ANCOM
Autoritatea Naţională pentru Administrare
şi Reglementare în Comunicaţii

Str. Delea Nouă nr.2, Sector 3, 030925 Bucureşti, România
Telefon: 0372 845 400 / 0372 845 454. Fax: 0372 845 402
E-mail: ancom@ancom.org.ro. Website: www.ancom.org.ro

Raport

privind incidentele care au afectat securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice în anul 2012

Cuprins

1. Introducere

În vederea asigurării unui sistem de comunicaţii fiabil şi sigur prin intermediul reţelelor de comunicaţii electronice, potrivit dispoziţiilor art. 46 din Ordonanţa de urgenţă a Guvernului nr. 111/2011 privind comunicaţiile electronice aprobată, cu modificări şi completări, prin Legea nr. 140/2012, furnizorii de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului trebuie să adopte şi să implementeze toate măsurile adecvate, de ordin tehnic sau organizatoric, în vederea administrării riscurilor la adresa securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice. În cadrul acestui raport, securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice reprezintă capacitatea unei reţele sau a unui serviciu de comunicaţii electronice de a rezista evenimentelor, accidentale sau rău intenţionate, care pot compromite sau afecta continuitatea furnizării reţelelor şi serviciilor, la un nivel de performanţă echivalent cu cel anterior producerii evenimentului.

De asemenea, conform dispoziţiilor art. 47 alin. (1) din Ordonanţa de urgenţă a Guvernului nr. 111/2011, „(*1) Furnizorii de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului au obligaţia de a notifica ANCOM, în cel mai scurt timp, cu privire la orice încălcare a securităţii sau pierdere a integrităţii care are un impact semnificativ asupra furnizării reţelelor sau serviciilor*".

Datele privind incidentele sunt fundamentale pentru dezvoltarea unei înţelegeri clare a naturii şi amplorii provocărilor existente la adresa securităţii şi integrităţii reţelelor şi serviciilor. Prin analiza incidentelor, ANCOM poate urmări eficienţa măsurilor de securitate adoptate de furnizori, precum şi a răspunsului acestora în momentul producerii incidentelor, poate colecta date referitoare la tipurile de ameninţări şi vulnerabilităţi ce vor fi utilizate în cadrul unei analize aprofundate a securităţii reţelelor şi serviciilor, constituind o bază pentru emiterea de recomandări şi ghiduri de bune practici.

2. Raportarea incidentelor care au afectat securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice în anul 2012

În vederea evaluării incidentelor ce au afectat securitatea şi integritatea reţelelor sau serviciilor, în ianuarie 2013, ANCOM a transmis furnizorilor de reţele şi servicii de comunicaţii electronice un chestionar privind incidentele cu impact semnificativ asupra securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii 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 puţin o oră. Chestionarul este inclus în Anexa 1 la prezentul raport şi a fost transmis tuturor furnizorilor care au raportat autorităţii că, la data de 30 iunie 2012, au furnizat un număr mai mare de 5.000 de conexiuni.

Astfel, ANCOM a solicitat informaţii referitoare la:

- data şi 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 urgenţă;
- Descrierea incidentului;
- Tipul cauzei incidentului;
- Mai multe informaţii despre cauza incidentului;
- Acţiuni de răspuns la incident;
- Măsurile luate sau planificate pentru a împiedica producerea unui incident similar/eliminarea cauzei incidentului;
- Alţi furnizori de reţele şi servicii de comunicaţii electronice afectaţi.

La solicitarea Autorităţii au răspuns 44 de furnizori de reţele şi servicii de comunicaţii electronice (totalizând mai mult de 90% din piaţa de comunicaţii electronice în funcţie 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 puţin 60 de minute în anul 2012 şi 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 reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului au fost centralizate, catalogate şi apoi analizate din 4 puncte de vedere:

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

Cele mai multe incidente raportate fac parte din categoria cauză externă/parte terţă. Marea majoritate a celor 64 de incidente din această categorie au fost cauzate de întreruperile din reţeaua de alimentare cu energie electrică şi secţionarea accidentală a cablurilor de către părţi terţe.

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

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

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

3.1. Impact asupra serviciilor şi 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 menţionat 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.

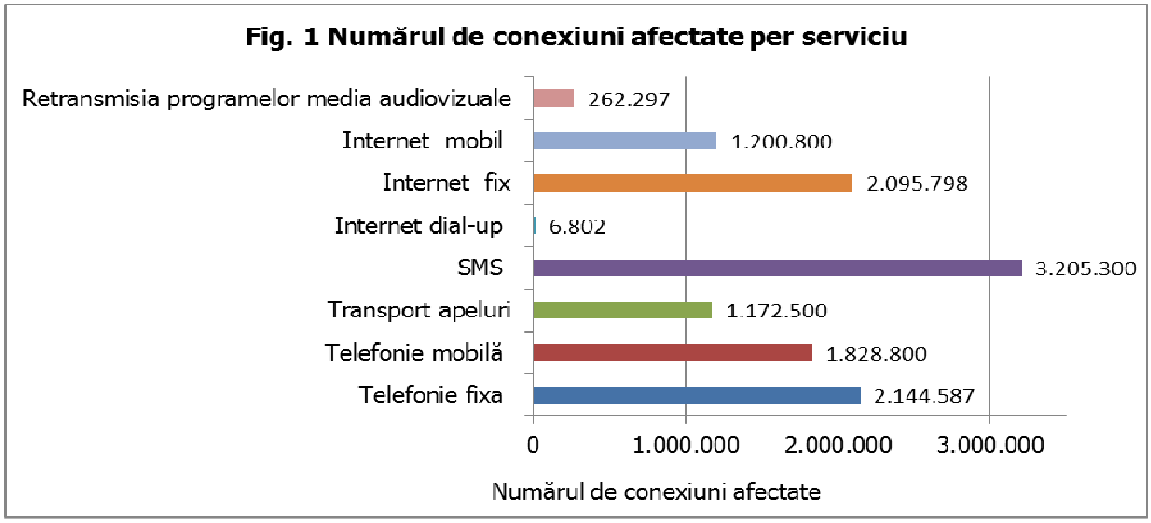


Figura 2 prezintă numărul de incidente care au afectat fiecare serviciu. A se nota faptul că unele incidente afectează două sau mai multe servicii.

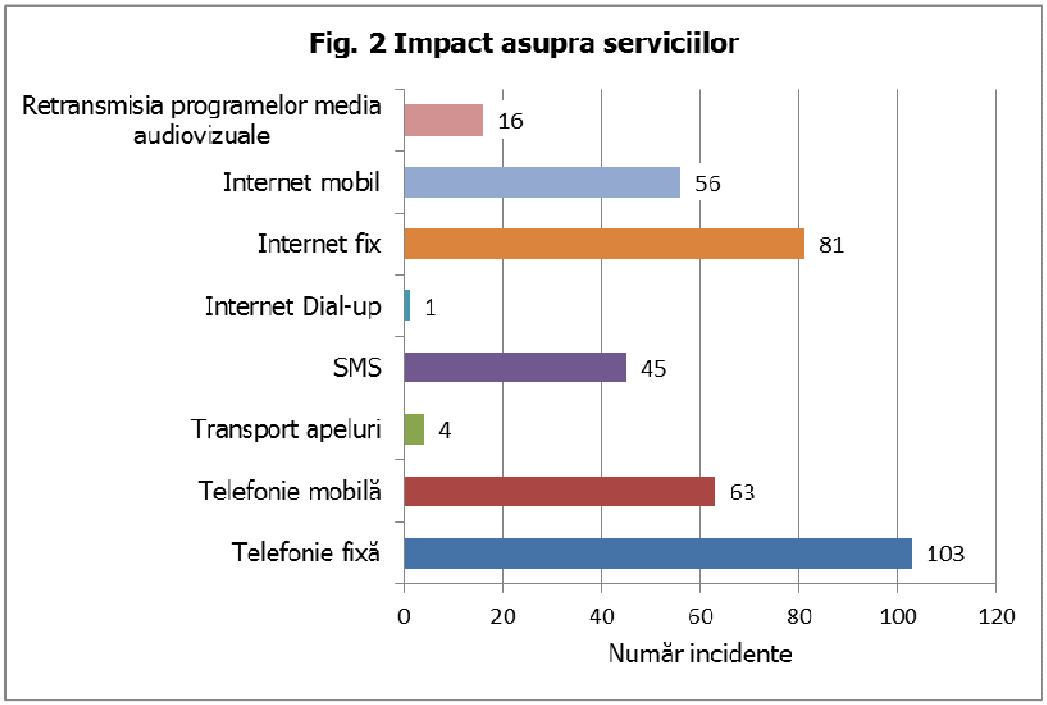
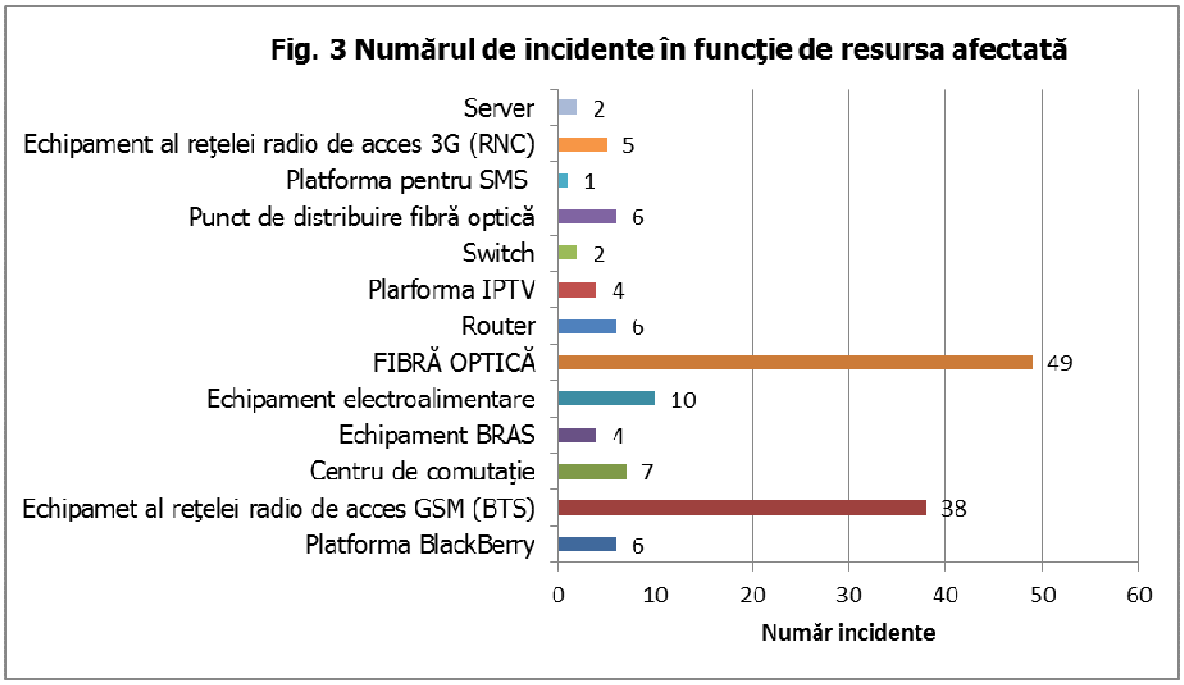


Figura 3 prezintă impactul incidentelor din 2012 asupra resurselor. Graficul prezintă numărul de incidente per resursă afectată.



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

3.2. Cauzele incidentelor raportate

Cauza unui incident reprezintă evenimentul sau factorul care declanşează incidentul. ANCOM a identificat 5 cauze ale incidentelor care afectează securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice: cauză externă/parte terţă, eroare de sistem, acţiune rău intenţionată, fenomen natural şi eroare umană.

Incidentele provocate de părţi externe au fost cauzate de distrugerea unor echipamente şi cabluri în urma unor lucrări de construcţie şi de defecţiuni în reţeaua de distribuţie a energiei electrice cauzate de părţi terţe.

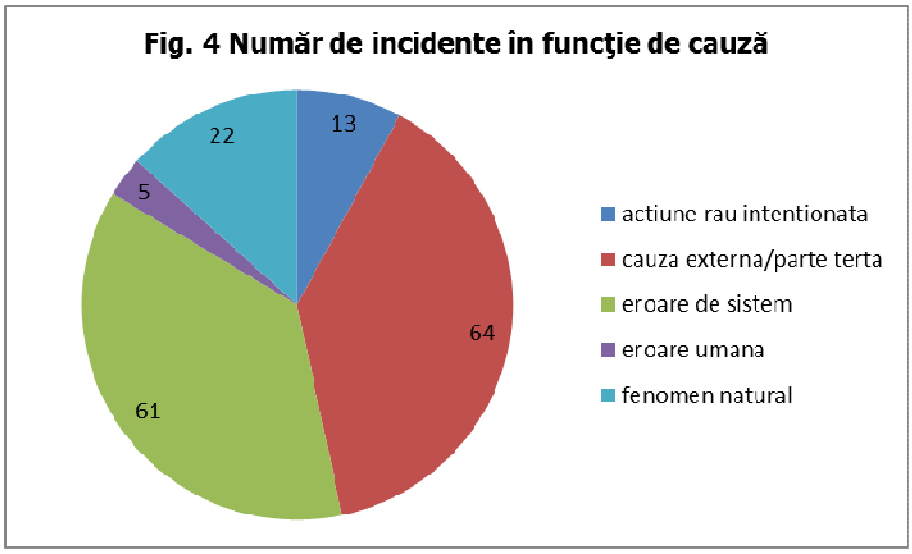
Incidentele cauzate de erori de sistem au fost de tipul erori software, dispozitive hardware blocate sau defectate, erori de configurare, congestii in reţea, etc.

În categoria acţiune rău intenţionată au fost încadrate incidentele cauzate de acţiunile 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 şi câteva cazuri în care rozătoarele au distrus cabluri ale furnizorilor afectaţi.

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

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

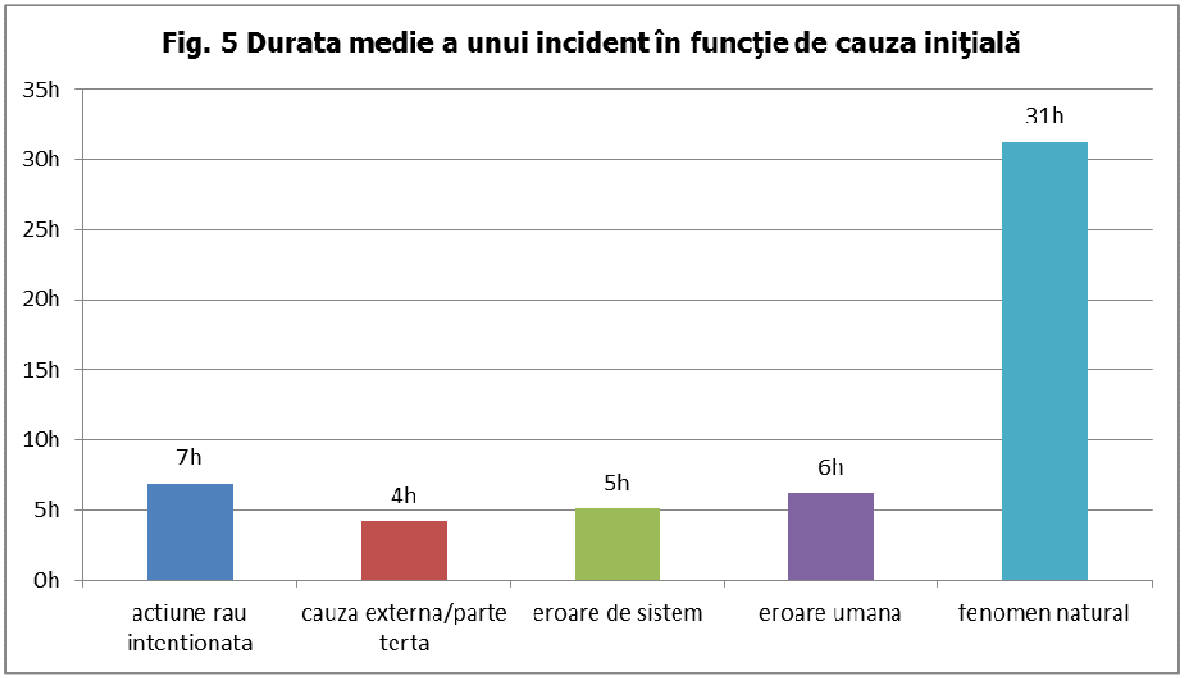


Majoritatea incidentelor au fost cauzate de părţi terţe şi erori de sistem.

3.3. Durata incidentelor şi durata de descoperire a incidentelor

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

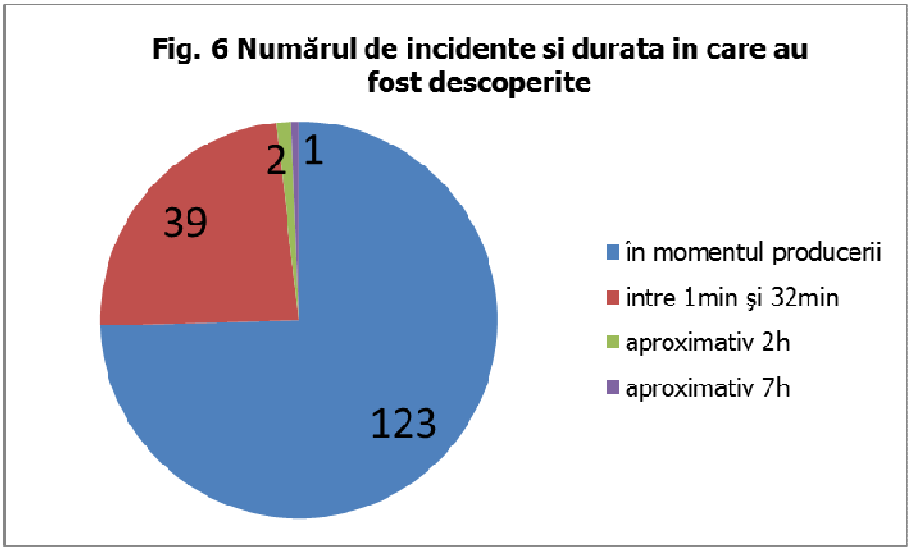
În figura 5 este prezentată durata medie a unui incident în funcţie de cauza iniţială. Se poate observa din grafic că incidentele cauzate de fenomene naturale au o durată mult mai mare decât oricare alt tip de incident. Acest fapt se datorează în principal căderilor masive de zăpadă din lunile de iarnă, 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 in momentul în care au avut loc,
- 39 au fost descoperite între 1 şi 32 de minute,
- 2 incidente în aproximativ 2 ore şi
- Un incident în aproximativ 7 ore de la momentul producerii lui.

Situaţia este ilustrată în figura 6.



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

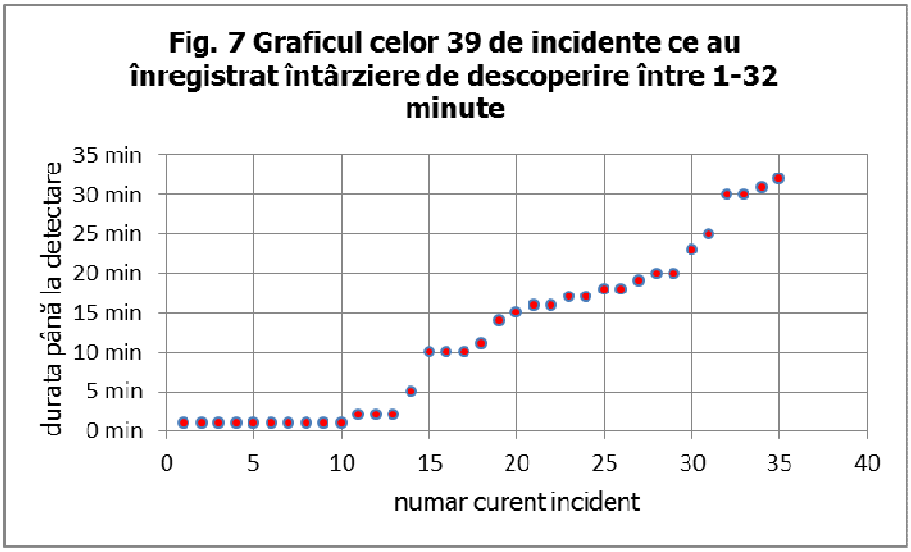
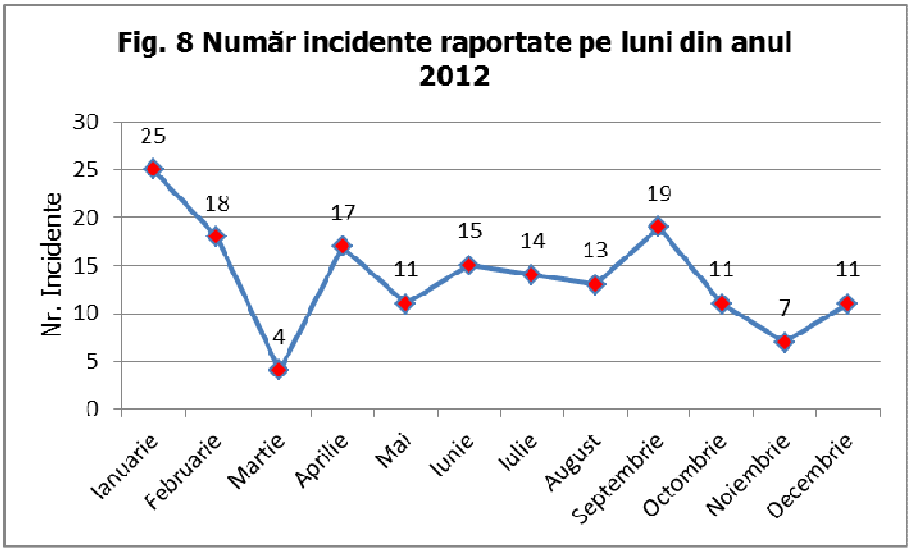
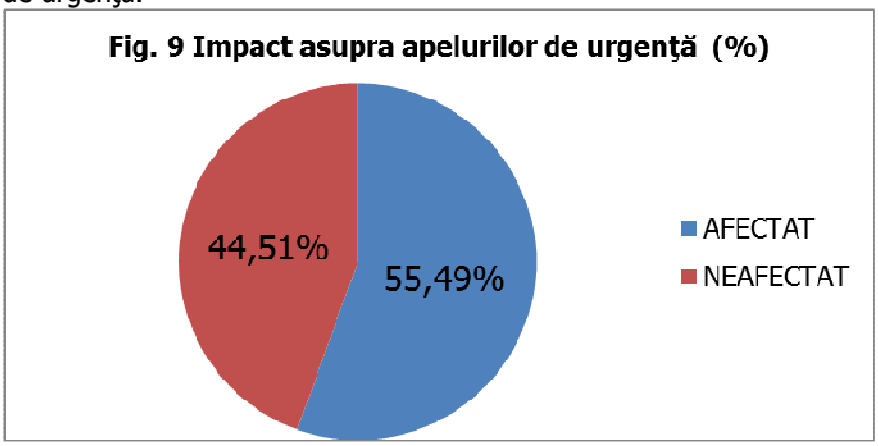


Figura 8 prezintă distribuţia incidentelor pe lunile anului 2012. Se poate observa că în luna ianuarie au fost înregistrate cele mai multe incidente. 26 din totalul de 165 de incidente raportate pe anul 2012 au avut loc în luna ianuarie datorită condiţiilor meteorologice nefavorabile.



3.4. Impact asupra apelurilor de urgenţă

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



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

4. Acţiuni de răspuns la incident

Remedierea problemelor apărute în urma incidentelor şi restabilirea serviciilor furnizate către utilizatorii finali implică un răspuns prompt din partea furnizorilor. Astfel, în condiţii normale, furnizorii urmăresc să remedieze problemele apărute într-un interval de timp cât mai scurt astfel încât să-şi îndeplinească obligaţiile contractuale faţă de clienţi.

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

- refacerea infrastructurii fizice prin înlocuirea cablurilor şi echipamentelor sustrase sau deteriorate,
- reconectarea echipamentului de transmisie la curent electric prin intervenţii cu grup electrogen,
- acțiuni de restaurare si troubleshooting,
- reconfigurări şi reiniţializări de echipamente,etc.

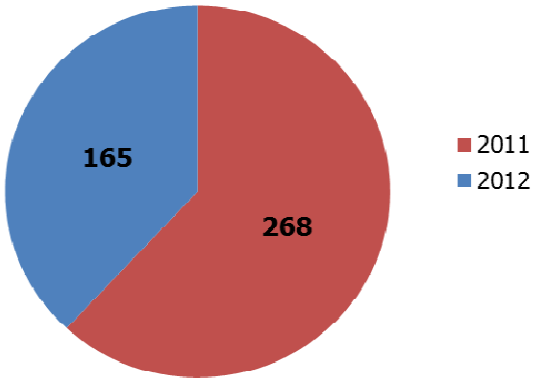
Măsurile de securitate reprezintă mijloace (de natură administrativă, tehnică, managerială sau juridică) de management al riscurilor, incluzând politici, acţiuni, planuri, echipamente, facilităţi, proceduri, tehnici etc. menite să elimine sau să reducă riscurile privind securitatea şi integritatea reţelelor sau a serviciilor de comunicaţii electronice. Măsurile de securitate sunt dedicate protecţiei resurselor (hardware, software, informaţii etc.), constituind practici/metode prin care vulnerabilităţile şi ameninţările se elimină sau se previn, se descoperă şi se raportează în scopul acţiunilor corective, minimizându-se efectele negative pe care le pot produce.

Astfel de măsuri pot fi preventive, corective sau de detectare. Măsurile preventive reduc vulnerabilităţile şi probabilitatea de apariţie a unui incident, implementarea lor conducând de exemplu la insuccesul unui potenţial atac. Măsurile corective reduc impactul/efectele unui incident şi restabilesc funcţionarea/operarea în condiţii normale. Măsurile de detectare descoperă incidente/atacuri şi activează măsuri preventive sau corective. Fiecare incident trebuie analizat de furnizor şi măsurile de securitate trebuie actualizate periodic pentru a elimina sau minimiza efectele acestuia.

5. Comparaţie între raportarea incidentelor din 2012 şi raportarea incidentelor din 2011

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

Fig. 10 Incidente raportate 2011 şi 2012



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

Figura 11 prezintă comparaţia dintre numărul de incidente din 2011 şi 2012 în funcţie de cauză.

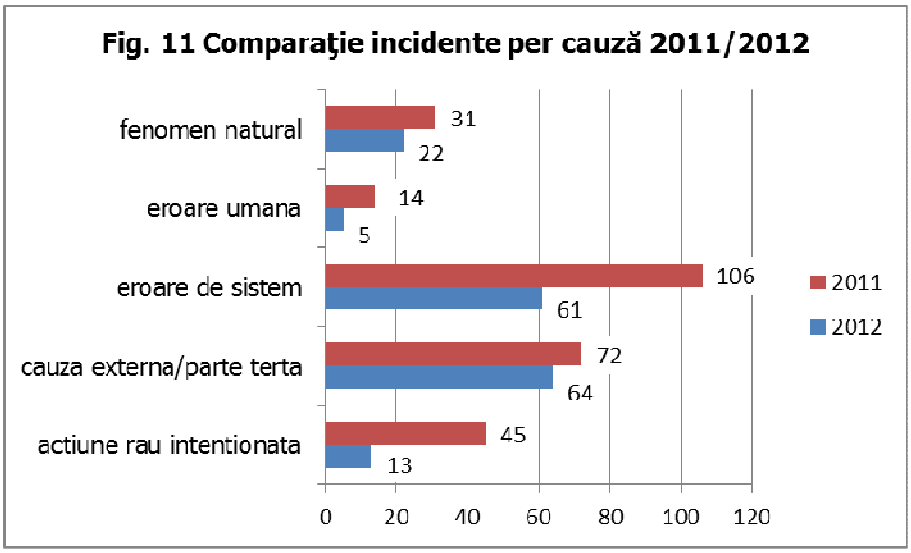
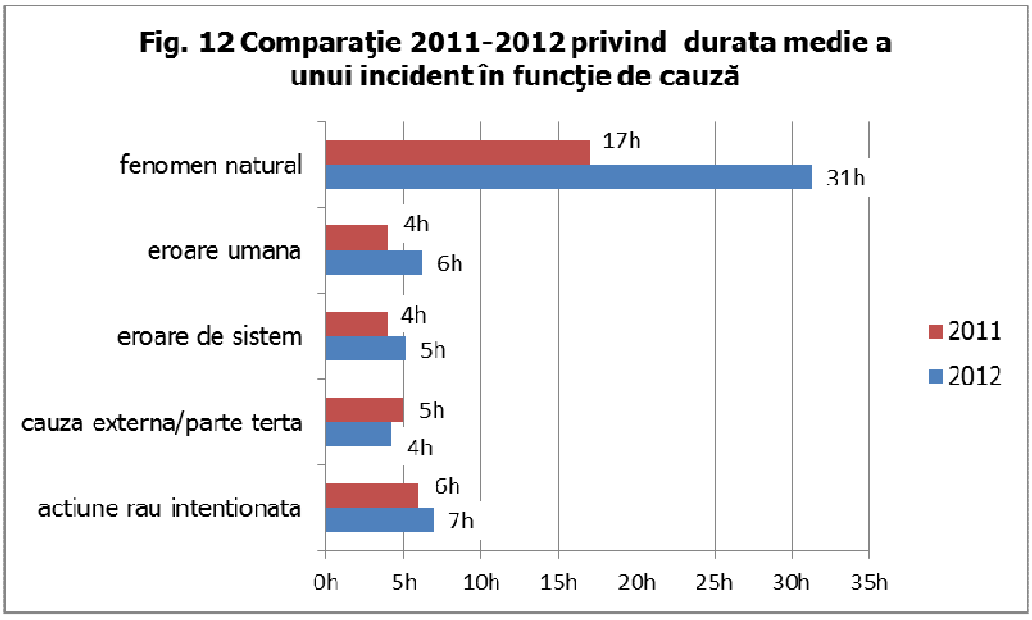


Figura 12 prezintă o comparare între 2011 şi 2012 a duratei medie a unui incident în funcţie de cauză. Se poate observa faptul că durata medie a unui incident cauzat de fenomene naturale s-a dublat în 2012 faţă de 2011.



6. Concluzii

Prin analizarea incidentelor cu impact semnificativ asupra reţelelor şi serviciilor de comunicaţii electronice, ANCOM poate identifica cauzele incidentului, poate urmări acţiunile furnizorului în vederea remedierii reţelelor şi serviciilor la un nivel corespunzător şi poate evalua nivelul de securitate al reţelelor şi serviciilor de comunicaţii electronice. Analizele statistice ale incidentelor constituie, de asemenea, un instrument eficient de a urmări tendinţele.

Datele privind incidentele sunt fundamentale pentru dezvoltarea unei înţelegeri clare a naturii şi amplorii provocărilor existente la adresa securităţii şi integrităţii reţelelor şi serviciilor prin analiza ameninţărilor şi vulnerabilităţilor la adresa securităţii şi integrităţii reţelelor şi serviciilor şi

prin identificarea de bune practici bazate pe lecţiile învăţate 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 şi analizării celor 165 de incidente raportate de către cei 10 furnizorii de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului se pot trage următoarele concluzii:

- Marea majoritate a incidentelor au afectat serviciile de telefonie furnizate prin intermediul unor reţele publice fixe sau cu mobilitate limitată (103 incidente) şi 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 şi BTS-uri din reţelele mobile.(49 de incidente în care au fost afectate tronsoane de fibră optică şi 38 de cazuri în care au fost temporar inactive BTS-uri).
- 39% din incidente au avut cauze externe/părţi terţe şi 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 întru-un interval cuprins între 1 şi 32 minute şi numai 3 incidente au fost descoperite intr-o perioadă mai lungă, respectiv în 2 ore, 2 ore şi 12min şi 7 ore.
- Luna ianuarie a înregistrat cele mai multe incidente (15% din incidente).
- În 55,5% din cazuri incidentele au afectat total sau parţial efectuarea apelurilor de urgenţă.

6.2. Concluzii privind deficienţele de raportare

Scopul principal al schemei de raportare este de a primi informaţii complete, corecte şi comparabile asupra incidentelor care au un impact semnificativ asupra securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice.

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

Una dintre cele mai importante deficienţe 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 acelaşi număr de conexiuni.

Câţiva 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 şi altele în care s-a folosit formatul ll.zz.aaaa fără a se specifica ce format s-a folosit).

În ceea ce priveşte resursele afectate, unele răspunsuri sunt prea punctuale iar altele sunt prea generale. Astfel, se vor revizui instrucţiunile 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. Menţionăm faptul că analiza incidentelor de către furnizor trebuie să conducă la revizuirea, actualizarea şi îmbunătăţirea 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 preşedintelui Autorităţii Naţionale pentru Administrare şi Reglementare în Comunicaţii privind stabilirea măsurilor minime de securitate ce trebuie luate de către furnizorii de rețele şi servicii de comunicații electronice şi raportarea incidentelor cu impact semnificativ asupra furnizării reţelelor şi serviciilor de comunicaţii electronice, furnizorii au obligaţia de a raporta incidentele cu impact semnificativ (care afectează un număr mai mare de 5.000 de conexiuni timp de cel puţin o oră) asupra securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice, inclusiv prin identificarea cauzelor incidentelor, precum şi a acţiunilor 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 sancţiuni în cazul în care nu sunt furnizate în mod complet şi corect informaţiile solicitate de ANCOM referitoare la incidentele cu impact semnificativ asupra furnizării reţelelor şi serviciilor de comunicaţii electronice.

Anexa nr. 1

FORMULAR DE RAPORTARE A INCIDENTELOR CARE AU AFECTAT SECURITATEA ŞI INTEGRITATEA REŢELELOR ŞI SERVICIILOR DE COMUNICAŢII ELECTRONICE		
1. Furnizor:		
2. Data şi ora		
2.1 Data şi ora la care s-a produs incidentul	Data:	Ora:
2.2 Data şi ora la care s-a descoperit incidentul	Data:	Ora:
3. Impactul incidentului şi tipul cauzei		

3.1 Serviciul/serviciile afectate:

☐ Servicii de telefonie destinate publicului:
☐ Servicii de telefonie furnizate prin intermediul unor reţele publice fixe sau cu mobilitate limitată
☐ Servicii de telefonie furnizate prin intermediul unor reţele publice mobile terestre
☐ Servicii de telefonie furnizate prin intermediul unor reţele publice cu transmisie prin satelit
☐ Servicii de transport apeluri

☐ Servicii de linii închiriate

☐ Servicii de transmisiuni de date (inclusiv VPN):
☐ La puncte fixe
☐ Cu mobilitate limitată
☐ SMS (numai în cazul reţelelor celulare)
☐ Mobil (inclusiv MVNO)

☐ Servicii de acces la Internet:
☐ Dial-up (numai pentru bucla locală)
☐ Conexiuni permanente la punct fix
☐ Conexiuni radio mobile (inclusiv MVNO)

☐ Retransmisia serviciilor de programe media audiovizuale liniare către utilizatorii finali:
☐ Cu acces fix prin satelit (tip DTH)
☐ Cu acces mobil prin satelit (tip S-DAB/DVB-S)
☐ Terestre cu acces la punct fix tip CATV, DVB-C/Mx, IPTV etc.
☐ Terestre dedicate tip T-DAB/DVB-T
☐ Radio Celulare Publice (tip Mobile TV)

☐ Alte servicii de comunicaţii electronice
- ☐ Servicii de radiocomunicaţii mobile profesionale
  - ☐ Comunicaţii voce
  - ☐ Mesagerie radio
  - ☐ Transmisii de date, telex
  - ☐ Localizare, poziţionare
- ☐ Alte tipuri de servicii
  - ☐ Servicii de comunicaţii electronice care permit servicii de voce
  - ☐ Servicii de comunicaţii electronice care permit accesul la servicii de conţinut
  - ☐ 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 urgenţă:

3.3 Descrierea incidentului:

3.4 Tipul cauzei incidentului:
☐ Eroare umană
☐ Eroare de sistem
☐ Fenomen natural
☐ Acţiune rău intenţionată
☐ Cauză externă/parte terţă

3.5 Mai multe informaţii despre cauza incidentului:

4. Alte informaţii despre incident

4.1 Acţiuni 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 Alţi furnizori de reţele şi servicii de comunicaţii electronice afectaţi:
4.4 Alte observaţii: