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

În temeiul prevederilor art. 3 lit. d), art. 10 alin. (1) pct. 1, art. 11 alin. (1) şi art. 12 alin. (1) şi (3) din Ordonanţa de urgenţă a Guvernului nr. 22/2009 privind înfiinţarea Autorităţii Naţionale pentru Administrare şi Reglementare în Comunicaţii, aprobată prin Legea nr. 113/2010, cu modificările şi completările ulterioare, precum şi ale art. 46 – 48 din Ordonanţa de urgenţă a Guvernului nr. 111/2011 privind comunicaţiile electronice, aprobată cu modificări şi completări, prin Legea nr. 140/2012,

PREŞEDINTELE AUTORITĂŢII NAŢIONALE PENTRU ADMINISTRARE ŞI REGLEMENTARE ÎN COMUNICAŢII

emite prezenta:

DECIZIE

privind stabilirea măsurilor minime de securitate ce trebuie luate de către furnizorii de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului şi raportarea incidentelor cu impact semnificativ asupra furnizării reţelelor şi serviciilor de comunicaţii electronice

Art. 1. – Prezenta decizie are ca obiect stabilirea:

a) măsurilor tehnice şi organizatorice care trebuie luate de furnizorii de reţele publice de comunicaţii electronice destinate publicului în vederea asigurării unui nivel adecvat al securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice;

b) circumstanţelor, formatului şi procedurilor aplicabile notificării privind încălcarea securităţii sau pierderea integrităţii cu un impact semnificativ asupra furnizării reţelelor şi serviciilor de comunicaţii electronice.

Art. 2. – În înţelesul prezentei decizii, următorii termeni se definesc astfel:

1. *securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice* – 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;

2. *incident* – un eveniment care poate afecta sau ameninţa, direct ori indirect, securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice; efectele cauzate de lucrările de întreţinere a reţelei, programate şi anunţate din timp utilizatorilor, nu sunt considerate incidente.

3. *incident cu impact semnificativ* – acel incident care afectează un număr mai mare de 5.000 de conexiuni, timp de cel puţin 60 de minute;

4. *măsuri de securitate* – mijloace (de natură administrativă, managerială, tehnică sau juridică) de management al riscurilor, incluzând politici, acţiuni, planuri, echipamente, facilităţi, proceduri, tehnici etc. menite să elimine ori să reducă riscurile privind securitatea şi integritatea reţelelor sau a serviciilor de comunicaţii electronice.

Art. 3. – (1) Furnizorii de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului au obligaţia de a lua toate măsurile de securitate adecvate pentru a administra riscurile la adresa securităţii reţelelor şi serviciilor de comunicaţii electronice astfel încât să asigure un nivel de securitate corespunzător riscului identificat şi să prevină sau să minimizeze impactul incidentelor de securitate asupra utilizatorilor şi reţelelor interconectate, având în vedere cele mai noi tehnologii şi, acolo unde este cazul, de a colabora cu alţi furnizori pentru implementarea acestor măsuri.

(2) Furnizorii de reţele publice de comunicaţii electronice au obligaţia de a lua toate măsurile de securitate necesare pentru a administra riscurile la adresa integrităţii reţelelor şi serviciilor de comunicaţii electronice, în scopul garantării integrităţii reţelelor şi al asigurării continuităţii furnizării serviciilor prin intermediul acestor reţele şi, acolo unde este cazul, de a colabora cu alţi furnizori pentru implementarea acestor măsuri.

(3) Măsurile minime de securitate pe care trebuie să le stabilească şi să le implementeze furnizorii, astfel încât să îndeplinească obligaţia prevăzută la alin. (1) şi, după caz, cea prevăzută la alin. (2) vor viza cel puţin domeniile identificate în anexa nr. 1.

(4) Furnizorii au obligaţia de a evalua şi, dacă este cazul, de a actualiza măsurile prevăzute la alin. (3) ori de câte ori este necesar, însă cel puţin o dată la 12 luni.

Art.4. – (1) Furnizorii de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului au obligaţia de a transmite Autorităţii Naţionale pentru

Administrare şi Reglementare în Comunicaţii, denumită în continuare *ANCOM*, o notificare privind existenţa unui incident cu impact semnificativ asupra securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice.

(2) În aplicarea alin. (1), furnizorii de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului au obligaţia de a transmite *ANCOM* o primă notificare, până cel târziu la ora 13.00 a zilei lucrătoare următoare celei în care a fost detectat incidentul cu impact semnificativ asupra securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice.

(3) Notificarea iniţială prevăzută la alin. (2) se transmite de către una dintre persoanele responsabile prevăzute la art. 6, ca înscris în formă electronică la adresa de poştă electronică incidente@ancom.org.ro, şi va cuprinde cel puţin următoarele elemente:

a) ora descoperirii incidentului;

b) serviciile şi/sau reţelele care sunt afectate de incident;

c) estimarea ariei geografice afectate, a numărului de conexiuni afectate, precum şi a efectelor incidentului asupra furnizării reţelelor şi serviciilor de către alţi furnizori, pe piaţa naţională de comunicaţii electronice sau pe cea din alt stat membru al Uniunii Europene;

d) estimarea efectelor în ceea ce priveşte apelarea numărului unic pentru apeluri de urgenţă 112;

e) o descriere sumară a cauzei/cauzelor care a/au provocat incidentul;

f) estimarea graficului de restabilire a furnizării reţelelor şi serviciilor de comunicaţii electronice în parametrii normali de funcţionare;

g) îndrumările oferite de furnizor utilizatorilor în vederea minimizării efectelor incidentului, dacă este cazul;

h) informaţiile oferite publicului cu privire la existenţa unui incident, modalitatea de comunicare şi ora la care au fost comunicate informaţiile, dacă este cazul;

i) alte aspecte/elemente care pot permite ANCOM să decidă dacă informarea publicului privind incidentul este sau nu în interesul public;

j) datele de contact (nume, prenume, număr de telefon, număr de fax, adresă de poştă electronică) ale persoanei/persoanelor care poate/pot da mai multe informaţii privind incidentul.

(4) Este considerată dată a transmiterii înscrisului în formă electronică data confirmării primirii de către ANCOM a acestui înscris. ANCOM asigură fără întârziere şi în mod automat confirmarea primirii înscrisului în formă electronică transmis la adresa de poştă electronică incidente@ancom.org.ro.

(5) În situaţia în care confirmarea primirii unui înscris în formă electronică nu s-a realizat în condiţiile alin. (4), este considerată dată a transmiterii data la care înscrisul în formă electronică a fost trimis, în măsura în care această dată poate fi determinată cu certitudine.

(6) În aplicarea alin. (1), furnizorii de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului au obligaţia de a transmite ANCOM o notificare finală privind existenţa unui incident cu impact semnificativ asupra securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice, în termen de două săptămâni de la detectarea acestuia, completând formularul-tip de raportare prevăzut în anexa nr. 2, cu respectarea instrucţiunilor de completare specificate în anexa nr. 3.

(7) În cazul în care, la momentul transmiterii notificării finale prevăzute la alin. (6), furnizorii nu au disponibile toate informaţiile prevăzute în formularul-tip de raportare, aceştia au obligaţia de a transmite o notificare suplimentară cu informaţiile respective, completând formularul-tip de raportare prevăzut în anexa nr. 2, imediat ce acestea sunt disponibile, dar nu mai târziu de 3 săptămâni de la detectarea incidentului cu impact semnificativ.

(8) Notificarea finală şi notificarea suplimentară prevăzute la alin. (6), respectiv alin. (7), se transmit către sediul central din municipiul Bucureşti sau către structura teritorială a ANCOM în raza căreia se situează sediul ori domiciliul furnizorului, în unul dintre următoarele moduri:

a) prin depunere, personal sau de către un reprezentant al furnizorului, sub luare de semnătură;

b) printr-un serviciu poştal;

c) ca înscris în formă electronică la adresa de poştă electronică incidente@ancom.org.ro, căruia i s-a încorporat, ataşat sau i s-a asociat logic o semnătură electronică extinsă, bazată pe un certificat calificat nesuspendat sau nerevocat la momentul respectiv şi generată cu ajutorul unui dispozitiv securizat de creare a semnăturii electronice.

(9) Este considerată dată a transmiterii, după caz, data înscrierii în registrul general de intrare-ieşire a corespondenţei al ANCOM, data confirmării primirii documentelor la sediul central al ANCOM printr-un serviciu poştal cu confirmare de primire sau data confirmării primirii înscrisului în formă electronică, în condiţiile alin. (4) şi (5).

(10) Formularul-tip de raportare prevăzut la alin. (6) poate fi obţinut de la sediul central, de la orice structură teritorială sau de pe pagina de internet a ANCOM.

(11) Începând cu data de 1 ianuarie 2014, transmiterea notificării finale şi a notificării suplimentare prevăzute la alin. (6), respectiv alin. (7), se va realiza exclusiv prin intermediul unei aplicaţii disponibile pe pagina de internet a ANCOM, ca înscris în formă electronică, căruia i s-a încorporat, ataşat sau i s-a asociat logic o semnătură electronică extinsă, bazată pe un certificat calificat nesuspendat sau nerevocat la momentul respectiv şi generată cu ajutorul unui dispozitiv securizat de creare a semnăturii electronice, prevederile Deciziei preşedintelui Autorităţii Naţionale pentru Administrare şi Reglementare în Comunicaţii nr. 336/2013 privind mijloacele şi modalitatea de transmitere a unor documente, date sau informaţii către Autoritatea Naţională pentru Administrare şi Reglementare în Comunicaţii şi privind modificarea Deciziei preşedintelui Autorităţii Naţionale pentru Comunicaţii nr. 77/2009 privind obligaţiile de informare a utilizatorilor finali de

către furnizorii de servicii de comunicaţii electronice destinate publicului fiind aplicabile în mod corespunzător.

Art.5. – (1) Ca urmare a primirii notificării iniţiale prevăzute la art. 4 alin. (2) şi atunci când consideră că este în interesul public, ANCOM poate informa publicul cu privire la existenţa unui incident cu impact semnificativ asupra securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice, prin intermediul paginii de internet a ANCOM, sau poate solicita furnizorului să informeze publicul în acest sens.

(2) La solicitarea ANCOM, furnizorul de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului are obligaţia de a asigura informarea publicului cu privire la existenţa situaţiei prevăzute la alin. (1), cel puţin prin una dintre următoarele modalităţi:

a) prin intermediul unei secţiuni speciale pe propria pagină de internet;

b) prin canalul propriu de televiziune;

c) prin intermediul poştei electronice;

d) prin intermediul serviciului de mesagerie scurtă;

e) prin mass-media.

(3) În cazul în care ANCOM nu a stabilit prin solicitarea prevăzută la alin. (2) modalităţile şi condiţiile pentru a se asigura informarea publicului, furnizorul de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului va realiza informarea cel puţin prin una dintre modalităţile prevăzute la alin. (2).

(4) Atunci când incidentul semnificativ care face obiectul notificării iniţiale prevăzute la art. 4 alin. (2) poate afecta furnizarea reţelelor şi serviciilor de către un furnizor din alt stat membru al Uniunii Europene, pe baza informaţiilor colectate, ANCOM decide cu privire la informarea autorităţii de reglementare din respectivul stat şi a Agenţiei Europene pentru Securitatea Reţelelor Informatice şi a Datelor, denumită în continuare *ENISA,* cu privire la acest incident.

(5) ANCOM transmite anual un raport succint Comisiei Europene şi ENISA cu privire la notificările primite potrivit art. 4 alin. (6), respectiv, art. 4 alin. (7).

Art.6. – Furnizorii de reţele publice de comunicaţii electronice sau servicii de comunicaţii electronice destinate publicului au obligaţia de a transmite ANCOM datele de contact ale persoanelor responsabile de raportarea incidentelor cu impact semnificativ asupra securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice, în termen de 5 zile de la intrarea în vigoare a prezentei decizii, precum şi orice modificare a acestor date, în termen de 5 zile de la survenirea modificărilor.

Art.7. – Anexele nr. 1 - 3 fac parte integrantă din prezenta decizie.

Art.8. – (1) Prezenta decizie se publică în Monitorul Oficial al României, Partea I şi intră în vigoare la data de 1 octombrie 2013, cu excepţia prevederilor art. 3 care intră în vigoare la data de 1 ianuarie 2014.

(2) Furnizorii de reţele publice de comunicaţii electronice sau servicii de comunicaţii electronice destinate publicului au obligaţia de a transmite ANCOM, până cel târziu la data de 15 octombrie 2013, câte o notificare privind fiecare incident cu impact semnificativ asupra securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice care a avut loc în anul 2013, până la data intrării în vigoare a prezentei decizii, completând formularul-tip de raportare prevăzut în anexa nr. 2, cu respectarea instrucţiunilor de completare din anexa nr. 3. Prevederile art. 4 alin. (8) şi (9) sunt aplicabile în mod corespunzător.

PREŞEDINTE,
MARIUS CĂTĂLIN MARINESCU

Bucureşti, 1 august 2013
Nr. 512

ANEXA nr. 1

Domeniile vizate de măsurile minime de securitate

I. Politica de securitate şi managementul riscului

Furnizorii de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului au obligaţia:

1) să stabilească o politică de securitate adecvată;

2) să stabilească un management al riscului care:

a) să stabilească domeniul de aplicare, precum şi criteriile de bază necesare procesului de management al riscului (criteriul de evaluare a riscului, criteriul de stabilire a impactului, criteriul de acceptare a riscului);

b) să identifice riscurile, prin identificarea resurselor furnizorului în cauză, ameninţărilor, vulnerabilităţilor, măsurilor existente şi a consecinţelor pe care pierderea/încălcarea securităţii le-ar putea avea asupra resurselor;

c) să estimeze riscurile prin evaluarea impactului pe care îl poate avea concretizarea unei ameninţări care exploatează o vulnerabilitate a unei resurse şi prin evaluarea probabilităţii de apariţie a incidentelor;

d) să evalueze riscul;

e) să evalueze opţiunile de tratare a riscului, să selecteze măsuri pentru tratarea riscului cu fixarea obiectivelor acestor măsuri şi să justifice riscurile acceptate care nu îndeplinesc criteriul de acceptare a riscului.

3) să stabilească o structură adecvată a rolurilor şi responsabilităţilor în asigurarea securităţii şi integrităţii reţelelor şi serviciilor;

4) să stabilească o politică cu privire la cerinţele de securitate pentru achiziţionarea de produse şi servicii de la terţe părţi şi pentru asigurarea întreţinerii sau gestiunii de către terţe părţi a produselor şi serviciilor (servicii IT, software, interconectare, baze de date, facilităţi asociate etc).

II. Securitatea resurselor umane

Furnizorii de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului au obligaţia:

1) să efectueze controale de verificare de fond a candidaţilor pentru angajare, a contractorilor şi a terţilor în conformitate cu legile aplicabile, reglementări şi etică, proporţionale cu riscurile percepute;

2) să se asigure că personalul lor are cunoştinţe suficiente de securitate şi este instruit permanent cu privire la securitatea şi integritatea reţelelor şi serviciilor;

3) să stabilească un proces corespunzător de gestionare a schimbărilor de personal sau a modificărilor de roluri şi responsabilităţi;

4) să stabilească un proces disciplinar pentru angajaţii care produc o încălcare a securităţii şi integrităţii reţelelor sau serviciilor de comunicaţii electronice.

III. Securitatea şi integritatea reţelelor, a facilităţilor asociate şi a informaţiilor

Furnizorii de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului au obligaţia:

1) să stabilească o securitate fizică adecvată a reţelei şi a infrastructurii asociate (stabilirea şi menţinerea unor măsuri care să protejeze în mod corespunzător împotriva accesului fizic neautorizat, distrugerilor provocate de incendii, inundaţii, cutremure, explozii, tulburări publice şi alte forme de dezastre naturale sau provocate de oameni);

2) să stabilească o securitate adecvată a utilităţilor-suport, cum ar fi furnizarea de energie electrică, combustibil sau răcirea echipamentelor;

3) să stabilească măsuri de securitate adecvate pentru accesul (logic) la reţea şi la sistemele informatice;

4) să stabilească măsuri de securitate adecvate pentru a asigura protecţia reţelelor şi serviciilor de comunicaţii electronice împotriva codurilor cu potenţial dăunător, codurilor mobile neautorizate şi a atacurilor informatice, inclusiv DoS/DDoS.

IV. Managementul operaţiunilor

Furnizorii de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului au obligaţia:

1) să stabilească proceduri operaţionale şi responsabilităţi adecvate;

2) să stabilească proceduri privind managementul schimbărilor efectuate în reţeaua de comunicaţii electronice şi în software-urile de aplicaţii;

3) să stabilească proceduri de gestionare a resurselor astfel încât disponibilitatea şi starea acestora să fie verificată.

V. Managementul incidentelor

Furnizorii de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului au obligaţia:

1) să stabilească procese şi proceduri pentru managementul incidentelor care afectează securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice (care să vizeze raportarea internă, evaluarea, răspunsul la incidente şi escaladarea acestuia), inclusiv prin definirea rolurilor şi responsabilităţilor;

2) să stabilească un sistem de detectare a incidentelor;

3) să stabilească o procedură adecvată de raportare a incidentelor către Autoritatea Naţională pentru Administrare şi Reglementare în Comunicaţii, precum şi către alte autorităţi responsabile, şi să stabilească planuri de comunicare a incidentelor către alte părţi externe (furnizori de reţele şi servicii de comunicaţii electronice afectaţi, media, clienţi, parteneri de afaceri etc.).

VI. Managementul continuităţii afacerii

Furnizorii de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului au obligaţia:

1) să stabilească o strategie pentru asigurarea continuităţii furnizării reţelelor şi serviciilor de comunicaţii electronice în situaţiile generate de perturbări grave ale funcţionării reţelei sau serviciului;

2) să deţină capabilităţi de implementare a strategiei de continuitate şi să stabilească planuri de continuitate şi de recuperare.

VII. Monitorizare, testare şi audit

Furnizorii de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului au obligaţia:

1) să stabilească politici de monitorizare a sistemelor, precum şi politici privind jurnalele de sistem;

2) să stabilească politici pentru testarea, inclusiv prin exerciţii, a planurilor de continuitate şi de recuperare în cazul perturbărilor grave ale funcţionării reţelei sau serviciului;

3) să stabilească politici pentru testarea echipamentelor, sistemelor şi software-lor, în special înainte de conectarea/punerea lor în funcţiune;

4) să stabilească o politică adecvată pentru evaluarea şi testarea securităţii tuturor resurselor (echipamente, sisteme şi software etc.);

5) să stabilească o politică pentru monitorizarea conformităţii şi pentru audit, cu un proces de raportare a conformităţii şi de rezolvare a deficienţelor constatate în timpul auditului.

ANEXA nr. 2

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 — Număr de conexiuni afectate .....
- ☐ Servicii de telefonie furnizate prin intermediul unor reţele publice mobile terestre — Număr de conexiuni afectate .....
- ☐ Servicii de telefonie furnizate prin intermediul unor reţele publice cu transmisie prin satelit — Număr de conexiuni afectate .....
- ☐ Servicii de transport apeluri — Număr de conexiuni afectate .....

☐ Servicii de linii închiriate — Număr de conexiuni afectate .....

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

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

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

☐ Alte servicii de comunicaţii electronice
- ☐ Servicii de radiocomunicaţii mobile profesionale
  - ☐ Comunicaţii voce — Număr de conexiuni afectate .....
  - ☐ Mesagerie radio — Număr de conexiuni afectate .....
  - ☐ Transmisii de date, telex — Număr de conexiuni afectate .....
  - ☐ Localizare, poziţionare — Număr de conexiuni afectate .....
- ☐ Alte tipuri de servicii
  - ☐ Servicii de comunicaţii electronice care permit servicii de voce — Număr de conexiuni afectate .....
  - ☐ Servicii de comunicaţii electronice care permit accesul la servicii de conţinut — Număr de conexiuni afectate .....
  - ☐ Alte tipuri de servicii decât cele de mai sus — Număr de conexiuni afectate .....

3.2 Parametrii de impact:

Numărul total de conexiuni afectate de incident:

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:

ANEXA nr. 3

Instrucţiuni de completare a formularului de raportare a incidentelor care au afectat securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice

<table>
<tr><td colspan="2">1. Furnizor</td></tr>
<tr><td colspan="2">Se va completa cu denumirea furnizorului care trimite raportul către ANCOM.</td></tr>
<tr><td colspan="2">2. Data şi ora</td></tr>
<tr><td>2.1 Data şi ora la care s-a produs incidentul</td><td rowspan="2">Se vor completa data şi ora la care s-a produs incidentul, respectiv la care s-a descoperit incidentul. Formatul de introducere a datei va fi de tipul zz.ll.aaaa.</td></tr>
<tr><td>2.2 Data şi ora la care s-a descoperit incidentul</td></tr>
<tr><td colspan="2">3. Impactul incidentului şi tipul cauzei</td></tr>
<tr><td colspan="2">3.1 Servicii afectate de incident:</td></tr>
<tr><td colspan="2">Se va/vor bifa serviciul/serviciile a cărui/căror furnizare a fost afectată de incident.
Câmpul „Numărul de conexiuni afectate” din dreptul fiecărui tip de serviciu se va completa corespunzător, fiecărui serviciu afectat în parte fiindu-i alocat numărul de conexiuni afectate de incident.
O conexiune reprezintă:
- în cazul serviciilor de acces la internet la puncte fixe: o conexiune de acces la internet;
- în cazul serviciilor de transmisiuni de date la puncte fixe: o conexiune de acces la servicii de transmisiuni de date;
- în cazul serviciilor de telefonie la punct fix: o linie telefonică alocată unui abonat de către un furnizor prin intermediul propriei reţele publice fixe pe care o operează sau prin reţeaua publică fixă a unui terţ; un abonat poate avea alocate una sau mai multe linii de acces;
- în cazul serviciilor de telefonie, acces la internet şi transmisiuni de date furnizate prin intermediul reţelelor radio mobile terestre: o cartelă SIM activă;
- în cazul serviciilor de retransmisie a programelor media audiovizuale liniare: o conexiune de retransmisie a programelor media audiovizuale.
În cazul serviciilor furnizate prin intermediul unor reţele publice mobile terestre, furnizorul va estima numărul de conexiuni afectate. Metoda de estimare a numărului de cartele SIM afectate de un incident este următoarea:
În momentul apariţiei unui incident se identifică celulele afectate.
Traficul total pierdut la nivelul tuturor celulelor afectate ($T_{pierdut}$) pe fiecare serviciu (voce şi date) se consideră a fi traficul înregistrat în săptămâna anterioară, în acelaşi interval de timp în care a avut loc incidentul, la nivelul acelor celule.
Traficul total înregistrat la nivelul reţelei (T_{retea}) se consideră a fi suma traficului din toate celulele din reţea în intervalul de timp respectiv, în săptămâna anterioară.
Numărul de cartele SIM afectate se calculează astfel:
$$N_{cartele\ SIM\ afectate} = N_{ds}\frac{T_{pierdut}}{T_{retea}}$$
N_{ds} reprezintă numărul de cartele SIM active pe respectivul serviciu la nivelul furnizorului, conform raportării în baza Deciziei preşedintelui Autorităţii Naţionale pentru Administrare şi Reglementare în Comunicaţii nr. 333/2013 privind raportarea unor date statistice de către furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului.
În calculul traficului, se are în vedere atât traficul originat, cât şi traficul terminat. Algoritmul propus se va aplica tuturor tipurilor de servicii la puncte mobile.</td></tr>
<tr><td colspan="2">3.2 Parametrii de impact:</td></tr>
<tr><td>Numărul total de conexiuni afectate de incident</td><td>Se va specifica numărul total de conexiuni afectate de incident. Acest număr se va calcula ca sumă a numărului de conexiuni afectate pe fiecare tip de servicu.</td></tr>
</table>

Resursele/echipa-mentele afectate	Se vor specifica resursele/echipamentele afectate de incident. Ca exemplu, este prezentată în continuare o listă de resurse ce pot fi afectate: - staţii de bază pentru PLMN (BSC, BTS, RNC, NodeB etc.): - reţea locală (cabluri de cupru, fibră etc.); - cabinete stradale; - echipamente de comutare sau rutare (comutatoare de reţea, routere, multiplexoare etc.) - noduri de transmisiuni; - centre de comutaţie; - centre de mesaje; - registre de utilizatori (HLR, VLR, AuC, Home Subscriber Server etc.); - backbone; - interconectări; - echipamente pentru alimentarea de rezervă cu energie electrică (baterii, generatoare); - sisteme de alimentare cu energie electrică.
Durata incidentului	Se va specifica 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 iniţiali. Timpul va fi exprimat în minute.
Aria/răspândirea geografică	Se va specifica regiunea geografică afectată de incident (de exemplu: regiunea, judeţele, localităţile).
Impactul asupra apelurilor de urgenţă	Se va specifica modul în care au fost afectate comunicaţiile către Sistemul naţional unic pentru apeluri de urgenţă.

3.3 Descrierea incidentului:

Se va completa cu orice informaţii şi detalii disponibile privind apariţia, dezvoltarea, impactul incidentului şi modalitatea în care au fost afectate resursele/echipamentele.

3.4 Tipul cauzei incidentului:

Se va/vor bifa cauza/cauzele incidentului: eroare umană, eroare de sistem, fenomen natural, acţiune rău intenţionată şi cauză externă/parte terţă. De obicei, categoria cauză externă/parte terţă poate fi corelată cu una din celelalte 4 cauze (de exemplu: în cazul unui cablu de fibră optică distrus în urma unor lucrări de construcţie, cauzele incidentului vor fi eroare umană şi cauză externă/parte terţă).

Unele incidente pot avea o cauză iniţială şi una subsecventă, incidentele apărând în urma unei succesiuni de evenimente sau factori (exemplu: în cazul unui incident datorat unei alimentări defectuoase cu energie electrică – suprasarcină care produce o defectare a unui echipament al furnizorului, cauza iniţială este eroare de sistem a unui echipament al furnizorului de utilităţi şi cauză externă/parte terţă, iar cauza subsecventă este eroare de sistem – defecţiune hardware a unui echipament de comunicaţii electronice). În acest caz, furnizorul va bifa cauza iniţială.

3.5 Mai multe informaţii despre cauza incidentului:

Câmpul va cuprinde descrierea detaliată a cauzei incidentului, inclusiv vulnerabilităţile exploatate. În cazul incidentelor apărute în urma unei succesiuni de evenimente, furnizorul va oferi atât detalii privind cauza iniţială, cât şi despre cauza/cauzele subsecvente.

4. Alte informaţii despre incident

4.1 Acţiuni de răspuns la incident (inclusiv momentul când au fost luate):

Câmpul va cuprinde descrierea detaliată a:

- măsurilor de securitate implementate până la momentul producerii incidentului în vederea minimizării riscului incidentului;
- acţiunilor întreprinse şi a măsurilor adoptate pentru a restabili serviciul la parametrii iniţiali în cazul în care incidentul afectează doar calitatea serviciului (nu există întrerupere în furnizarea serviciului);
- acţiunilor întreprinse şi a măsurilor adoptate pentru a aduce serviciul la un nivel acceptabil, precum şi pentru a restabili serviciul la parametrii iniţiali în cazul întreruperii furnizării serviciului, inclusiv momentele de timp în care au fost acestea realizate.

4.2 Măsurile luate sau planificate pentru a împiedica producerea unui incident similar/eliminarea cauzei incidentului (inclusiv momentul când au fost/vor fi luate):
Câmpul va cuprinde descrierea detaliată a acţiunilor realizate pentru a minimiza nivelul de risc şi pentru a preîntâmpina reapariţia incidentului (de exemplu: revizuire măsuri de securitate şi proceduri, renegociere SLA-uri, instruiri de personal, achiziţie de echipamente sau sisteme de backup etc), precum şi momentul când au fost luate sau când vor fi luate aceste măsuri.
4.3 Alţi furnizori de reţele şi servicii de comunicaţii electronice afectaţi:
Acest câmp se completează cu detalii despre furnizorul şi resursele/serviciile acestuia afectate de incidentul în cauză, inclusiv cazurile în care furnizori din alte state membre ale Uniunii Europene au fost afectaţi. De asemenea, se descrie modul de colaborare cu alţi furnizori în vederea soluţionării incidentului, inclusiv acţiunile comune de răspuns la incident.
4.4 Alte observaţii:
Acest câmp se completează cu orice alte detalii sau observaţii care nu au fost incluse în câmpurile de mai sus.