

Raport privind incidentele care au afectat securitatea și integritatea rețelelor și serviciilor de comunicații electronice în anul 2018



Reproducerea integrală sau parțială a conținutului acestui document este permisă în condițiile în care materialul reprodus sau citat va fi prezentat ca provenind din *Raportul privind incidentele care au afectat securitatea și integritatea rețelelor și serviciilor de comunicații electronice în anul 2018* al Autorității Naționale pentru Administrare și Reglementare în Comunicații sau însoțit de una din următoarele specificări:

- Sursa: Raportul privind incidentele care au afectat securitatea și integritatea rețelelor și serviciilor de comunicații electronice în anul 2018 al Autorității Naționale pentru Administrare și Reglementare în Comunicații;
- Sursa: Autoritatea Națională pentru Administrare și Reglementare în Comunicații;
- Sursa: ANCOM;
- O formulare clară cu același sens ca cele de mai sus.

CUPRINS

1.	Introducere	1
2.	Raportarea incidentelor care au afectat securitatea și integritatea rețelelor și serviciilor de comunicații electronice în anul 2018	2
3.	Analiza incidentelor raportate.....	2
3.1	Impactul asupra serviciilor și utilizatorilor.....	2
3.2	Impactul asupra resurselor afectate	5
3.3	Cauzele incidentelor raportate	16
3.4	Durata incidentelor și durata de descoperire a incidentelor.....	22
3.5	Impactul asupra apelurilor de urgență	24
4.	Acțiunile de răspuns la incident.....	24
5.	Concluzii	25
5.1	Concluzii în urma analizei incidentelor	25
5.2	Concluzii calitative	27

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 aceluiași 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 Decizia¹ 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 2018 au existat 7 incidente care să se încadreze în pragurile stabilite în ghidul² ENISA de raportare a incidentelor. Pe baza rapoartelor furnizate de statele membre ale Uniunii Europene, ENISA publică³ 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/Article_13a_ENISA_Technical_Guideline_On_Incident_Reporting_v2_1.pdf

³ Rapoartele ENISA sunt disponibile la următoarea adresă: <https://www.enisa.europa.eu/topics/incident-reporting>

2. Raportarea incidentelor care au afectat securitatea și integritatea rețelelor și serviciilor de comunicații electronice în anul 2018

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 pagina⁴ de internet a ANCOM.

În cadrul notificării finale, informațiile raportate de furnizori în 2018 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 2018 au fost raportate 556 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:

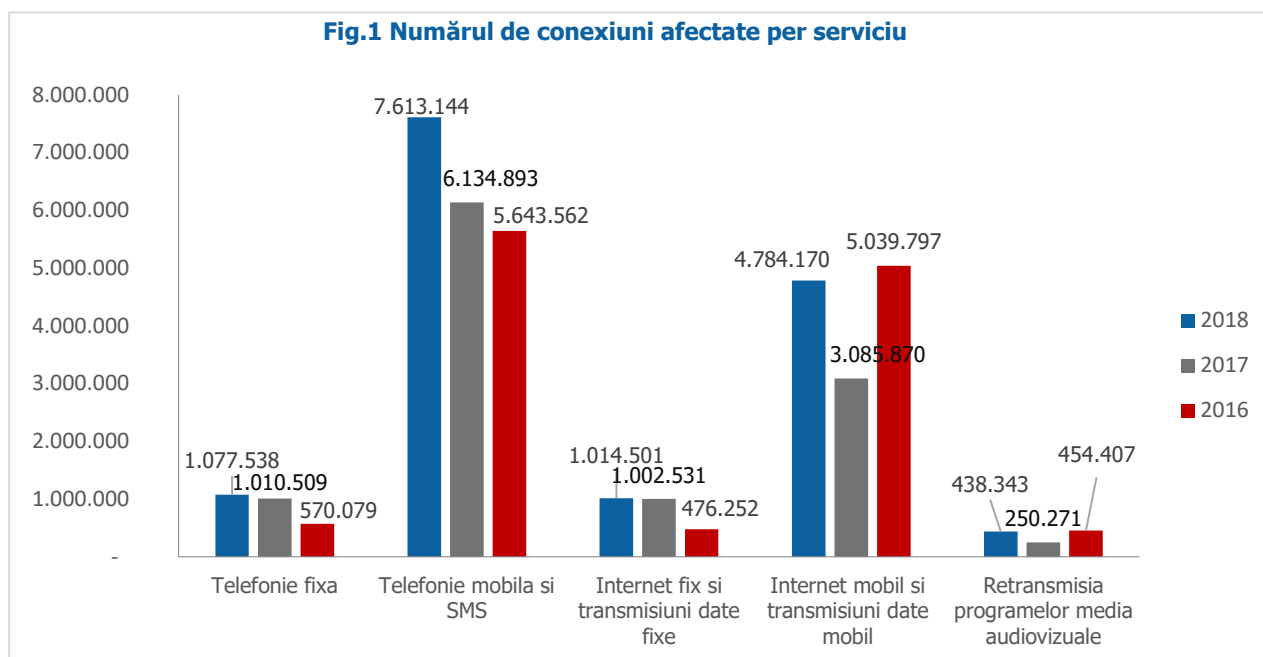
1. Impactul asupra serviciilor și utilizatorilor;
2. Impactul asupra resurselor afectate;
3. Cauzele incidentelor raportate;
4. Durata incidentelor și durata de descoperire,
5. Impactul asupra apelurilor de urgență.

3.1 Impactul asupra serviciilor și utilizatorilor

În 2018 s-au raportat 556 de incidente cu impact semnificativ asupra rețelelor și serviciilor de comunicații electronice.

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 2018 este reprezentat în graficul de mai jos.



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.

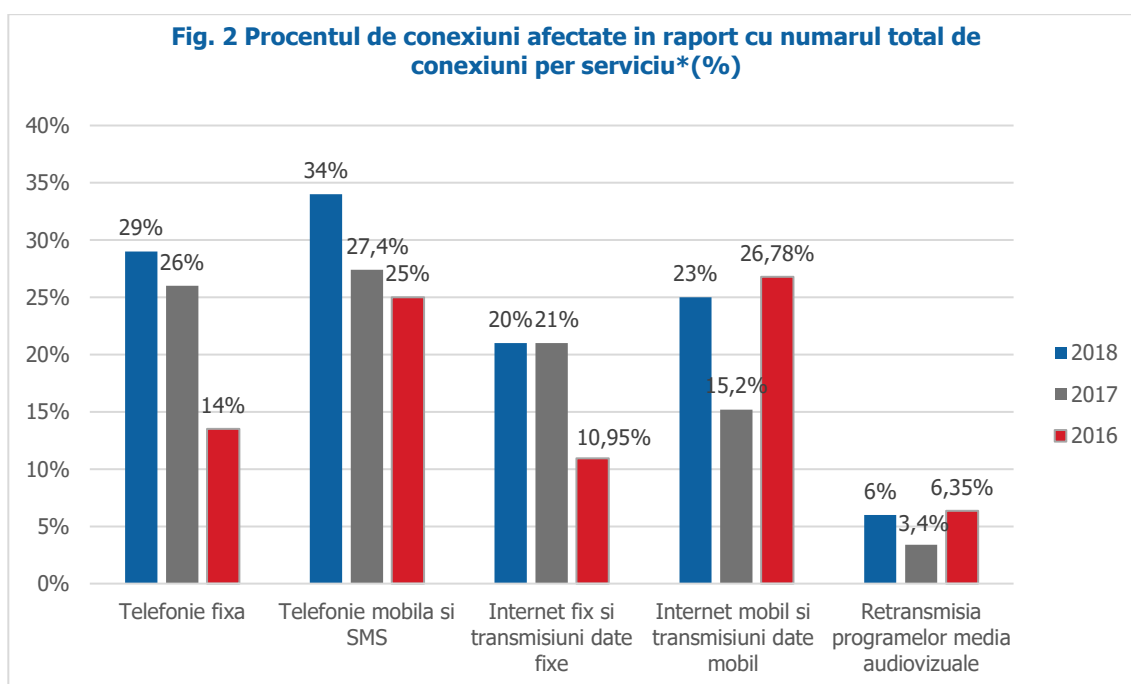
În 2018 cele mai afectate au fost serviciile de telefonie mobilă și SMS (7.613.144 conexiuni afectate). În Fig.1 se poate observa faptul că serviciile de retransmisia programelor media audiovizuale au fost afectate în mică măsură. Comparativ cu ceilalți ani, în 2018 se remarcă o creștere a numărului de conexiuni afectate în cazul serviciilor de telefonie fixă, telefonie mobilă, precum și în cazul serviciilor de internet fix și transmisiuni de date la puncte fixe. O posibilă explicație a acestei creșteri în cazul serviciilor de internet fix și transmisiuni de date la puncte fixe poate fi că numărul⁷ conexiunilor aferente acestui serviciu la nivel național este pe un trend crescător (în 2016 s-au înregistrat 4,3 milioane conexiuni, în 2017 s-au înregistrat 4,8 milioane conexiuni, iar în 2018 s-au înregistrat 4,9 milioane conexiuni).

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.

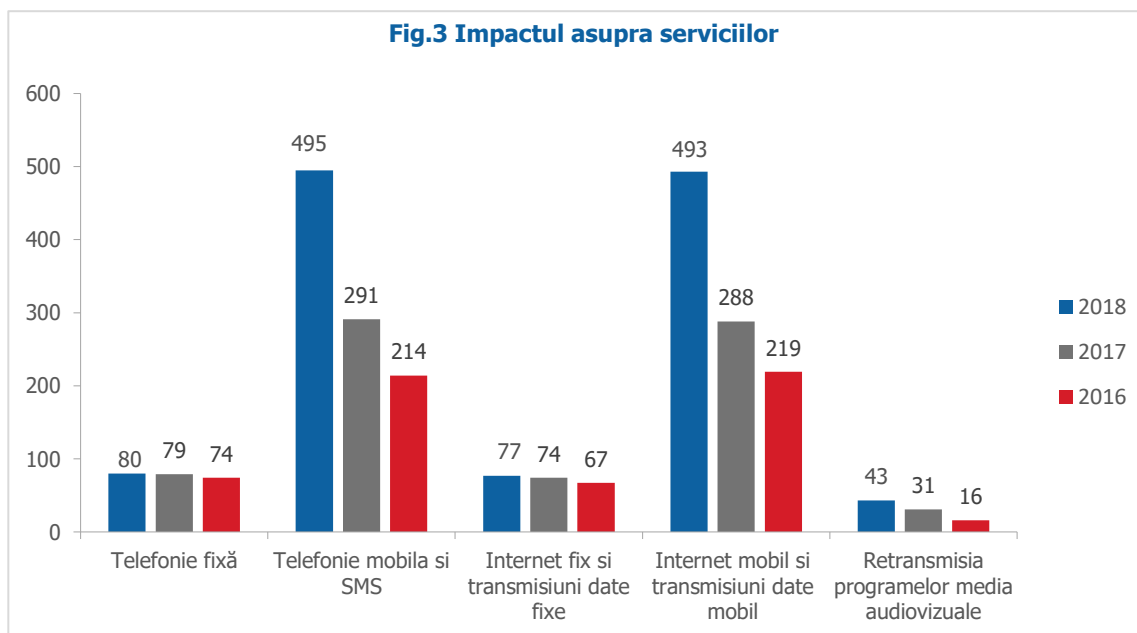
⁷ Conform Raportului privind datele statistice, semestrul I 2018, care poate fi accesat la următoarea adresă: https://statistica.ancom.org.ro:8000/sscpds/public/files/165_ro



* Conform Raportului privind datele statistice, semestrul II 2018

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 2018 la numărul total de conexiuni raportate de furnizori.

Figura de mai jos reprezintă numărul de incidente care au afectat fiecare serviciu în anul 2018.

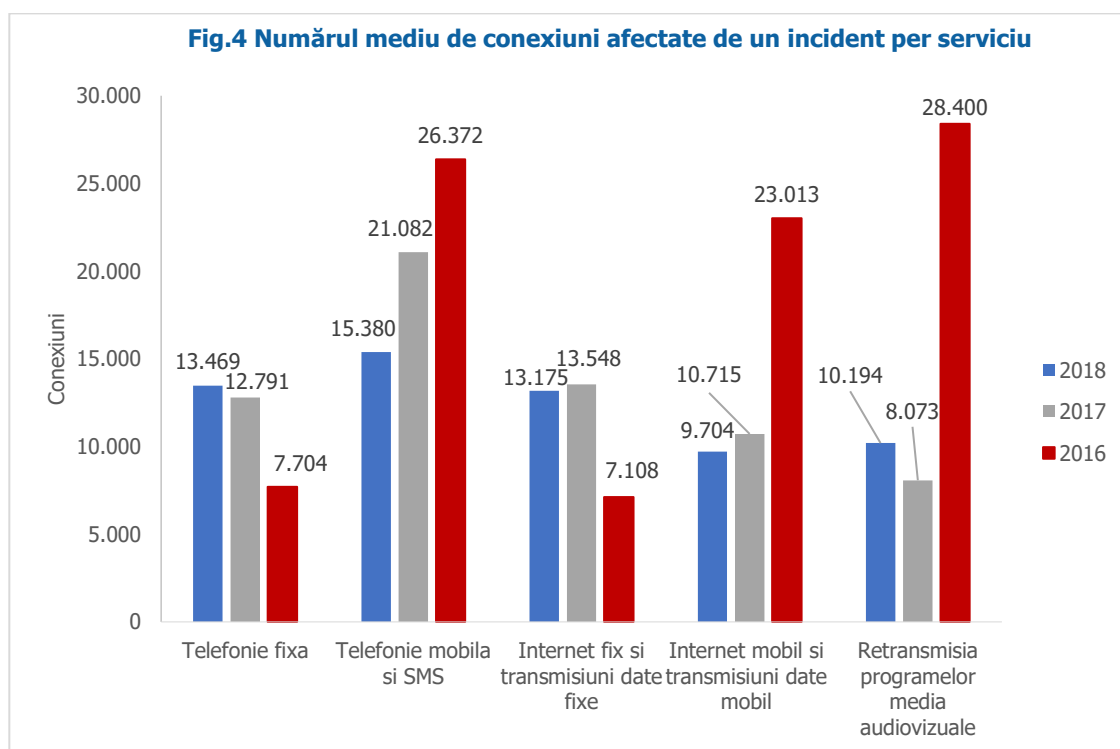


În Fig. 3 se observă că cele mai multe dintre incidentele raportate în 2018 au afectat serviciile de telefonie mobilă și serviciile de acces la internet mobil și transmisiuni de date la puncte mobile (495, respectiv 493 incidente). Cel mai puțin afectat serviciu este cel de retransmitere a programelor media audiovizuale, 43 incidente afectând acest serviciu în anul 2018. În figura de mai sus se poate observa că numărul de incidente care au afectat fiecare serviciu în anul 2018 este în creștere comparativ cu anii precedenți.

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 2018 este de 24.252 conexiuni, în scădere față de 2017 (29.755 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.

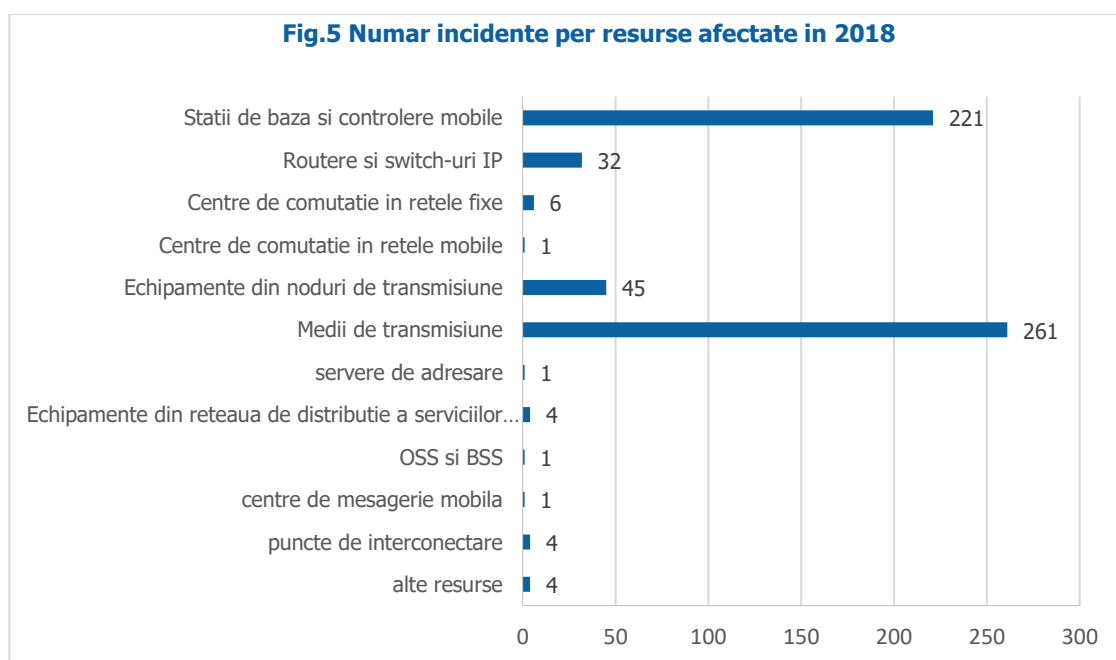


Se poate observa că, deși comparativ cu anii anteriori, numărul incidentelor care au afectat principalele servicii de comunicații electronice se află în creștere, situația din 2018 privind numărul mediu de conexiuni în cazul serviciului de telefonie mobilă, internet mobil și transmisiuni date mobil, precum și internet fix și transmisiuni date fixe este îmbunătățită comparativ cu anii precedenți. În schimb, numărul mediu de conexiuni afectate în cazul serviciilor de telefonie fixă și retransmisia programelor media audiovizuale este în creștere.

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*⁸, elaborat de ANCOM. Astfel, graficul următor evidențiază numărul de incidente ce au afectat fiecare categorie de resurse în parte în anul 2018.

⁸ 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



În Fig.5 se poate observa că în cazul celor mai multe incidente, resursele afectate fac parte din categoria Medii de transmisiune (261 incidente) și Stații de bază și controlere mobile (221 incidente).

În analiza acestei situații trebuie adăugat faptul că în cazul a 19 dintre incidente au fost afectate concomitent mai multe categorii de resurse. Dintre acestea, 12 incidente s-au datorat fenomenelor naturale (furtună de zăpadă, viscol, cod galben de ploi), în majoritatea cazurilor multiple categorii de echipamente rămânând fără alimentare cu energie electrică. De asemenea, există câteva cazuri în care, în cadrul aceleiași rețele s-au produs concomitent două incidente. O astfel de situație se regăsește în exemplul următor: ca urmare a unei defecțiuni electrice, bateriile UPS-ului s-au defectat, în același timp s-a constatat defectarea unui switch. Un alt exemplu de situație similară este: un cablu de fibră optică a fost secționat, în același timp cu o serie de echipamente care au rămas fără alimentare cu energie electrică, după ce sursa de alimentare a acestora s-a ars din cauza unor supratensiuni în rețeaua electrică.

În cazul a 221 dintre incidente, resursa afectată face parte din categoria Stații de bază și controlere mobile, iar aproximativ 93% dintre acestea (205 incidente) fac parte din categoria Cauză externă/ Parte terță și se datorează problemelor de alimentare cu energie electrică. 11 dintre incidentele care au afectat resursele din categoria Stații de bază și controlere mobile fac parte din categoria Eroare de sistem și s-au datorat defectării unor echipamente de alimentare cu energie electrică (precum generatoarele fixe), ori defectării unor echipamente de control al temperaturii (echipament de aer condiționat). În cazul a 5 dintre incidentele care au afectat categoria Stații de bază și controlere mobile, acestea s-au datorat fie furtului bateriilor din site-uri, fie unor fenomene naturale care au dus la infiltrarea apei în cabinet.

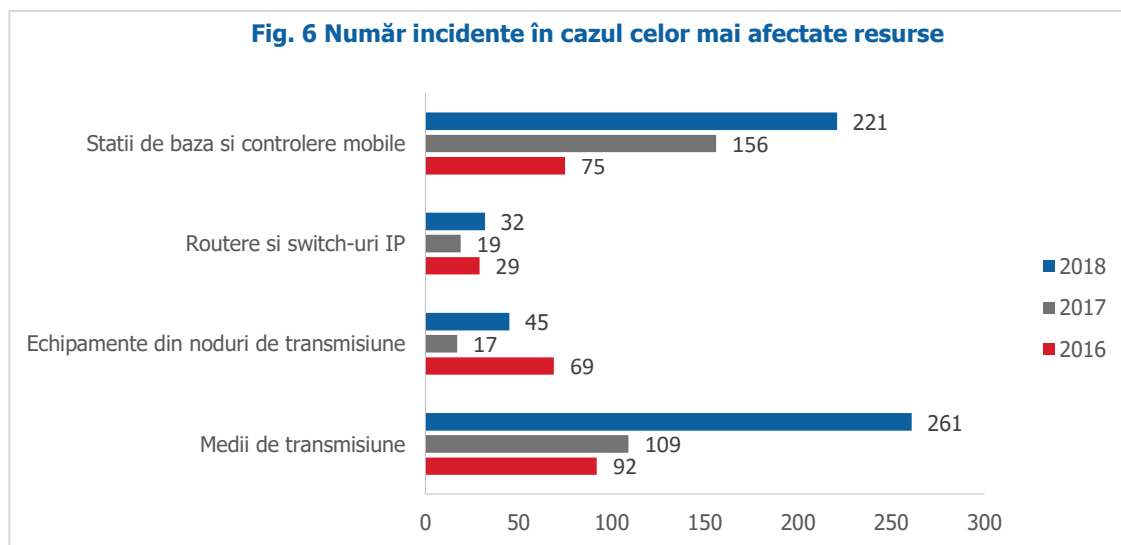
În cazul a 261 dintre incidente, resursa afectată face parte din categoria Medii de transmisiune. 41 dintre acestea fac parte din categoria cauză externă/eroare umană și au constat în secționarea fibrei optice în urma lucrărilor efectuate de terți (lucrări civile, lucrări de toaletare a copacilor, ori lucrări desfășurate la rețeaua electrică), ori, în câteva cazuri, ruperea fibrei a fost cauzată de utilaje auto de mari dimensiuni. 204 dintre incidentele care au afectat resursele din categoria Medii de transmisiune s-au datorat fie unor cauze externe constând în erori de comunicare intervenite la nivelul rețelelor partenere (în 166 dintre cazuri), fie în accidente în urma cărora cablul de fibră optică a fost afectat (în 38 cazuri). Exemple de astfel de accidente: căderea accidentală a unor stâlpi de tensiune, accidente rutiere, incendii). De asemenea, au existat câteva cazuri datorate erorii umane (de exemplu, în cadrul unor lucrări programate s-a depășit fereastra

de mentenanță) și fenomenelor naturale (viituri, inundații, căderi masive de zăpadă, vânt puternic). În cazul unui singur incident în care a fost afectată categoria Medii de transmisiune, acesta s-a datorat vandalizării cablului de fibră optică. În cele mai multe cazuri, afectarea acestei resurse a avut drept consecință izolarea mai multor echipamente care fac parte din categoriile Stații de bază și controlere mobile, Routere și switch-uri IP și Echipamente din noduri de transmisiune.

În cazul a 45 dintre incidente, resursa afectată face parte din categoria Echipamente din noduri de transmisiune, iar în cazul a 32 dintre incidente, resursa afectată face parte din categoria Routere și switch-uri IP (majoritatea dintre acestea s-au produs în urma defectării echipamentelor la nivel software sau hardware). Într-o măsură mai mică au fost afectate resursele din categoriile, Centre de comutație în rețele fixe (6 incidente), Echipamente din rețeaua de distribuție a serviciilor de retransmisie de programe media audiovizuale liniare (4 incidente), Puncte de interconectare (4 incidente), Centre de comutație în rețele mobile (1 incident), Servere de adresare (1 incident), Centre de mesagerie mobilă (1 incident), OSS și BSS⁹ (1 incident).

De remarcat faptul că deși a fost raportat un număr foarte mic de incidente din categoriile OSS și BSS, respectiv Centre de comutație în rețele mobile, în cadrul acestora au fost raportate peste 1.500.000 de conexiuni afectate.

Pentru a avea o imagine mai clară privind resursele afectate, în continuare este prezentată situația pe ultimii 3 ani a numărului de incidente în cazul celor mai afectate resurse.

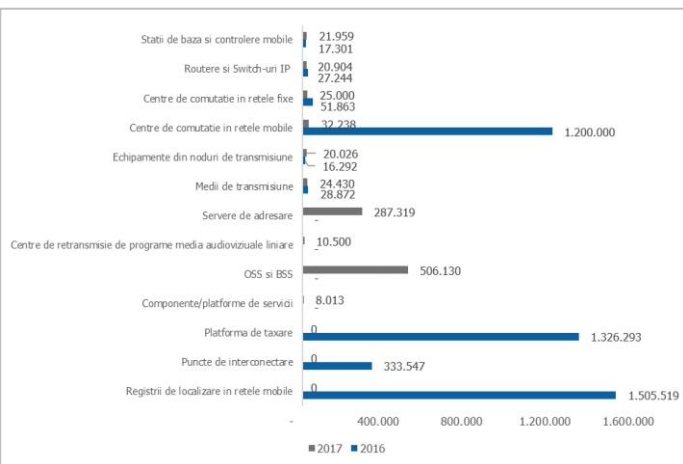
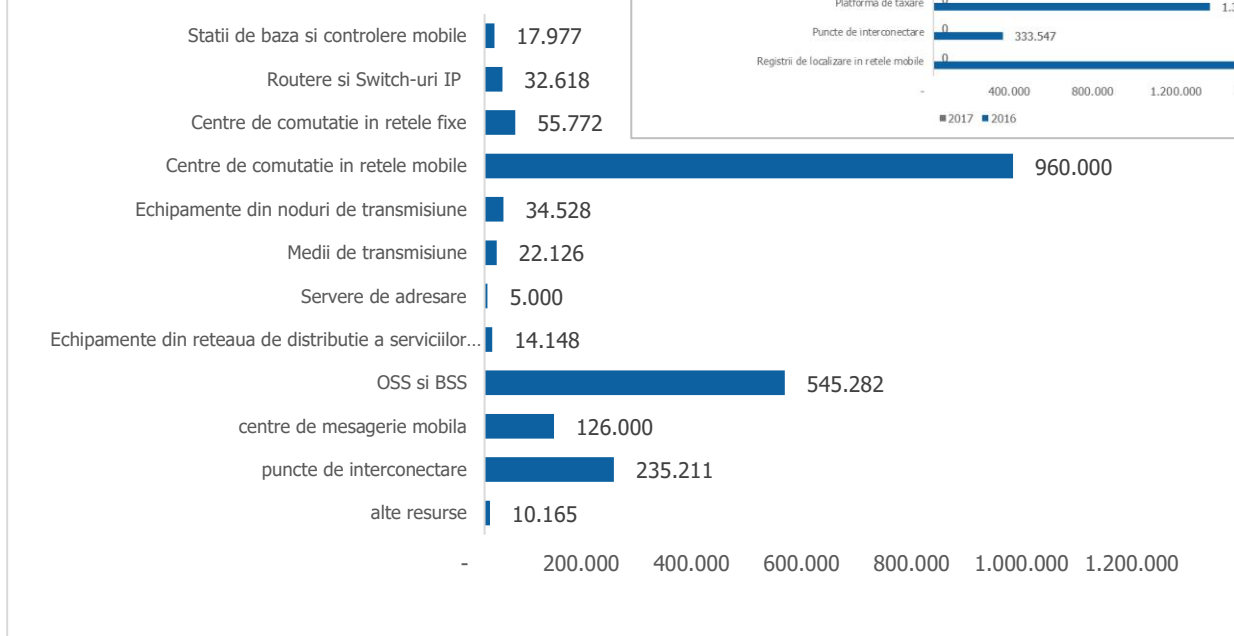


Se poate observa că numărul echipamentelor afectate din categoriile analizate în graficul de mai sus a crescut în 2018 comparativ cu anul precedent, înregistrând creșteri semnificative în cazul Echipamentelor din noduri de transmisiune (o creștere de 165%) dar și în cazul Mediilor de transmisiune (cu 139%).

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.

⁹ OSS (Operations Support Systems) și BSS (Business Support Systems)

Fig.7 Nr. mediu de conexiuni in functie de resursa afectata in 2018



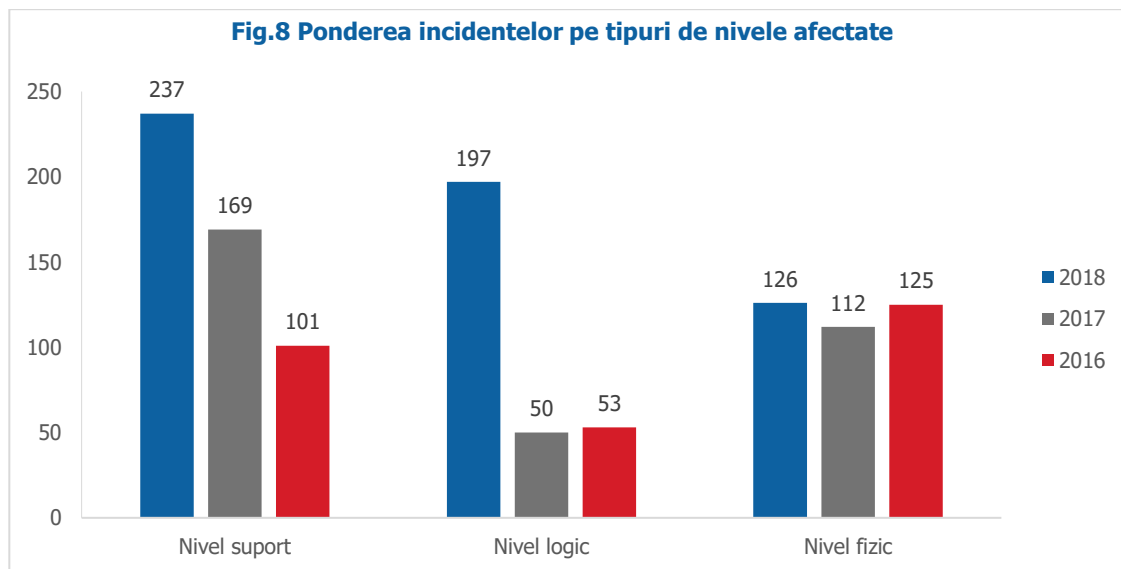
Se poate observa că resursele din cele 2 categorii (Centre de comutație în rețele mobile, OSS și BSS) care se evidențiază în figura 7 cu numărul mediu cel mai mare de conexiuni afectate, fac parte din rețeaua centrală. Având în vedere numărul mic de incidente care afectează aceste categorii de resurse, rezultă că acestea sunt afectate rar dar în momentul în care se produce un incident, impactul este considerabil, ajungând să afecteze, în anumite cazuri, o mare parte din baza de clienți a unui furnizor.

Incidentele în cadrul cărora au fost afectate resursele constând în Centre de comutație în rețele mobile și OSS și BSS au avut drept cauză o eroare de sistem, serviciile fiind afectate în acest caz la nivel național.

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 556 de incidente asupra resurselor în funcție de cele trei niveluri enunțate mai sus.

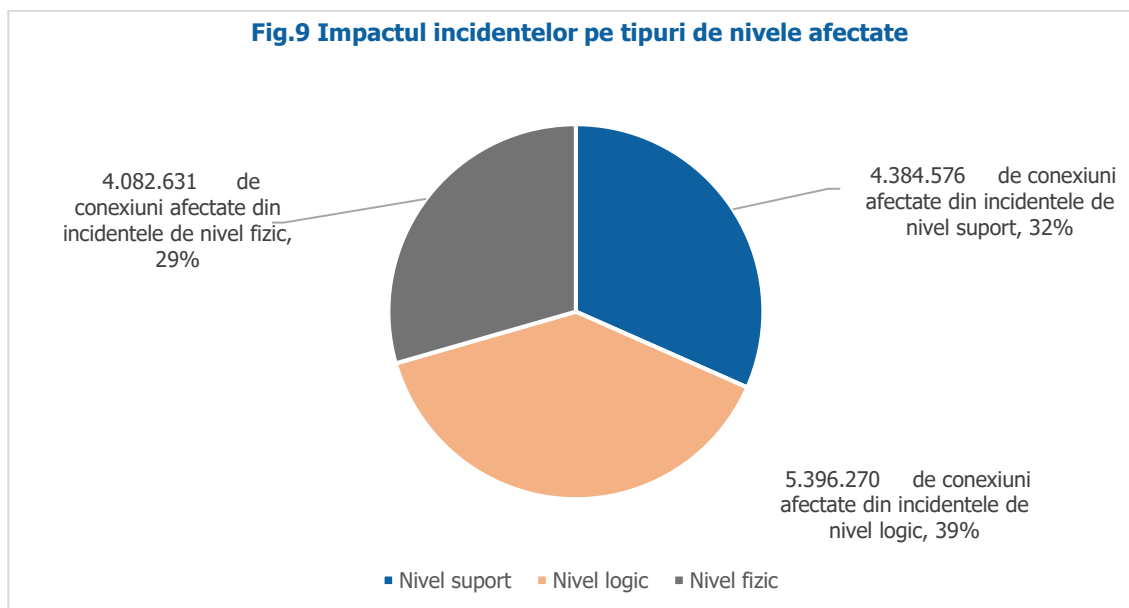


De precizat faptul că în cazul a 4 dintre incidentele prezentate în acest grafic (2018), resursele au fost afectate pe mai multe nivele (respectiv fizic și suport).

În figura 8 se poate observa că numărul incidentelor care au afectat resursele la cele trei nivele este în creștere comparativ cu anii precedenți, în cazul nivelului logic, această creștere fiind una semnificativă (de la 50 de incidente în 2017, la 197 incidente raportate în 2018). 166 dintre incidentele care au afectat resursele la nivel logic în 2018 s-au datorat erorii de comunicare intervenite la nivelul rețelelor partenere.

Așa cum am mai precizat în cadrul acestui document, în 2018 au existat cazuri în care au fost înregistrate două incidente în același timp în cadrul aceleiași rețele. Ca urmare, în câteva situații resursele au fost afectate pe mai multe nivele concomitent. În acest context, pot fi date ca exemple incidente care au afectat resursele la nivel fizic și suport. Primul exemplu se referă la incidente care s-au datorat secționării fibrei optice dar și lipsei de alimentare cu energie electrică a unor echipamente. Cel de-al doilea exemplu se referă la un incident datorat unor șocuri în rețeaua furnizorului de energie electrica, care au creat probleme la nivelul unei centrale iar pentru redresarea problemelor create a fost nevoie de configurări software, dar și de înlocuirea unor echipamente care s-au defectat ca urmare a producerii incidentului.

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



Numărul mediu de conexiuni afectate de un incident de nivel:

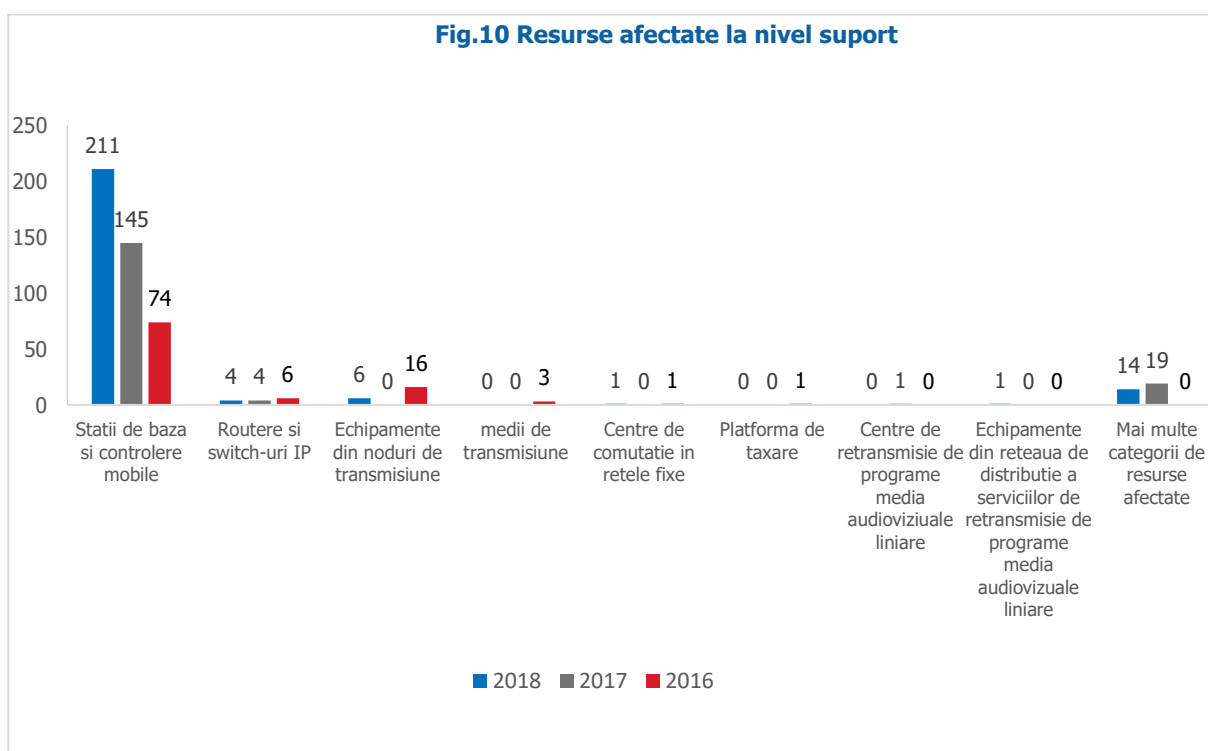
- suport – 18.500 conexiuni, în scădere față de anul precedent (28.817 conexiuni în 2017)
- logic – 27.392 conexiuni, în scădere față de anul precedent (39.057 conexiuni în 2017)
- fizic – 32.402 conexiuni, în creștere față de anul precedent (23.968 conexiuni în 2017)

Numărul mediu de conexiuni afectate în cazul incidentelor în care resursele au fost afectate la nivel fizic și suport, este de 94.781 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.



În 2018 au fost raportate 237 incidente care au afectat resursele la nivel suport.

Majoritatea incidentelor (223) 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, ori lucrări neanunțate (și de durată) în rețeaua națională de alimentare cu 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 unui generator electric.

Restul incidentelor ce au afectat resursele la nivel suport s-au datorat unor fenomene naturale severe, precum și unor erori de sistem ce au afectat redresoare, unitatea de control a sursei de alimentare, echipamente de electroalimentare etc.

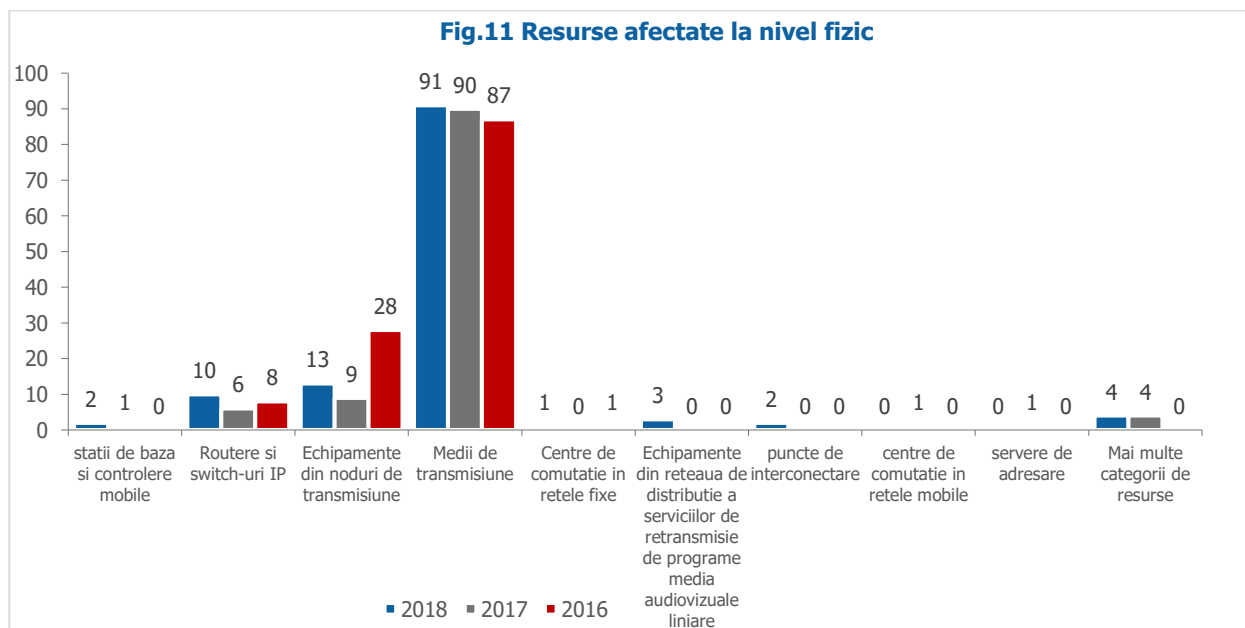
Resursele afectate la nivel suport fac parte în principal din categoria stații de bază și controlere mobile (211 incidente). Alte resurse afectate sunt din categoriile: routere și switch-uri IP (4 incidente), Echipamente din noduri de transmisiune (6 incidente), Centre de comutație în rețele fixe (1 incident), Echipamente din rețeaua de distribuție a serviciilor de retransmisie de programe media audiovizuale liniare (1 incident), iar în cazul a 14 dintre incidente, la nivel suport au fost afectate mai multe categorii de resurse (constând în principal în categoriile: Stații de bază și controlere mobile, Echipamente din noduri de transmisiune și Routere și switch-uri IP, Centre de comutație în rețele fixe), acestea fiind cauzate de fenomene naturale severe, ori în cazul unui incident, acțiunii rău intenționate (în urma vandalizării unor site-uri).

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 anii precedenți, 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 4.384.576 de conexiuni afectate în incidentele raportate, înregistrând o scădere față de anul precedent, când au fost raportate 5.290.210 de conexiuni afectate), 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.



La nivel fizic, cea mai afectată resursă este fibra optică (încadrată în categoria medii de transmisiune). Din cele 91 de incidente care au afectat la nivel fizic această categorie de resurse, în 41 dintre aceste cazuri incidentele se datorează lucrărilor efectuate de terți, într-un singur caz incidentul s-a datorat acțiunilor rău-intenționate (în principiu aceste acțiuni reprezentând tentative de furt) iar în 5 cazuri, incidentele s-au datorat fenomenelor naturale (de ex. fibra a fost ruptă în urma unei viituri. În alt caz, în urma fenomenelor naturale extreme, au căzut copaci, stâlpi, fibra optică ajungând pe linia de tramvai. În cazul unui incident mai grav, au fost înregistrate 8 secționări ale fibrei optice ca urmare a condițiilor meteorologice extreme).

38 de incidente care au afectat mediile de transmisiune la nivel fizic s-au datorat unor factori externi (incendii, căderea unui stâlp de tensiune ca urmare a unui accident auto), existând și cazuri în care

cauza secționării fibrei nu a fost raportată. În cazul celorlalte incidente care au afectat mediile de transmisiune la nivel fizic, este vorba de întreruperea comunicării între diverse echipamente din cauza erorii umane, în acest caz fiind afectate linkurile radio (exemple de astfel de incidente constând în: depășirea ferestrei de mentenanță în cadrul unor lucrări programate, ori întreruperea din greșeală a unui link de transmisiuni).

În majoritatea cazurilor, 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, planificarea unor soluții redundante 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 unor defecțiuni hardware în urma cărora stațiile de bază agregate în acesta au devenit neoperaționale, fie în urma fenomenelor naturale (zăpezi abundente).

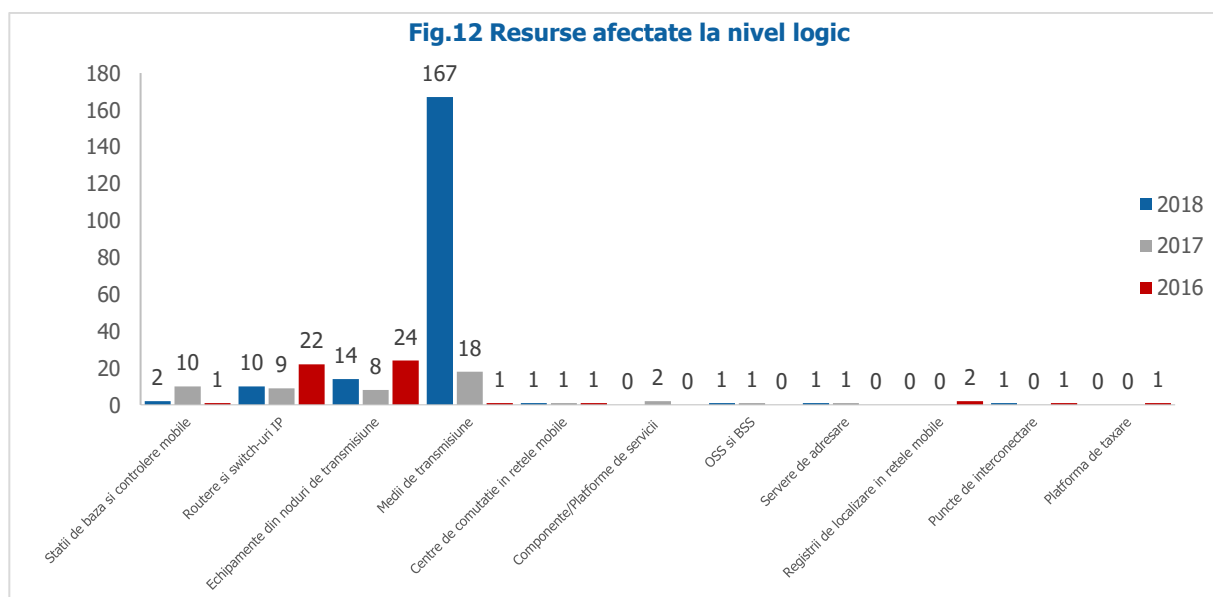
Incidentele în cazul cărora au fost afectate la nivel fizic resursele care fac parte din categoriile Echipamente din rețeaua de distribuție a serviciilor de retransmisie de programe media audiovizuale liniare și Centre de comutație în rețele fixe au avut drept cauză Eroare de sistem și s-au datorat defectării la nivel hardware a unor echipamente.

În 4 cazuri, incidentele au afectat mai multe categorii de resurse la nivel fizic, un astfel de exemplu constând în secționarea unui cablu de fibră optică concomitent cu defectarea unor cartele aparținând unor resurse din categoria Echipamente din noduri de transmisiune.

Nivelul logic

În urma raportărilor furnizorilor, s-au înregistrat 197 de incidente care au afectat resursele la nivel logic, situația fiind în depreciere comparativ cu cea de anul trecut, perioadă în care au fost raportate 50 de astfel de incidente. 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. Resursele afectate în cea mai mare măsură fac parte din categoriile Medii de transmisiune (167 incidente), Echipamente din noduri de transmisiune (14 incidente) și Routere și switch-uri (10 incidente).

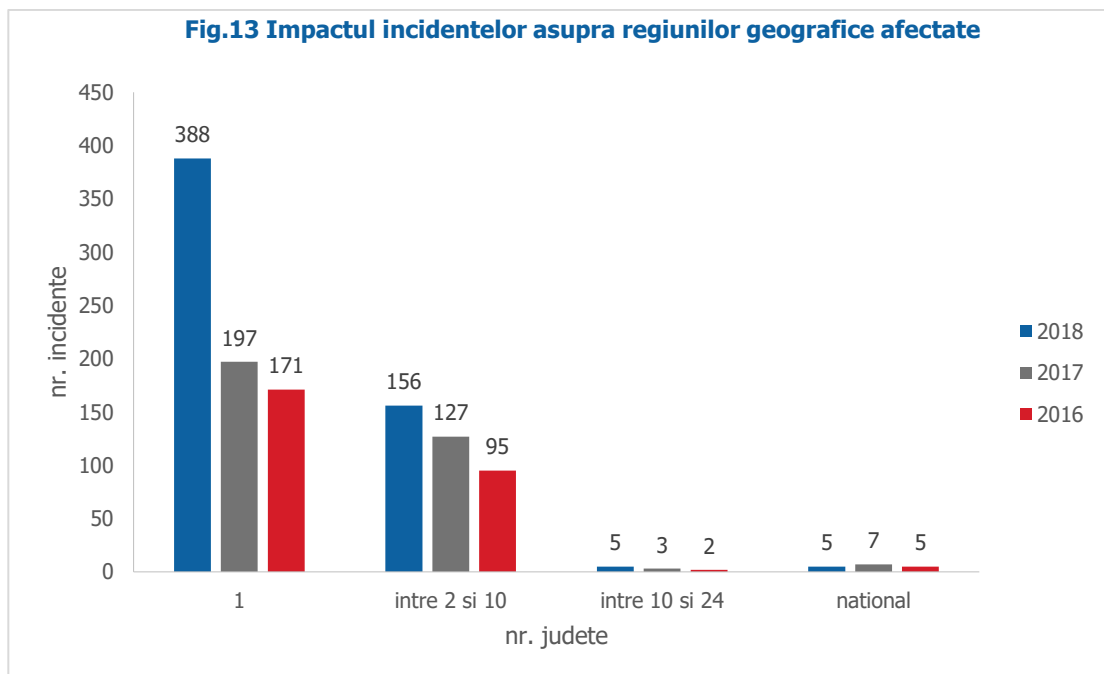
Statistica realizată în acest caz este reprezentată în figura 12.



Dintre cele 167 dintre incidentele în cadrul cărora Mediile de transmisiune au fost afectate la nivel logic, 166 se datorează incidentelor care s-au produs în rețelele partenere, iar într-un caz incidentul s-a datorat unei erori de sistem (constând într-o eroare de procedură) în care termenul stabilit al unei lucrări programate în cadrul rețelei (cu scopul de a mări capacitatea unui link de transmisiuni) a fost depășit!

Aria geografică

În ceea ce privește regiunea geografică afectată de incidente, în cele mai multe cazuri (388), incidentele raportate au afectat un singur județ, 156 de incidente au avut impact asupra unei arii geografice cuprinse între două județe și 10 județe, 5 incidente au avut impact asupra unei arii geografice cuprinse între 10 și 24 județe iar în cazul a 5 incidente, furnizorii au raportat că impactul a fost la nivel național. În acest ultim caz, echipamentele afectate fac parte din categoriile Routere și switch-uri IP, Puncte de interconectare, Centre de comutație în rețele mobile, OSS și BSS, Servere de adresare. Durata medie a incidentelor cu impact la nivel național este de aproximativ 4 ore. Majoritatea acestora s-au datorat erorii de sistem.



De menționat este faptul că, în urma producerii a două dintre incidente au fost afectate serviciile de roaming. În ambele cazuri resursa afectată face parte din categoria Puncte de interconectare. Cele două incidente s-au datorat fie erorii de sistem (ca urmare a defectării unui card dintr-un echipament de transmisiuni aflat într-un centru de colocare) fie erorii umane (ca urmare a configurării greșite în cadrul unei lucrări).

Pentru o imagine mai clară a numărului de incidente care a afectat fiecare județ în parte, această situație este prezentată în figura 14.

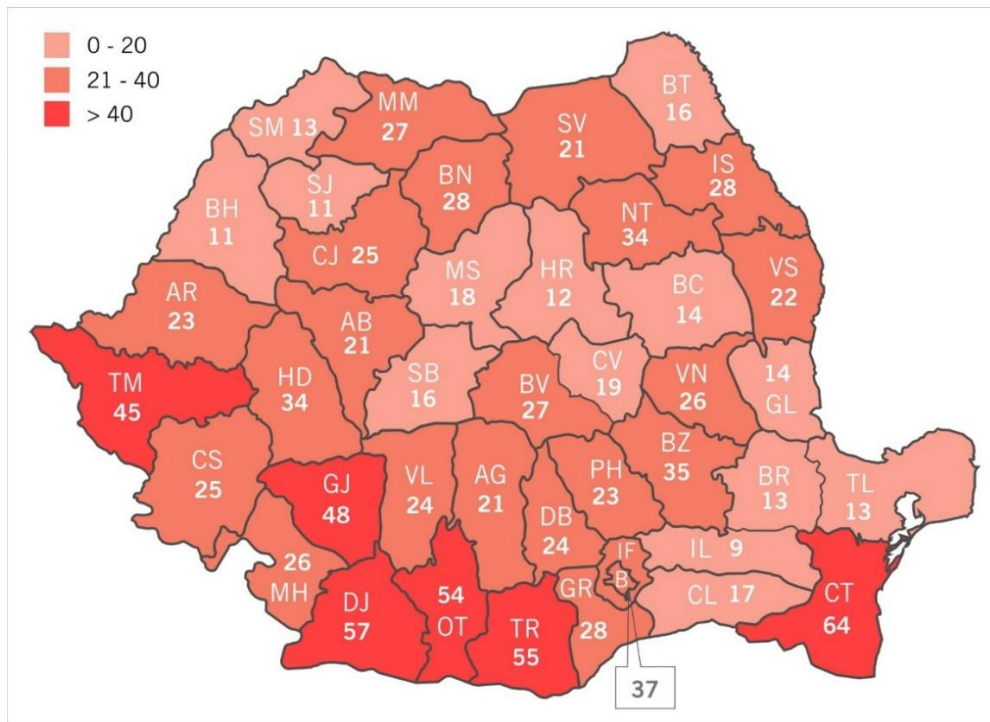


Fig. 14

De precizat faptul că numărul incidentelor însumate la nivel național nu coincide cu numărul de incidente raportate în 2018 (556 incidente) pentru că în cazul a 166 incidente, acestea au avut impact asupra cel puțin a două județe.

Conform raportărilor, cele mai multe incidente au afectat județele Constanța (64 incidente), Dolj (57 incidente), Teleorman (55 incidente) și Olt (54 incidente).

Județele cel mai puțin afectate sunt Ialomița (9 incidente), Bihor și Sălaj (câte 11 incidente).

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

Situația privind incidentele care au avut drept cauză problemele de alimentare cu energie electrică la nivel național, sunt prezentate în figura 15.

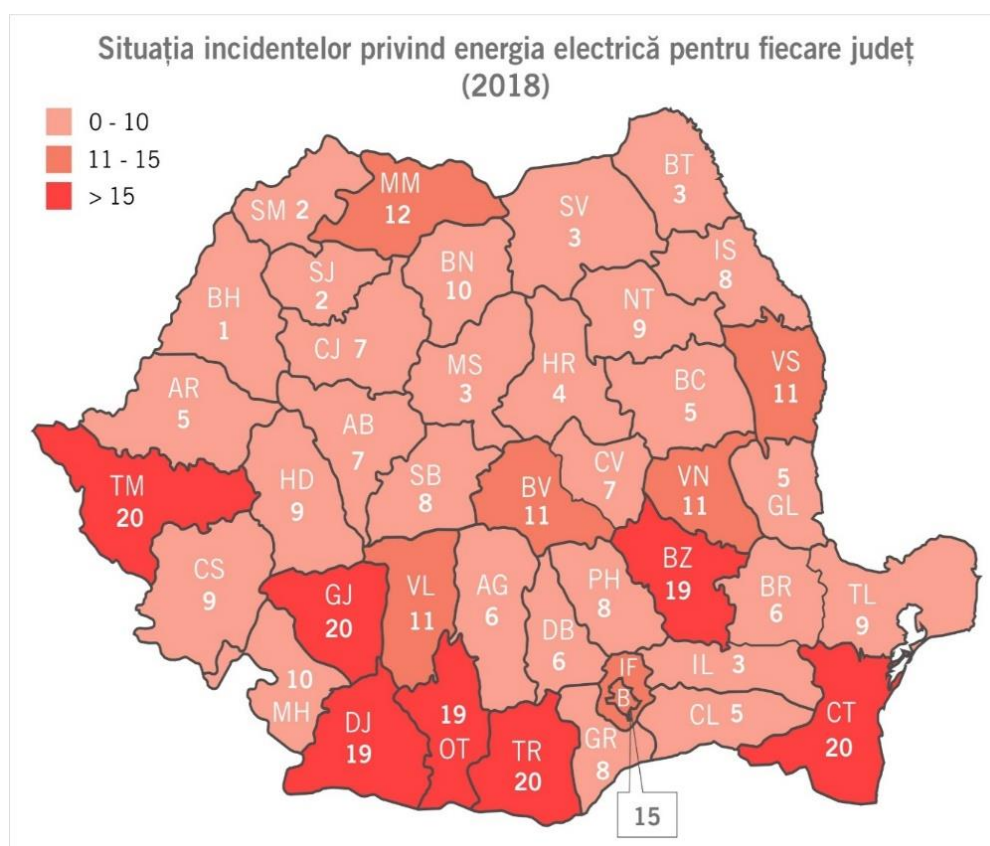


Fig. 15

Conform raportărilor furnizorilor, cele mai multe incidente care s-au datorat problemelor de alimentare cu energie electrică s-au înregistrat în Constanța, Teleorman, Gorj și Timiș (câte 20 incidente), Olt, Dolj și Buzău (câte 19 incidente).

Comparativ cu anul precedent, în 2018, în cazul celor mai multe dintre județe, numărul incidentelor care s-au datorat problemelor de alimentare cu energie electrică a crescut, în unele cazuri această creștere fiind semnificativă (de exemplu, în Teleorman - de la 10 incidente înregistrate în 2017, la 20 de incidente raportate în 2018, sau în județul Olt - de la 5 incidente care s-au produs în 2017, la 19 incidente raportate în 2018).

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).

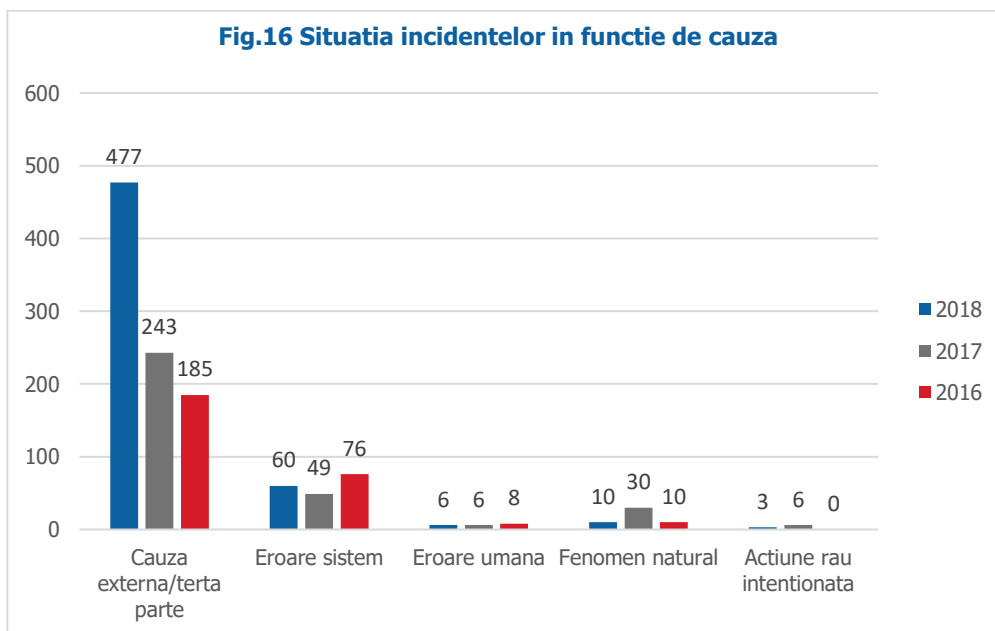
Pentru a împiedica apariția acestui tip de incident, printre măsurile planificate de furnizori se află: achiziționarea de generatoare mobile și dotarea cât mai multor puncte de prezență cu grupuri electrogene, verificarea periodică preventivă a generatoarelor și bateriilor, schimbarea bateriilor în vederea creșterii autonomiei, revizuirea sistemului de alarme. Unul dintre furnizori a avut în vedere analizarea împreună cu furnizorul de energie electrică a unor modalități de prevenire a incidentelor cauzate de întreruperea furnizării energiei electrice. În vederea intervenirii într-un timp cât mai scurt în astfel de cazuri, un furnizor a prevăzut suplimentarea numărului de vehicule speciale de transport pentru zone greu accesibile în condiții meteorologice extreme. În cele mai multe cazuri (aproximativ 86%) furnizorii nu au raportat măsuri întreprinse pentru a împiedica apariția acestui tip de incident.

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.

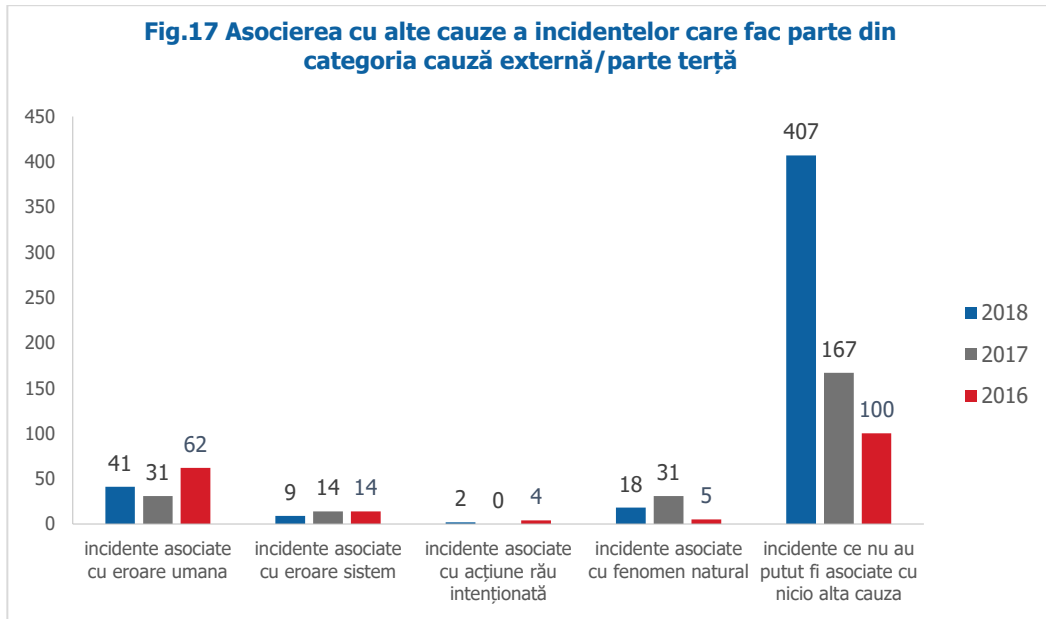
Situația incidentelor în funcție de cauză este prezentată mai jos.



Așa cum se poate vedea în Fig.16, la fel ca și în anii precedenți, în 2018 majoritatea incidentelor fac parte din categoria cauză externă/parte terță (477 incidente, reprezentând aproximativ 86% din totalul de incidente raportate în 2018). 60 dintre incidente fac parte din categoria eroare de sistem, 10 incidente fac parte din categoria fenomen natural, 6 incidente fac parte categoria eroare umană și 3 dintre incidente au fost încadrate în categoria acțiune rău intenționată.

Se poate observa o creștere semnificativă a numărului de incidente din categoria cauză externă/ parte terță (comparativ cu anul precedent, numărul acestora aproape s-a dublat în 2018).

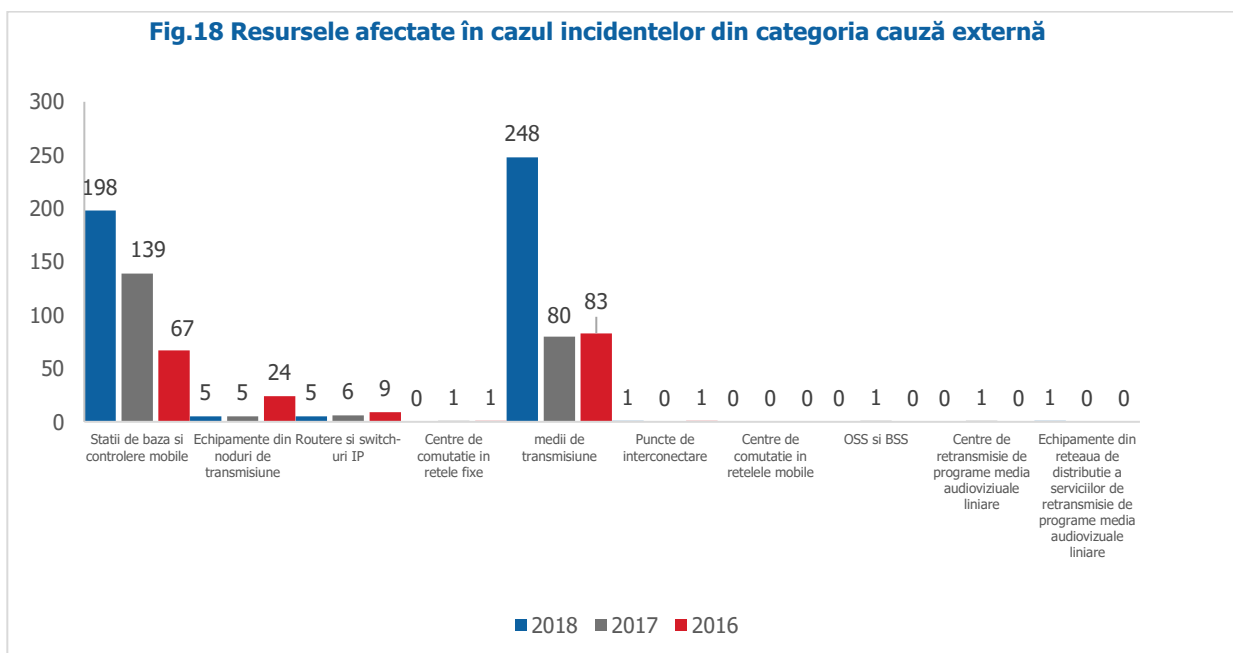
Incidentele din categoria cauză externă pot fi corelate cu una din celelalte 4 categorii de cauze.



Astfel, dintre cele 477 incidente încadrate în această categorie, 41 au fost asociate cu eroare umană, 9 incidente au fost asociate cu eroare de sistem, două incidente au fost asociate cu acțiune rău intenționată și 18 incidente au fost asociate cu fenomen natural.

407 incidente din categoria cauză externă/parte terță nu au putut fi asociate cu nicio altă cauză dintre cele menționate în cadrul Deciziei 512. Majoritatea dintre acestea s-au datorat problemelor de alimentare apărute în rețeaua furnizorului de energie electrică (201 incidente). Alte cauze ale producerii acestor incidente s-au datorat problemelor de funcționare a unor echipamente din în cadrul rețelelor partenere (166 de incidente), ori ruperii (din cauze necunoscute sau neraportate de către furnizori) a fibrei optice, accidentelor rutiere etc.

Întrucât principalele cauze pentru producerea incidentelor raportate în 2018 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.



*Graficul reprezintă resurse unic afectate în cadrul incidentelor

Se poate observa că în cazul incidentelor din categoria cauză externă cele mai afectate resurse sunt mediile de transmisiune și stațiile de bază și controlerele mobile. Categoriile de resurse afectate în mică măsură sunt Routere și switch-uri IP, Echipamente din noduri de transmisiune, Puncte de interconectare și Echipamente din rețeaua de distribuție a serviciilor de retransmisie de programe media audiovizuale liniare.

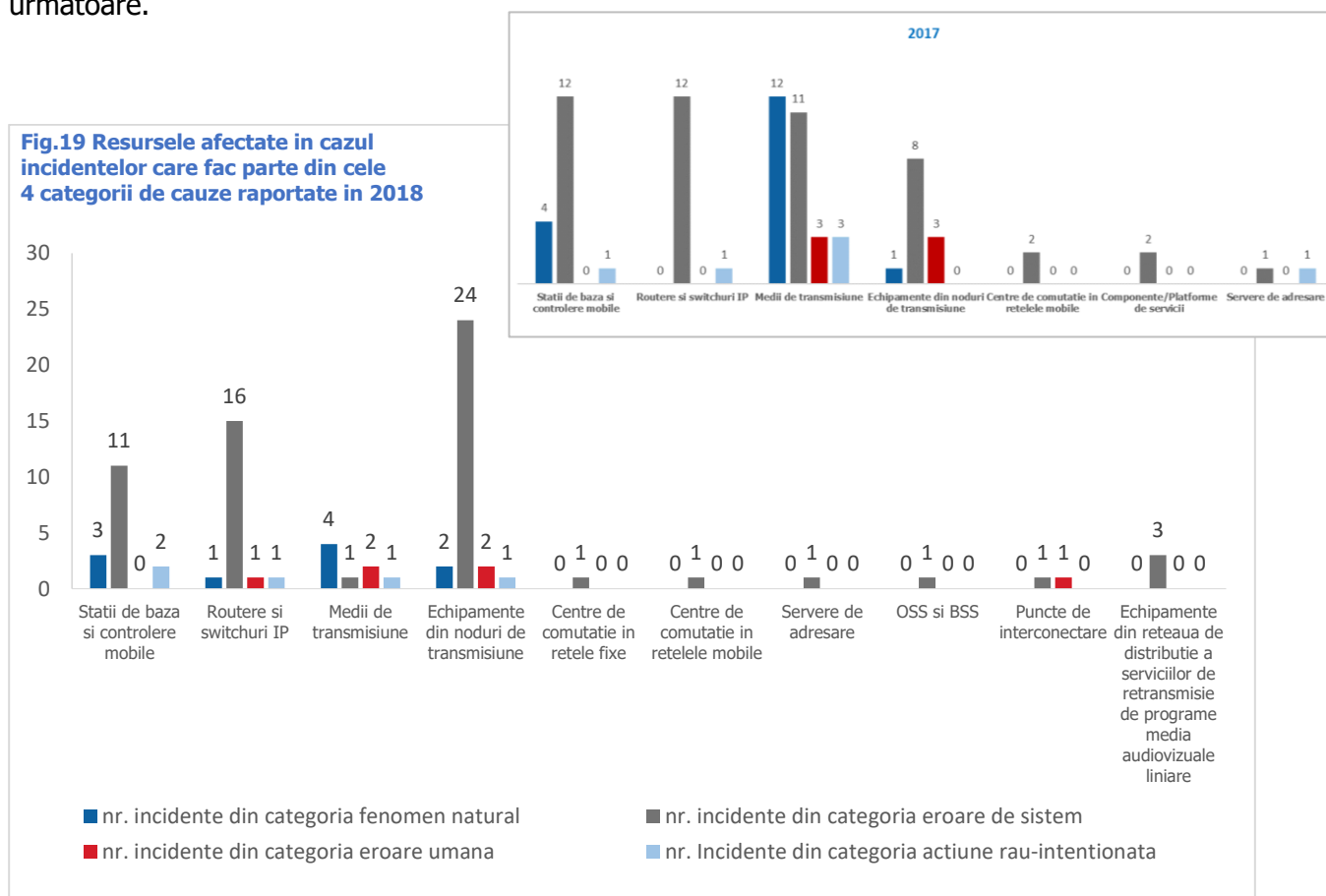
De precizat faptul că în graficul de mai sus sunt reprezentate resursele unic afectate în cadrul unui incident. Pe lângă acestea, există 19 incidente care fac parte din categoria cauză externă/parte terță în cadrul fiecăruia dintre acestea fiind afectate mai multe categorii de echipamente. În majoritatea cazurilor, cauza externă a fost asociată cu Fenomen natural.

Mediile de transmisiune au fost afectate în principal în urma problemelor înregistrate la nivelul rețelelor partenerere, a lucrărilor efectuate de terți, ori ca urmare a fenomenelor naturale extreme.

Conform raportărilor, incidentele 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 întreruperilor energiei electrice furnizată de rețelele de distribuție națională). Comparativ cu anii precedenți, această valoare este în creștere în 2018.

Tot în cazul incidentelor din categoria cauză externă, echipamentele din categoria Echipamente din noduri de transmisiune și categoria Routere și switch-uri au fost afectate în principal din cauza șocurilor de energie electrică, care au avut drept urmare (în câteva cazuri) defectarea unor echipamente.

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



În cazul a două dintre incidente care fac parte din categoria Eroare de sistem, respectiv categoria Acțiune rău intenționată, acestea au afectat mai multe categorii de resurse. Primul incident s-a datorat defectării unor echipamente, iar cel de-al doilea s-a produs în urma vandalizării unor site-uri (bateriile au fost furate), mai multe echipamente rămânând fără alimentare cu energie electrică.

Se poate observa faptul că resursele din categoriile Echipamente din noduri de transmisiune, Routere și switch-uri 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 (ninsori abundente, vânt puternic) în urma cărora anumite echipamente au fost afectate la nivel fizic (de exemplu, ca urmare a căderilor masive de zăpadă, fibra optică a fost întreruptă). În cazul incidentelor cauzate de eroare umană, resursele au fost afectate în principal în cadrul lucrărilor programate, fie datorită configurării greșite a echipamentelor, fie datorită depășirii ferestrei de mentenanță. În cazul incidentelor din categoria acțiune rău-intenționată, două dintre acestea s-au datorat acțiunilor de vandalism la nivelul stațiilor de bază, iar în cazul unui incident, secționării intenționate a cablurilor de fibră optică.

În cazul a 4 incidente, echipamentele din categoria Routere și Switch-uri, Servere de adresare, Centre de comutație în rețele mobile, respectiv OSS și BSS au fost afectate în urma unor erori de sistem, având impact la nivel național asupra serviciilor.

Comparativ cu anul precedent, în 2018 se poate observa o creștere a numărului incidentelor din categoria Eroare de sistem, care au afectat resurse din categoria Echipamente din noduri de transmisiune, dar și o scădere semnificativă acelor datorate fenomenelor naturale, respectiv erorii de sistem, care au afectat resurse din categoria Medii de transmisiune.

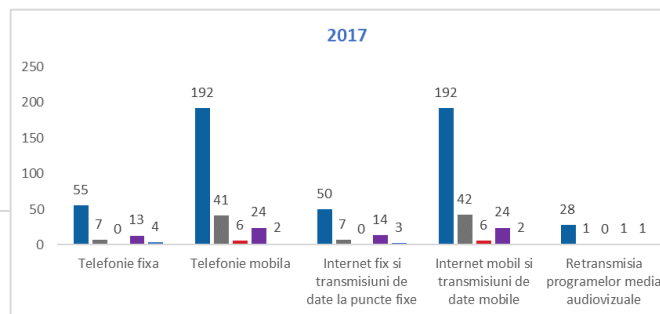
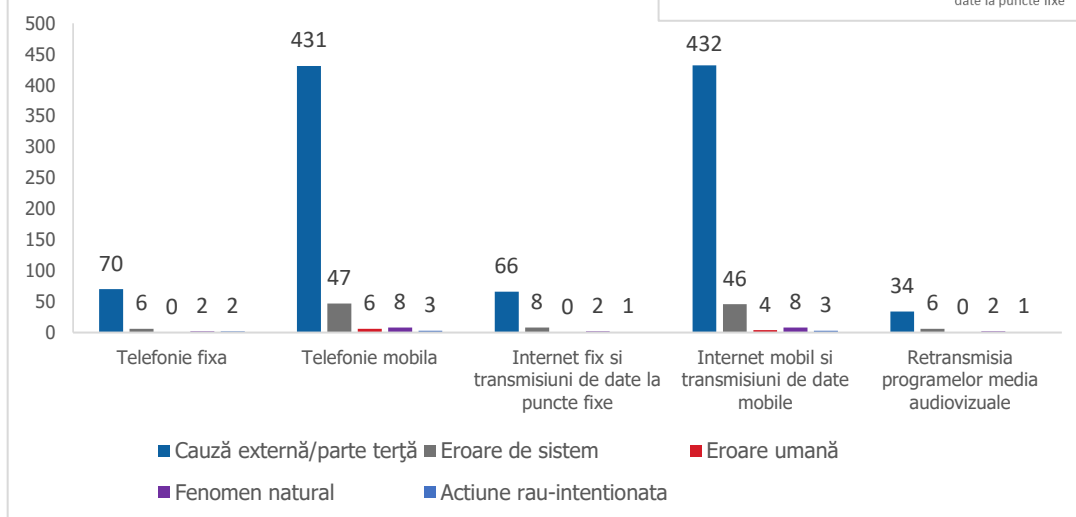
Făcând o analiză a categoriilor de resurse afectate pentru fiecare tip de cauză, din raportările furnizorilor s-a constatat faptul că în cazul incidentelor încadrate în cele 4 categorii de cauze, Stațiile de bază și controlerele mobile au fost afectate în principal la nivel suport din cauza unor probleme de alimentare cu energie electrică (ca urmare a defectării unor echipamente de electroalimentare, de exemplu generatoare fixe), ori din cauza unor erori software apărute.

Conform raportărilor, resursele din categoria medii de transmisiune au fost afectate fie ca urmare a fenomenelor meteorologice nefavorabile (zăpezi abundente, vânt puternic), fie în urma configurărilor greșite din cadrul unor lucrări programate, fie în urma vandalizării cablurilor de fibră optică.

Echipamentele din categoria Routere și switch-uri au fost afectate în urma defectării anumitor echipamente (switch-uri), ori problemelor de natură software, ori ca urmare a actelor de vandalism, ori ca urmare a fenomenelor naturale.

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

Fig.20 Numărul incidentelor pentru toate tipurile de servicii în funcție de cauză în 2018



De precizat faptul că în acest caz suma incidentelor pentru toate tipurile de servicii afectate, în funcție de cauză (Fig.20) diferă de numărul total al incidentelor per tip de cauză (reprezentat în Fig.16) deoarece un incident poate afecta mai multe servicii simultan.

Din Fig.20 se observă că, similar cu anul precedent, cele mai afectate servicii în 2018, 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. Acestea s-au mai datorat problemelor apărute la nivelul rețelelor partenere.

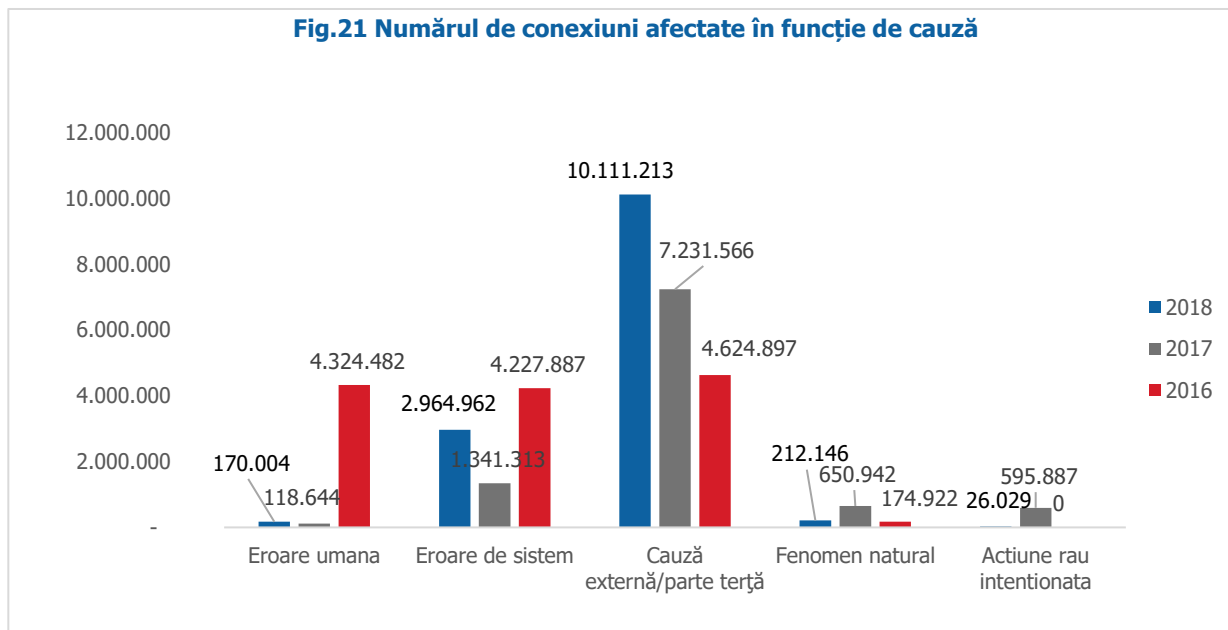
În cazul incidentelor care fac parte din categoriile eroare de sistem și fenomen natural și care au afectat serviciile de acces la internet mobil, transmisiuni de date mobile și serviciile de telefonie mobilă, acestea s-au produs în principal datorită defecțiunilor software sau hardware ale unor echipamente,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

Incidentele din categoria acțiune rău-intenționată s-au datorat actelor de vandalism, în urma cărora multiple echipamente au rămas fără alimentare cu energie electrică, ori cablurile de fibră optică au fost secționare, fapt care a afectat furnizarea principalelor servicii de comunicații electronice.

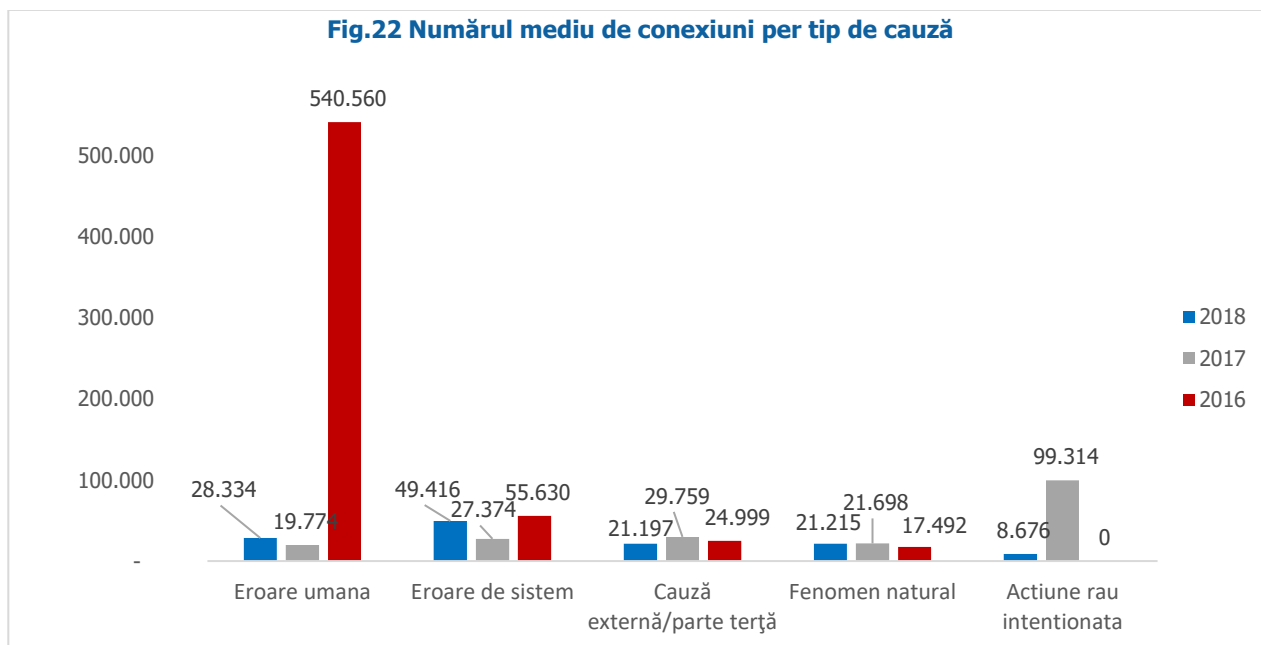
Serviciile de retransmisie a programelor audiovizuale au fost afectate în principal în cazul incidentelor care fac parte din categoria cauză externă/parte terță (34 incidente). Acestea s-au datorat în mare parte avariilor la nivelul fibrei optice. În privința a 6 incidente, acestea au fost cauzate de defectări ale unor echipamente.

Comparativ cu anul precedent, se poate observa că numărul incidentelor din categoria cauză externă/parte terță, care au afectat serviciile de comunicații electronice au înregistrat creșteri semnificative în 2018. În schimb, situația incidentelor din categoria fenomen natural, care au afectat serviciile de telefonie și date mobile precum și serviciile de telefonie și date fixe este mult îmbunătățită în 2018.

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



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



În graficul de mai sus se poate observa faptul că incidentele din categoria eroare de sistem afectează, în medie, cel mai mare număr de conexiuni (49.416 conexiuni). Această situație este

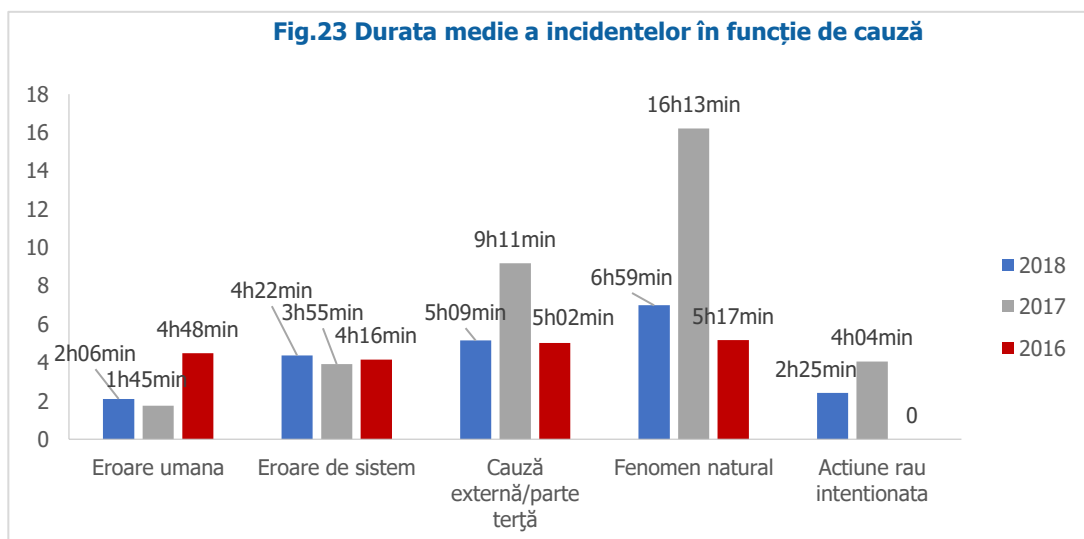
justificată prin faptul că, deși a fost raportat un număr mic de incidente din această categorie, în cadrul acestora s-a înregistrat un număr foarte ridicat de conexiuni afectate. Un exemplu în acest sens îl constituie incidentul datorat defectării unui echipament din categoria Centre de comutație în rețele mobile, care a afectat peste 900.000 de conexiuni, impactul acestuia fiind la nivel național. Față de anul precedent, situația privind numărul mediu de conexiuni afectate datorită acțiunilor rău intenționate, s-a îmbunătățit considerabil. În 2018, incidentele din categoria acțiune rău intenționată au afectat în medie cel mai mic număr de conexiuni (8.676).

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 2018 este de 2.808 ore, durata medie a unui incident fiind de aproximativ 5 ore și 3 minute. Aceste valori sunt mai mici decât cele înregistrate în anul 2017, când durata totală a incidentelor a fost de 2.945 ore, iar durata medie a fost de 8 ore și 49 minute.

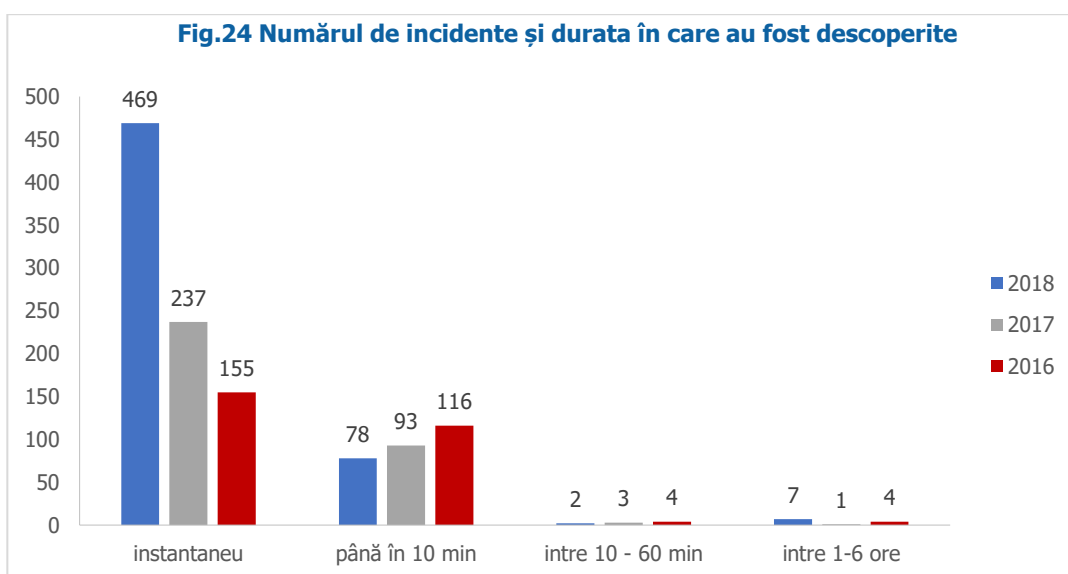
În figura de mai jos este ilustrată durata medie a unui incident în funcție de cauza incidentului.



Valoarea cea mai mare a duratei medii aparține categoriei de cauze fenomen natural (6 ore și 59 minute). Acest lucru se datorează faptului că intervenția la echipamentele afectate a fost realizată cu întârziere de către echipele de pe teren fie din cauza accesului îngreunat de condițiile meteorologice (viscol, ninsori abundente), fie din cauza drumurilor blocate (din cauza stâlpilor de medie și înaltă tensiune doborâți). În ceea ce privește incidentele care au afectat mai multe categorii de resurse, durata medie a acestora a fost de 1774 minute (aproximativ 30 ore) și s-au datorat în mare parte fenomenelor naturale, în majoritatea cazurilor echipamentele rămânând fără alimentare cu energie electrică.

Comparativ cu anul precedent se poate observa că durata medie a unui incident din categoria eroare de sistem, respectiv din categoria eroare umană au înregistrat o ușoară creștere în 2018, în schimb durata medie în cazul incidentelor datorate fenomenelor naturale, acțiunilor rău-intenționate și din categoria cauză externă au scăzut considerabil.

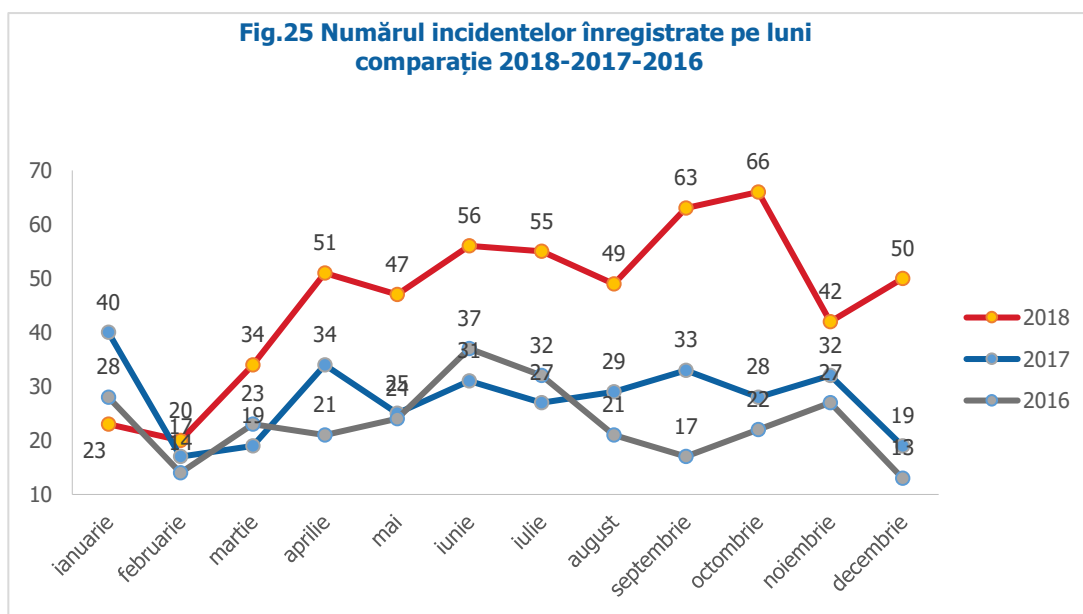
Situația privind numărul de incidente și durata în care au fost descoperite este prezentată mai jos.



Din Fig.24 se poate observa că cele mai multe incidente (469) au fost descoperite în momentul producerii lor și că 7 incidente au fost descoperite într-un interval mare de timp (cel mai lung interval de timp în care a fost descoperit un incident a fost de 2 ore și 30 minute).

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 2018.



Spre deosebire de anii precedenți (2017 și 2016), când s-au produs în medie 28 de incidente, respectiv 23 de incidente pe lună, în 2018 au fost raportate în medie 46 de incidente pe lună. Se poate observa că în 2018, luna octombrie este perioada în care s-au raportat cele mai multe incidente (66). Cauzele producerii a 47% dintre acestea fac parte din categoria cauză externă/parte terță.

3.5 Impactul asupra apelurilor de urgență

97% dintre incidentele raportate în anul 2018 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 2018, au fost cele de telefonie mobilă (în acest caz fiind afectat implicit și serviciul de urgență 112). Față de anul 2017, numărul incidentelor care au afectat apelurile de urgență a crescut de la 320 de incidente (însemnând 96% din totalul incidentelor din 2017) la 541 de incidente în anul 2018 (însemnând 97% din totalul incidentelor din 2018).

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);
- Intervenția echipelor tehnice cu echipamente de alimentare cu energie electrică (în cazul incidentelor în care diferite echipamente au rămas fără alimentare);
- 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 redirectionarea 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);
- Urmărirea/primirea periodică a rapoartelor privind evoluția fenomenelor meteorologice și remedierea cu prioritate a deranjamentelor din nodurile care concentrează un număr mare de clienți afectați (în cazul incidentelor cauzate de fenomene naturale).

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 distrugerii la nivel fizic ale diferitelor resurse (ex. instalare camere de luat vederi);

- Stabilirea unor reguli noi privind lucrările programate realizate de producătorii de echipamente;
- Înlocuirea unor echipamente vechi cu unele de generație nouă;
- Stabilirea împreună cu rețeaua parteneră a unor soluții în vederea evitării pe viitor a situațiilor similare;
- Colectarea de log-uri în vederea efectuării ulterioare a unei analize în detaliu a incidentelor;
- Relocarea unor echipamente în locații mai sigure (ca urmare a actelor de vandalism);
- Verificarea suplimentară a detaliilor care privesc lucrările programate în cadrul rețelei;
- Suplimentarea vehiculelor speciale de transport în vederea accesului în zone greu accesibile;
- Analizarea împreună cu furnizorii de utilități a cauzelor care au dus la producerea incidentelor;
- Asigurarea redundanței căilor de transmisiune.

Menționăm faptul că în cazul majorității incidentelor raportate în 2018 (situație similară cu cea din 2017), 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.

Întrucât în cadrul analizei incidentelor au putut fi observate raportarea unor incidente similare care s-au repetat la un anumit interval de timp (având aceeași cauză, afectând aceeași zonă geografică etc.), ANCOM subliniază importanța acestor măsuri planificate în scopul de a împiedica producerea unui incident similar și recomandă furnizorilor să prevadă astfel de măsuri.

5. Concluzii

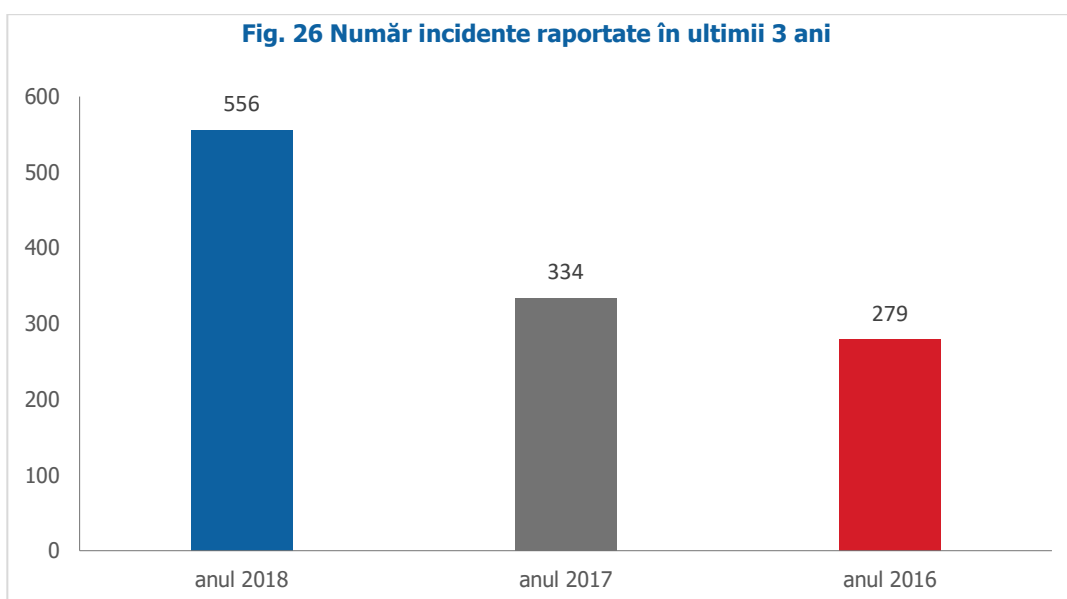
Prin raportarea incidentelor cu impact semnificativ asupra rețelelor și serviciilor de comunicații electronice, ANCOM este informată cu privire la cauzele incidentului, poate urmări acțiunile furnizorului în vederea remedierii rețelelor și serviciilor la un nivel corespunzător și poate evalua nivelul 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 amplitudinii 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 556 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 2018, se pot desprinde următoarele concluzii:

- analizând situația privind numărul de incidente cu impact semnificativ raportate în ultimii 3 ani, se poate identifica o tendință crescătoare.



- asemenea anilor 2016 și 2017, în 2018 cele mai afectate servicii, din punct de vedere al numărului de conexiuni, au fost serviciile de telefonie mobilă și SMS (7.613.144 conexiuni afectate).
- numărul mediu al conexiunilor afectate de un incident în 2018 (24.252 conexiuni) este în scădere față de 2017 (29.755 conexiuni).
- din punctul de vedere al numărului de incidente, cele mai multe dintre incidentele cu impact semnificativ raportate în 2018 au afectat serviciile de telefonie mobilă și serviciile de acces la internet mobil (495, respectiv 493 incidente cu impact semnificativ).
- numărul incidentelor cu impact semnificativ ce au afectat fiecare categorie de servicii a crescut în 2018 față de anii precedenți.
- serviciul de retransmitere a programelor media audiovizuale este afectat de un număr mic de incidente cu impact semnificativ (43 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.
- în cadrul a 19 dintre incidente au fost afectate concomitent mai multe categorii de resurse, cauzele producerii acestora fiind asociate în principal cu fenomene naturale.
- numărul incidentelor care au afectat principalele categorii de resurse (Medii de transmisiune, Stații de bază și controlere mobile, Echipamente din noduri de transmisiune și Routere și switch-uri IP) a crescut în 2018 față de 2017.
- incidentele ce au afectat resurse ce fac parte din rețeaua centrală (OSS și BSS și centre de comutație în rețelele mobile) au afectat un număr foarte mare de conexiuni. Aceste incidente sunt foarte puține ca număr dar au un impact major din punctul de vedere al numărului de conexiuni afectate.
- din punctul de vedere al ariei geografice afectate, în 388 din cazuri (70% din numărul total de incidente) a fost afectat un singur județ iar 5 incidente s-au petrecut la nivel național în 2018. Cele mai afectate din punctul de vedere al numărului de incidente sunt județele Constanța (64 incidente), Dolj (57 incidente), Teleorman (55 incidente) și Olt (54 incidente), și cel mai puțin afectate județe sunt Ialomița (9 incidente), respectiv Bihor și Sălaj, în cazul cărora au fost raportate câte 11 incidente cu impact semnificativ petrecute în 2018.

- 86% din totalul incidentelor raportate în 2018 fac parte din categoria cauză externă/parte terță (477 incidente).
- în cazul incidentelor din categoria cauză externă cele mai afectate resurse sunt:
 - mediile de transmisiune (în cazul a 248 de incidente cu impact semnificativ) și
 - stațiile de bază și controlerile mobile (în cazul a 198 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 24 de incidente cu impact semnificativ),
 - Routere și switch-uri IP (în cazul a 16 incidente cu impact semnificativ).
- durata totală a incidentelor raportate pe anul 2018 este de 2.808 ore, în scădere față de anul 2017 (2.945 ore). Durata medie a unui incident în 2018 este de 5 ore și 3 minute, de asemenea în scădere față de 2017 (8 ore și 49 minute) și față de 2016 (7 ore și 31 minute).
- 97% dintre incidentele raportate în anul 2017 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 2018 este în creștere față de anii precedenți (cu peste 66% mai multe incidente față de 2017);
- Durata totală a incidentelor a înregistrat o scădere semnificativă față de anul precedent, astfel încât durata medie a unui incident a scăzut de la 8 ore și 49 minute în 2017, la 5 ore și 3 minute în 2018.

În cadrul analizei efectuate de ANCOM pe baza informațiilor raportate de către furnizori, s-a constatat faptul că există incidente cu impact semnificativ, care s-au produs în repetate rânduri, având aceeași cauză și având impact asupra aceleiași zone geografice. Pentru o mai bună înțelegere a situației, ANCOM își propune să analizeze mai în detaliu aceste cazuri subliniind totodată importanța adoptării unor astfel de măsuri și amintește furnizorilor obligația *de a lua toate măsurile de securitate adecvate pentru a administra riscurile la adresa securității rețelelor și serviciilor de comunicații electronice astfel încât să asigure un nivel de securitate corespunzător riscului identificat și să prevină și să minimizeze impactul incidentelor de securitate asupra utilizatorilor și rețelelor interconectate* (conform prevederilor Art.3 (1) din Decizia nr. 512/2013).



Autoritatea Națională pentru Administrare și Reglementare în Comunicații
Str. Delea Nouă nr.2, Sector 3, 030925 București, România
Tel: +40 372 845 400 / 0372 845 454; Fax: +40 372 845 402; e-mail: ancom@ancom.org.ro