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

SINTEZA OBSERVAŢIILOR
la proiectul de 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

Perioada de consultare pentru proiectul deciziei preşedintelui Autorităţii Naţionale pentru Administrare şi Reglementare în Comunicaţii 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 (denumit în continuare *Proiectul*), publicat pe pagina de internet a Autorităţii Naţionale pentru Administrare şi Reglementare în Comunicaţii (în continuare, *ANCOM*) la data de 24 aprilie 2013, a expirat la data de 27 mai 2013.

Proiectul supus consultării are ca obiect stabilirea:

a) măsurilor tehnice şi organizatorice care trebuie luate de furnizorii de reţele publice de comunicaţii electronice sau de servicii 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.

Proiectul prevede o serie de obligaţii în sarcina furnizorilor de reţele publice de comunicaţii electronice şi servicii de comunicaţii electronice destinate publicului, precum:

a) 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;

b) 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;

c) de a evalua şi, dacă este cazul, de a actualiza măsurile prevăzute mai sus ori de câte ori este necesar, însă cel puţin o dată la 12 luni;

d) de a transmite ANCOM, o notificare iniţială, în termen de 6 ore de la detectarea unui incident cu impact semnificativ asupra securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice;

e) 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;

f) de a asigura informarea publicului cu privire la existenţa unui incident cu impact semnificativ asupra securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice, la solicitarea ANCOM.

În conformitate cu dispoziţiile art. 135 alin. (4) din Ordonanţa de urgenţă a Guvernului nr. 111/2011 privind comunicaţiile electronice, aprobată cu modificări şi completări, prin Legea nr. 140/2012, ANCOM are obligaţia de a publica, pe pagina de internet, un material de sinteză a observaţiilor primite cu privire la proiectul deciziei supus consultării publice, în care va preciza şi poziţia sa faţă de aceste observaţii.

Observaţiile şi propunerile primite de către ANCOM în cursul procedurii de consultare publică au vizat următoarele aspecte:

1. Definiţia noţiunii „securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice";

2. Definiţia noţiunii „incident cu impact semnificativ", respectiv pragurile ce declanşează raportarea incidentelor;

3. Obligaţia de notificare iniţială a incidentelor cu impact semnificativ;

4. Obligaţia de notificare finală şi cea suplimentară a incidentelor cu impact semnificativ;

5. Informarea publicului cu privire la existenţa unui incident cu impact semnificativ asupra securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice;

6. Obligaţia de notificare a fiecărui incident cu impact semnificativ din anul 2013 până la intrarea în vigoare a deciziei;

7. Incidentele care afectează furnizarea reţelelor şi serviciilor de către alţi furnizori (inclusiv din alt stat membru al Uniunii Europene);

8. Implementarea măsurilor minime de securitate;

9. Propuneri privind includerea în proiectul de decizie a altor prevederi;

10. Alte propuneri.

1. Definiţia noţiunii „securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice"

1.1. S-a solicitat modificarea definiţiei acestei noţiuni în sensul eliminării sintagmei „*la un nivel de performanţă echivalent cu cel anterior producerii evenimentului*" deoarece, în cazul serviciilor de tip „best effort", calitatea serviciului înregistrează diferenţe în timp. Modificarea definiţiei în sensul propus de către respondent va conduce la eliminarea legăturii de interdependenţă între afectarea continuităţii furnizării reţelelor şi serviciilor şi afectarea nivelului de performanţă înregistrat anterior producerii unui incident.

ANCOM recunoaşte că, în special pentru serviciile de tip „best effort", ca de exemplu acces la internet şi pentru servicii furnizate prin intermediul reţelelor publice mobile terestre, calitatea serviciilor variază în timp datorită unor factori ce nu pot fi calificaţi drept cauze ale incidentelor de securitate (utilizarea unor tehnologii diferite pentru zone geografice diferite, nivelul diferit de concentrare a utilizatorilor în anumite zone - pentru servicii mobile, trafic ridicat la ore de vârf - pentru servicii de acces la internet etc).

Incidentul de securitate produce, la rândul său, variaţii ale calităţii/performanţei serviciului furnizat sau conduce la întreruperea temporară a furnizării acestuia. Ceea ce trebuie precizat este faptul că definiţia propusă prin proiectul de decizie are în vedere acea variaţie a calităţii şi performanţei reţelei/serviciului care nu este datorată unor condiţii existente în operarea normală, ci **este datorată incidentelor de securitate**. Sintagma „*la un nivel de performanţă echivalent cu cel anterior producerii evenimentului*" a fost introdusă în cadrul definiţiei securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice pentru a cuprinde şi incidentele care afectează echipamente de comunicaţii, dar nu produc o întrerupere a furnizării serviciilor şi reţelelor de comunicaţii electronice. Avem în vedere, de exemplu, cazul în care un echipament de comunicaţii (BTS, router etc.) se defectează, însă serviciul este în continuare furnizat utilizatorilor (la un nivel scăzut de performanţă), deoarece semnalul este direcţionat pe altă cale posibilă. În acest caz, securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice a fost afectată, însă nu a avut loc o întrerupere a furnizării serviciilor către utilizatorii finali.

Ghidul Agenţiei Europene pentru Securitatea Reţelelor Informatice și a Datelor (ENISA) privind măsurile minime de securitate se înscrie în aceeaşi linie cu cele precizate mai sus, prin trimitere la literatura tehnică privind reţelele şi interconectarea acestora care defineşte integritatea

ca fiind „capacitatea sistemului de a păstra calităţile sale specificate din perspectiva performanţei şi funcţionalităţii”[1].

1.2. Un respondent a propus utilizarea sintagmei „*securitatea reţelelor şi serviciilor de comunicaţii electronice*” în locul celei de „*securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice*” în tot cuprinsul Proiectului şi definirea acesteia prin referire la confidenţialitate, integritate şi disponibilitate, argumentând că integritatea reprezintă o componentă a securităţii, alături de confidenţialitate şi disponibilitate, propunerea invocând în acest sens o analogie cu noţiunea de „securitate cibernetică”, noţiune definită în cuprinsul Hotărârii Guvernului nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică.

Cadrul legal european şi naţional se referă atât la securitatea, cât şi la integritatea reţelelor şi serviciilor de comunicaţii electronice. Ordonanţa de urgenţă a Guvernului nr. 111/2011 include un capitol special dedicat *securităţii şi integrităţii* reţelelor şi serviciilor de comunicaţii electronice care transpune în legislaţia naţională prevederile Capitolului IIIA – „Securitatea şi integritatea reţelelor şi serviciilor” din Directiva 2002/21/CE privind un cadru de reglementare comun pentru reţelele şi serviciile de comunicaţii electronice, revizuită (Directiva cadru revizuită).

Securitatea informaţiei/cibernetică se defineşte într-adevăr prin raportare la cele trei dimensiuni/componente: confidenţialitatea, integritatea şi disponibilitatea informaţiilor.

ANCOM consideră că există diferenţe între *securitatea informaţiei* şi *securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice*, iar cele două concepte, precum şi definiţiile lor nu trebuie confundate.

Astfel, confidenţialitatea, integritatea şi disponibilitatea pot fi alăturate doar prin raportare la securitatea informaţiilor. Confidenţialitatea este aplicabilă informaţiilor, desemnând acea proprietate a informaţiei de a nu fi disponibilă sau dezvăluită unor persoane, entităţi sau procese neautorizate. Integritatea informaţiilor asigură corectitudinea/acurateţea acestora, pe când integritatea reţelelor şi serviciilor de comunicaţii electronice trebuie privită într-un cadru mult mai larg, reprezentând capacitatea sistemului de a păstra calităţile sale specificate din perspectiva performanţei şi funcţionalităţii. Disponibilitatea este proprietatea unei resurse de a fi accesibilă la momentul oportun şi uşor de utilizat la cererea unei entităţi autorizate, acest concept putând fi corelat atât cu securitatea informaţiei, cât şi cu securitatea reţelelor şi serviciilor de comunicaţii electronice.

Prin urmare, propunerea respondentului de a reformula sintagma „securitatea reţelelor şi serviciilor de comunicaţii electronice” nu poate fi primită, ANCOM urmând a se referi la „securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice” în cuprinsul Deciziei, în acord cu cadrul legal naţional şi european din domeniul comunicaţiilor electronice.

2. Definiţia noţiunii „incident cu impact semnificativ”, respectiv pragurile ce declanşează raportarea incidentelor

2.1. În opinia unor respondenţi, stabilirea generică a numărului de 5.000 de conexiuni afectate ca unul dintre criteriile utilizate pentru calificarea unui incident de securitate ca fiind semnificativ, este neadecvată. Astfel, în scopul respectării principiului nediscriminării şi tratamentului egal şi pentru asigurarea relevanţei din punct de vedere statistic, în locul numărului de conexiuni afectate se recomandă utilizarea unui procent din numărul total de utilizatori ai serviciului furnizorului respectiv. În plus, aceştia apreciază că pragul fix de 5.000 de conexiuni afectate, aplicabil tuturor furnizorilor indiferent de dimensiunea lor conduce la un dezechilibru de raportare, implicând riscul ca furnizorii cu un număr mare de utilizatori să raporteze incidente mult mai des decât ceilalţi furnizori şi presupune costuri excesive în raport cu beneficiul adus. De asemenea, a fost adus în discuţie şi faptul că utilizarea unui asemenea prag ar conduce la excluderea furnizorilor cu mai puţin de 5.000 de utilizatori (care reprezintă peste 90% din totalul furnizorilor de comunicaţii electronice din piaţă) de la obligaţia de raportare a incidentelor de securitate.

[1] ENISA, *Technical Guideline for Minimum Security Measures, Guidance on the security measures in Article 13a*, Version 1.0, December 2011, p. 2

Ghidul ENISA „Technical Guidelines for Reporting Incidents” la care mai mulţi respondenţi fac referire vizează relaţia dintre ENISA şi autorităţile de reglementare în domeniul comunicaţiilor electronice din statele membre ale Uniunii Europene şi este rezultatul colaborării între părţile implicate în ceea ce priveşte realizarea obiectivului comun de sporire a securităţii şi integrităţii reţelelor şi serviciilor. Acest cadru a fost necesar pentru a asigura comparabilitatea notificărilor transmise de statele membre către ENISA prin stabilirea informaţiilor/elementelor care trebuie raportate, asigurându-se astfel armonizarea raportărilor la nivel european şi extragerea unor rezultate comparabile privind incidentele raportate. În acelaşi timp, ghidul oferă sprijin autorităţilor de reglementare din statele membre în implementarea art.13a din Directiva cadru revizuită în privinţa stabilirii schemei de raportare naţională a incidentelor la adresa securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice. Schema de raportare naţională este însă diferită de la un stat la altul, fiecare stat fiind liber să aleagă praguri de raportare corespunzătoare obiectivelor urmărite.

ANCOM consideră că utilizarea unui procent din numărul total de utilizatori ai serviciului furnizorului respectiv, propunere înaintată de câţiva respondenţi, nu este o soluţie fezabilă în determinarea impactului unui incident, deoarece acest procent se rezumă tot la stabilirea unor valori absolute, dar care se schimbă/variază în timp urmând variaţia normală a numărului de utilizatori ai unui serviciu. În acelaşi timp, utilizarea unui prag procentual pe serviciu ar conduce la o discriminare între diferite tipuri de servicii de comunicaţii electronice, dat fiind faptul că numărul de utilizatori diferă de la un serviciu la altul.

În ceea ce priveşte aspectele invocate de respondenţi cu privire la faptul că furnizorii cu un număr mic de utilizatori nu vor intra sub incidenţa obligaţiei de raportare, ANCOM precizează că raţiunea exceptării acestora de la o asemenea obligaţie rezidă tocmai în aceea că incidentele raportate de către aceştia au un impact nesemnificativ ţinând cont de numărul redus al utilizatorilor afectaţi.

Astfel, pentru exemplificare, la nivel naţional, în rândul furnizorilor cu mai puţin de 5.000 de utilizatori, există 19 furnizori de servicii de telefonie furnizate prin intermediul unor reţele publice fixe sau cu mobilitate limitată, 883 furnizori de servicii de acces la internet prin conexiuni permanente la punct fix, 385 furnizori de servicii de retransmisie a programelor media audiovizuale liniare. Chiar dacă numărul furnizorilor cu mai puţin de 5.000 de utilizatori este semnificativ, aceştia reprezintă un procent redus din cota de piaţă. Media aritmetică a numărului de utilizatori pentru un astfel de furnizor (cu mai puţin de 5.000 de utilizatori) este de 957 de utilizatori în cazul serviciilor de telefonie furnizate prin intermediul unor reţele publice fixe sau cu mobilitate limitată, 351 de utilizatori pentru servicii de acces la internet prin conexiuni permanente la punct fix, 985 de utilizatori pentru servicii de retransmisie a programelor media audiovizuale liniare.

În acelaşi timp, ANCOM atrage atenţia că impactul semnificativ al unui incident trebuie evaluat/raportat la nivelul întregii pieţe de comunicaţii electronice naţionale, accentul nefiind pus pe impactul pe care incidentul îl are asupra unui singur furnizor de comunicaţii electronice.

Principalul motiv pentru care ENISA a specificat pragurile de raportare ca procent din numărul total de utilizatori a fost diversitatea pieţelor naţionale de comunicaţii electronice. Prin stabilirea unor praguri procentuale, ENISA a urmărit să cuprindă toate/majoritatea statelor europene în cadrul raportării, obiectiv ce nu ar fi fost realizabil prin fixarea unor praguri numerice/valorice. Astfel, în cazul în care pragul era stabilit ca număr, exista riscul ca anumite state să fie excluse din aplicarea prevederilor directivei cadru dacă numărul stabilit de ENISA ar fi fost prea mare (state cu număr mic de utilizatori de servicii de comunicaţii electronice).

În cazul raportărilor naţionale, situaţia este diferită, deoarece obiectivul raportărilor naţionale diferă de cel aferent raportărilor la nivel european. ENISA doreşte să cuprindă toate statele membre în raportare, pe când autoritatea de reglementare, ţinând cont de specificul furnizorilor la nivel naţional (mulţi furnizori cu un număr mic de utilizatori şi puţini furnizori cu un număr mare de utilizatori în cazul României), intenţionează să cuprindă incidentele cu impact semnificativ la nivel naţional şi nu neapărat toţi furnizorii existenţi pe piaţă.

Ca urmare a motivelor precizate anterior, ANCOM consideră că exprimarea printr-un număr fix de conexiuni este cea mai potrivită metodă pentru exprimarea valorii pragului de raportare şi elimină incertitudinea pe care o generează introducerea unor praguri exprimate procentual.

În ceea ce priveşte valoarea pragului de raportare, unii respondenţi au exprimat opinia potrivit căreia pragul ales de ANCOM duce la numeroase notificări în rândul unor furnizori cu un număr mare de utilizatori, iar pentru realizarea colectării, centralizării şi publicării informaţiilor

despre incidentele cu impact semnificativ, aceşti furnizori depun un efort enorm ce presupune costuri excesive. ANCOM precizează că în urma chestionarului realizat de ANCOM în 2012 referitor la măsurile de securitate implementate de furnizori a reieşit că aceştia monitorizează incidentele care afectează reţeaua de comunicaţii electronice şi majoritatea au şi proceduri interne de raportare a incidentelor care să le faciliteze procesul notificării. În plus, prin proiectul de decizie, ANCOM a stabilit în sarcina furnizorilor de reţele şi servicii de comunicaţii electronice obligaţia de a lua măsuri de securitate adecvate în ceea ce priveşte managementul incidentelor. Astfel, furnizorii trebuie 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, să stabilească un sistem de detectare a incidentelor. Implementarea unor măsuri adecvate în domeniile stabilite de ANCOM va contribui la realizarea unor notificări eficiente, cu un efort redus din partea furnizorilor.

ANCOM şi-a propus ca, prin intermediul notificărilor privind incidentele cu impact semnificativ, să primească semnale privind problemele cu care se confruntă diferiţi furnizori de-a lungul timpului. Aceste semnale vor determina Autoritatea să analizeze în detaliu aceste cazuri şi să ia măsuri menite să sprijine furnizorii care se confruntă cu astfel de probleme. Ţinând cont de competenţele sale, ANCOM poate interveni pentru rezolvarea acestor probleme. Astfel, prin stabilirea pragului fix de 5.000 de conexiuni afectate, ANCOM a urmărit să monitorizeze o gamă largă de incidente, precum cele datorate alimentării cu energie electrică, dar şi incidente cauzate de furturile de cablu, echipamente sau materiale, incidente frecvente şi cu impact major asupra furnizorilor de reţele şi servicii de comunicaţii electronice, care n-ar fi incluse în raportări urmând alte praguri de raportare. Pragul a fost stabilit identic pentru toate serviciile, ANCOM respectând principiul nediscriminării şi tratamentului egal al tuturor tipurilor de servicii de comunicaţii electronice. În cazul în care pragul de raportare ar fi diferit pentru fiecare serviciu de comunicaţii electronice, serviciilor/utilizatorilor li s-ar acorda importanţă diferită, rezultând o apreciere diferenţiată şi practic incorectă/nejustificată a serviciilor de comunicaţii electronice, respectiv a utilizatorilor de servicii.

2.2. Un respondent precizează că în cazul serviciilor furnizate prin intermediul reţelelor radio mobile, numărul de utilizatori afectaţi este unul estimat, bazat pe utilizarea normală a sistemelor afectate, pe comportamentul de trafic al întregii baze de clienţi, la nivelul întregului teritoriu acoperit de reţeaua furnizorului.

Un alt respondent a evidenţiat faptul că nu există un indicator care să reflecte în mod obiectiv şi realist numărul de utilizatori aflaţi sub acoperirea unei celule care ar putea fi deserviţi într-un anumit interval de timp.

Numărul conexiunilor afectate de un incident în cazul serviciilor furnizate prin intermediul reţelelor mobile nu poate fi determinat cu precizie şi prin urmare va fi estimat de către furnizori aşa cum este prevăzut şi în instrucţiunile de completare a formularului de raportare a incidentelor care au afectat securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice (Anexa nr. 3 la Proiect). Pentru ca datele din cadrul raportărilor incidentelor cu impact semnificativ primite de ANCOM să fie corecte şi comparabile, ANCOM a propus utilizarea următoarei metode de estimare:

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 reţele publice de comunicaţii electronice sau de servicii de comunicaţii 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.

Totodată, ANCOM va constitui un grup de lucru din care vor face parte reprezentanţi ai furnizorilor vizaţi şi reprezentanţi ai ANCOM în scopul elaborării unui ghid în care se vor lămuri eventualele aspecte neclare care ar putea apărea în timp în ceea ce priveşte transmiterea notificărilor/completarea formularului de raportare a incidentelor care au afectat securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice.

2.3. Potrivit unuia dintre respondenţi, este necesar să se facă distincţie în cadrul Deciziei între incidentele de securitate cibernetică şi alte incidente de securitate care pot afecta reţelele şi serviciile la care se referă Proiectul pentru evitarea suprapunerilor de competenţe în domeniul securităţii serviciilor de comunicaţii electronice şi securităţii cibernetice.

Potrivit recitalului 44 din Directiva 2009/140/CE a Parlamentului European şi a Consiliului de modificare a directivelor 2002/21/CE privind cadrul legal de reglementare comun pentru reţelele şi serviciile de comunicaţii electronice, 2002/19/CE privind accesul la reţelele de comunicaţii electronice şi la infrastructura asociată, precum şi interconectarea acestora şi 2002/20/CE privind autorizarea reţelelor şi serviciilor de comunicaţii electronice „(...) *autorităţile naţionale de reglementare ar trebui să dispună de mijloacele necesare îndeplinirii atribuţiilor lor, inclusiv de competenţele de a obţine informaţii suficiente pentru a fi în măsură să evalueze nivelul de securitate a reţelelor şi serviciilor, precum şi de a obţine date complete şi certe referitoare la incidentele reale privind securitatea care au avut un impact semnificativ asupra funcţionării reţelelor şi serviciilor.* (...)".

De asemenea, în conformitate cu prevederile art. 13a paragrafele (2) şi (3) din Directiva cadru revizuită, „*Statele membre se asigură că întreprinderile care furnizează reţele publice de comunicaţii electronice sau servicii de comunicaţii electronice accesibile publicului notifică autorităţii naţionale de reglementare* ***orice încălcare a normelor de securitate sau pierdere a integrităţii care a avut un impact semnificativ asupra funcţionării reţelelor sau a serviciilor***." (subl. ns.)

Aceste dispoziţii legale europene au fost transpuse în legislaţia naţională prin prevederile art. 47 alin. (1) din Ordonanţa de urgenţă a Guvernului nr. 111/2011 şi, în conformitate cu preverile art. 48 din acelaşi act normativ, prin prezentul Proiect se creează cadrul legal subsecvent pentru asigurarea implementării acestora.

Astfel, ANCOM, abilitată cu prerogative legale în domeniul securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice, prin prezentul Proiect şi-a propus să primească din partea furnizorilor informaţii referitoare la o gamă largă de incidente. Aşa cum este precizat şi în Expunerea de motive a Proiectului, printre cauzele unui incident care afectează securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice, se regăseşte şi categoria acţiunilor rău-intenţionate ce include incidentele cauzate de acţiunile efectuate în mod deliberat, cum sunt atacurile informatice/cibernetice (accesul neautorizat la echipamente de reţea, platforme, aplicaţii software, baze de date, atacuri de tip DoS/DDoS). De asemenea, conform Proiectului, furnizorii vor avea obligaţia 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.

Incidentele raportate către ANCOM se referă la acele incidente care afectează echipamentele furnizorilor în mod direct, şi nu la acele incidente care afectează utilizatorii finali. De asemenea, aceste raportări au ca obiect incidentele cu impact semnificativ asupra securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice şi nu incidentele informatice în sine. În acest sens, precizăm faptul că, potrivit raportărilor primite până acum de ANCOM, incidentele informatice/de securitate cibernetică sunt neînsemnate cantitativ în comparaţie cu ceilalţi factori ce determină apariţia incidentelor cu impact semnificativ asupra securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice. În cazul primirii unor notificări ce indică incidente de securitate cibernetică, ANCOM va colabora cu CERT-RO în vederea prevenirii şi analizei acestor incidente/tipuri de incidente, având în vedere atribuţiile şi activitatea CERT-RO desfăşurată în scopul realizării prevenirii, analizei, identificării şi reacţiei la incidente în cadrul infrastructurilor cibernetice ce asigură funcţionalităţi de utilitate publică.

De asemenea, aşa cum am precizat mai sus, potrivit Proiectului, furnizorii vor avea obligaţia 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. Impunerea acestei obligaţii s-a realizat în baza art. 46 şi 48 din Ordonanţa de urgenţă a Guvernului nr. 111/2011, dispoziţii legale ce asigură transpunerea în legislaţia naţională a prevederilor art. 13a paragrafele (1) şi (2) şi art. 13b paragraf (1) din Directiva cadru revizuită.

Prin urmare, ANCOM nu consideră necesară distincţia în cadrul Deciziei între incidentele de securitate cibernetică şi alte incidente de securitate care pot afecta reţelele şi serviciile de comunicaţii electronice. De asemenea, competenţele ANCOM de reglementare şi control în domeniul securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice sunt în acord cu prevederile Ordonanţei de urgenţă a Guvernului nr. 111/2011 şi ale Directivei cadru revizuite.

3. Obligaţia de notificare iniţială a incidentelor cu impact semnificativ

3.1. O parte dintre respondenţi au sesizat faptul că nivelul de detalii din cadrul primei notificări este mult prea ridicat, transmiterea unei notificări iniţiale atât de complexe urmând a presupune eforturi considerabile din partea furnizorilor, aceştia propunând eliminarea anumitor informaţii cerute în contextul obligaţiei de a transmite notificarea iniţială.

Prin intermediul notificării iniţiale, ANCOM doreşte să primească o serie de informaţii sumare cu privire la producerea unui incident cu impact semnificativ care să îi permită evaluarea timpurie a incidentelor şi impactului acestora asupra utilizatorilor serviciilor şi reţelelor de comunicaţii electronice, precum şi adoptarea de măsuri potrivit competenţelor sale legale (informarea publicului, a autorităţilor naţionale de reglementare în comunicaţii din alte state membre ale UE, a ENISA etc). Gradul de complexitate a informaţiilor cerute în cadrul primei notificări nu este unul ridicat.

Majoritatea furnizorilor au proceduri de raportare internă a tuturor incidentelor care să le permită selectarea/culegerea adecvată a informaţiilor aferente primei notificări. ANCOM consideră că după detectarea incidentului, furnizorul trebuie să se concentreze în primul rând pe acţiunile de răspuns la incident, de limitare a efectului incidentului, iar notificarea iniţială trebuie să implice alocarea unor resurse minime. Aşadar, prin transmiterea notificărilor privind incidentele cu impact semnificativ, nu se doreşte impunerea în sarcina furnizorilor a unor sarcini excesive care să implice antrenarea unor resurse semnificative.

Toate informaţiile solicitate în cadrul acestei notificări sunt necesare pentru a oferi o imagine succintă asupra incidentului petrecut. Majoritatea informaţiilor solicitate sunt corelate între ele/condiţionate şi presupun un răspuns sumar. Informaţiile privind ora descoperirii incidentului, serviciile şi/sau reţelele care sunt afectate de incident, aria geografică afectată, numărul de conexiuni afectate, efectele în ceea ce priveşte apelarea numărului unic pentru apeluri de urgenţă 112 şi cauza/cauzele care a/au provocat incidentul sunt fundamentale în ceea ce priveşte definirea şi estimarea impactului unui incident.

Estimarea graficului de restabilire a furnizării reţelelor şi serviciilor de comunicaţii electronice în parametrii normali de funcţionare este o informaţie relevantă în cazul incidentelor de lungă durată având în vedere interesul utilizatorilor privind restabilirea serviciilor afectate. În cazul majorităţii incidentelor, dat fiind faptul că acestea durează puţin, furnizorul va preciza doar că incidentul a fost remediat, fără a mai fi necesară indicarea unui termen estimativ de remediere. De asemenea, îndrumările în vederea minimizării efectelor incidentului sunt de regulă oferite de furnizor utilizatorilor în cazul incidentelor de lungă durată. Există o condiţionare între cele două categorii de informaţii prin faptul că de obicei acestea vizează incidentele de lungă durată, acest aspect facilitând procesul raportării.

De asemenea, o parte din informaţiile solicitate vor fi furnizate doar dacă este cazul. Astfel, există probabilitatea ca informaţiile cu privire la existenţa unui incident să nu fie oferite publicului în termenul alocat notificării iniţiale, răspunsul la această cerinţă fiind în acest caz foarte scurt, nefiind necesară alocarea unor resurse semnificative de natură umană sau de alt fel.

Elementele care pot permite ANCOM să decidă dacă informarea publicului privind incidentul este sau nu în interesul public sunt importante deoarece ANCOM va folosi aceste informaţii pentru a decide asupra oportunităţii de informare a publicului, potrivit prevederilor art. 47 alin. (2) din Ordonanţa de Urgenţă a Guvernului nr. 111/2011.

3.2. Anumiţi respondenţi au susţinut că termenul propus de ANCOM pentru transmiterea notificării iniţiale este extrem de scurt şi chiar imposibil de respectat. În opinia acestora, notificarea iniţială într-un termen foarte redus ar fi inutilă din perspectiva informării publicului (informarea ar fi ulterioară restabilirii continuităţii furnizării reţelelor şi serviciilor, iar termenul de 6 ore nu ar permite furnizarea unor informaţii cu un grad de acurateţe şi certitudine adecvat.

Aşa cum este precizat şi mai sus, ANCOM doreşte să primească informaţii minime/sumare cu privire la producerea unui incident cu impact semnificativ, gradul de complexitate al informaţiilor cerute în cadrul primei notificări nefiind unul ridicat. Astfel, transmiterea acestor informaţii se poate face într-un timp scurt de la detectarea incidentului. În alegerea termenului pentru transmiterea notificării iniţiale (6 ore de la detectarea incidentului cu impact semnificativ), ANCOM a ţinut cont atât de complexitatea informaţiilor solicitate, de practicile altor ţări, cât şi de avantajele/dezavantajele alegerii unui termen redus/îndelungat. Utilizatorii serviciilor de comunicaţii electronice sunt interesaţi să afle informaţii despre incident, în special în ceea ce priveşte termenul restabilirii furnizării serviciului cât mai repede posibil din momentul apariţiei incidentului. Un interval de timp redus aferent notificării iniţiale ar permite informarea utilizatorilor în timp util (la un moment cât mai apropiat de detectarea incidentului).

Opţiunea ANCOM pentru termenul de 6 ore a avut în vedere şi practica altor state membre ale Uniunii Europene care au implementat art. 13a din Directiva cadru revizuită. Multe state europene au stabilit un termen foarte scurt în care să se realizeze prima notificare. Astfel, reglementarea din Finlanda admite maxim 3 ore pentru această notificare, în cazul Portugaliei, Spaniei, Irlandei, termenul este de două ore, iar alte state (Austria, Danemarca etc) folosesc formulări de tipul „imediat de la detectare", „cât mai repede din momentul apariţiei" etc pentru a desemna termenul de notificare.

ANCOM ţine cont de precizările unor respondenţi care susţin că termenul de 6 ore pentru transmiterea primei notificări este foarte redus/ nu ar permite furnizarea unor informaţii cu un grad de acurateţe şi certitudine adecvat şi stabileşte un alt termen de transmitere a notificării iniţiale de către furnizori. Astfel, prima notificare se va realiza până cel târziu la ora 11:00 a zilei lucrătoare următoare celei în care a fost detectat incidentul cu impact semnificativ asupra securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice. Momentul începerii curgerii acestui termen aferent notificării corespunde momentului detectării incidentului, şi nu expirării termenului de 60 de minute indicat în definiţia incidentului cu impact semnificativ.

3.3. Unul dintre respondenţi a solicitat clarificări cu privire la modul în care trebuie să se raporteze afectarea apelurilor de urgenţă în cazul în care aceste apeluri au fost preluate de către alţi furnizori de servicii de comunicaţii electronice la puncte mobile care asigură furnizarea serviciului în acea zonă.

Pentru reţelele publice mobile terestre, în cazul în care un incident afectează accesul utilizatorilor la numărul unic pentru apeluri de urgenţă 112, există posibilitatea ca apelurile să fie direcţionate spre a fi preluate de către alţi furnizori de servicii de telefonie mobilă. Utilizatorul poate aşadar să apeleze numărul unic pentru apeluri de urgenţă 112 dacă aria geografică în care acesta se află este acoperită de un alt furnizor de servicii de telefonie furnizate prin intermediul unor reţele publice mobile terestre. În această situaţie, furnizorii vor menţiona în formularul de raportare că apelurile către 112 au fost afectate, deoarece acestea nu au putut fi efectuate prin propria reţea. Suplimentar, se poate menţiona că apelurile au fost preluate şi s-au efectuat prin alte reţele. ANCOM va considera şi aceste cazuri în analiza incidentelor şi le va trata separat.

4. Observaţie referitoare la obligaţia de notificare finală şi cea suplimentară a incidentelor cu impact semnificativ

4.1. Unul dintre respondenţi a propus completarea dispoziţiilor art. 4 alin. (9) din proiectul de decizie astfel încât, în ceea ce priveşte notificările transmise în formă electronică, data primirii acestora să fie considerată fie data transmiterii confirmării primirii, fie data transmiterii de către furnizor a notificării în măsura în care această dată poate fi determinată cu certitudine.

Pentru un plus de claritate a textului Proiectului, ANCOM a acceptat această propunere, completând prevederile art. 4 alin. (9) după cum urmează: „Art. 4 - (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)*".

De asemenea, din aceleaşi considerente, având în vedere că începând cu data de 1 ianuarie 2014, transmiterea notificării finale şi a celei suplimentare se va realiza exclusiv prin intermediul unei aplicaţii disponibile pe pagina de internet a ANCOM, ca înscris în formă electronică, ANCOM a procedat la completarea dispoziţiilor art. 4 alin. (11) din proiect în sensul că în acest caz sunt aplicabile în mod corespunzător 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.

5. Informarea publicului cu privire la existenţa unui incident cu impact semnificativ asupra securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice

5.1. Anumiţi respondenţi au propus completarea prevederilor deciziei în scopul detalierii criteriilor pe baza cărora ANCOM va decide asupra informării publicului cu privire la existenţa unui incident cu impact semnificativ asupra securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice, această propunere fiind justificată prin faptul că informarea publicului cu privire la existenţa unui incident cu impact semnificativ poate aduce prejudicii furnizorilor.

Aşa cum este prevăzut în cadrul Proiectului, ca urmare a primirii notificării iniţiale, 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. În ceea ce priveşte criteriile pe baza cărora ANCOM va decide asupra informării publicului, ANCOM va analiza şi va decide de la caz la caz cu privire la aplicarea măsurii informării publicului, pe baza datelor aflate la dispoziţia sa (inclusiv a argumentelor temeinice oferite de furnizorii în cauză care ar putea justifica nepublicarea informaţiilor referitoare la incidentul cu impact semnificativ).

Astfel, ANCOM va analiza cu atenţie întreg scenariul incidentului raportat, impactul pe care l-ar avea publicarea informaţiilor asociate acestuia, beneficiile şi dezavantajele unei astfel de măsuri. Cu titlu de exemplu, ANCOM ar avea serioase rezerve în a oferi informaţii publicului despre un anumit incident cu impact semnificativ în situaţia în care s-ar dovedi existenţa unor vulnerabilităţi de ordin tehnic, funcţional etc. ce ar putea fi uşor exploatate de persoane rău intenţionate sau în cazul în care publicarea informaţiilor ar fi de natură să conducă la întârzieri în procesul de restabilire a furnizării serviciilor de comunicaţii electronice.

Suplimentar, având în vedere că ameninţările la adresa securităţii şi integrităţii reţelelor şi serviciilor sunt din ce în ce mai complexe, interdependenţa cu alte sectoare economice este tot mai strânsă şi tehnologia care stă la baza reţelelor de comunicaţii electronice se află în continuă dezvoltare, ANCOM consideră că fixarea unor criterii stricte pe baza cărora ANCOM să decidă în privinţa oportunităţii de informare a publicului despre incident nu ar fi indicată. De asemenea, nici identificarea exactă a tuturor aspectelor/elementelor ce ar trebui învederate de furnizori pentru ca ANCOM să poată decide dacă informarea publicului privind incidentul este sau nu în interesul public nu este posibilă şi nici oportună, orice asemenea identificare dovedindu-se limitativă, neputând acoperi toate situaţiile concrete ce pot apărea în practică.

5.2. Informarea publicului cu privire la existenţa unui incident cu impact semnificativ poate aduce prejudicii asupra imaginii furnizorilor şi creează distorsiuni majore la nivel concurenţial.

Cu referire la impactul pe care informarea publicului o poate avea asupra furnizorilor şi a mediului concurenţial, precizăm că prevederile referitoare la informarea publicului au scopul protejării utilizatorilor finali şi asigurării/sporirii transparenţei informaţiilor cu privire la incidentele care afectează în mod semnificativ securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice. ANCOM consideră că obţinerea de către utilizatorii finali a unor informaţii relevante şi uşor accesibile cu privire la incidentele care afectează securitatea şi integritatea reţelelor şi

serviciilor de comunicaţii electronice este în interesul acestora. Prin asigurarea transparenţei în ceea ce priveşte incidentele cu impact semnificativ, utilizatorii pot aprecia într-o oarecare măsură modul în care furnizorii implementează măsurile de securitate. Între incidentele de securitate şi implementarea măsurilor de securitate există o strânsă legătură, o securitate sporită micşorând riscurile la adresa furnizării reţelelor şi serviciilor de comunicaţii electronice şi implicit numărul de incidente. În acelaşi timp, în urma implementării măsurilor de securitate corespunzătoare, numărul incidentelor va fi diminuat, iar utilizatorii vor beneficia de servicii continue, furnizate în condiţii adecvate de securitate.

Aşa cum este precizat şi la punctul anterior, ANCOM va analiza cu atenţie fiecare incident şi va decide de la caz la caz cu privire la aplicarea măsurii informării publicului, ţinând cont de informaţiile pe care le are la dispoziţie, inclusiv de argumentele temeinice oferite de furnizorii în cauză care ar putea justifica nepublicarea informaţiilor referitoare la incidentul cu impact semnificativ, precum şi de alte riscuri asociate publicării ce ar putea afecta furnizorii respectivi.

Totodată, ANCOM consideră că, în cazul în care furnizorii vor pune la dispoziţie utilizatorilor informaţiile privind incidentele din proprie iniţiativă, aceştia vor percepe informaţiile ca o dovadă a angajamentului şi a capacităţii furnizorului de a restabili rapid serviciile şi de a creşte încrederea utilizatorilor în utilizarea serviciilor de comunicaţii electronice. Utilizatorii pot fi educaţi cu privire la posibilele ameninţări la adresa funcţionării serviciului şi cauzele întreruperii furnizării serviciului. Informarea utilizatorilor este astfel şi o cale de a îmbunătăţi comunicarea între furnizor şi utilizatori.

5.3. În cadrul consultării publice, a fost sugerată completarea prevederilor deciziei cu o dispoziţie referitoare la demersurile pe care ANCOM ar trebui să le întreprindă în sensul de a aduce la cunoştinţa furnizorului intenţia sa de a informa publicul cu privire la incidentele cu impact semnificativ, înainte de a face publice aceste informaţii prin intermediul paginii proprii de internet.

Potrivit prevederilor art. 47 alin. (3) din Ordonanţa de urgenţă a Guvernului nr. 111/2011, text prin care se asigură transpunerea în legislaţia naţională a prevederilor art. 13a paragraful (3) din Directiva cadru revizuită, decizia privind publicarea informaţiilor privind incidentele de securitate este luată de ANCOM atunci când Autoritatea consideră că informaţia este în interesul public. Potrivit art. 4 alin. (3) din Proiect, ANCOM trebuie să primească în cadrul notificării iniţiale informaţiile necesare cu privire la incident pentru a decide în privinţa necesităţii, utilităţii şi oportunităţii de publicare. Astfel, printre altele, ANCOM trebuie să fie informată dacă furnizorul, din proprie iniţiativă, a pus la dispoziţia publicului informaţiile cu privire la incident şi să aibă la dispoziţie elementele care, în coroborare cu alte date aflate la dispoziţia Autorităţii, îi pot permite să decidă dacă informarea privind incidentul respectiv este sau nu în interesul public. Aşadar, în cadrul notificării iniţiale, furnizorii au posibilitatea de a-şi exprima opinia cu privire la riscurile şi beneficiile publicării informaţiilor referitoare la un incident, în opinia ANCOM nefiind necesar un mecanism ulterior de validare a mesajului ce urmează a fi transmis către public. Suplimentar, în cazul incidentelor de lungă durată, utilizatorii sunt interesaţi să afle cât mai rapid cauzele incidentelor şi măsurile de răspuns, mecanismul de validare întârziind nejustificat de mult publicarea informaţiilor.

5.4. ANCOM trebuie să stabilească condiţiile în care se va face publicarea de către furnizori a informaţiilor despre incidentele cu impact semnificativ. În plus, decizia trebuie să prevadă în mod expres că furnizorul va selecta dintre modalităţile enumerate, mijlocul/mijloacele de informare care se dovedesc a fi cele mai adecvate în raport cu caracteristicile incidentului respectiv.

Conform Proiectului, ca urmare a primirii notificării iniţiale 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. Condiţiile în care se va face publicarea de către furnizori a informaţiilor privind incidentele cu impact semnificativ, inclusiv mijlocul/mijloacele de informare care se dovedesc a fi cele mai adecvate vor fi stabilite de ANCOM prin solicitarea transmisă furnizorilor. Acestea vor ţine cont de caracteristicile şi particularităţile incidentului, de serviciul afectat, de numărul de conexiuni afectate şi de aria geografică a incidentului. În cazul în care ANCOM nu stabileşte în solicitare condiţiile în care se face publicarea, furnizorul va stabili condiţiile în care aceasta se face.

În vederea clarificării prevederilor deciziei, ANCOM a introdus un nou alineat la art. 5 după cum urmează: *„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)".*

5.5. Un respondent a propus în cursul procedurii de consultare publică adăugarea unei noi modalităţi de informare a publicului de către furnizori şi anume o soluţie de răspuns vocal interactiv (IVR).

Soluţia de răspuns vocal interactiv (IVR) propusă de respondent ca modalitate de informare a publicului de către furnizori nu se încadrează în categoria mijloacelor de informare prevăzute în cuprinsul proiectului de Decizie (o secţiune specială pe propria pagină de internet, canalul propriu de televiziune, poşta electronică, serviciul de mesagerie scurtă, mass-media), acestea fiind caracterizate prin faptul că informarea se realizează la iniţiativa furnizorului, şi nu la cererea utilizatorului de servicii de comunicaţii electronice. Modalitatea propusă poate fi corelată cu serviciul de relaţii cu clienţii, care este un serviciu la cerere, pus la dispoziţia utilizatorilor de către furnizori independent de obligaţiile impuse în sarcina acestora de către ANCOM. Autoritatea atrage atenţia asupra faptului că modalităţile de informare prevăzute în cuprinsul Proiectului nu exclud informarea utilizatorilor, la cererea acestora, prin intermediul serviciului de relaţii cu clienţii, ca o modalitate suplimentară de informare a utilizatorilor. Desigur, utilizarea unei asemenea modalităţi în mod exclusiv, fără a fi însoţită de cel puţin una dintre modalităţile prevăzute în mod expres în cuprinsul Deciziei, nu înseamnă îndeplinirea obligaţiei legale de informare a publicului, aşa cum aceasta este reglementată de Decizie.

6. Obligaţia de notificare a fiecărui incident cu impact semnificativ din anul 2013 până la intrarea în vigoare a deciziei

6.1. Unul dintre respondenţi a solicitat prelungirea la 60 de zile a termenului în care furnizorii au obligaţia de a transmite câte o notificare privind fiecare incident cu impact semnificativ care a avut loc în anul 2013 până la data intrării în vigoare a Deciziei. De asemenea s-a solicitat ca aceste notificări să urmeze formatul utilizat în cadrul chestionarelor adresate de ANCOM până în prezent cu privire la incidentele de securitate.

ANCOM a transmis în anul 2012 şi 2013 două chestionare/solicitări de informaţii privind incidentele cu impact semnificativ ce au avut loc în anul precedent solicitării. Formularul de raportare cuprins în Anexa nr. 2 din Proiect este foarte asemănător cu cel pus la dispoziţie furnizorilor în cadrul raportărilor precedente, elementele de noutate ce au survenit ulterior chestionarelor referindu-se la secţiunea referitoare la serviciile afectate, în sensul că structura acesteia este în acord cu alte dispoziţii legale relevante, în speţă Anexa nr. 2 la Decizia preşedintelui Autorităţii Naţionale pentru Administrare şi Reglementare în Comunicaţii nr. 987/2012 privind regimul de autorizare generală pentru furnizarea reţelelor şi a serviciilor de comunicaţii electronice. De asemenea, formatul propus prin proiectul de decizie supus consultării, comparativ cu cel utilizat în cadrul chestionarelor anterioare adresate de ANCOM furnizorilor, cuprinde anumite clarificări şi explicaţii utile furnizorilor în procesul de completare a formularelor de raportare.

Totodată, termenul de răspuns solicitat de ANCOM pentru formularea răspunsului la cele două chestionare a fost de maxim trei săptămâni, termen apreciat de furnizori ca suficient pentru acest gen de solicitare de informare.

Prin urmare, ANCOM consideră că termenul de 30 de zile de la intrarea în vigoare a deciziei este suficient pentru ca furnizorii să poată transmite în mod corect şi complet informaţiile privind incidentele cu impact semnificativ din anul 2013, conform instrucţiunilor de completare din Anexa nr. 3 la Proiect. De asemenea, faţă de considerentele prezentate mai sus, ANCOM apreciază că utilizarea unui alt format de raportare decât cel propus prin prezentul Proiect nu este oportună.

7. Incidentele care afectează furnizarea reţelelor şi serviciilor de către alţi furnizori (inclusiv din alt stat membru al Uniunii Europene)

7.1. Unul dintre respondenţi a solicitat indicarea în cuprinsul proiectului a elementelor în baza cărora un furnizor poate estima impactul unui incident de securitate asupra furnizării reţelelor şi serviciilor de către alţi furnizori.

Furnizorii de reţele şi servicii de comunicaţii electronice sunt singurii în măsură să decidă dacă un incident afectează un alt furnizor de pe piaţa naţională de comunicaţii electronice sau de pe cea dintr-un alt stat membru al Uniunii Europene. Doar furnizorii pot estima efectele/impactul acestor incidente asupra altor furnizori având în vedere că ei cunosc caracteristicile tehnice ale furnizării reţelelor şi serviciilor de comunicaţii electronice şi deţin toate informaţiile privind relaţiile cu alţi furnizori. Elementele de impact asupra furnizării reţelelor şi serviciilor de către alţi furnizori diferă de la un incident la altul, iar detalierea aspectelor în baza cărora un furnizor poate estima efectele unui incident asupra furnizării reţelelor şi serviciilor de către alţi furnizori nu se poate realiza a priori de către ANCOM. În cadrul notificărilor, furnizorii vor transmite ANCOM acele informaţii privind afectarea unui alt furnizor de pe piaţa naţională sau de pe cea dintr-un alt stat membru al Uniunii Europene, care sunt cunoscute de furnizorul care raportează, indiferent de gradul de detaliere sau de complexitate al acestor date. În ipoteza primirii unor informaţii sumare din partea furnizorilor, însă cunoscând furnizorul care este afectat, ANCOM se poate adresa acestuia, în cazul în care este un furnizor de pe piaţa naţională, respectiv autorităţii de reglementare dintr-un alt stat membru al Uniunii Europene pentru informaţii mai detaliate privind efectele incidentului asupra respectivului furnizor. În practică, este de aşteptat ca furnizorii să colaboreze pentru înlăturarea efectelor unui incident, potrivit obligaţiilor ce le revin conform proiectului de decizie, ajutorul ANCOM putând fi acordat doar în cazul în care colaborarea dintre furnizori nu funcţionează.

Exemple de incidente care pot afecta mai mulţi furnizori sunt cele ce privesc legăturile de interconectare (inclusiv în centre neutre de colocare sau în Internet InterExchange-uri), cazul serviciului de tranzit sau transport apeluri. Incidentele pot afecta şi furnizarea reţelelor şi serviciilor de comunicaţii electronice din alte state membre ale Uniunii Europene. Astfel de incidente pot apărea, de exemplu, atunci când sunt afectate legături de interconectare stabilite la nivel internaţional, în cazul în care elemente de reţea sunt utilizate în comun de mai mulţi furnizori din state diferite, în cazul unor fenomene naturale cum ar fi furtuni sau cutremure care se extind în afara graniţelor unei singure ţări.

7.2. Acelaşi respondent a solicitat completarea textului Proiectului în sensul introducerii obligaţiei ANCOM de a înştiinţa furnizorii ce activează la nivel naţional referitor la primirea unei informări din partea unei autorităţi de reglementare în comunicaţii dintr-un alt stat membru al Uniunii Europene cu privire la existenţa unui incident ce poate afecta furnizarea reţelelor şi serviciilor de către furnizori din România.

Scopul raportării ad-hoc între autorităţile de reglementare din diferite ţări europene este tocmai răspunsul cât mai rapid la incidentele cu impact semnificativ care implică/pot implica furnizori din două sau mai multe state membre ale Uniunii Europene. De asemenea, ANCOM consideră că restabilirea furnizării reţelelor şi serviciilor într-un timp cât mai scurt este obiectivul major care trebuie avut în vedere în momentul apariţiei unui incident. Prin urmare, ANCOM va informa furnizorii ce activează la nivel naţional în cazul în care va primi din partea unei alte autorităţi de reglementare o informare cu privire la existenţa unui incident ce poate afecta un furnizor naţional, respectiv furnizarea reţelelor şi serviciilor de comunicaţii electronice către utilizatorii din România. Totuşi, este de aşteptat ca furnizorii din România să ia la cunoştinţă de incidentele care afectează propriile reţele şi servicii şi să devină conştienţi de ameninţările existente, în urma colaborării cu ceilalţi furnizori implicaţi şi independent de acţiunile autorităţii de reglementare. Cu toate acestea, având în vedere şi faptul că pot exista situaţii în care această informare poate fi utilă, de exemplu în cazul în care furnizorul are nevoie de informaţii cu privire la modalităţile de minimizare a efectelor unui incident şi acestea sunt disponibile prin intermediul unei autorităţi de reglementare dintr-un alt stat membru al Uniunii Europene, ANCOM va proceda la o astfel de informare pentru furnizorii din România.

Astfel, ANCOM nu consideră necesară introducerea acestei prevederi în cuprinsul deciziei.

8. Implementarea măsurilor minime de securitate

8.1. În opinia anumitor respondenţi, implementarea măsurilor minime de securitate presupun în realitate un efort considerabil din partea furnizorilor, inclusiv de ordin financiar, fiind necesar ca măsurile de securitate să fie implementate gradual, într-un termen mai mare, în raport cu capacitatea tuturor furnizorilor de a implementa aceste măsuri.

Printre obiectivele deciziei se numără şi stabilirea măsurilor tehnice şi organizatorice care trebuie luate de furnizorii de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului în vederea asigurării unui nivel adecvat al securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice. După cum am arătat mai sus, stabilirea acestor măsuri s-a realizat în baza art. 46 şi 48 din Ordonanţa de urgenţă a Guvernului nr. 111/2011, dispoziţii legale ce asigură transpunerea în legislaţia naţională a prevederilor art. 13a paragrafele (1) şi (2) şi art. 13b paragraf (1) din Directiva cadru revizuită.

ANCOM consideră că asigurarea unui nivel înalt al securităţii este un obiectiv de importanţă majoră ce ar trebui inclus în priorităţile furnizorilor de reţele şi servicii de comunicaţii electronice. Implementarea măsurilor de securitate va conduce la creşterea încrederii utilizatorilor în serviciile primite, la îmbunătăţirea calităţii serviciilor şi va contribui la asigurarea continuităţii furnizării reţelelor şi serviciilor de comunicaţii electronice.

Aşa cum este prevăzut şi în expunerea de motive a deciziei, o securitate adecvată a reţelelor şi serviciilor de comunicaţii electronice poate fi realizată prin stabilirea şi implementarea unui set adecvat de măsuri de securitate. Măsurile vor ţine cont de profilul furnizorului, de condiţiile sale operaţionale, iar stabilirea acestora va fi dependentă de riscurile identificate de furnizor la adresa securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice. Pentru o implementare eficientă a măsurilor, acestea trebuie monitorizate şi evaluate în mod continuu şi actualizate/îmbunătăţite periodic.

ANCOM atrage atenţia că asigurarea unui nivel adecvat al securităţii şi integrităţii reţelelor şi serviciilor nu reprezintă un produs, ci un proces care trebuie menţinut pe toată perioada furnizării reţelelor şi serviciilor. Cerinţele în privinţa asigurării unui nivel sporit de securitate pot fi identificate doar printr-o evaluare sistematică a riscurilor la adresa securităţii. Rezultatele evaluării riscurilor vor ajuta la determinarea acţiunilor corespunzătoare şi a priorităţilor implementării măsurilor de securitate în scopul protejării împotriva acestor riscuri. Asigurarea unui nivel adecvat de securitate este un proces continuu de punere în aplicare, revizuire, actualizare a măsurilor de securitate. Managementul riscului trebuie să fie parte integrantă a tuturor activităţilor desfăşurate în vederea asigurării securităţii şi integrităţii reţelelor şi serviciilor.

Procesul de implementare a măsurilor de securitate corespunzătoare are un caracter gradual. ANCOM are în vedere faptul că majoritatea furnizorilor vor urma abordarea „de la simplu la complex". Astfel, este posibil ca, iniţial, furnizorii care nu au implementat până în prezent măsuri de securitate adecvate să stabilească măsuri de bază şi să includă apoi, treptat, altele, un nivel avansat al acestor măsuri fiind atins după mai multe iteraţii. În acest caz, efortul implementării nu va fi unul semnificativ, resursele necesare (umane, financiare) fiind antrenate treptat. Totuşi, măsurile de securitate implementate de furnizori trebuie să abordeze toate domeniile enunţate în Anexa nr. 1 la proiectul de decizie. Pentru a accentua procesul continuu de revizuire şi îmbunătăţire a măsurilor de securitate, ANCOM a prevăzut în Proiect obligaţia în sarcina furnizorilor de a evalua, cel puţin o dată la 12 luni, şi de a actualiza, ori de câte ori se dovedeşte necesar în urma procesului de evaluare, măsurile de securitate stabilite şi implementate de furnizori (care să abordeze toate domeniile din Anexa nr.1 la Proiect). Astfel, măsurile de securitate trebuie să fie analizate şi evaluate cel puţin o dată la 12 luni sau ori de câte ori apar schimbări semnificative în mediul organizaţional, în condiţiile de desfăşurare a afacerii, în cadrul legal sau în condiţiile tehnice, pentru a asigura o securitate şi integritate a reţelelor şi serviciilor adecvată şi eficace. Măsurile de securitate, precum şi obiectivele acestor măsuri pot fi îmbunătăţite în urma rezultatelor analizelor de risc, a acţiunilor preventive şi corective, a analizelor privind conformitatea cu politicile şi procedurile organizaţiei, a evaluării periodice a eficienţei măsurilor de securitate, luând în considerare rezultatele auditurilor de securitate, a incidentelor înregistrate, precum şi a sugestiilor/feedback-ului diferitelor părţi interesate.

Conform unui raport realizat de ANCOM în anul 2012 privind măsurile implementate de furnizori pentru asigurarea securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice, majoritatea furnizorilor chestionaţi (care deţineau la sfârşitul anului 2011 peste 90% din cota de piaţă a serviciilor de comunicaţii electronice la nivel naţional) aveau o preocupare activă în

asigurarea securităţii şi integrităţii reţelelor şi serviciilor, implementând măsuri de securitate în majoritatea domeniilor de securitate stabilite de ANCOM în Anexa nr. 1 la Proiect. Cu toate acestea, doar o parte dintre aceşti furnizori au implementat măsuri documentate. Astfel, nu toţi furnizorii deţin proceduri clare şi documentate pentru asigurarea continuităţii reţelelor şi serviciilor, în majoritatea cazurilor stabilirea unor măsuri de securitate efectuându-se reactiv, în momentul apariţiei unui incident. În plus, conform aceluiaşi raport, puţini dintre furnizori au o abordare completă a domeniului securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice, majoritatea axându-se doar pe anumite domenii de interes.

Totodată, ANCOM atrage atenţia respondenţilor că procesul de implementare a măsurilor de securitate trebuia iniţiat o dată cu intrarea în vigoare a Ordonanţei de urgenţă a Guvernului nr. 111/2011 privind comunicaţiile electronice (sfârşitul anului 2011), furnizorii trebuind să aibă implementate până la această dată măsuri consistente pentru asigurarea securităţii şi integrităţii reţelelor şi serviciilor, acest lucru fiind de altfel şi în interesul furnizorilor.

Prin urmare, ANCOM consideră că termenul de 1 ianuarie 2014 de implementare a măsurilor de securitate adecvate este unul realist, obligaţia putând fi îndeplinită de furnizori în timp util.

8.2. Unul dintre respondenţi a apreciat că nedefinirea termenului "adecvat" din cuprinsul art. 3 alin. (1) din cadrul proiectului de decizie lasă la aprecierea fiecărui furnizor alegerea măsurilor.

Art. 3 din cadrul proiectului de decizie stabileşte în sarcina furnizorilor 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.

Măsurile de securitate vor fi stabilite şi implementate de către furnizori în funcţie de riscurile identificate la adresa securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice şi totodată vor acoperi domeniile stabilite de ANCOM prin decizie (Anexa nr.1 la decizie). Pentru stabilirea acestor domenii, ANCOM a ţinut cont de ghidul ENISA privind măsurile minime de securitate. Sintagma „măsuri de securitate adecvate" trebuie înţeleasă prin raportare la procesul intern, specific fiecărui furnizor, de management al riscurilor, proces complex care trebuie să stea la baza stabilirii acestor măsuri. Conform deciziei, stabilirea unui management al riscului reprezintă o obligaţie în sarcina furnizorilor, acest proces amplu fiind inclus în prima anexă a Deciziei alături de alte domenii vizate de măsurile minime de securitate ce trebuiesc stabilite şi implementate de către furnizori. Expunerea de motive a deciziei prezintă pe scurt etapele managementului riscului. Astfel, identificarea riscurilor trebuie realizată pentru a determina cauza posibilă a unei întreruperi în asigurarea continuităţii furnizării reţelelor şi serviciilor de comunicaţii electronice (breşă de securitate sau o pierdere a integrităţii), precum şi pentru a se obţine informaţii privind modul şi locul producerii acestei întreruperi. Identificarea ameninţărilor, a vulnerabilităţilor, a resurselor ce pot fi afectate, a consecinţelor pe care încălcarea securităţii le-ar avea asupra resurselor, a probabilităţii de apariţie a incidentelor sunt esenţiale în procesul de management al riscurilor. Opţiunile pentru tratarea riscului trebuie selectate pe baza rezultatului identificării, estimării şi evaluării riscului (activităţi în strânsă legătură care se succed), precum şi a beneficiilor şi a costurilor preconizate pentru implementarea acestor opţiuni.

Cu alte cuvinte, implementarea unor măsuri avansate de securitate nu este suficientă, în sine, pentru asigurarea unei securităţi adecvate. Aceste măsuri de securitate trebuie să răspundă ameninţărilor cu care se confruntă furnizorul și trebuie să ţină cont de vulnerabilitățile sale, fiind în acelaşi timp raportate la nivelul dezvoltării aplicaţiilor/sistemelor/mecanismelor de securitate existent la momentul implementării sau actualizării acestor măsuri.

Dacă ANCOM constată în urma verificărilor efectuate că măsurile stabilite de furnizori nu asigură un nivel de securitate corespunzător, Autoritatea poate impune, conform art. 49 alin. (2) din Ordonanţa de urgenţă a Guvernului nr. 111/2011, măsuri specifice de securitate astfel încât acestea să fie adecvate riscurilor identificate.

8.3. În opinia unui respondent, protejarea împotriva codurilor cu potenţial dăunător, codurilor mobile neautorizate şi a atacurilor informatice, inclusiv DoS/DDoS reprezintă o sarcină care ar trebui să cadă în sarcina utilizatorului final, fiind extrem de dificilă şi scumpă filtrarea în timp real a traficului de ordinul zecilor de Gbps pentru identificarea codurilor.

Măsurile minime de securitate pe care trebuie să le stabilească şi implementeze furnizorii de reţele şi servicii de comunicaţii electronice astfel încât să acopere domeniile stabilite de ANCOM prin decizie se referă de principiu la sporirea securităţii în reţeaua furnizorului. Măsurile de securitate nu se referă la traficul utilizatorului, protecţia reţelelor şi serviciilor de comunicaţii electronice împotriva codurilor cu potenţial dăunător, codurilor mobile neautorizate şi a atacurilor informatice, inclusiv DoS/DDoS însemnând de fapt protecţia echipamentelor de comunicaţii, software, aplicaţii etc aflate în posesia furnizorilor şi care sunt implicate în procesul de furnizare a reţelelor şi serviciilor de comunicaţii electronice către utilizatorii finali. Suplimentar, furnizorii ar trebui să protejeze utilizatorii independent de obligaţiile stabilite de ANCOM prin decizie. De exemplu, furnizorii ar trebui să ofere utilizatorilor recomandări/îndrumări privind protecţia terminalelor proprii împotriva programelor malware, spyware, viruşi, troieni etc. Asemenea celorlalte domenii de securitate stabilite de ANCOM, acest domeniu este detaliat în expunerea de motive a deciziei.

9. Propuneri privind includerea în proiectul de decizie a altor prevederi

9.1. O parte dintre respondenţi sunt de părere că obligaţia ca furnizorii să stabilească şi să implementeze măsuri de securitate în domeniile prevăzute în proiectul de decizie nu poate fi suficientă pentru a garanta integritatea reţelelor şi pentru a asigura continuitatea furnizării serviciilor, în lipsa unor proceduri care să permită verificarea acestor măsuri şi evaluarea securităţii reţelelor şi serviciilor, de către ANCOM. Astfel, potrivit acestor respondenţi, proiectul de decizie trebuie completat cu prevederi referitoare la evaluarea măsurilor de securitate, introducerea obligaţiei ca furnizorii să informeze periodic ANCOM cu privire la măsurile de securitate stabilite şi implementate, introducerea obligaţiei ca furnizorii să prezinte ANCOM, anual, rezultatele unui audit intern realizat cu resurse proprii furnizorilor şi ale unui audit extern, independent.

Controlul respectării prevederilor Ordonanţei de urgenţă a Guvernului nr. 111/2011, ale legislaţiei speciale din domeniul comunicaţiilor electronice şi ale actelor normative sau individuale subsecvente emise de ANCOM în baza acestora, este în sarcina ANCOM, care acţionează prin personalul de specialitate împuternicit în acest scop. Potrivit aceleiaşi Ordonanţe de urgenţă, ANCOM poate verifica şi evalua măsurile stabilite de furnizori pentru a garanta securitatea şi integritatea reţelelor şi serviciilor, precum şi respectarea acestora în cazurile de încălcare a securităţii reţelelor şi serviciilor sau pierdere a integrităţii reţelelor, putând impune măsuri în acest sens. După adoptarea Deciziei supuse consultării, ANCOM va monitoriza implementarea acesteia prin monitorizarea incidentelor din reţelele de comunicaţii electronice şi prin verificarea măsurilor de securitate implementate de furnizori.

Referitor la auditul de securitate, potrivit art. 49 alin. (1) lit. b) din Ordonanţa de urgenţă a Guvernului nr. 111/2011, ANCOM poate solicita furnizorilor de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului să se supună, pe cheltuiala proprie, unui audit de securitate realizat de un organism independent sau de o altă autoritate competentă şi să transmită ANCOM rezultatele auditului. Autoritatea consideră că auditarea anuală a tuturor furnizorilor de reţele şi servicii de comunicaţii electronice nu este o măsură proporţională datorită costurilor mari pe care le-ar presupune. Necesitatea unui audit va fi evaluată de la caz la caz, în funcţie de riscurile identificate. Cu titlu de exemplu, ANCOM consideră că un audit de securitate este justificat în cazul în care există suspiciuni privind implementarea defectuoasă a măsurilor de securitate.

De asemenea, după cum am precizat la pct. 8.2., stabilirea măsurilor de securitate este un proces intern de management al riscurilor, specific fiecărui furnizor, ce se adresează ameninţărilor cu care se confruntă fiecare dintre aceştia, în funcţie de vulnerabilităţile proprii, fiind în acelaşi timp raportat la nivelul dezvoltării aplicaţiilor/sistemelor/mecanismelor de securitate deţinute şi utilizate la momentul implementării sau actualizării acestor măsuri. Astfel, Anexa nr. 1 a Proiectului detaliază obligaţii de rezultat, măsurile concrete ce trebuie adoptate pentru atingerea acestor obiective sunt specifice fiecărui furnizor, fiind lăsate la aprecierea acestora. Furnizorii vor informa periodic ANCOM asupra nivelului de securitate existent prin transmiterea notificărilor privind incidentele cu impact semnificativ, precum şi prin furnizarea tuturor informaţiilor necesare evaluării

securităţii şi integrităţii reţelelor şi serviciilor. În cazurile de încălcare a securităţii reţelelor şi serviciilor sau de pierdere a integrităţii reţelelor, ANCOM poate impune adoptarea anumitor măsuri de către furnizori care să contribuie la rezolvarea problemelor identificate.

Faţă de aceste considerente şi având în vedere faptul că, potrivit art. 48 din Ordonanţa de urgenţă a Guvernului nr. 111/2011, Autoritatea stabileşte cadrul legislativ secundar necesar pentru implementarea dispoziţiilor art. 46 şi 47, ANCOM nu consideră necesară includerea în cuprinsul Proiectului a unor prevederi care să detalieze modalităţile de evaluare de către ANCOM a securităţii reţelelor şi serviciilor de comunicaţii electronice.

9.2. Unul dintre respondenţi a propus introducerea în cadrul proiectului de decizie a unor sancţiuni pentru nerespectarea obligaţiilor referitoare la măsurile de securitate şi la notificarea încălcării securităţii, astfel încât furnizorii să fie pe deplin informaţi în legătură cu riscurile la care se expun în cazul nerespectării prevederilor deciziei.

Procedura de constatare, notificare şi sancţiunile pentru nerespectarea obligaţiilor ce fac obiectul Proiectului sunt clar specificate în cadrul Ordonanţei de urgenţă a Guvernului nr. 111/2011, în *Capitolul XII- Supraveghere, control şi sancţiuni*. Astfel, conform art. 142 pct. 15, 16 şi 52 din acest act normativ, încălcarea obligaţiilor furnizorilor de a lua toate măsurile necesare pentru a administra riscurile ce pot afecta securitatea reţelelor şi serviciilor, precum şi măsuri pentru garantarea integrităţii reţelelor şi asigurarea continuităţii furnizării serviciilor prin intermediul acestor reţele, obligaţii prevăzute la art. 46 alin. (1) şi (3), încălcarea obligaţiei de notificare prevăzute la art. 47 alin. (1), precum şi nerespectarea măsurilor şi obligaţiilor impuse în temeiul prevederilor art. 48 constituie contravenţii şi se sancţionează conform art. 143, fiind constatate de către personalul de control din cadrul ANCOM prin procesul-verbal de constatare a contravenţiei şi de aplicare a sancţiunii (art. 144).

Faţă de cele de mai sus, ANCOM consideră că regimul sancţionator specificat de cadrul legal este clar şi nu trebuie preluat în cadrul Deciziei.

10. Alte propuneri

10.1. Una dintre sugestiile primite în cadrul consultării publice se referă la organizarea de către ANCOM a unei întâlniri anuale cu furnizorii de reţele şi servicii de comunicaţii electronice şi cu cercetători/experţi independenţi în domeniul securităţii, în cadrul căreia să poată fi semnalate şi discutate vulnerabilităţile identificate la nivelul reţelelor şi serviciilor de comunicaţii electronice, ulterior acestor întâlniri ANCOM putând să emită recomandări/obligaţii către furnizori cu referire la soluţionarea problemelor de securitate semnalate, urmărind apoi aplicarea acestora.

În vederea analizării/estimării nivelului de securitate şi integritate a reţelelor şi serviciilor de comunicaţii electronice existent şi pentru determinarea stadiului de implementare a măsurilor de securitate şi analiza acestor măsuri, precum şi pentru a identifica numărul şi impactul incidentelor, atât asupra utilizatorilor, cât şi asupra furnizorilor, ANCOM va organiza periodic întâlniri cu furnizorii de reţele şi servicii de comunicaţii electronice. ANCOM are în vedere şi organizarea unor întâlniri cu alte părţi interesate în domeniul securităţii (cercetători/experţi independenţi, organizaţii de profil) pentru a discuta despre diverse tipuri de vulnerabilităţi şi ameninţări identificate la nivelul reţelelor de comunicaţii electronice, practici întâlnite şi probleme identificate în procesul de management al riscurilor etc. În scopul sprijinirii furnizorilor în implementarea măsurilor de securitate adecvate, ANCOM a inclus în planul de acţiuni pe anul curent şi elaborarea unui ghid privind implementarea măsurilor minime de securitate.

10.2. Unul dintre respondenţi a apreciat în cuprinsul sugestiilor transmise Autorităţii că, pentru asigurarea informării utilizatorilor, raportul anual de activitate al ANCOM ar trebui să conţină informaţii generale privind notificările referitoare la incidentele cu impact semnificativ primite de ANCOM.

ANCOM intenţionează să realizeze anual studii/rapoarte privind securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice în urma analizei incidentelor şi evaluării situaţiei implementării de către furnizori a măsurilor de securitate. Aceste rapoarte vor oferi informaţii de interes, în ceea ce priveşte securitatea, pentru utilizatorii de servicii de comunicaţii electronice şi pentru alte părţi interesate. Autoritatea a publicat în cursul anului 2012 trei studii/rapoarte privind securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice.

De asemenea, ANCOM va include în rapoartele anuale de activitate informaţii privind notificările primite de la furnizori referitoare la incidentele cu impact semnificativ asupra securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice, precum şi informaţii privind alte studii în domeniu, desfăşurate de ANCOM. Raportul anual de activitate pe anul 2012 al Autorităţii[2] conţine informaţii despre incidentele ce au avut loc în anul 2011.

Suplimentar, conform proiectului de decizie, ca urmare a primirii notificării iniţiale 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.

Aceste acţiuni vor contribui la o informare adecvată a publicului despre nivelul securităţii şi integrităţii reţelelor şi serviciilor şi vor spori transparenţa faţă de utilizatori.

Alte modificări ale proiectului de decizie efectuate de ANCOM

ANCOM a transmis, în cursul lunii ianuarie 2013, un chestionar către furnizorii de reţele şi servicii de comunicaţii electronice prin care le solicita acestora informaţii privind incidentele cu impact semnificativ din 2012, chestionar care a avut un formular de raportare asemănător celui din proiectul din decizie. În urma analizei răspunsurilor furnizorilor, s-au constatat deficienţe în completarea formularului de raportare. În consecinţă, ANCOM a decis modificarea şi completarea Formularului de raportare a incidentelor care au afectat securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice propus prin Anexa nr. 2 la Proiect şi a Instrucţiunilor de completare a Formularului de raportare a incidentelor care au afectat securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice, prevăzute în Anexa nr. 3, astfel:

- formularul de raportare va cuprinde la punctul 3.1 Serviciul/serviciile afectate, în dreptul fiecărui serviciu, un câmp unde se va completa numărul de conexiuni afectate de incident, iar la punctul 3.2 se va solicita numărul total de conexiuni afectate de incidentul respectiv. Această modificare este necesară deoarece una din cele mai importante deficienţe constatate este necompletarea numărului de conexiuni afectate pentru fiecare serviciu afectat. Completând un singur număr la parametrul de impact „Numărul de conexiuni afectate de incident per serviciu" nu este clar dacă acel număr reprezintă suma numărului de conexiuni afectate pentru toate serviciile sau dacă a fost afectat acelaşi număr de conexiuni pentru fiecare serviciu bifat în parte.

- la instrucţiunile de completare a formularului de raportare se va adăuga o precizare suplimentară privind formatul de introducere a datei. Astfel, formatul va fi de tipul zz.ll.aaaa. Clarificarea acestui aspect este necesară întrucât, cu ocazia raportărilor anterioare, furnizorii au folosit atât formatul zz.ll.aaaa, cât şi formatul ll.zz.aaaa, fără a specifica tipul formatului folosit, aceasta conducând la incertitudine în ceea ce priveşte data producerii incidentului.

[2] http://www.ancom.org.ro/uploads/links_files/Raport_Anual_final_site_5_iunie_2013.pdf