



Raport

**privind incidentele care au afectat securitatea și integritatea
rețelelor și serviciilor de comunicații electronice în anul 2012**

Cuprins

1. INTRODUCERE	3
2. RAPORTAREA INCIDENTELOR CARE AU AFECTAT SECURITATEA ȘI INTEGRITATEA REȚELELOR ȘI SERVICIILOR DE COMUNICAȚII ELECTRONICE ÎN ANUL 2012	3
3. ANALIZA INCIDENTELOR RAPORTATE.....	4
3.1 IMPACT ASUPRA SERVICIILOR SI UTILIZATORILOR.....	4
3.2 CAUZELE INCIDENTELOR RAPORTATE	6
3.3 DURATA INCIDENTELOR ȘI DURATA DE DESCOPERIRE A INCIDENTELOR	7
3.4 IMPACT ASUPRA APELURILOR DE URGENȚĂ.....	9
4. ACȚIUNI DE RĂSPUNS LA INCIDENT	9
5. COMPARAȚIE ÎNTRE RAPORTAREA INCIDENTELOR DIN 2012 ȘI RAPORTAREA INCIDENTELOR DIN 2011.....	10
6. CONCLUZII.....	11
6.1 CONCLUZII PRIVIND ANALIZA INCIDENTELOR.....	12
6.2 CONCLUZII PRIVIND DEFICIENȚELE DE RAPORTARE	12

1. Introducere

În vederea asigurării unui sistem de comunicații fiabil și sigur prin intermediul rețelelor de comunicații electronice, potrivit dispozițiilor art. 46 din Ordonanța de urgență a Guvernului nr. 111/2011 privind comunicațiile electronice aprobată, cu modificări și completări, prin Legea nr. 140/2012, furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului trebuie să adopte și să implementeze toate măsurile adecvate, de ordin tehnic sau organizatoric, în vederea administrării riscurilor la adresa securității și integrității rețelelor și serviciilor de comunicații electronice. În cadrul acestui raport, 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.

De asemenea, conform dispozițiilor art. 47 alin. (1) din Ordonanța de urgență a Guvernului nr. 111/2011, „(1) Furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului au obligația de a notifica ANCOM, în cel mai scurt timp, cu privire la orice încălcare a securității sau pierdere a integrității care are un impact semnificativ asupra furnizării rețelelor sau serviciilor”.

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 incidentelor, ANCOM poate urmări eficiența măsurilor de securitate adoptate de furnizori, precum și a răspunsului acestora în momentul producerii incidentelor, poate colecta date referitoare la tipurile de amenințări și vulnerabilități ce vor fi utilizate în cadrul unei analize aprofundate a securității rețelelor și serviciilor, constituind o bază pentru emiterea de recomandări și ghiduri de bune practici.

2. Raportarea incidentelor care au afectat securitatea și integritatea rețelelor și serviciilor de comunicații electronice în anul 2012

În vederea evaluării incidentelor ce au afectat securitatea și integritatea rețelelor sau serviciilor, în ianuarie 2013, ANCOM a transmis furnizorilor de rețele și servicii de comunicații electronice un chestionar privind incidentele cu impact semnificativ asupra securității și integrității rețelelor și serviciilor de comunicații electronice din anul 2012. Un incident cu impact semnificativ a fost definit acel incident care afectează un număr mai mare de 5.000 de conexiuni timp de cel puțin o oră. Chestionarul este inclus în Anexa 1 la prezentul raport și a fost transmis tuturor furnizorilor care au raportat autorității că, la data de 30 iunie 2012, au furnizat un număr mai mare de 5.000 de conexiuni.

Astfel, ANCOM a solicitat informații referitoare la:

- data și ora la care s-a produs incidentul, respectiv la care s-a descoperit incidentul;
- serviciul/serviciile a căror furnizare a fost afectată de incident;
- numărul total de conexiuni afectate de incident pentru fiecare serviciu afectat în parte;
- 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.

La solicitarea Autorității au răspuns 44 de furnizori de rețele și servicii de comunicații electronice (totalizând mai mult de 90% din piața de comunicații electronice în funcție de veniturile înregistrate în anul 2012). 10 furnizori au raportat 165 incidente care au afectat un număr mai mare de 5.000 de conexiuni timp de cel puțin 60 de minute în anul 2012 și 34 de furnizori au raportat că nu au înregistrat incidente care să se încadreze în pragurile specificate.

3. Analiza incidentelor raportate

Cele 165 de incidente raportate de către cei 10 furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului au fost centralizate, catalogate și apoi analizate din 4 puncte de vedere:

1. Impact asupra serviciilor și utilizatorilor:
 - Conexiuni afectate,
 - Servicii afectate,
 - Resurse afectate.
2. Cauzele incidentelor raportate,
3. Durata incidentelor și durata de descoperire,
4. Impact asupra apelurilor de urgență.

Cele mai multe incidente raportate fac parte din categoria cauză externă/parte terță. Marea majoritate a celor 64 de incidente din această categorie au fost cauzate de întreruperile din rețeaua de alimentare cu energie electrică și secționarea accidentală a cablurilor de către părți terțe.

Din categoria eroare de sistem fac parte 61 de incidente ce au fost cauzate, în principal, de erori software și defectări hardware ce au afectat BTS-uri, servere, centre de comutație, etc.

13 din incidentele raportate au fost cauzate de acțiuni rău intenționate. Toate acestea se datorează furturilor cablurilor de cupru și vandalizărilor fibrei optice. În marea majoritate a cazurilor, aceste incidente au afectat serviciile de telefonie fixă și accesul la internet prin conexiuni permanente la punct fix.

În 2012 au fost raportate și 22 de incidente datorate fenomenelor naturale care au cauzat întreruperi în rețeaua de alimentare cu energie electrică.

3.1. Impact asupra serviciilor și utilizatorilor

Numărul mediu de conexiuni afectate de un incident din 2012 este de 72.224 de conexiuni.

În figura 1 este prezentat numărul de conexiuni afectate per serviciu. Se poate observa faptul că serviciile de transmisiuni de date SMS au fost cele mai afectate în anul 2012.

Trebuie menționat faptul că cifrele privind conexiunile afectate sunt estimative deoarece unii furnizori fie nu au furnizat date exacte privind numărul de conexiuni afectate precizând doar că au fost afectate anumite servicii fie au specificat doar că au fost afectate peste 5.000 de conexiuni.

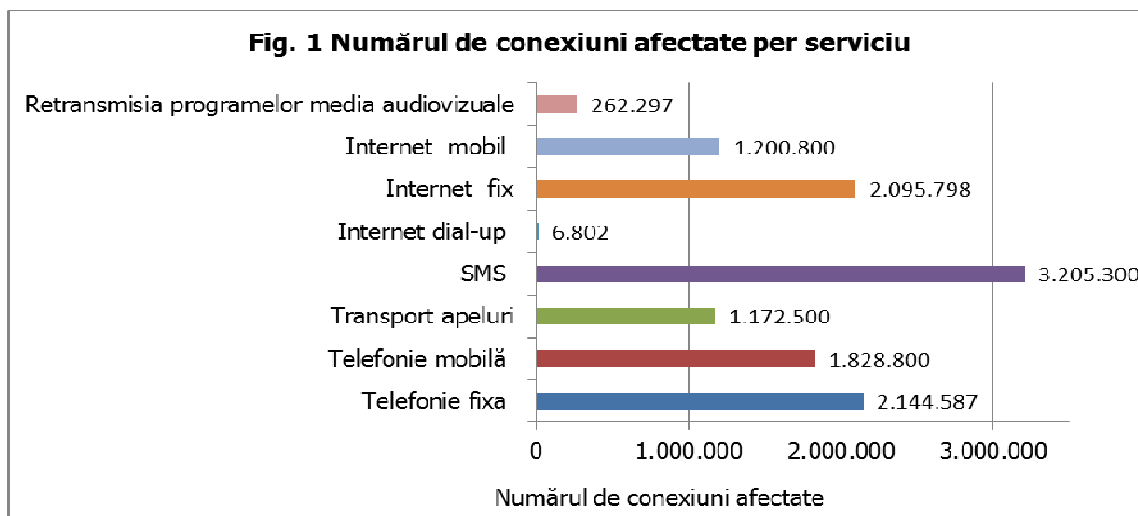


Figura 2 prezintă numărul de incidente care au afectat fiecare serviciu. A se nota faptul că unele incidente afectează două sau mai multe servicii.

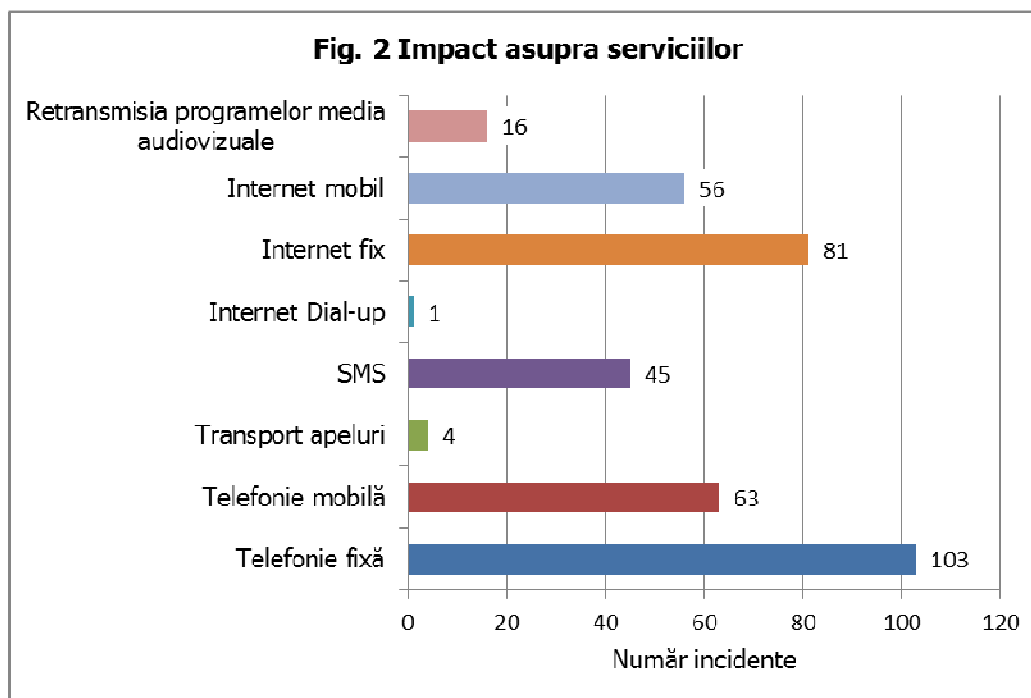
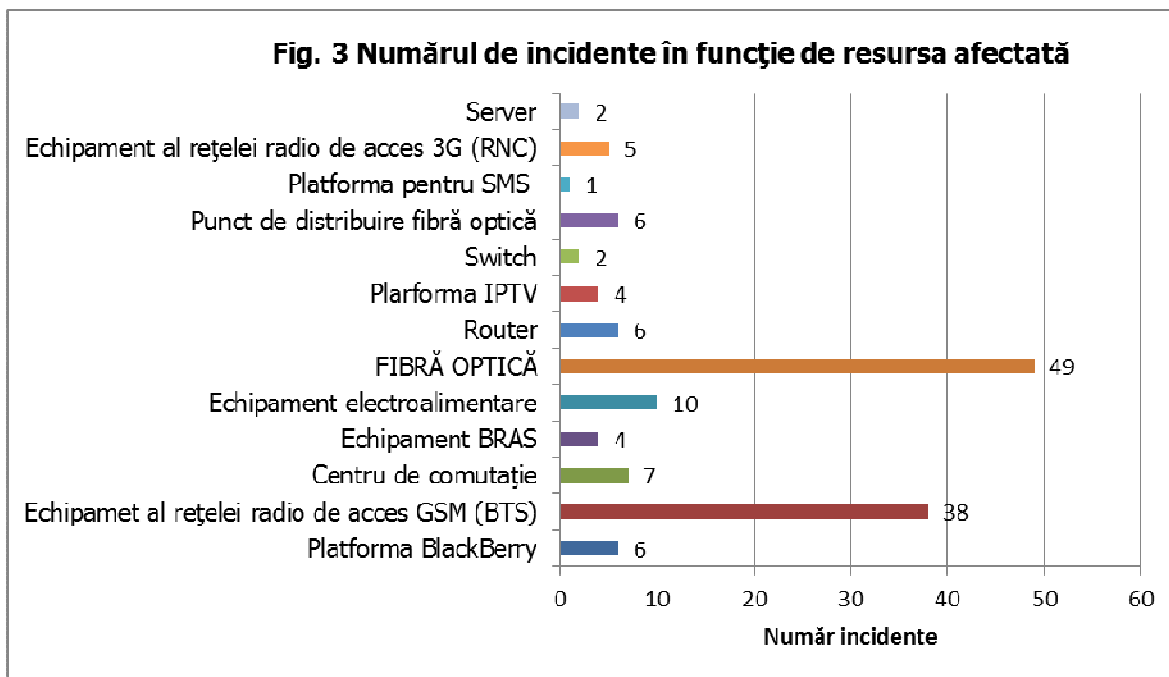


Figura 3 prezintă impactul incidentelor din 2012 asupra resurselor. Graficul prezintă numărul de incidente per resursă afectată.



În cazul a 25 de incidente nu se cunosc informații privind resursele afectate de incident datorită raportării incomplete de către furnizor.

3.2. Cauzele incidentelor raportate

Cauza unui incident reprezintă evenimentul sau factorul care declanșează incidentul. ANCOM a identificat 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.

Incidentele provocate de părți externe au fost cauzate de distrugerea unor echipamente și cabluri în urma unor lucrări de construcție și de defecțiuni în rețeaua de distribuție a energiei electrice cauzate de părți terțe.

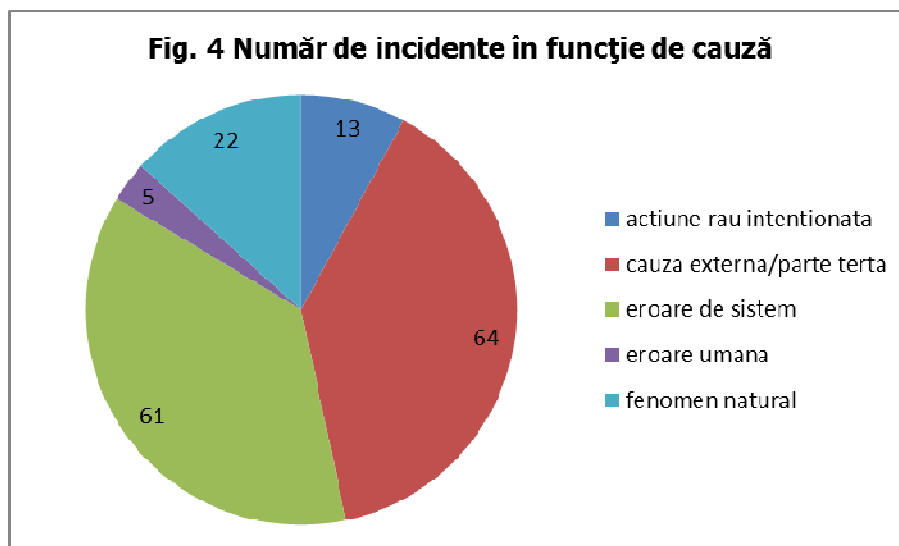
Incidentele cauzate de erori de sistem au fost de tipul erori software, dispozitive hardware blocate sau defectate, erori de configurare, congestii în rețea, etc.

În categoria acțiune rău intenționată au fost încadrate incidentele cauzate de acțiunile efectuate în mod deliberat (ex.: furt de cablu de cupru, secționare cablu fibră optică).

Incidentele cauzate de fenomene naturale sunt, în principal, datorate căderilor masive de zăpadă din lunile de iarnă. Tot printre acestea se numără și câteva cazuri în care rozătoarele au distrus cabluri ale furnizorilor afectați.

În categoria eroare umană au fost încadrate incidente cauzate de operarea și configurarea defectuoasă a echipamentelor, sistemelor și utilităților.

Figura 4 prezintă numărul de incidente raportate pentru anul 2012 în funcție de cauză.

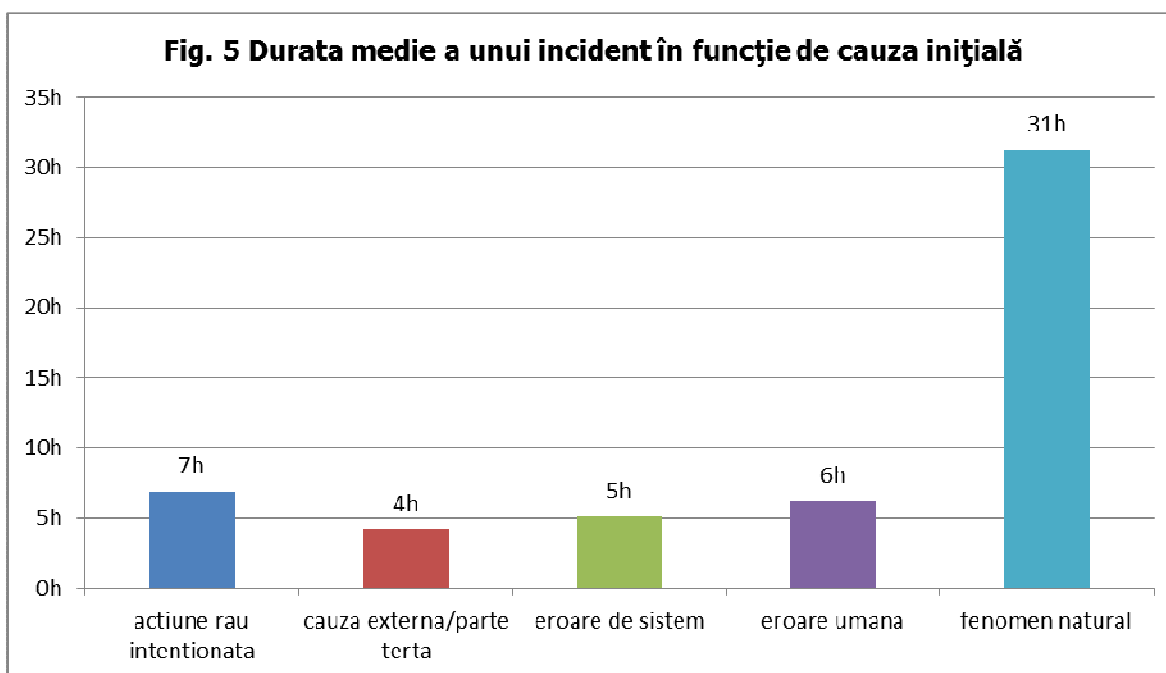


Majoritatea incidentelor au fost cauzate de părți terțe și erori de sistem.

3.3. Durata incidentelor și durata de descoperire a incidentelor

Durata totală a incidentelor raportate pe anul 2012 este de 1.428 ore și durata medie a unui incident este de 8,65 ore.

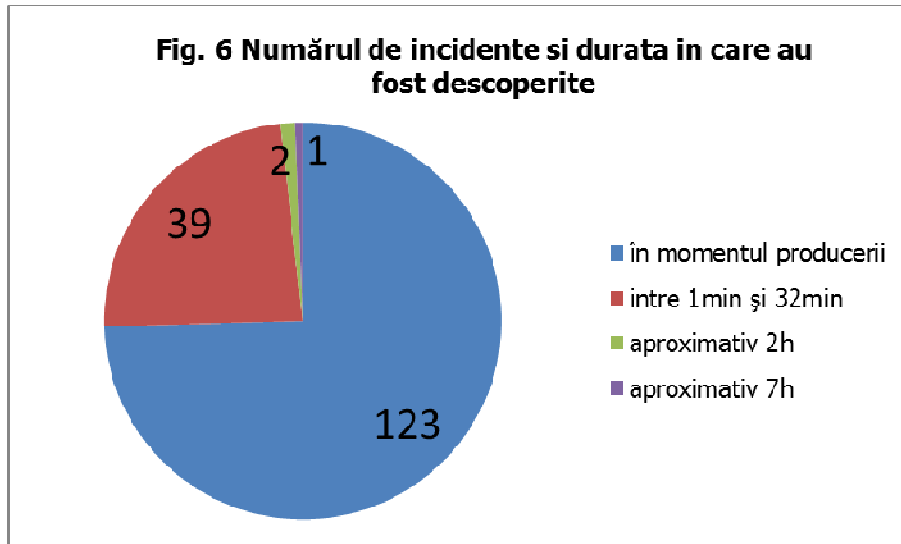
În figura 5 este prezentată durata medie a unui incident în funcție de cauza inițială. Se poate observa din grafic că incidentele cauzate de fenomene naturale au o durată mult mai mare decât oricare alt tip de incident. Acest fapt se datorează în principal căderilor masive de zăpadă din lunile de iarnă, care fac accesul către site-urile afectate foarte dificil sau chiar împiedică pentru o anumită perioadă de timp accesul la acestea.



Din cele 165 de incidente raportate în anul 2012:

- 123 de incidente au fost descoperite în momentul în care au avut loc,
- 39 au fost descoperite între 1 și 32 de minute,
- 2 incidente în aproximativ 2 ore și
- Un incident în aproximativ 7 ore de la momentul producerii lui.

Situația este ilustrată în figura 6.



În figura 7 este prezentat graficul celor 39 de incidente ce au înregistrat întârzieri de descoperire între 1 și 32 de minute.

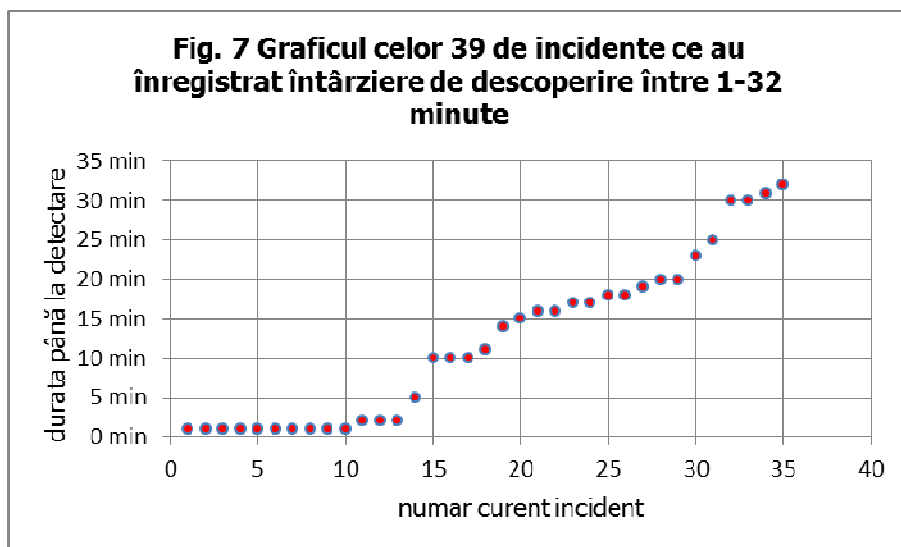
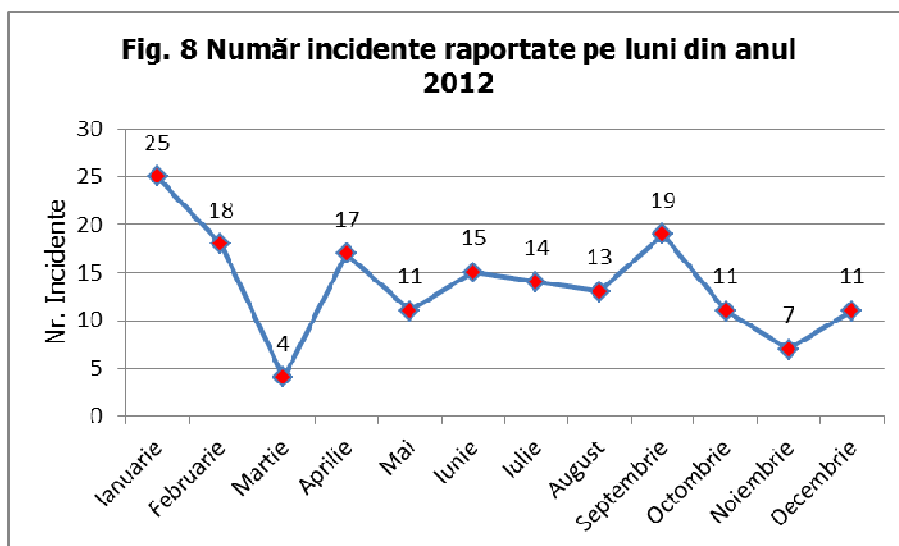
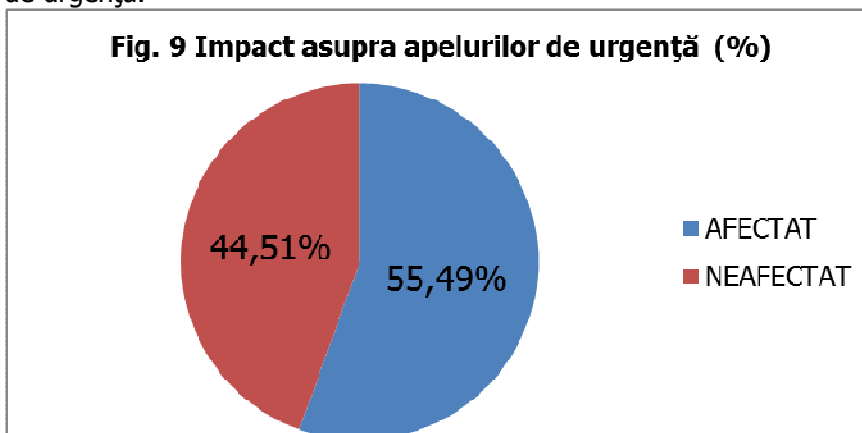


Figura 8 prezintă distribuția incidentelor pe lunile anului 2012. Se poate observa că în luna ianuarie au fost înregistrate cele mai multe incidente. 26 din totalul de 165 de incidente raportate pe anul 2012 au avut loc în luna ianuarie datorită condițiilor meteorologice nefavorabile.



3.4. Impact asupra apelurilor de urgență

55,49% din incidentele raportate în anul 2012 au avut un posibil impact asupra efectuării apelurilor de urgență. Figura 9 prezintă procentul incidentelor care au avut un posibil impact asupra apelurilor de urgență.



Datorită procentului mare de incidente care au afectat serviciile de telefonie fixă și telefonie mobilă rezultă, de asemenea, un procent mare de incidente care au afectat apelurile de urgență. Trebuie menționat că, în cazul rețelelor mobile, atunci când se produce un incident care a afectat furnizarea serviciilor, un utilizator poate apela numărul unic pentru apelurile de urgență dacă zona în care se află acesta este acoperită de alt furnizor de servicii de telefonie mobilă.

4. Acțiuni de răspuns la incident

Remediarea problemelor apărute în urma incidentelor și restabilirea serviciilor furnizate către utilizatorii finali implică un răspuns prompt din partea furnizorilor. Astfel, în condiții normale, furnizorii urmăresc să remedieze problemele apărute într-un interval de timp cât mai scurt astfel încât să-și îndeplinească obligațiile contractuale față de clienți.

Acțiunile de răspuns luate pentru remedierea problemelor apărute în urma incidentelor au constat în:

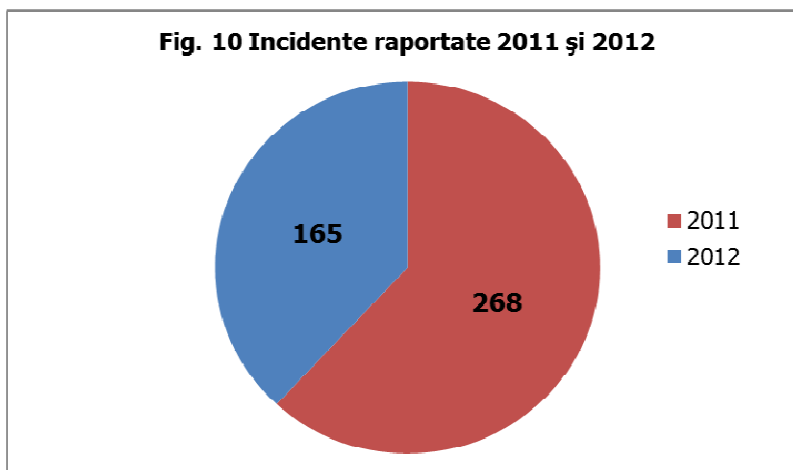
- refacerea infrastructurii fizice prin înlocuirea cablurilor și echipamentelor sustrate sau deteriorate,
- reconectarea echipamentului de transmisie la curent electric prin intervenții cu grup electrogen,
- acțiuni de restaurare și troubleshooting,
- reconfigurări și reinițializări de echipamente, etc.

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 rețelilor sau a serviciilor de comunicații electronice. Măsurile de securitate sunt dedicate protecției resurselor (hardware, software, informații etc.), constituind practici/metode prin care vulnerabilitățile și amenințările se elimină sau se previn, se descoperă și se raportează în scopul acțiunilor corective, minimizându-se efectele negative pe care le pot produce.

Astfel de măsuri pot fi preventive, corective sau de detectare. Măsurile preventive reduc vulnerabilitățile și probabilitatea de apariție a unui incident, implementarea lor conducând de exemplu la insuccesul unui potențial atac. Măsurile corective reduc impactul/efectele unui incident și restabilesc funcționarea/operarea în condiții normale. Măsurile de detectare descoperă incidente/atacuri și activează măsuri preventive sau corective. Fiecare incident trebuie analizat de furnizor și măsurile de securitate trebuie actualizate periodic pentru a elimina sau minimiza efectele acestuia.

5. Comparație între raportarea incidentelor din 2012 și raportarea incidentelor din 2011

Figura 10 prezintă numărul total de incidente raportate în 2012 în comparație cu numărul total de incidente raportate în 2011.



Se poate observa, în anul 2012, o scădere a numărului de incidente semnificative raportate de către furnizori. Aceasta poate fi datorită unor deficiențe în raportare sau unor măsuri de securitate mai stricte implementate de furnizori.

Figura 11 prezintă comparația dintre numărul de incidente din 2011 și 2012 în funcție de cauză.

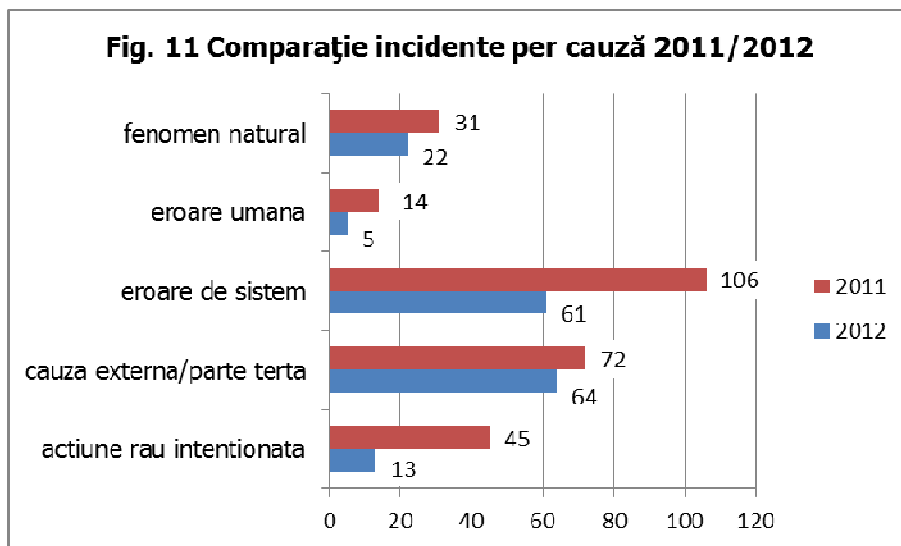
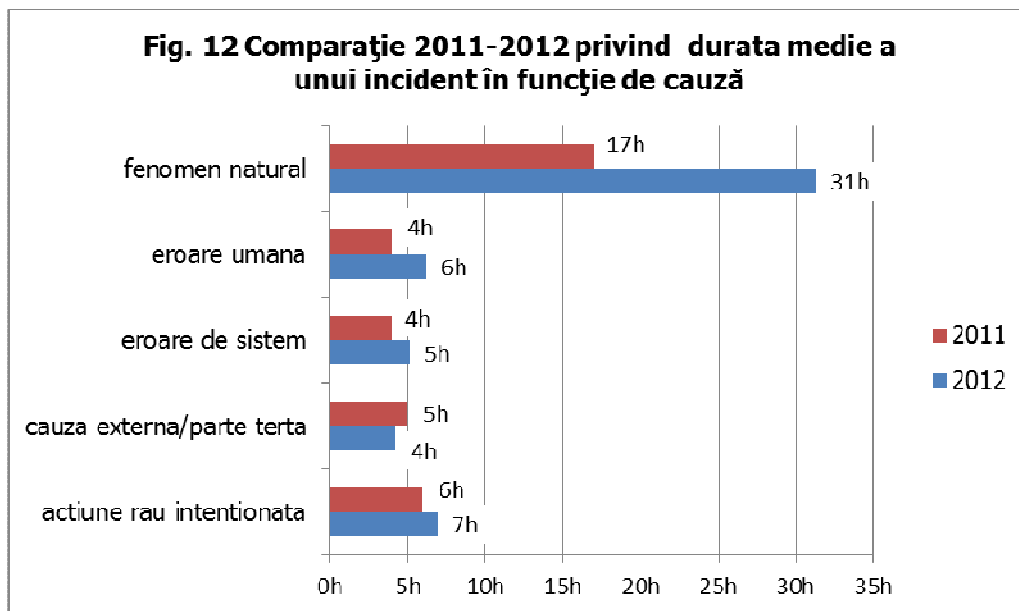


Figura 12 prezintă o comparare între 2011 și 2012 a duratei medii a unui incident în funcție de cauză. Se poate observa faptul că durata medie a unui incident cauzat de fenomene naturale s-a dublat în 2012 față de 2011.



6. Concluzii

Prin analizarea incidentelor cu impact semnificativ asupra rețelelor și serviciilor de comunicații electronice, ANCOM poate identifica 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. Analizele statistice ale incidentelor constituie, de asemenea, un instrument eficient de a urmări tendințele.

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.

6.1. Concluzii privind analiza incidentelor

Acest raport prezintă o imagine de ansamblu asupra incidentelor raportate în anul 2012. În urma centralizării, catalogării și analizării celor 165 de incidente raportate de către cei 10 furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului se pot trage următoarele concluzii:

- Marea majoritate a incidentelor au afectat serviciile de telefonie furnizate prin intermediul unor rețele publice fixe sau cu mobilitate limitată (103 incidente) și servicii de acces la internet prin conexiuni permanente la punct fix (81 incidente).
- Serviciul cel mai afectat din punct de vedere al numărului de conexiuni este serviciul de transmisiuni de date – SMS (aproximativ 3.205.300 conexiuni afectate).
- Resursele cele mai afectate de incidente au fost tronsoanele de fibră optică și BTS-uri din rețelele mobile.(49 de incidente în care au fost afectate tronsoane de fibră optică și 38 de cazuri în care au fost temporar inactive BTS-uri).
- 39% din incidente au avut cauze externe/părți terțe și 37% din incidente au fost cauzate de erori de sistem.
- Incidentele cauzate de fenomene naturale au o durată mult mai mare decât oricare alt tip de incident (s-a înregistrat o durată medie de 31 ore).
- 75% din incidente au fost descoperite instantaneu iar restul de 25% au fost descoperite ulterior producerii. Astfel, 39 de incidente au fost descoperite într-un interval cuprins între 1 și 32 minute și numai 3 incidente au fost descoperite într-o perioadă mai lungă, respectiv în 2 ore, 2 ore și 12min și 7 ore.
- Luna ianuarie a înregistrat cele mai multe incidente (15% din incidente).
- În 55,5% din cazuri incidentele au afectat total sau parțial efectuarea apelurilor de urgență.

6.2. Concluzii privind deficiențele de raportare

Scopul principal al schemei de raportare este de a primi informații complete, corecte și comparabile asupra incidentelor care au un impact semnificativ asupra securității și integrității rețelelor și serviciilor de comunicații electronice.

În urma analizării tuturor celor 165 de formulare completate de către furnizorii care au raportat incidente pe anul 2012 s-au constatat mai multe deficiențe.

Una dintre cele mai importante deficiențe este necompletarea numărului de conexiuni afectate pentru fiecare serviciu afectat. Completând un singur număr la capitolul „Numărul de conexiuni afectate de incident per serviciu” nu este clar dacă acel număr reprezintă suma numărului de conexiuni afectate pentru toate serviciile sau în cazul tuturor serviciilor a fost afectat același număr de conexiuni.

Câțiva dintre furnizori nu au estimat numărul de conexiuni afectate specificând fie doar serviciul afectat fie doar că au fost afectate peste 5.000 de conexiuni (5.000 de conexiuni afectate fiind pragul de raportare).

Formatul de introducere a datei de către furnizorul afectat a făcut dificilă, în unele cazuri, centralizarea raportărilor (au fost cazuri în care s-a folosit formatul zz.ll.aaaa și altele în care s-a folosit formatul ll.zz.aaaa fără a se specifica ce format s-a folosit).

În ceea ce privește resursele afectate, unele răspunsuri sunt prea punctuale iar altele sunt prea generale. Astfel, se vor revizui instrucțiunile de completare a formularului pentru a fi mai clar ce elemente trebuie completate la raportarea de către furnizori.

Majoritatea furnizorilor nu au completat câmpurile privind măsurile luate sau planificate pentru a împiedica producerea unui incident similar/eliminarea cauzei incidentului. Menționăm faptul că analiza incidentelor de către furnizor trebuie să conducă la revizuirea, actualizarea și îmbunătățirea măsurilor de securitate implementate de furnizor pentru a elimina sau a reduce riscurile privind producerea unor incidente asemănătoare pe viitor.

Conform proiectului de decizie al președintelui Autorității Naționale pentru Administrare și Reglementare în Comunicații privind stabilirea măsurilor minime de securitate ce trebuie luate de către furnizorii de rețele și servicii de comunicații electronice și raportarea incidentelor cu impact semnificativ asupra furnizării rețelelor și serviciilor de comunicații electronice, furnizorii au obligația de a raporta incidentele cu impact semnificativ (care afectează un număr mai mare de 5.000 de conexiuni timp de cel puțin o oră) asupra securității și integrității rețelelor și serviciilor de comunicații electronice, inclusiv prin identificarea cauzelor incidentelor, precum și a acțiunilor de răspuns la incidente, a măsurilor luate sau planificate pentru a împiedica producerea unor incidente similare sau pentru eliminarea cauzei incidentelor. Astfel, pentru o raportare cât mai corectă, trebuie să existe o monitorizare permanentă a raportărilor furnizorilor, inclusiv prin aplicarea unor sancțiuni în cazul în care nu sunt furnizate în mod complet și corect informațiile solicitate de ANCOM referitoare la incidentele cu impact semnificativ asupra furnizării rețelelor și serviciilor de comunicații electronice.

FORMULAR DE RAPORTARE A INCIDENTELOR CARE AU AFECTAT SECURITATEA ȘI INTEGRITATEA REȚELELOR ȘI SERVICIILOR DE COMUNICAȚII ELECTRONICE	
1. Furnizor:	
2. Data și ora	
2.1 Data și ora la care s-a produs incidentul	Data: _____ Ora: _____
2.2 Data și ora la care s-a descoperit incidentul	Data: _____ Ora: _____
3. Impactul incidentului și tipul cauzei	
3.1 Serviciul/serviciile afectate:	
<input type="checkbox"/> Servicii de telefonie destinate publicului: <input type="checkbox"/> Servicii de telefonie furnizate prin intermediul unor rețele publice fixe sau cu mobilitate limitată <input type="checkbox"/> Servicii de telefonie furnizate prin intermediul unor rețele publice mobile terestre <input type="checkbox"/> Servicii de telefonie furnizate prin intermediul unor rețele publice cu transmisie prin satelit <input type="checkbox"/> Servicii de transport apeluri <input type="checkbox"/> Servicii de linii închiriate <input type="checkbox"/> Servicii de transmisiuni de date (inclusiv VPN): <input type="checkbox"/> La puncte fixe <input type="checkbox"/> Cu mobilitate limitată <input type="checkbox"/> SMS (numai în cazul rețelelor celulare) <input type="checkbox"/> Mobil (inclusiv MVNO) <input type="checkbox"/> Servicii de acces la Internet: <input type="checkbox"/> Dial-up (numai pentru bucla locală) <input type="checkbox"/> Conexiuni permanente la punct fix <input type="checkbox"/> Conexiuni radio mobile (inclusiv MVNO) <input type="checkbox"/> Retransmisia serviciilor de programe media audiovizuale liniare către utilizatorii finali: <input type="checkbox"/> Cu acces fix prin satelit (tip DTH) <input type="checkbox"/> Cu acces mobil prin satelit (tip S-DAB/DVB-S) <input type="checkbox"/> Terestre cu acces la punct fix tip CATV, DVB-C/Mx, IPTV etc. <input type="checkbox"/> Terestre dedicate tip T-DAB/DVB-T <input type="checkbox"/> Radio Celulare Publice (tip Mobile TV) <input type="checkbox"/> Alte servicii de comunicații electronice <input type="checkbox"/> Servicii de radiocomunicații mobile profesionale <input type="checkbox"/> Comunicații voce <input type="checkbox"/> Mesagerie radio <input type="checkbox"/> Transmisii de date, telex <input type="checkbox"/> Localizare, poziționare <input type="checkbox"/> Alte tipuri de servicii <input type="checkbox"/> Servicii de comunicații electronice care permit servicii de voce <input type="checkbox"/> Servicii de comunicații electronice care permit accesul la servicii de conținut <input type="checkbox"/> Alte tipuri de servicii decât cele de mai sus	

3.2 Parametrii de impact:

Numărul de conexiuni afectate de incident per serviciu:

Resursele/echipamentele afectate:

Durata incidentului:

Aria/răspândirea geografică:

Impactul asupra apelurilor de urgență:

3.3 Descrierea incidentului:**3.4 Tipul cauzei incidentului:**

- Eroare umană
- Eroare de sistem
- Fenomen natural
- Acțiune rău intenționată
- Cauză externă/parte terță

3.5 Mai multe informații despre cauza incidentului:**4. Alte informații despre incident****4.1 Acțiuni de răspuns la incident (inclusiv momentul când au fost luate):**

4.2 Măsurile luate sau planificate pentru a împiedica producerea unui incident similar/eliminarea cauzei incidentului (inclusiv momentul când au fost/vor fi luate):

4.3 Alți furnizori de rețele și servicii de comunicații electronice afectați:

4.4 Alte observații: