru fiecare tip de cauză, din raportările furnizorilor s-a constatat faptul că în cazul incidentelor încadrate în cele 4 categorii de cauze, Stațiile de bază și controlerele mobile au fost afectate în principal din cauza unor erori software apărute,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

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 cele mai afectate servicii, indiferent de cauză, sunt serviciile de acces la internet mobil și transmisiuni de date mobile și serviciile de telefonie mobilă. Cele mai multe incidente care au afectat acest tip de 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.

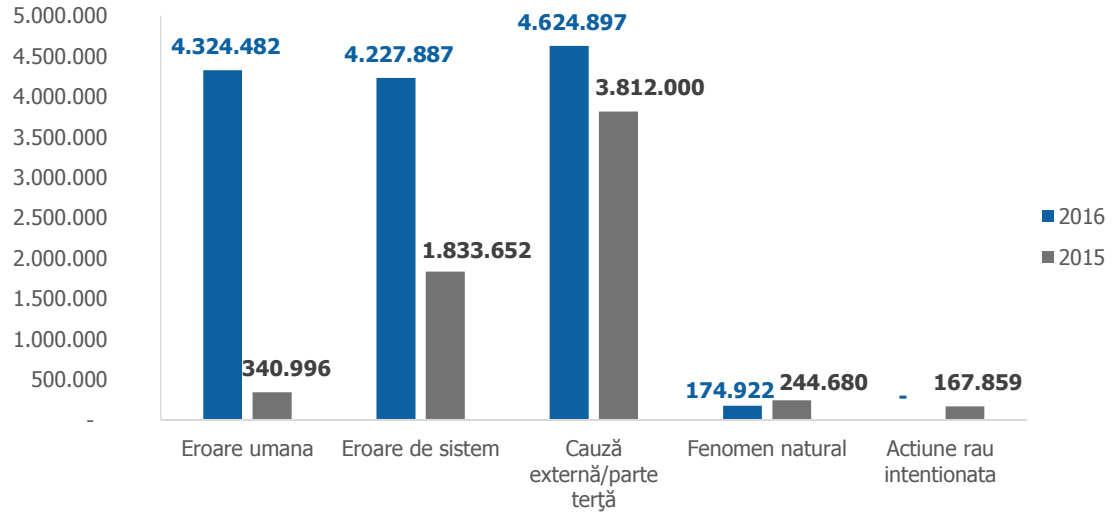
În cazul incidentelor care fac parte din categoriile eroare de sistem și cauză externă/parte terță și care au afectat serviciile de acces la internet mobil, transmisiuni de date mobile și serviciile

de telefonie mobilă, acestea s-au produs în principal datorită defecțiunilor software sau hardware ale unor echipamente, respectiv datorită problemelor alimentării cu energie electrică.

Serviciile de retransmisie a programelor audiovizuale au fost afectate în principal în cazul incidentelor care fac parte din categoria cauză externă/parte terță (12 incidente). Acestea s-au datorat în mare parte avariilor la nivelul fibrei optice. În privința a 3 incidente, acestea au fost cauzate de defectări ale unor echipamente.

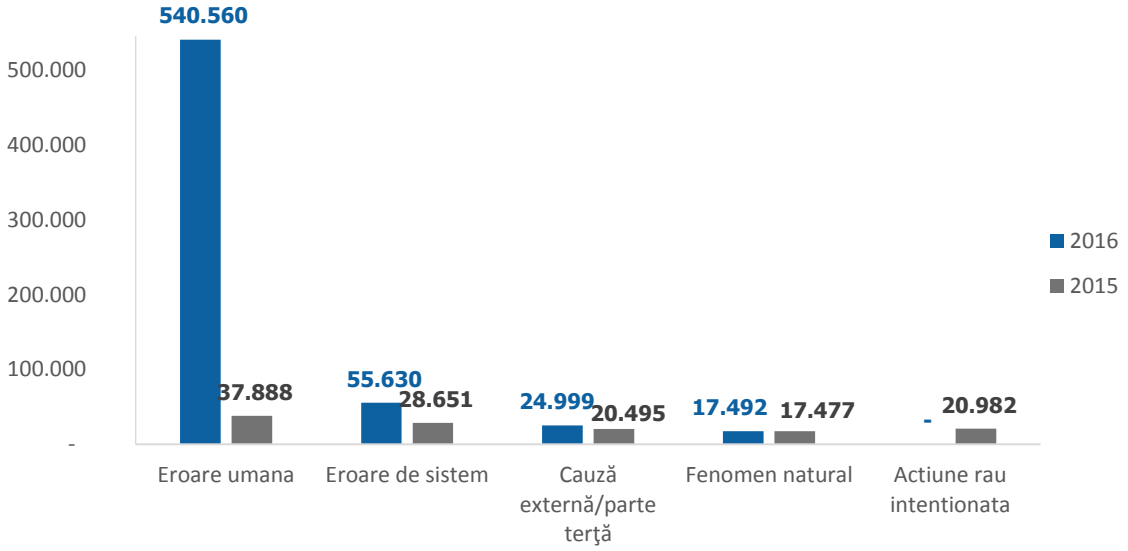
Statistica privind numărul de conexiuni afectate în funcție de cauză este prezentată mai jos:

Fig.20 Numărul de conexiuni afectate în funcție de cauză



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

Fig.21 Numărul mediu de conexiuni per tip de cauză



În graficul de mai sus se poate observa faptul că incidentele care au drept cauză eroarea umană afectează, în medie, cel mai mare număr de conexiuni. Cu toate acestea, situația prezentată în graficul de mai sus este una particulară datorată, pe de o parte, existenței unui incident care a

afectat un număr considerabil de conexiuni, iar pe de altă parte, numărului mic de incidente având drept cauză eroarea umană. Incidentele din categoria fenomen natural au afectat în medie cel mai mic număr de conexiuni (17.492).

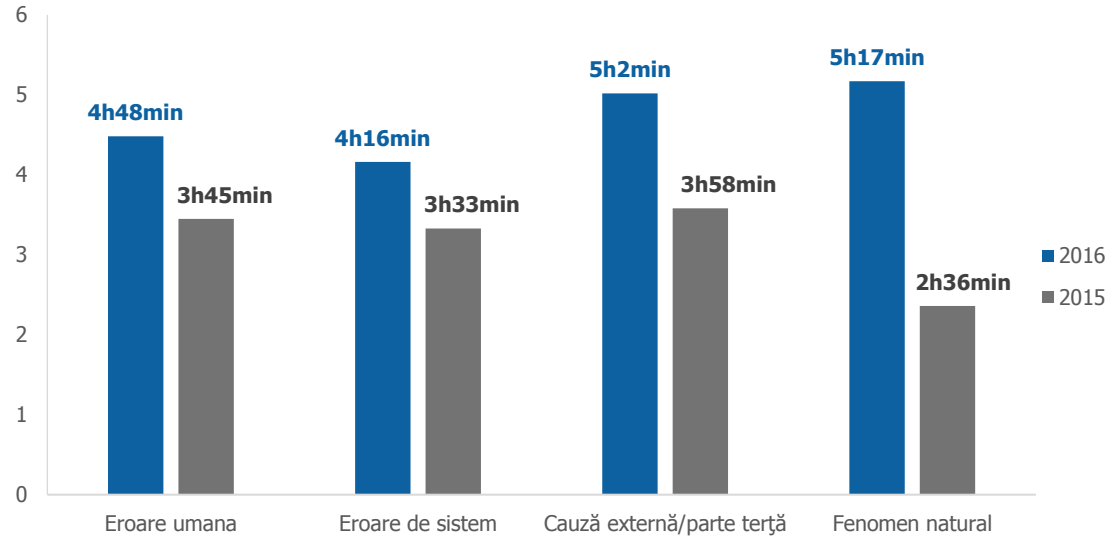
3.4 Durata incidentelor și durata de descoperire a incidentelor

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 2016 este de 1.347 ore, durata medie a unui incident fiind de aproximativ 7,5 ore (7 ore și 31 minute).

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

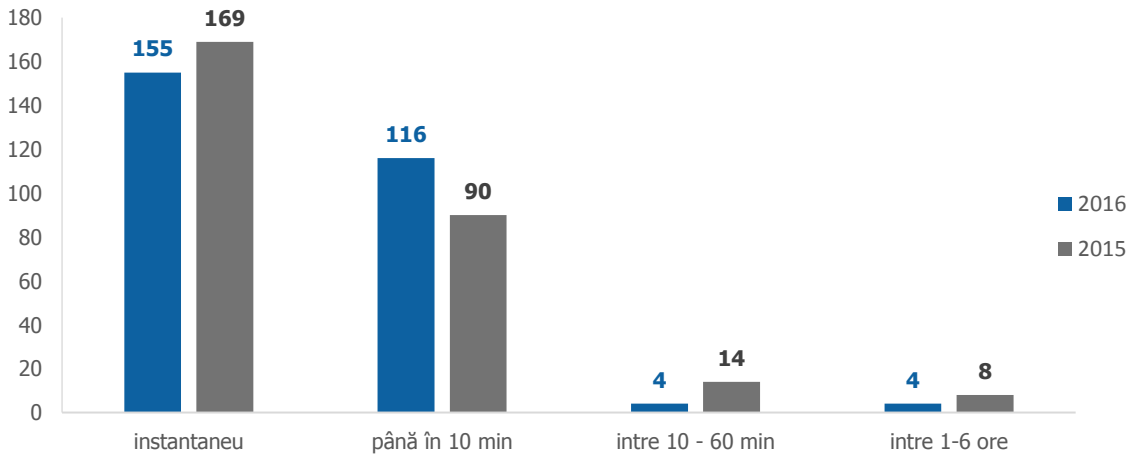
Fig.22 Durata medie a incidentelor în funcție de cauză



Valoarea cea mai mare a duratei medii aparține categoriei de cauze fenomen natural (5 ore și 17minute). Acest lucru se datorează accesului îngreunat de condițiile meteorologice la echipamentele afectate.

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

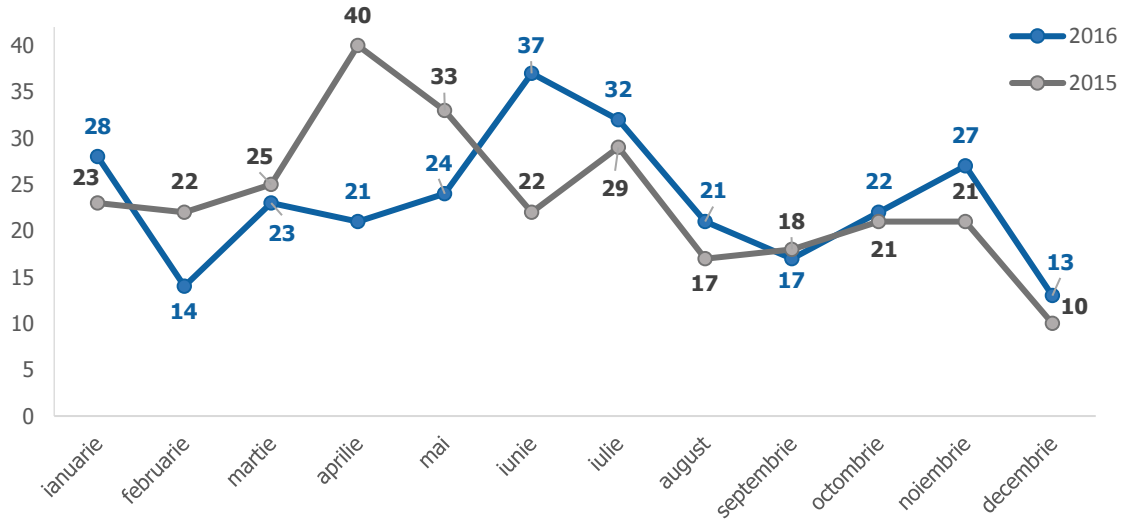


Din Fig.23 se poate observa că cele mai multe incidente (155) au fost descoperite în momentul producerii lor și că foarte puține incidente au fost descoperite în intervale mari de timp (1 incident descoperit în aproximativ 3 ore, 2 în aproximativ 5 ore și unul în 6 ore).

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 2016.

Fig.24 Numărul incidentelor înregistrate pe luni comparație 2016-2015



În 2016, precum și în 2015, s-au petrecut în medie 23 de incidente pe lună. Se poate observa că, spre deosebire de anul 2015 unde lunile aprilie și mai sunt perioadele în care s-au raportat cele mai multe dintre incidente (40, respectiv 33), în 2016, lunile cu cele mai multe incidente sunt iunie și iulie (37, respectiv 32). Lunile cel mai puțin afectate în 2016 sunt lunile februarie și decembrie.

3.5 Impactul asupra apelurilor de urgență

96% dintre incidentele raportate în anul 2016 au avut un posibil impact asupra efectuării 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 2016, au fost cele de telefonie mobilă (în acest caz fiind afectat implicit și serviciul de urgență 112). Față de anul 2015, numărul incidentelor care au afectat apelurile de urgență în anul 2016 a crescut de la 252 (însemnând 90% din totalul incidentelor din 2015) la 268 de incidente (însemnând 96% din totalul incidentelor din 2016).

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.

În scopul remedierii problemelor apărute, furnizorii au raportat acțiuni de răspuns precum:

- 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 (ex. procedura de restaurare a serviciilor, procedura de configurare echipamente de interconectare etc.);
- Revizuirea și modificarea politicilor implementate în sistemul de monitorizare (ex. implementarea unui filtru în sistemul de monitorizare a alarmelor apărute în rețea);
- 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 2016, 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. 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.

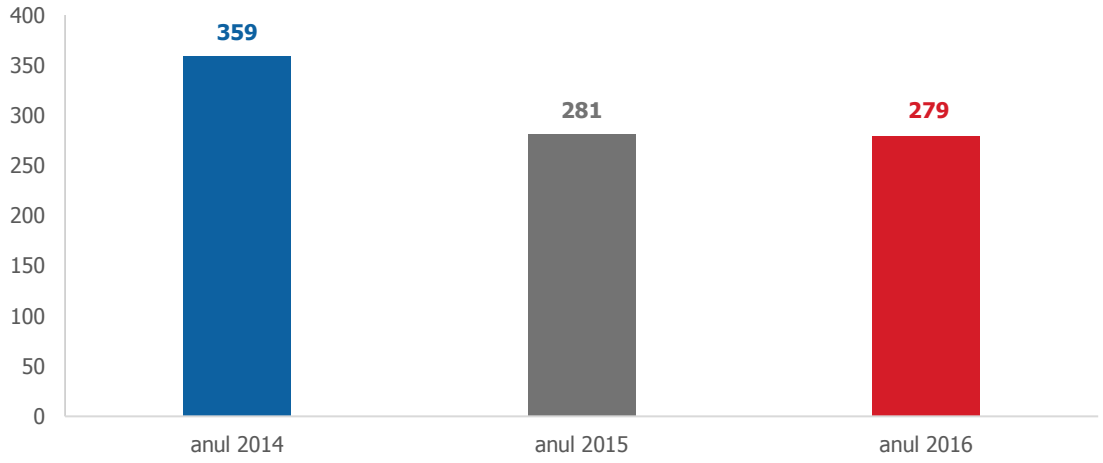
Datele privind incidentele sunt fundamentale pentru dezvoltarea unei înțelegeri clare a naturii și amplorii provocărilor existente la adresa securității și integrității rețelelor și serviciilor prin analiza amenințărilor și vulnerabilităților la adresa securității și integrității rețelelor și serviciilor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

5.1 Concluzii în urma analizei incidentelor

În urma centralizării și analizării celor 279 de incidente cu impact semnificativ raportate de către furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului, pentru anul 2016, se pot desprinde următoarele concluzii:

- analizând situația privind numărul de incidente cu impact semnificativ raportate în ultimii 3 ani, se poate identifica o tendință ușor descrescătoare. În 2016 și 2015 numărul incidentelor rămâne aproape constant și în scădere față de valoarea înregistrată în 2014.

Fig. 25 Număr incidente raportate în ultimii 3 ani



- asemenea anilor 2014 și 2015, în 2016 cele mai afectate servicii, din punct de vedere al numărului de conexiuni, au fost serviciile de telefonie mobilă și SMS (5.643.562 conexiuni afectate).
- numărul conexiunilor afectate în cazul serviciilor mobile a înregistrat o creștere majoră în 2016 în comparație cu 2015 ceea ce a determinat ca și numărul mediu al conexiunilor afectate de un incident în 2016 (47.859 conexiuni) să fie în creștere față de 2015 (22.773 conexiuni).
- din punctul de vedere al numărului de incidente, cele mai multe dintre incidentele cu impact semnificativ raportate în 2016 au afectat serviciile de acces la internet mobil și serviciile de telefonie mobilă (219, respectiv 214 incidente cu impact semnificativ).
- numărul incidentelor cu impact semnificativ ce au afectat fiecare categorie de servicii a rămas oarecum constant în ultimii doi ani.

- serviciul de retransmitere a programelor media audiovizuale este afectat de un număr mic de incidente cu impact semnificativ (16 incidente cu impact semnificativ).
- din punct de vedere al resurselor afectate, în cele mai multe cazuri, acestea fac parte din categoriile:

  a) Medii de transmisiune,
  b) Stații de bază și controlere mobile și
  c) Echipamente din noduri de transmisiune.
- numărul echipamentelor afectate din categoria stații de bază și controlere mobile a scăzut în 2016 față de 2015 dar a crescut numărul de echipamente afectate din noduri de transmisiune, routere și switch-uri IP.
- incidentele ce au afectat resurse ce fac parte din rețeaua centrală (regiștrii de localizare, platforma de taxare și centre de comutație în rețelele mobile) au afectat în mod firesc, un număr foarte mare de conexiuni. Aceste incidente sunt foarte puține ca număr dar au un impact major din punctul de vedre al numărului de conexiuni afectate.
- numărul incidentelor ce au afectat resursele la nivel logic și la nivel suport a scăzut în 2016 față de 2015, în schimb a crescut numărul incidentelor ce au afectat resursele la nivel fizic.
- din punctul de vedere al ariei geografice afectate, în 171 din cazuri (61% din numărul total de incidente) a fost afectat un singur județ iar 5 incidente s-au petrecut la nivel național în 2016. Cele mai afectate din punctul de vedere al numărului de incidente sunt județele București și Ilfov, cu 35 de incidente cu impact semnificativ, și cel mai puțin afectat județ este Satu Mare, cu 6 incidente cu impact semnificativ petrecute în 2016.
- 66% din totalul incidentelor raportate în 2016 fac parte din categoria cauză externă/parte terță (185 incidente).
- în cazul incidentelor din categoria cauză externă cele mai afectate resurse sunt:
  - mediile de transmisiune (în cazul a 83 de incidente cu impact semnificativ),
  - stațiile de bază, controlerele mobile (în cazul a 67 de incidente cu impact semnificativ) și
  - echipamentele din noduri de transmisiune (în cazul a 24 de incidente cu impact semnificativ).
- în cazul incidentelor din categoria erori de sistem cele mai afectate resurse sunt din categoriile:
  - echipamente din noduri de transmisiune (în cazul a 39 de incidente cu impact semnificativ),
  - routere și switch-uri IP (în cazul a 26 de incidente cu impact semnificativ).
- durata totală a incidentelor raportate pe anul 2016 este de 1.347 ore, în creștere față de anul 2015 (1.050 ore), iar durata medie a unui incident în 2016 este de aproximativ 7,5 ore (7 ore și 31 minute), de asemenea în creștere față de 2015 (3 ore și 44 minute).
- 96% dintre incidentele raportate în anul 2016 au avut un posibil impact asupra efectuării apelurilor de urgență

5.2 Concluzii calitative

Analizând incidentele cu impact semnificativ raportate în ultimii ani, se pot trage următoarele concluzii:

- Numărul de incidente în 2016 este în scădere față de anul 2014 și s-a menținut constant față de anul 2015;

- Din punctul de vedere al numărului de conexiuni afectate în 2016 se poate observa o tendință negativă față de anul 2015, având în vedere numărul crescut de conexiuni afectate în 2016 față de cel din 2015.
- Durata totală a incidentelor a înregistrat o creștere semnificativă față de anul 2015, astfel încât durata medie a unui incident a crescut de la 3 ore și 44 minute în 2015 la 7 ore și 31 minute în 2016.

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 2016, un chestionar[8] adresat furnizorilor, ce a urmărit analiza/evaluarea stadiului de implementare a măsurilor de securitate în domeniul managementului incidentelor. Raportul privind răspunsurile la acest chestionar a fost publicat în luna aprilie 2017[9].

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

[9] Raportul este disponibil la adresa: http://www.ancom.org.ro/uploads/links_files/Raport_privind_implementarea_msurilor_de_securitate_%C3%AEn_domeniul_managementului_incidentelor_in_anul_2015.pdf